

Schedule 5

Systems Technical Specifications

Schedule 5(a)	Cybersecurity
Schedule 5(b)	Digital Communications Network
Schedule 5(c)	Electronic Access Control System (EACS)
Schedule 5(d)	Enterprise Asset Management System (EAMS)
Schedule 5(e)	European Train Control System (ETCS)
Schedule 5(f)	Fire Protection System (FPS)
Schedule 5(g)	Hazard Detection and Early Warning System (HDEWS)
Schedule 5(h)	Integrated Control and Supervision System Specifications (ICSS)
Schedule 5(i)	Interlocking System (IXL)
Schedule 5(j)	Medium Voltage Power System (MVPS) and Low Voltage Power System (LVPS)
Schedule 5(k)	Closed-Circuit Television (CCTV)
Schedule 5(l)	Network Timing System (NTS)
Schedule 5(m)	Operation Control Center (OCC)
Schedule 5(n)	Public Address and Customer Information System (PACIS)
Schedule 5(o)	Signaling Engineering Rules (SER)
Schedule 5(p)	Telephony System
Schedule 5(q)	Traffic Management System (TMS)
Schedule 5(r)	Wireless Communication System (WCS)
Schedule 5(s)	Traction Power Supply System (TPSS)
Schedule 5(t)	Glossary of Terms, Abbreviations, and Definitions



Schedule 5(a)

Cybersecurity

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0005 – Cybersecurity

Rev. 0.0

A handwritten signature in black ink, appearing to read "B Greaney".

Authored:

Ben Greaney, Senior Cybersecurity Specialist

10/15/2025

Date

A handwritten signature in black ink, appearing to read "Thomas Newey".

Checked:

Thomas Newey, Telecoms Lead

10/15/2025

Date

A handwritten signature in black ink, appearing to read "Bruno Comperat".

Checked:

Bruno Comperat, Deputy Director of Rail Engineering

10/16/2025

Date

A handwritten signature in black ink, appearing to read "Ryan Scott".

Approved:

Ryan Scott, Director of Rail Engineering

10/16/2025

Date

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Released:

Amit Joshi, Configuration Manager

10/16/2025

Date



Document Revision History – Cybersecurity Specifications**First Edition****September 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition



TABLE OF CONTENTS

1	SCOPE OF THE DOCUMENT	5
1.1	SCOPE DESCRIPTION	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.2	PROJECT PHASE DEFINITION.....	7
2.3	DEFINITIONS.....	9
3	SYSTEM UNDER CONSIDERATION AND THREAT LANDSCAPE.....	11
3.1	SYSTEM UNDER CONSIDERATION (SUC).....	11
3.2	CYBERSECURITY ROLES AND RESPONSIBILITIES.....	17
3.3	CYBERSECURITY DESIGN PRINCIPLES.....	20
3.4	CYBERSECURITY DESIGN OBJECTIVES.....	21
3.5	THREATS TO THE RAILWAY	22
3.6	THREAT SOURCE CAPABILITY.....	23
3.7	VECTORS OF ATTACK.....	24
3.8	VULNERABILITIES.....	24
3.9	RAILWAY SYSTEM THREAT EVENT IMPACTS	25
3.10	SYSTEM UNDER CONSIDERATION THREATS	25
3.11	SECURITY LEVELS.....	32
4	CYBERSECURITY MANAGEMENT.....	34
4.1	CYBERSECURITY MANAGEMENT PLAN.....	34
4.2	SECURITY TRAINING.....	35
4.3	ASSURANCE, AUDIT AND COMPLIANCE.....	36
4.4	SUPPLY CHAIN RISK MANAGEMENT	38
4.5	PRODUCT LIFECYCLE AND OBSOLESCENCE.....	39
5	CYBERSECURITY RISK MANAGEMENT	42
5.1	RISK ASSESSMENT ACTIVITIES.....	42
5.2	RISK ASSESSMENTS.....	43
6	CYBERSECURITY SYSTEM REQUIREMENTS.....	45
6.1	NETWORK SEGMENTATION.....	45
6.2	NETWORK SECURITY.....	46
6.3	REMOTE ACCESS	48
6.4	WIRELESS SECURITY	50
6.5	ENDPOINT SECURITY.....	51
6.6	VULNERABILITY AND PATCH MANAGEMENT.....	53
6.7	IDENTITY AND ACCESS MANAGEMENT	54
6.8	CRYPTOGRAPHY AND KEY MANAGEMENT.....	57
6.9	CYBERSECURITY OPERATIONS CENTRE (CSOC).....	60
6.10	BACKUP AND RESTORATION	67
6.11	PHYSICAL SECURITY	68
6.12	INFORMATION SECURITY	70



6.13	APPLICATION PROGRAMMING INTERFACES SECURITY	72
7	SECURITY VALIDATION, VERIFICATION, AND TESTING	73
8	LIFECYCLE PHASE REQUIREMENTS & DELIVERABLES.....	75
9	HANDOVER	80



1 SCOPE OF THE DOCUMENT

1.1 Scope Description

- 1.1.1 The scope of this Technical Specification is to define the cybersecurity requirements for the CHSR Project.
- 1.1.2 These requirements shall be implemented and managed in conjunction with the scope of works as outlined in the CHSR scope of works.
- 1.1.3 The requirements are formulated using the following words and their meanings:
- **“Shall”**: Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure).
 - **“Must”**: Indicates an obligation or a mandatory requirement.
 - **“Should”**: Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents.
 - **“May”**: Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1.1 The TSCC Contractor shall review the documents listed in the following table and ensure that the cybersecurity work complies with the objectives of these standards. Where applicable, the TSCC Contractor shall demonstrate alignment through referenced requirements, mapped evidence, or objective fulfillment within the assurance Case.

ID	Reference Document	Details
1	IEC62443-3-3	Defines cybersecurity controls for industrial automated control systems, associated with Security Level Targets
2	CENELEC TS 50701	Details on how to apply IEC62443 to the railway system. Contains detailed information on a recommended risk assessment, assurance, and V&V process for cybersecurity.
3	Subset-026	Functional and Safety requirements for ETCS Provides input documentation to define what needs to be protected by the cybersecurity function
4	Subset-98	RBC-RBC Safe Communication Interface
5	Subset-137	Communications requirements, including security
6	Subset-146	Key management and additional communication security requirements
7	TSA SD 1580	Transportation Security Administration directive outlining obligations for rail and mass transit: • Obligation to appoint a coordinator • Mandatory cybersecurity incident reporting • Obligation to have Incident Response Plans • Obligation to complete periodic vulnerability assessments
8	NIST SP 800-53	Defines security control guidelines that are used to define system specific requirements. The references section of 800-53 can be used to find specific requirements, the TSCC Contractor should use the most current version of this document to find up-to-date references and guidance.
9	NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security reference for ICS-specific risk identification, control selection, and response planning May be used by contractor as a secondary reference for best practice to complement 62443 and TS 50701
10	California Consumer Privacy Act (CCPA)	Applicable where personally identifiable information (PII) may be collected, stored, or transmitted by rail operational systems.



11	National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)	Framework for developing a cybersecurity program that aligns with best practice Used to define a security program and map controls to a purpose
12	NIST SP 800-61	Computer Security Incident Handling Guide, used as guidance for CSOC and incident response planning.
13	ISO27001	Defines information security management system requirements Shall be used by the TSCC Contractor to define controls for protecting data in the Asset Management System and other IT/enterprise systems that store information as part of the contract
14	OWASP Top Ten	Defines commonly overlooked and exploited vulnerabilities in web application development and includes mitigation strategies Applicable to any system that interacts via a web browser or web-based input fields

TABLE 1 - REFERENCE STANDARDS & DOCUMENTS

2.2 Project Phase Definition

TS 50701 Phase	Sub-Phase	Definitions
Prerequisites		Establish the railway operator's security program and identify applicable legal and regulatory frameworks.
Concept		Identify the System under Consideration (SuC), define security-related controls, create a high-level zone model, determine applicable security standards, and define the project's purpose and scope. Output: Cybersecurity Management Plan.
System definition and Operational Context		Define system boundaries, review logical and physical network plans, and establish zones and conduits within the network.
Risk analysis and Evaluation		Perform cybersecurity risk assessments to identify threats and define countermeasures for zones and conduits. Consider business continuity, incident response, and recovery.
Specification of System Requirements		Refine requirements specific to each zone in the SuC, producing detailed cybersecurity requirements.
Architecture and apportionment of system requirements		Update risk assessments if needed, apply security requirements to the railway environment, and consider security-related application conditions.
Design	Design Stages: - Preliminary Design - Detailed Design - Design Review	Finalize the solution design, ensuring no conflicts between cybersecurity and functional architecture.



Implementation, Manufacture or Procurement	Implementation Stages: • Development • Factory Acceptance Testing (FAT) • Site Acceptance Testing (SAT) • Procurement	Develop, manufacture, and procure all necessary materials and services. Implement cybersecurity features and conduct acceptance testing.
Integration		Review network plans with new equipment, inventory systems and applications, and conduct qualification of security components through testing and vulnerability scanning.
System Validation		Provide objective evidence that the SuC meets cybersecurity requirements; update the cybersecurity assurance case.
System Acceptance	Handover/Testing Stages: • Pre-Handover (Pre-Operational Testing) • Pre-Handover (Operational Testing) • Handover	Handover security responsibility from system integrator to railway operator. Manage remote access and approvals as roles transition.
Operation, Maintenance, and Performance Monitoring	• Operational Stages: • Post-Handover (Defects Liability Period, DLP) • Post-DLP • Hand back	Maintain logical and physical network plans, continuously monitor and manage cybersecurity. Handback: Formal return of assets/systems to the authority at end of O&M contract, including cybersecurity assurance, documentation, and knowledge transfer.
Decommissioning		Safely retire systems, ensuring all cybersecurity considerations are addressed.

TABLE 2 - PROJECT PHASE DEFINITION

2.3 Definitions

Term	Definition
Asset	Any component, device, system, data, or facility within the SuC that has value to the Operator or is critical to safe and secure operations.
Assurance Case	A structured argument, supported by objective evidence, that demonstrates the cybersecurity risks of the SuC are adequately mitigated and that all requirements of this specification have been fulfilled.
Authority	The governing, client, or oversight body responsible for cybersecurity acceptance, contractual compliance, and ongoing assurance activities.
Backup	A copy of data or configurations maintained to ensure system recovery in the event of failure, compromise, or loss.
Conduit	A communication path between zones that enforces security requirements and controls on data exchange between zones.
Configuration	The set of parameters, files, and setup options that define the operation and security behavior of a system, device, or software component.
TSCC Contractor	The party responsible for delivering the systems and cybersecurity works described in this specification, including design, implementation, testing, and initial support.
Control System	Operational Technology (OT) components such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), SCADA systems, and other embedded systems responsible for controlling rail infrastructure or equipment.
Critical System	Any system whose failure or compromise would impact the safety, availability, reliability, or security of rail operations.
Cybersecurity Control	A safeguard or countermeasure prescribed for the SuC to reduce cybersecurity risks, aligned with IEC 62443-3-3 foundational and system requirements.
Cybersecurity Operations Centre (CSOC)	Dedicated workstations and resources responsible for monitoring, analyzing, and responding to cybersecurity threats affecting the SuC.
Handover	The formal point in the project lifecycle when responsibility for part or all of the SuC is transferred from the TSCC Contractor to the Authority, Operator, or Maintainer.
Maintainer	The entity responsible for maintaining the SuC, including patching, upgrades, fault management, and lifecycle support. May be the same as or different to the Operator.
Network Segmentation	The practice of dividing a network into multiple zones or segments to control the flow of traffic and reduce the attack surface.
Operator	The appointed entity responsible for operating the SuC after handover, including system operation, incident response, and cybersecurity monitoring.
Patch	A software, firmware, or configuration update that addresses known vulnerabilities, performance issues, or cybersecurity defects in the SuC.
Personnel	Any internal staff, subcontractors, or third-party support staff engaged by the TSCC Contractor, Operator, Maintainer, or Authority in connection with the SuC. Note: Personnel excludes public users such as passengers.
Security Incident	Any detected or suspected event that may result in unauthorized access, use, disclosure, disruption, modification, or destruction of assets.
Security Information and Event Management (SIEM)	A platform that collects, aggregates, analyzes, and correlates security logs and events to detect anomalies or cybersecurity incidents.
Security Level (SL)	A defined level of cybersecurity robustness required for a system or zone based on threat, risk, and consequence, based on the IEC62443 standard. This includes SL-T (Target), SL-C (Capability), SL-A (Achieved).
SuC (System under Consideration)	The complete set of infrastructure, devices, endpoints, components, personnel, processes, and supporting technologies that contribute to the operation and security of the assets identified for cybersecurity consideration.



Term	Definition
Validation	The process of confirming that the SuC meets operational needs and performs securely in its intended environment.
Verification	The process of confirming that a system meets specific cybersecurity requirements during design, development, and implementation.
Zone	A logical or physical grouping of assets with similar cybersecurity requirements, isolated from other zones using technical or procedural measures.

TABLE 3 - CYBERSECURITY DEFINITIONS

3 SYSTEM UNDER CONSIDERATION AND THREAT LANDSCAPE

3.1 System under Consideration (SuC)

- 3.1.1 The SuC defines the system boundary and scope for cybersecurity related assessments and security controls as outlined in this technical specification.
- 3.1.2 For this technical specification, all systems outside of the SuC shall be considered external interfaces and untrusted networks.
- 3.1.3 The TSCC Contractor shall formally document all systems in scope of the SuC and seek approval from relevant senior stakeholders.
- 3.1.4 The TSCC Contractor shall document details about the SuC to inform cybersecurity works, including the operational context, the purpose of the SuC, how the assets and systems within the SuC shall be used, and how long the SuC shall be operational
- 3.1.5 The TSCC Contractor shall organize all SuC systems into separate zones based on the following factors:
 - Criticality to the safety of passengers
 - RAMS/Safety Integrity Levels
 - Criticality to business feasibility and operations targets
 - Physical location (e.g., Trackside, equipment rooms, OCC)
 - Functionality
 - Trust Zones (IT, OT, DMZ, Public Wi-Fi).
- 3.1.6 Criticality ratings of systems shall be aligned with an appropriate risk management framework as agreed by senior stakeholders.
- 3.1.7 Criticality ratings shall be defined using the worst-case scenario consequence associated with each zone, whether that consequence is to safety, business, operations, or RAM requirements.
- 3.1.8 Assets with different criticality ratings must not be in the same zone, if the assets are required to be in the same zone due to functionality reasons, the highest level of criticality applies to all assets.
- 3.1.9 Communication between zones shall occur over secure conduits.
- 3.1.10 Secure conduits between two zones shall inherit the highest criticality rating of those zones.
- 3.1.11 A high-level zone and conduit diagram shall be developed in the early stages of design to define the initial cybersecurity architecture of the CHSR System Deployment. The diagram shall be maintained and updated throughout the design lifecycle to accurately reflect changes in system boundaries, trust relationships, and inter-zone communications.
- 3.1.12 Each defined zone shall have a formal description detailing its functionality, purpose, and interfaces in addition to SL-T requirements and any applicable technical or operational requirements.
- 3.1.13 The SuC shall comprise all infrastructure, devices, endpoints, components, maintenance and test/commissioning tools (including engineering/maintenance laptops, vendor service laptops, protocol analyzers, data loggers, oscilloscopes and other network-capable instruments), whether permanently connected or temporarily connected during maintenance or commissioning activities, contractor, subcontractor and third-party personnel, processes and supporting technologies that contribute to the operation, maintenance, testing, commissioning and security of the assets identified in the initial SuC definition. At a minimum, each asset listed below must have a System Owner who shall be accountable for the cybersecurity requirements for the asset and be the risk owner for all cybersecurity risks



associated with that asset. Assets such as CCTV cameras and Building Management Systems that are implemented in different locations may have multiple individual System Owner's, the TSCC Contractor shall specify where this is the case to ensure that risks are managed appropriately.

3.1.14 The below table contains a list of assets that shall be used as the initial SuC, the TSCC Contractor shall assign each asset in the SuC a criticality rating.

ID	Asset	Description
S_1	ETCS_RBC	A key component of train control and protection is the Radio Block Centre (RBC). The RBC is a safety critical system that communicates with the on-board systems via radio to issue and update movement authorities based on current track conditions, train positions, and interlocking system information. Movement authorities are permissions issued to a train that specifies how far and under what conditions the train is allowed to proceed along the track.
S_2	Interlocking-Object Controllers	Localized safety rated computing devices that are responsible for edge computation typically take input from several sensors, such as interlocking information, and perform logical functions before forwarding to centralized systems. Assets connected to the object controller: • Switch Machines • Derailers • Signals • Axle Counters
S_3	ETCS-Balise	On-track systems that send pre-configured messages to the train when a train crosses a certain section of track where the Balise is located. Balises are digitally programmed using a dedicated device which determines what messages are sent to the train, they are powered by radio frequency traffic sent by train.
S_4	TMS-ATO	Automatic Train Operation informs train drivers if they are on schedule by taking input from TMS and sending them information via the FRMCS, the ATO also takes control of the speed of the train to ensure that the train is running on schedule. The ATO can also apply the brakes when pulling into stations to ensure the train aligns with the platform.
S_5	WCS-FRMCS	FRMCS (Future Railway Mobile Communication System) is the successor technology to GSM-R for the provision of a dedicated and standardized radio communication system for voice and data communications services between the train and the wayside. • FRMCS is one of the components of the Wireless Communication Systems (WCS) • The FRMCS/WCS will have an external interface with local law enforcement communications networks



ID	Asset	Description
S_6	WCS and DCN - NMS	Network Management Systems exist for each network, including the DCN and WCS. The NMS is responsible for centralized management and monitoring of network devices to ensure that they comply with the network policy. The NMS is a key component of network security.
S_7	Interlocking-CBI	Computer Based Interlocking is the core, centralized system for making interlocking decisions. The interlocking system is responsible for making safety decisions based on track conditions. Traditional interlocking systems use hardwired, non-digital signals as input with trackside hardware dedicated to local interlocking; modern interlocking systems are moving towards digital, IP-based communications and towards centralized interlocking systems. In the context of CHSR, the CBI takes input from the Object Controllers, which are trackside devices that take hardwired input signals. The signals between object controllers and the CBI are digital (IP-based). Each interlocking system uses two or more CPUs to make safety decisions which determine if train routes can proceed, multiple CPUs are used to verify the integrity of safety decisions by ensuring the deterministic output of two or more CPUs are the same. Interlocking logic uses pre-computed deterministic decisions based on all input combinations.
S_8	TMS	The Traffic Management System is a centralized platform used to plan, monitor, optimize, and control train movements across the rail network. The TMS integrates live operational data with timetable information to enable decision making complemented by automatic train path conflict detection and automatic route setting.
S_9	FPS	Each facility, station and trainset will be equipped with various sensors and suppression systems to detect fires, alert customers and employees, and suppress the fire. Different fire suppression mechanisms are effective depending on the location, it is important to ensure that cybersecurity equipment outlined in this specification are not located where fire suppression mechanisms that damage equipment are located. The Fire Prevention System covers the following main functions: • Fire Detection, • Fire Alarming, Fire Suppression.
S_10	EACS	Access to the technical buildings is controlled by the Electronic Access Control System to prevent unauthorized access.



ID	Asset	Description
		Modern EACS can be integrated with logical access control, meaning a smart card or similar authentication mechanism can be used to verify an identity on a workstation. EACS systems are also commonly integrated with public key infrastructure or other cryptography systems and rely on encryption to prevent cloning or replay attacks.
S_11	CCTV	Closed Circuit Television cameras support various other efforts, including incident response and physical security. Main objectives of CCTV include but are not limited to; crime deterrence, real-time security supervision, supervision of the station, real-time monitoring of physical areas, and railway operations. CCTV systems can be used to monitor equipment rooms containing sensitive cybersecurity equipment or workstations that could be used to gain a foothold on the network.
S_12	Intrusion Detection and Prevention/Protection	Physical intrusion and prevention systems detect or prevent unauthorized individuals or objects that access restricted areas, such as the rail corridor. These systems may use digital communications to send detections back to the OCC or other monitoring systems. Certain prevention systems may rely on digital processors to make decisions whether to be locked, open, or closed.
S_13	EAMS	The Enterprise Asset Management System is a centralized platform used to systematically track, manage, and optimize all physical and logical assets involved in the delivery and support of the CHSR railway system throughout the entire system lifecycle. The Enterprise Asset Management System contains the Asset Inventory which shall be a centralized source of truth where all asset information, including relevant cybersecurity details, is stored.
S_14	HDEWS	The Hazard Detection and Early Warning System is a combination of sensors and other input/output devices that actively monitor civil components and environmental conditions to alert staff that a potential natural event or damage to the civil works that may have operational impacts.
S_15	NTS	The Network Timing System is the authoritative time distribution infrastructure responsible for ensuring that all devices across the rail system (and SuC) are synchronized. Timing servers commonly send timing traffic via IP-based communications, such as NTP which uses UDP.
S_16	ICSS	The Integrated Control and Supervisory System is an integrated HMI for multiple subsystems, including the monitoring and control of: • DCN • NTS • EACS • CCTV



ID	Asset	Description
		• Telephony • PACIS • WCS • Hazard Detection and Early Warning System • Enterprise Asset Management System • LV Power Supply • Fire Protection System • Building Management Systems
S_17	Telephony System	The Telephony system shall provide effective landline communication across the California High-Speed Rail (CHSR) System. The Telephony system shall ensure CHSR staff's internal voice communications and links with the public network and emergency services. • Operational Communication • Emergency Communication • Passenger Safety and Security Communication • Administration / Business communication
S_18	DCN	Data Communications Network is the core communications infrastructure that interconnects the distributed components of a railway network. The DCN is a combination of fiber optic cable, switches, and ethernet cables that run along the corridor.
S_19	AFC	The Automatic Fare Collection (AFC) system enables automated fare payment, validation, and revenue accounting for the rail network. It includes front-of-house devices (gates, platform/on-board validators, ticket vending machines, top-up kiosks, POS), customer media and channels (contactless EMV, transit smartcards, barcodes/QR, mobile wallets, web/app accounts), handheld inspection devices, station/depot controllers, AFC back-office applications (tariff and capping engine, clearing and settlement, reconciliation, dispute handling, revenue assurance), data stores, and the communications that link these components. Typical interfaces include payment acquirers/banks, customer service/CRM, finance/ERP and revenue accounting, data warehouse/analytics, work management/EAM, mobile apps and portals, and, where required, inter-agency or inter-modal clearing houses. AFC typically operates in connected and offline modes with deferred synchronization and relies on timely distribution of fare rules, hotlists/whitelists, and accurate time. Maintenance and test/commissioning tools (e.g., service laptops, key-loaders, test cards, vendor utilities) are included when they interface with AFC components.
S_20	PACIS	The Public Address and Customer Information System is an overarching asset that interfaces with all passenger information systems.



ID	Asset	Description
		Passenger Information Display System (PIDS) and Passenger Announcement (PA) Local Control Units use PA speakers to provide information to passengers in stations, platforms and facilities.
S_21	ECCS	The Energy Control and Command System (ECCS) supervises and controls traction power facilities and overhead contact line system equipment. ECCS transmits relevant information to perform switching circuit breakers, change of maximum train current, changes to the power supply system and pantograph management.
S_22	MV/LV Power Systems	The MV/LV Power system provides regulated, reliable electrical power to all railway subsystems not involved in train propulsion, including signaling, communications, stations, control rooms, tunnel ventilation, fire safety, AFC, and ancillary infrastructure.
S_23	BESS	The Battery Energy Storage System shall be used to store electrical energy that is output from the solar panels. The BESS discharges electricity to power CHSR systems.
S_24	Battery Management System	Sometimes referred to as BMS, but not to be confused with the Building Management System (also BMS), the Battery Management System monitors cell voltages, temperature, and current charge, while managing the charging, discharging, and fault protection of the batteries in the BESS.
S_25	Solar Panels	The solar panels convert solar into energy that will be stored in the BESS and used to power the CHSR systems. The Solar Panels, BESS, and Battery Management System will have an HMI (workstation) for operator management, the TSCC Contractor likely needs to consider the applicability of industry standards such as NERC CIP if the BESS/Battery Management System/Solar Panels are connected to the grid.
S_26	BMS	The Building Management System is a centralized controller for building services across stations and other CHSR facilities. Systems that are commonly interfaced with the BMS include HVAC, lighting, fire systems, elevators, escalators and LV monitoring. The interfaces between these systems are commonly digital (IP-based) using common protocols such as BACnet and Modbus.
S_27	HVAC	Heating, Ventilation, and Air Conditioning systems control the environmental conditions of buildings, specifically the air quality and temperature. HVAC systems may be responsible for controlling aspects of the environmental conditions within rooms containing critical equipment, such as station equipment rooms or server rooms, where computing equipment that requires specific conditions to operate without being damaged may be located.



ID	Asset	Description
S_28	Lighting	Controls the lighting throughout buildings and on station platforms, can be used for a variety of purposes including safety and passenger flow management.
S_29	Elevators and Escalators	Elevators and Escalators move passengers safely between floors on a station, they are controlled by dedicated computing devices (usually PLCs) and may interface with the BMS or other control system.
S_30	PWS	Passenger Wi-Fi (System) is a dedicated network that may be located at the stations, on-board, or both. The purpose of the passenger wi-fi is to provide passengers or customers with access to the internet. The public wi-fi system is separate from the network provided for CHSR assets.
S_31	ETCS-KMS	The Key Management System is an ETCS function that manages cryptographic keys across the operational lifecycle for ETCS messaging and related rail applications. The KMS can perform all the traditional roles of a cryptographic system including generation, distribution, rotation, storage, archival, and destruction. The KMS will work with the closely with the Public Key Infrastructure (PKI), the KMS will be used to manage session keys once the authentication process has been facilitated by the PKI. Typical interfaces include ETCS onboard and trackside subsystems, the Radio Block Centre (RBS)/interlockings and back-office systems, as defined in the applicable ETCS specifications.

3.1.15 The TSCC Contractor shall protect the reliability and integrity of essential functions, essential functions are the functions that are required to enable the operation of the SuC, examples of essential functions are:

- Trains movement safety (signaling, interlocking, TMS, ETCS, FRMCS)
- OCC Communications with operational teams.
- Consistent power supply for systems.
- Emergency incident response.

3.1.16 The TSCC Contractor shall document all essential functions to be used as input for cybersecurity assessments.

3.2 Cybersecurity Roles and Responsibilities

3.2.1 The table below outlines the roles and their responsibilities as described throughout this technical specification.



Role	Responsibilities
Cybersecurity Lead	The Cybersecurity Lead is responsible for ensuring the execution and coordinating all tasks relating to governance, risk, and compliance that are associated with achieving the objectives and requirements outlined in this technical specification. The Cybersecurity Lead shall enable the secure design and implementation of the CHSR system by performing the cybersecurity integrator function, this function consists of facilitating co-engineering workshops, which are workshops where SMEs, System Owners, the Cybersecurity Lead, and other relevant stakeholders develop solutions that fit system operational, functional, safety, and cybersecurity requirements simultaneously and design reviews. The Cybersecurity Lead is the owner and author of the cybersecurity management plan and centralized cybersecurity risk register, assurance case and shall also facilitate all steering committee meetings. The Cybersecurity Lead shall have a deep understanding of cybersecurity threats, risk, vulnerabilities, assurance, and compliance with appropriate certification or experience. The Cybersecurity Lead is not a hands-on configuration role and shall primarily be concerned with ensuring that the CHSR system achieves the cybersecurity objectives in alignment with the businesses risk appetite, however, the Cybersecurity Lead shall have a detailed understanding of cybersecurity controls as they shall be responsible for calculating the risk likelihood based on a technical understanding of the security controls that have been implemented. The Cybersecurity Lead shall facilitate and lead all risk assessments, threat modelling exercises, co-engineering workshops, assurance case development, compliance documentation development, cybersecurity reporting, cybersecurity penetration test scoping, and other tasks. The Cybersecurity Lead shall also be the point of contact for interpretation of all cybersecurity requirements to ensure a consistent approach is taken throughout the project, the Cybersecurity Lead shall be responsible for ensuring that requirements are updated to reflect any new regulation, legislation, or Authority standards that have been created between the creation of the technical specification and the start of the project. The Cybersecurity Lead may have direct reports that may have individual tasks delegated to them either due to time constraints or specific expertise as required.
Cybersecurity Services Lead	The Cybersecurity Services Lead is the System Owner of the technical aspects of the cybersecurity specification; the Cybersecurity Services team shall be responsible for enabling the implementation of controls as agreed and co-engineered with the Cybersecurity Lead. The specification outlines several centralized services and security products, including authentication, identity and access management, encryption technologies, anti-malware,



Role	Responsibilities
	remote access, and other solutions. These solutions must all be co-engineered in a similar fashion to other systems, subsystems, and assets, and therefore a dedicated lead shall be allocated to the procurement and configuration of these systems. The Cybersecurity Services Lead shall be an integrator and on-boarding point of contact to assist System Owners in achieving the technical security controls outlined in the specification. The Cybersecurity Services Lead is expected to work closely with network teams, including the DCN System Owner, FRMCS System Owner, and other System Owners responsible for the implementation and configuration of network technologies. The Cybersecurity Services Lead includes several technologies, not limited to: Intrusion Detection and Prevention Systems, SIEM, Firewalls, Directory Services (Auth and Identity), Remote Access Solutions, Backups, PKI, and others as defined in this technical specification. The Cybersecurity Services Lead shall act as the CSOC lead and a blue team lead, configuring preventive and detective controls in compliance with this specification while enabling operational and safety functions.
Lead Engineer	The Lead Engineer in the context of this technical specification refers to the engineer in charge, SCADA engineer or other senior engineer that is accountable for the delivery of the scope of works and provides the Statement of No Objection (SONO) or equivalent signature on any design decisions or deliverables.
Senior Stakeholders	Refers to the Authority stakeholders and TSCC Contractor stakeholders that are delegated for the purpose of decision making, SONOs, and design leads. The Senior Stakeholders shall be responsible for aligning the cybersecurity works with the business by reviewing documentation, deliverables, processes, procedures, and other information and attending the steering committee where updates will be provided and issues shall be discussed.
System Owner	The System Owner is the accountable entity for a particular system, subsystem, or asset that is part of the project. The System Owner shall be delegated by the Lead Engineer or other senior TSCC Contractor personnel with authority to do so. The System Owner owns all cybersecurity risk associated with their individual system and is accountable for ensuring the cybersecurity controls are implemented to mitigate cybersecurity risks and achieve compliance with the technical specification. The System Owner may delegate actions or risks to their sub-ordinates; however, they cannot delegate ownership and therefore shall be ultimately accountable for all reporting and control implementation.



Role	Responsibilities
	The System Owner shall attend co-engineering and threat modelling workshops and shall be responsible for ensuring that the correct resources are in the room to design secure solutions and provide a detailed technical understanding of the systems to the Cybersecurity Lead to enable effective threat modelling and risk assessments. The System Owner is responsible for reaching out to central service teams, including the Cybersecurity Services Lead, to ensure that all systems are on-boarded to centralized systems, including sending log information to the SIEM, defining detection use-cases with the CSOC team, on-boarding authentication, and others as defined in this technical specification.

3.3 Cybersecurity Design Principles

- 3.3.1 The TSCC Contractor shall leverage the principles described in this section to inform the end-to-end design and deployment of systems, assets, endpoints, networks, and other technology. These principles shall be applied consistently across all stages of the lifecycle, including design, integration, commissioning, handover, and operations.
- 3.3.2 Cybersecurity and safety shall be co-engineered throughout all design, construction, and integration activities, ensuring alignment with RAMS (Reliability, Availability, Maintainability, and Safety) principles and lifecycle processes.
- 3.3.3 The TSCC Contractor shall follow a risk-centric secure-by-design approach. The secure-by-design principle refers to defining security controls early in the design process. To achieve this, cybersecurity risk assessments must be conducted at each stage of the contract and inform all design and deployment decisions that influence the cybersecurity risk posture of the SuC. Each security control must be traceable to an identified risk or compliance requirement, and the rationale for control selection or rejection must be documented and available for audit.
- 3.3.4 The TSCC Contractor shall implement the defense-in-depth principle. The principle states that layered and sequential controls are implemented to ensure that if one or more security controls fail, another control will prevent a potential compromise. Each layer of defense shall be clearly defined and aligned with the zone and conduit model to ensure layered protection exists at boundaries and within zones.
- 3.3.5 The TSCC Contractor shall implement the principle of least privilege for all permission assignments. The principle requires all entities, including human users and service accounts, to be granted only the minimum set of permissions required to perform their authorized functions. Permissions must be reviewed periodically, revoked when no longer required, and enforced through technical means such as access control lists, role-based access control, and system policies.
- 3.3.6 The TSCC Contractor shall implement the deny-by-default principle. The principle requires all communications or commands to be implicitly prevented unless explicitly allowed. Each allow rule shall be documented with adequate justification, examples include firewall rules or defined input ranges for controls systems. All changes to allow rules must follow formal change management processes and include traceable evidence of risk justification, compliance alignment, or operational need.
- 3.3.7 The TSCC Contractor shall provide evidence during the Verification and Validation phases to demonstrate that each cybersecurity design principle has been effectively implemented, with coverage across the SuC's people, process, and technology components.



3.4 Cybersecurity Design Objectives

- 3.4.1 This section outlines the objectives of the cybersecurity scope of works. If any of the following objectives are degraded or otherwise unable to be achieved, this shall be considered “Compromise” from a cybersecurity perspective.
- 3.4.2 **Confidentiality:** Refers to the protection of sensitive information from unauthorized access. In the context of the scope of this technical specification, this may refer to contractual information, personnel details, design documentation, operational data that could be used nefariously, secrets such as passwords, keys, and certificates, access codes for physical sites, asset inventory entries, software code, intellectual property, and other information where unauthorized access may have adverse impacts.
- 3.4.3 **Integrity:** Refers to protecting the accuracy and trustworthiness of information. In the context of the scope of this technical specification, this may refer to the ability to trust train movement decisions are made based on data that has not been tampered with and reflects real-world conditions or ensuring that software code, asset information, or PLC logic has not been altered.
- 3.4.4 **Availability:** Refers to implementing mechanisms to ensure systems, assets, networking equipment, and information shall be available when required to perform work or facilitate operations. In the context of this technical specification, this may refer to up-time of operational assets, availability of design documentation or information to contractor staff when required, or reliable infrastructure that achieves service level agreement targets.
- 3.4.5 **Safety:** Refers to implementing controls to protect the human factor from negative consequences induced by technology, in the context of this technical specification, this may refer to the protection of train movement logic or safety critical systems from manipulation, unauthorized control, or denial of service.
- 3.4.6 **Authenticity:** Refers to the ability to verify that the source of a command or communication is a trusted, authenticated, and verifiable source. In the context of this technical specification, this may refer to any system-to-system communication, such as a PLC in a parent/child configuration or train commands being issued by the RBC.
- 3.4.7 **Non-repudiation:** Refers to the ability to trace any action taken on a system, such as a configuration change, back to the entity that performed that action. In the context of this technical specification, this may refer to actions being logged on endpoints and assets that can be traced back to the individual (or system) that performed the changes.
- 3.4.8 **Visibility:** Refers to the ability to monitor systems from an operational and security perspective to detect anomalies. In the context of this technical specification, this may refer to automatic supervision of train systems or access to maintenance data.
- 3.4.9 **Control:** Refers to the ability for engineers to direct, interact with, or influence process controls. In the context of this technical specification, this may refer to human machine interfaces being denied communication to end-systems.
- 3.4.10 **Resilience:** refers to the ability of the SuC to recover from incidents, attacks, or faults while maintaining critical operational and safety functions. This includes failover mechanisms, redundancy, and service continuity during partial system failure.
- 3.4.11 **Auditability:** refers to the ability of systems to record and retain logs, actions, and decisions to enable forensic investigation, compliance assurance, and incident accountability.
- 3.4.12 **Fail-Secure and Fail-Safe:** Refers to systems being designed to fail in a secure and safe manner. In the event of component failure, suspected compromise, or unexpected input, systems shall enter a



known safe state that avoids further compromise and ensures safety is preserved. In the context of this technical specification, fail-safe modes shall always take precedence over fail-secure, meaning that fail-secure modes must not compromise the safety of operations. A common fail-secure mode is “fail-close”, where all communication or new executions are prevented until a secure state has been restored.

3.5 Threats to the railway

3.5.1 The following threat sources shall be considered when performing threat modelling and risk assessments. These threats represent common vectors relevant to safety-critical infrastructure and must be addressed through appropriate controls, design features, and operational mitigations:

- Internal Threats, including:
 - Coerced staff intentionally infecting systems
 - Disgruntled employees sabotaging systems
 - Intentional misconfiguration to perform overtime work
 - Unintentional misconfiguration
 - Social engineering or Phishing
 - Security control bypass
 - Privileged user misuse or credential abuse by internal staff
 - Staff using unauthorized tools, USBs, or software in operational environments
 - Negligent use of remote access tools or poor password hygiene by authorized users
 - **Inadequate cybersecurity training across roles and system phases**
 - **Misinterpretation of critical alerts or alarms**
 - **Poor incident response under pressure or unclear escalation procedures.**
- State-sponsored or nation-state actors, including:
 - Advanced persistent threats (APTs) pre-positioning themselves in critical infrastructure
 - Attacks seeking to cause disruption, destruction, or service degradation
 - Espionage seeking to steal operational details, design documents, or intellectual property
 - Supply chain interdiction or tampering prior to delivery of hardware or software
 - Coordination of cyber operations with physical or kinetic threats.
- Financially motivated cyber criminals, including:
 - Ransomware groups
 - Initial Access brokers
 - Business Email Compromise
 - Data theft for resale or extortion (e.g., credentials, design data, passenger data).



- Politically motivated attacks, including:
 - Acts of terror, attempting to cause harm or chaos
 - Hacktivism, trying to raise awareness for political issues
 - Tampering with public information systems to spread disinformation
 - Disruption of infrastructure for economic or reputational sabotage.
- Supply-chain threats, including:
 - Pre-installed malware in OEM components or contractor-provided systems
 - Weak coding practices
 - Back-door code
 - Software or hardware tampering during transit or integration
 - Compromise of privileged accounts that vendors have used for configuration/commissioning purposes and have not been disabled or had their privileges revoked
 - Shared vendor credentials reused across clients leaking via another breach
 - Unvetted firmware or component origin (e.g., counterfeit or grey market hardware)
 - Compromise via embedded dependencies (e.g., third-party libraries or modules).
- Third-Party and TSCC Contractor Threats
 - External vendors with privileged access to IT/OT systems
 - Subcontractor laptops introducing malware
 - Poor cybersecurity hygiene by maintenance contractors
 - Shared accounts or credentials between organizations.

3.6 Threat Source Capability

- 3.6.1 The TSCC Contractor shall consider the details outlined in this section during threat modelling and risk assessment exercises.
- 3.6.2 The TSCC Contractor shall consider that generative AI and other sources provide threat sources with a broad fundamental knowledge of how the systems and products are used in the SuC.
- 3.6.3 The TSCC Contractor shall consider that generative AI provides threat sources with automatically generated high-quality social engineering content, including spear phishing emails with replicated tone and other impersonation tactics such as deepfakes.
- 3.6.4 The TSCC Contractor shall consider that the threat sources may have access to commercial off-the-shelf product documentation and detail as provided to clients, **including manuals, configuration guides, and firmware/software update histories.**
- 3.6.5 The TSCC Contractor shall assume that the threat sources are well-resourced, with access to specialized tooling, dedicated computing power, and adequate man-hours to perform sophisticated, long-term attacks.
- 3.6.6 The TSCC Contractor shall assume that threat sources can acquire similar hardware and software to those used in the SuC to practice attack techniques.



- 3.6.7 The TSCC Contractor shall review updated threat guidance from federal agencies and leading industry security firms prior to performing threat modelling and risk assessments to ensure up-to-date capabilities are considered.
- 3.6.8 **The TSCC Contractor shall account for the possibility that threat actors may hire local individuals to gain physical entry, impersonate, tailgate, or socially engineer staff to bypass cyber controls and gain direct access to CHSR infrastructure.**

3.7 Vectors of Attack

- 3.7.1 At a minimum, the TSCC Contractor shall implement controls to detect and prevent the following techniques that threat sources may use to compromise systems. These techniques represent established vectors relevant to operational technology and rail infrastructure and shall be revisited as threat intelligence evolves:
- Exploitation of remote access solutions
 - Lateral movement from external networks
 - Credential Theft
 - Introduction of Malware via Physical Media
 - Vulnerability Exploitation
 - Supply Chain Compromise
 - Privilege Escalation
 - Session Hijacking
 - Living off the Land Techniques (using intended functionality to cause harm to systems)
 - Wireless Attacks
 - Exploitation of external interfaces, such as APIs
 - Physical access to devices or interface ports
 - Social Engineering
 - Privilege misuse.

3.8 Vulnerabilities

- 3.8.1 At a minimum, The TSCC Contractor shall implement controls to mitigate the following vulnerabilities that may be exploited by threat sources:
- Lack of segmentation between system and external networks
 - Improper zoning
 - Inadequate control of communications between zones
 - Misconfiguration or lack of hardening controls on devices
 - Unpatched Common Vulnerabilities and Exposures (CVEs)
 - Excessive privileges
 - Weak authentication (default/hard-coded passwords, single factor, password policy not enforced)
 - Lack of access control / Weak authorization controls
 - Unnecessary dependence on non-critical systems
 - Lack of communication protection mechanisms
 - Lack of endpoint protection
 - Lack of at-rest encryption (disk, volume, backup, information)



- Usage of undocumented or unsanctioned applications or systems on the network.
- Use of unvalidated open-source or third-party libraries with unknown or unpatched vulnerabilities
- Use of deprecated software, protocols, or firmware that have reached end-of-support.
- Weak coding practices including inadequate input validation or code injection checks
- Physical access bypassing cybersecurity controls

3.9 Railway System Threat Event Impacts

3.9.1 In addition to regular threat events as outlined in industry standards, the following threat events must be considered by the TSCC Contractor when determining the worst-case risk scenarios and performing threat modelling exercises:

- Compromise of a system or asset leading to denial, loss, or manipulation of train control, asset visibility, service availability, ability to operate trains, or integrity of safety systems or logic.
- Compromise of networking infrastructure or communications infrastructure rendering assets unable to communicate, trains unable to receive information, or loss of visibility across the network.
- Injection, jamming, or spoofing of network communications resulting in illegitimate or unsafe commands being executed, system misbehaviour, or denial-of-service conditions.
- Manipulation of train control systems to create phantom traffic (ghost/phantom/orphan trains) or similar dummy data, tricking the system into making decisions based on false information.
- Manipulation of cab signaling display or other driver advisory systems leading to degraded decision making or unsafe train movements.
- Compromise of IT, enterprise, public wi-fi, ticketing, supporting, or interfacing systems leading to downstream or upstream impacts to SuC systems and train operations.
- Infection of systems with ransomware allowing an attacker to hold systems and train operations to ransom by rendering them unusable.
- Execution of destructive malware, such as wipers that are configured to intentionally cause a physical failure of the device (such as turning on and off sensors or circuit breakers until they malfunction). Destructive malware exists to render a system permanently unusable.
- Theft of confidential information or operational information which may be used to cause reputational damage, be sold for financial gain, or used to compromise the SuC in the future.
- Compromise of public facing information systems, including visual displays, wi-fi captive portals, or audio systems, leading to the broadcast of undesirable messages to customers.
- Unintentional or intentional misconfiguration of systems leading to degraded operations, rendering systems inoperable, or compromise of cybersecurity objectives.
- Compromise of monitoring and alerting systems used for intrusion detection, access control, or system health, resulting in silent system failures or delayed responses.

3.10 System under Consideration Threats

3.10.1 This section details several threats that shall be considered during threat modelling exercises for the individual assets listed in section 3.1; it is not exhaustive and shall be reviewed and expanded as threat intelligence and system context evolve.

ID	Asset	Threats
S_1	ETCS_RBC	• Manipulation of information being sent to or from RBC, including false movement authority or speed restriction messages. • Flooding or other denial of service attacks thwarting traffic to or from RBC



ID	Asset	Threats
		• Spoofing, tampering, jamming or other wireless signal attacks • Forced failures or errors, leading to on-board systems entering fail-safe states or degraded operational modes, such as shunting mode
S_2	Interlocking-Object Controllers	• Manipulation of traffic between CBI and Object Controllers or other systems causing loss of data integrity • Manipulation of code or logic via remote access or maintenance ports (static, not during runtime - unauthorized changes to codebase) • Manipulation of interlocking logic (during runtime - manipulation of CPUs/Memory) • Injection or manipulation of communications between interlocking systems • Denial of Service attacks via connection paths or physical attacks on hardwired connections
S_3	ETCS-Balise	• Alteration of Balise programming, causing inconsistent or unexpected messaging between trains and Balises or Balises and interfacing devices, causing failures • Manipulation of Balise data integrity, such as distance between Balises or signal status, causing failures
S_4	TMS-ATO	• Tampering of speed or braking instructions to trainset • Denial of Service of speed or braking data
S_5	WCS-FRMCS	• Spoofed or unauthorized cells, towers, receivers, SIM-cards, senders, devices or other infrastructure sending, receiving, or manipulating traffic • Denial of Service via flooding attacks or jamming attacks • Voice over IP threats (spoofed caller, blocked traffic, eavesdropping, injected traffic) • Compromise via exposed endpoint interfacing with emergency networks • Misconfigured segmentation of WCS allowing network hopping • Voice Cloning or Deepfake Attacks (Use of AI-generated speech to impersonate authorized individuals (e.g., OCC supervisors), potentially influencing train drivers or station staff)
S_6	WCS and DCN - NMS	• Unauthorized modification of network security or segmentation configurations; enabling new communication paths for additional compromise • Unauthorized access to network configuration information and network monitoring



ID	Asset	Threats
		• Compromise of credentials or secrets available on the NMS; credentials or secrets used to achieve privileged access to other devices • Denial-of-service via configuration changes, such as VLAN changes or firewall changes • Loss of network visibility due to spoofed data or denial of service
S_7	Interlocking-CBI	• System compromise of Maintenance and Diagnostic Terminal data leading to loss of confidentiality, integrity, or availability of data. Manipulation of traffic between the interlocking and RBC or other systems causing data mismatch • Manipulation of interlocking code via remote access or maintenance ports (static, not during runtime - unauthorized changes to codebase) • Manipulation of interlocking logic (during runtime - manipulation of CPUs/Memory) • Injection or manipulation of communications between adjacent or local interlocking systems • Denial of Service attacks via connection paths or physical attacks on hardwired connections • Traffic sniffing of interlocking traffic, confidentiality compromise of packet structure and contents
S_8	TMS	• Unauthorized manual enforcement of degraded mode or alternative modes of operation, engineering possessions, fallback plans, or other operational functions • Unauthorized changes to train paths, scheduling, and timings • Alteration or corruption of timetables • Injection of unsafe movement plans being sent to interlocking or other interfacing systems • TMS Data manipulation in-transit to other interfacing systems, such as ICSS
S_9	FPS	• Unauthorized disablement of, or changes to fire detection parameters or suppression system logic • Manipulation of trigger mechanisms causing a false trigger or preventing a necessary trigger of fire alarms or suppression systems • Intercepted, spoofed, or modified traffic to interfacing systems, creating false fire alerts at OCC or to interfacing emergency services, or preventing operator alert system functionality



ID	Asset	Threats
S_10	EACS	- Unauthorized access using cloned access cards, replay attacks, spoofed access codes, or physical manipulation of access control hardware (system on a chip) - Compromise or manipulation of access control servers or workstations - Unauthorized addition or removal of user or access rights - Compromise of EACS via ICSS, HR System, FPS door control, or other interfacing system
S_11	CCTV	- Spoofed, manipulated, or unavailable video footage of any location across the rail system - Unauthorized access to, or control of video feeds of sensitive areas or to monitor individuals - Spoofed anti-tampering alarm messages to OCC - Unauthorized access to, deletion of, or manipulation of archived video footage - Compromise of CCTV camera remote connectivity (connectivity that facilitates access via mobile devices or other internet facing devices) - IoT vulnerabilities & Power over Ethernet misconfiguration
S_12	Intrusion Detection and Prevention/Protection	- Denial of Service of intrusion detection sensors, devices, alerts, or functionality via device exploitation or tampering with signals - Disablement or alteration of prevention system code with logical components, such as electric gates - Unauthorized changes to trigger levels of detection mechanisms, such as infrared cameras
S_13	EAMS	- Unauthorized modification, deletion, or addition of asset inventory entries or data - Unauthorized exfiltration or access to asset inventory data; including sensitive rail system information - Web-based vulnerability exploitation (OWASP) for cloud-based or local EAMS accessed via a browser - Exploitation or compromise of EAMS via interfaces with rail assets, HR systems, business enterprise systems, or via insecure APIs - Unauthorized modification of trigger values such as part replacement or business KPIs
S_14	HDEWS	Injection of false sensor data either at the device level, in communications paths, or at the monitoring system



ID	Asset	Threats
		- Tampering with, or blocking sensor information to prevent effective decision making - Unauthorized modification of trigger values, such as earthquake detection alarms
S_15	NTS	- Spoofing, jamming, hijacking, or otherwise preventing communications with trusted sources of time information used by the time server to verify the accuracy of clocks. - False time injection between server and network system endpoint (man/adversary-in-the-middle) - Manipulation of NTP (Network Time Protocol) settings or synchronization mechanisms, resulting in systemic time drift across the network. - Denial of time synchronization service from trusted NTS sources, affecting coordination of logging, alarms, or train control events. - Tampering with time source prioritization, causing fallback to unauthorized or rogue NTS servers. - Certificates, software licenses, or other time defined restrictions causing failures due to time changes
S_16	ICSS	- ICSS HMI/Workstation graphical user interface misuse - Lateral movement/Zone hopping/network segmentation compromise via ICSS interfaces to controlled or supervised systems - Unauthorized code or command execution on systems connected to the ICSS - Manipulation of data displayed on ICSS workstation/HMI - Theft of credentials or secrets used to control interfacing systems via ICSS - Tampering with alarming systems to prevent alarms from triggering or intentionally triggering alarms on ICSS
S_17	Telephony System	- Voice over IP threats (spoofed caller, blocked traffic, eavesdropping, injected traffic) - Jamming or other denial of service mechanism - Access to, deletion of, or alteration of recorded voice data - Voice Cloning or Deepfake Attacks (Use of AI-generated speech to impersonate authorized individuals (e.g., OCC supervisors), potentially influencing train drivers or station staff) - Unauthorized use of public/emergency intercom systems to overwhelm control center operators, cause panic, or obscure real emergencies



ID	Asset	Threats
S_18	DCN	• Reconfiguration of routing information, switching information, or other configurations causing network traffic to not reach the desired destination • Boundary networking equipment vulnerability exploitation to achieve access to network • Sniffing of operational data or packets containing secrets, such as passwords or encryption keys • Denial of Service by overloading network with traffic • Broadcast storms or similar legacy network threats
S_19	AFC	• Abuse of payment system to avoid fare • Denial of Service to keep gates open/closed or shut down payment systems • Credential Theft or Cloning (Theft, cloning, or replay of smartcards, QR codes, or mobile tickets to gain unauthorized access or share credentials) • Fraudulent Top-Ups or Account Tampering (Manipulation of stored value accounts or top-up services to increase credit without payment) • NFC or RFID Exploits (Use of NFC sniffer tools or malicious readers to capture or manipulate card data in the field) • API or Web Portal Exploits (Exploitation of mobile/web ticketing APIs (e.g., fare history, user identity, session hijacking) to bypass controls)
S_20	PACIS	• Injection, manipulation, or broadcast of unauthorized, misleading, offensive, or malicious messages via display or audio systems (including replay of archived or pre-approved emergency announcements to trigger false alerts or obscure actual incidents) • Unauthorized access to message scheduling interfaces or remote control • Tampering with synchronization, event triggers, or display timing logic leading to misleading or confusing passenger information • Denial of service attacks against PIDS controllers, PA servers, or network links, resulting in blackouts or delayed messaging • Malicious or negligent configuration or content upload by insiders with legitimate access rights
S_21	ECCS/Power SCADA	• Disabling or changing traction power output to systems causing denial of service or safety incidents • Tampering or falsification of traction power data



ID	Asset	Threats
		Causing damage to substations or power circuits through malicious actions
S_22	MV/LV Power Systems	- Disabling or changing power output to systems causing denial of service - Tampering or falsification of MV/LV power data - Causing damage to substations or power circuits through malicious actions
S_23	BESS	- Unauthorized charge or discharge commands - Tampering or falsification of charge status
S_24	Battery Management System	- Unauthorized charge or discharge commands - Tampering or falsification of charge status or other data - Graphical User Interface misuse - Grid/external power feed or interface misuse
S_25	Solar Panel System	- Tampering or falsification of output data from solar panels - Modification of logic for controlling solar panels
S_26	BMS	Unauthorized modification of building conditions, including lighting, environmental conditions, water, plumbing, or disablement of passenger services
S_27	HVAC	- Unauthorized changes to passenger or station staff area environmental conditions, such as station temperature - Compromise of HVAC system to cause server rooms, equipment rooms, OCC rooms, battery storage, or other rooms containing computing equipment to be unfit for purpose
S_28	Lighting	Unauthorized disablement or enablement of lighting at stations, buildings, or OCC
S_29	Elevators and Escalators	- Compromise of elevator or escalator controls, disabling them or modifying conditions while in use by passengers or causing a denial of service - Disablement or misuse of elevator communication and monitoring devices
S_30	PWS	- Poor segmentation enabling hopping from passenger WI-FI to other networks - Unencrypted traffic sniffed by other passengers - Spoofed access points, leading passengers to connect to fake networks



ID	Asset	Threats
		- Captive portal compromise, presenting undesirable messages or redirecting passengers to phishing links - Denial of Service by passenger connected to network
S_31	ETCS-KMS	- Theft of session keys or other secrets - Denial of Service via key rotation, revocation, disablement, deletion, or other means - Denial of Service causing sessions keys or other secrets to not be available

3.11 Security Levels

- 3.11.1 Security Level Targets (SL-Ts) as outlined in the IEC62443 standard shall be defined by Cybersecurity Lead for each zone using a risk-based methodology.
- 3.11.2 The Cybersecurity Lead must gather evidence that demonstrates that the Security Level Achieved (SL-A) has been independently verified as achieving the SL-T requirements during the final stages of deployment and testing.
- 3.11.3 The TSCC Contractor must implement compensating controls throughout the deployment contract where SL-T controls can't be implemented. Each compensating control must be risk-assessed, documented with justification, and independently verified as achieving the required SL-A during both design and after deployment. The System Owners shall lead the design of compensating controls and co-engineer each control with the cybersecurity lead to ensure they achieve the objective of the SL-T.
- 3.11.4 Security controls must not impact Safety Integrity Levels (SILs).
- 3.11.5 Security controls in safety critical zones with assigned SILs must be deployed prior to the SIL assessment. If the required SIL cannot be achieved due to constraints imposed by security controls, compensating controls must be designed to achieve an equivalent level of risk reduction as the SL-T.
- 3.11.6 The TSCC Contractor shall implement SL-T 4 controls for systems deemed to be critical to safety, operations, or feasibility of the California Highspeed Rail.
- 3.11.7 The TSCC Contractor shall implement SL-T 3 controls for systems that are deemed to be non-critical.
- 3.11.8 The TSCC Contractor shall review CENELEC TS 50701 considerations for implementing SL-T controls for rail systems.
- 3.11.9 The TSCC Contractor shall assign conduit SL-T's based on the highest-level SL-T of a zone that is sending information via the conduit.
- 3.11.10 The TSCC Contractor shall document details about each conduit between two zones, including which protocols are used and how each SL-T requirement is met. The System Owners shall ensure that these details are reflected in any interface documentation, such as an interface control document.
- 3.11.11 The System Owner must factor SL-T requirements into procurement processes, each component procured shall have a Security Level Capability (SL-C) that aligns with the SL-T of the zone where it shall be deployed. The cybersecurity requirements must be provided to the procurement team to ensure they are factored when selecting a product.



- 3.11.12 The TSCC Contractor shall identify where the SL-C of components does not meet the SL-T requirements, the System Owner shall co-engineer compensating controls with the Cybersecurity Lead to ensure the SL-A is equivalent to the SL-T.
- 3.11.13 The TSCC Contractor shall document all compensating controls as countermeasures with detailed justification and mapping to individual requirements.
- 3.11.14 SL-T assignments must be traceable to threat scenarios identified during risk assessments and documented in the zone and conduit design documentation.
- 3.11.15 The SL-A for each zone and conduit must be supported by testing evidence, configuration data, and commissioning reports that demonstrate that all applicable controls were implemented and effective.
- 3.11.16 Where SL-A testing is not feasible on the production system, representative test environments must be used to demonstrate compliance.
- 3.11.17 The TSCC Contractor shall not downgrade SL-T assignments for project convenience or similar reasons unless formally justified through risk reassessment and approved by the Cybersecurity Lead, Lead Engineer, and the Authority.
- 3.11.18 The System Owner shall work with the Cybersecurity Lead to plan testing, verification, and validation activities. Evidence that these activities have been completed with all detected issues remediated shall be provided to the Cybersecurity Lead to inform the Assurance Case.
- 3.11.19 SL-T and SL-A mappings must be incorporated into the Assurance Case and traceable to the corresponding testing, verification, and validation activities.



4 CYBERSECURITY MANAGEMENT

4.1 Cybersecurity Management Plan

- 4.1.1 The Cybersecurity Lead shall develop a Cybersecurity Management Plan that details how the requirements of this technical specification shall be met. The CSMP shall be reviewed and approved by the Authority prior to any security-critical works.
- 4.1.2 The Cybersecurity Management Plan shall detail the roles and responsibilities of staff participating in the delivery of the cybersecurity specification. Where multiple organizations are involved (e.g., subcontractors, integration teams, assurance providers), clear delineation of responsibility and reporting lines must be documented, including System Owners that shall own the risks of each system, subsystem, or asset.
- 4.1.3 The Cybersecurity Management Plan shall map deliverables and activities to the overall deployment schedule. Key cybersecurity activities must be integrated into system engineering, safety, and RAM processes.
- 4.1.4 The Cybersecurity Management Plan shall detail how cybersecurity requirements will inform design and deployment activities. This includes how security objectives, risk assessments, and security level targets influence network architecture, system configurations, and procurement.
- 4.1.5 The Cybersecurity Management Plan shall detail communications interfaces with other delivery teams, including relevant SMEs that will be informed, consulted, or responsible for aspects of cybersecurity activities and deliverables. The TSCC Contractor shall ensure that interfaces with systems engineering, safety, operations, RAMS, physical security, and third-party contractors are actively managed.
- 4.1.6 Progress towards achieving the tasks and objectives outlined in the Cybersecurity Management Plan and technical specification shall be shared and discussed during Security Steering Committee meetings. The Security Steering Committee shall be facilitated by the Cybersecurity Lead and have appropriate Authority stakeholders, including the Authority CISO or equivalent, legal, safety, and risk management teams, and TSCC Contractor stakeholders, including the Engineering Lead, Cybersecurity Services Lead, and appropriate resources as delegated by the parties involved.
- 4.1.7 Any issues with the management, design, or implementation of Cybersecurity requirements or Cybersecurity Services shall be raised and discussed in the steering committee to enable resolution.
- 4.1.8 The Authority may use the steering committee to communicate additional standards, compliance obligations, or audit requirements to the Cybersecurity Lead.
- 4.1.9 The Cybersecurity Management Plan shall include the following sections at a minimum:
- **Introduction:** This section shall provide background information, aims and objectives, purpose, and scope of the plan.
 - **Context:** This section shall outline the relevant legislation, standards, and considerations throughout the system's lifecycle.
 - **Management principles:** This section addresses the fundamental principles governing the cybersecurity management approach.
 - **Governance:** This section describes the structure and mechanisms that shall be used to oversee the delivery of cybersecurity activities, including the scope and high-level agenda of the steering committee meetings.
 - **Organization:** Details the roles and responsibilities of the cybersecurity team, stakeholders, SMEs from various domains, communication plans, System Owners, and domain team interfaces.



- **Cybersecurity Document and Configuration Management:** The TSCC Contractor shall describe the tools, repositories, and configuration management systems that shall be used to manage cybersecurity-related documentation, track changes, enforce traceability, and maintain version control of configuration files, design baselines, and security control mappings.
- **Cybersecurity Risk Management:** This section shall detail the steps that shall be taken and reference documentation to enable a risk-based approach to cybersecurity. The CSMP shall also define the governance process for reviewing and accepting residual risks, including decision authority, escalation thresholds, and documentation of residual risk justifications. System Owner risk ownership obligations, activities, and reporting cadences shall also be defined in this section.
- **Cybersecurity Supply Chain Risk Management:** This section shall detail the steps that shall be taken to mitigate supply chain risks, including how cybersecurity requirements will inform procurement activities and how vendors and products shall be assessed.
- **Cybersecurity Assurance:** This section shall detail the activities that shall be undertaken during verification and validation process to provide assurance that the cybersecurity system is fit for purpose and implemented to the standards of this specification.
- **Cybersecurity Design Principles:** This section shall provide an overview of design principles that shall be followed and a high-level overview of control categories and their purpose.
- **Secure-by-Design Approach:** This section shall provide a detailed breakdown of how cybersecurity is embedded early in system development and tracked through design changes. This shall include alignment with the system engineering process across all lifecycle phases, including cybersecurity risk reviews, control selection, validation steps, and transition checkpoints.
- **Cybersecurity Co-engineering:** The CSMP shall define how cybersecurity activities interface with RAMS and safety processes. This includes participation in HAZOPs, SIL assessments, and safety case reviews where cybersecurity affects safety-critical systems or logic.
- **Verification and Validation:** This section shall detail the activities involved in validating the choice of security controls, verifying the implementation and effectiveness of the security controls, and testing security controls to provide additional assurance that the controls are functioning correctly.
- **Vulnerability Management:** This section shall outline how cybersecurity vulnerabilities will be identified and managed throughout the deployment lifecycle and detail the testing activities, including Vulnerability Assessment and Penetration Testing (VAPT) that shall be performed.
- **Cybersecurity Incident Response:** This section shall detail processes and procedures for detecting and responding to incidents throughout the contract.
- **Cybersecurity Training:** The CSMP shall reference the Cybersecurity Training Plan and its integration with broader training and induction processes. It must identify dependencies and ensure cybersecurity readiness aligns with the project schedule.
- **Cybersecurity Metrics and KPIs:** The CSMP shall define Key Performance Indicators (KPIs), metrics, or quality gates used to measure the implementation, progress, and effectiveness of cybersecurity activities across design, testing, integration, and handover phases.
- **Cybersecurity Deliverables and Reporting:** This section shall outline how progress on cybersecurity activities is communicated to stakeholders and the details relating to the delivery of cybersecurity deliverables.
- **Cybersecurity Handover Activities:** This section shall outline the steps that shall be taken during the handover of cybersecurity related information to ensure it is done in a secure manner to the Authority and Operator.

4.2 Security Training

- 4.2.1 The TSCC Contractor must develop a Cybersecurity Training Plan, or embed cybersecurity training into a broader training plan, to ensure that personnel complete the required training as outlined in this section. The training plan must define training objectives, delivery methods, frequency, and responsible roles, and it shall be reviewed and approved by the Authority.



- 4.2.2 All TSCC Contractor or subcontractor personnel that perform works within the SuC must complete cybersecurity awareness training.
- 4.2.3 Cybersecurity awareness training shall include:
- Common social engineering attacks
 - Strong password and authenticator management
 - Action that shall be taken if they detect a potential incident
 - Common risks associated with the scope of work
 - Relevant policies, standards, and guidelines to be followed.
- 4.2.4 High-risk stakeholders shall be identified and receive targeted training to ensure they understand their roles and responsibilities and associated risks. These individuals must receive targeted, role-specific training to ensure they understand their cybersecurity responsibilities and associated risks. High-risk stakeholders include senior stakeholders, those responsible for providing Statement of No Objection (SONO), the Lead Engineer, and System owners or their delegates.
- 4.2.5 All TSCC Contractor staff, subcontractor staff, and staff that write code, programs, software, logic, or processes for components of the SuC must complete secure software development training or have appropriate certification to demonstrate their capabilities; The training must be used to inform staff of common vulnerabilities introduced by poor coding practices, how to test code for security vulnerabilities, and secure system development lifecycle practices. The training shall detail common vulnerabilities (e.g., OWASP, CWE Top 25) and threats.
- 4.2.6 All TSCC Contractor and subcontractor staff shall be encouraged to report cybersecurity vulnerabilities or perceived risks to the Cybersecurity Lead via their System Owner, the TSCC Contractor shall develop an incentive program to encourage reporting.
- 4.2.7 **Secure software development training or equivalent certification must be delivered by an industry-recognized organization that is approved by the Authority. Training providers should demonstrate currency, technical relevance, and should demonstrate credibility in ICS/OT and rail environments.**
- 4.2.8 **Cybersecurity training completion records must be maintained and reviewed quarterly to ensure continued compliance. Personnel that fail to complete refresher training within defined intervals must have their access suspended until training is complete.**
- 4.2.9 **Cybersecurity training content shall be periodically updated to reflect changes in the threat landscape, emerging technologies, updated regulations, and lessons learned from incidents.**
- 4.2.10 **Cybersecurity training shall be integrated into onboarding processes, system induction, and change-of-role procedures to ensure staff receive timely and relevant instruction.**
- 4.2.11 **The Cybersecurity Training Plan shall define processes for evaluating training effectiveness, such as assessments, feedback, or training audits. These results shall be reported to the Authority and used to inform continuous improvement.**

4.3 Assurance, Audit and Compliance

- 4.3.1 In addition to the audits and verification activities that the TSCC Contractor shall perform, the TSCC Contractor must agree to facilitate any audits requested by the Authority or Lead Engineer to verify that all the planned cybersecurity measures are properly applied.



- 4.3.2 The TSCC Contractor shall periodically audit systems, assets, and endpoints to detect potential non-compliance, compromise, or fraudulent activity throughout the deployment and maintenance periods. Audit frequency and scope shall be risk-based and aligned with lifecycle phases.
- 4.3.3 The TSCC Contractor shall make available, on request, all the necessary elements, such as people, documents, or source code, to facilitate these activities.
- 4.3.4 Cybersecurity deliverables from the TSCC Contractor shall be formally reviewed and validated by the Cybersecurity Lead and Lead Engineer throughout the project. These reviews must include technical validation of assumptions, alignment with SL-Ts, and consistency across interface boundaries.
- 4.3.5 The TSCC Contractor may choose to have the deliverables independently verified (cost to be borne by the TSCC Contractor)
- 4.3.6 The Authority may choose to have cybersecurity deliverables independently verified (cost to be borne by the Authority)
- 4.3.7 The TSCC Contractor shall develop an Assurance Case throughout the contract which is supported by a continuously updated library of evidence including the following:
- Data
 - Scripts
 - Documentation
 - Meeting Minutes
 - Notes
 - Findings
 - Opinions
 - Recommendations
 - Emails
 - Risk Documentation
 - Test Results
 - V&V Activities and Evidence
 - Cybersecurity Requirements Analysis
 - Vulnerability Assessment Results
 - Penetration Test Results.
- 4.3.8 The TSCC Contractor shall store supporting information and reports in an appropriate system; the information must be available to authorized stakeholders through a standard document management or ticketing system. The system shall enforce version control and audit logging, and support traceability to individual requirements.
- 4.3.9 The Assurance Case shall be created and maintained by the Cybersecurity Lead; the Cybersecurity Lead shall request information from System Owners who shall be responsible for providing evidence as required.
- 4.3.10 The Assurance Case shall include a high-level summary that details how the cybersecurity specification requirements are achieved and directly reference evidence items that demonstrate how the requirements have been met.
- 4.3.11 The target audience for the Assurance Case shall be Authority Stakeholders and approving bodies; it shall provide a sufficient overview of the cybersecurity works that accurately represents the steps taken



while enabling effective decision making. The structure of the Assurance Case must support rapid traceability from cybersecurity objectives to risk mitigation and verification results.

- 4.3.12 The TSCC Contractor may use a solution that is used for other domains of the contract to store the supporting evidence for the Assurance Case; cybersecurity information shall be segregated from information of other domains using access control to ensure only authorized parties have access.
- 4.3.13 The TSCC Contractor shall provide summaries of the Assurance Case on an on-going basis, as agreed with relevant Authority stakeholders, or quarterly at a minimum.
- 4.3.14 The Assurance Case and supporting evidence shall be reviewed by an independent party on a periodic basis, as agreed with the Authority, to provide assurance to the Authority that cybersecurity works are proceeding appropriately and that the information in the Assurance Case remains accurate with appropriate evidence.
- 4.3.15 The final Assurance Case shall be independently reviewed in the final phases of the contract to ensure that the cybersecurity practices and activities performed during the contract align with this technical specification. The review must validate the completeness of security controls, adequacy of risk treatments, and alignment with SL-T/SL-A outcomes.
- 4.3.16 The final Assurance Case sign-off or SONO shall represent the acceptance of the cybersecurity works; the sign-off must include signatures of Authority stakeholders and Lead Engineer.
- 4.3.17 The TSCC Contractor shall have an independent contractor verify the compliance of the design to ensure it aligns with the requirements established in this technical specification.
- 4.3.18 The TSCC Contractor shall track and report cybersecurity non-conformances raised during audits or testing and manage them using a formal non-conformance reporting and resolution process that includes impact assessment, corrective action, and traceable closure.

4.4 Supply Chain Risk Management

- 4.4.1 The supply chain of system components is a potential attack vector that threat sources may exploit to compromise SuC. This includes hardware, software, firmware, services, and data sources originating from third parties or sub-suppliers.
- 4.4.2 The TSCC Contractor must establish processes and procedures for supply chain risk management that are reviewed and approved by the Authority and relevant stakeholders.
- 4.4.3 The TSCC Contractor shall be responsible for ensuring that risks associated with the supply chain of system components within the SuC are identified and mitigated, including:
 - Vendors and manufacturers
 - Software developers and integrators
 - Contracted installation or commissioning teams
 - Cloud or third-party service providers.
- 4.4.4 The TSCC Contractor shall define a cybersecurity baseline that the vendors and procured components must comply with to ensure they align with the requirements of this technical specification and the SL-C requirements for each zone.
- 4.4.5 The TSCC Contractor must assess individual hardware and software component vendors' cybersecurity practices to ensure they have an effective risk management program, follow secure development and engineering practices, and manage their individual supplier's cybersecurity risks (fourth parties).



- 4.4.6 The TSCC Contractor shall document evidence for each supplier which demonstrates that the supplier has good security practices and that an appropriate assessment has been completed.
- 4.4.7 The TSCC Contractor's assessment must influence procurement decisions when selecting individual components.
- 4.4.8 Supply chain risk assessments shall follow the agreed risk assessment process and include consideration of:
- Geopolitical risk of supplier location
 - History of vendor compromise or backdoor discovery
 - Access granted to the SuC (direct or remote).
- 4.4.9 TSCC Contractor suppliers and vendors that perform hands-on work and configuration of systems within the SuC must be appropriately trained and managed.
- 4.4.10 The TSCC Contractor shall identify, and document risks related to the country of origin and control of chipsets, firmware, embedded devices, or software. These evaluations shall align with U.S. national security guidance or directives (e.g., DHS BODs, NIST IRs, NDAA).
- 4.4.11 The TSCC Contractor shall identify strategies for alternatives, including any costs (price, people, resources, system availability) to move to a new component or supplier.
- 4.4.12 The TSCC Contractor shall appoint an independent cybersecurity reviewer to assess the effectiveness of the supply chain risk management approach. This assessment shall be documented and submitted to the Authority at major project milestones.
- 4.4.13 The TSCC Contractor shall maintain a list of all third-party and open-source components used in software or firmware provided as part of the SuC. **This list shall take the form of a Software Bill of Materials (SBOM) and must be updated and reviewed as part of system acceptance.**
- 4.4.14 **The TSCC Contractor must evaluate the cybersecurity implications of any third-party libraries, runtime environments, or remote update mechanisms included in deliverables. Remote update connectivity must be co-engineered between the Cybersecurity Lead, System Owner, and Cybersecurity Services Lead to facilitate connectivity in compliance with this technical specification.**
- 4.4.15 **The TSCC Contractor shall subject all procured firmware and software (including vendor-supplied images) to integrity checks and malware scanning prior to installation into any zone within the SuC.**
- 4.4.16 **The TSCC Contractor shall document and maintain a chain-of-custody log for critical components (e.g., networking equipment, PLCs, safety interfaces) from procurement through to commissioning.**
- 4.4.17 **The Authority reserves the right to require supplier substitution in the event of perceived cybersecurity risk, and the TSCC Contractor shall cooperate and facilitate transition activities.**

4.5 Product Lifecycle and Obsolescence

- 4.5.1 The TSCC Contractor shall document End of Support (EoS) and End of Life (EoL) dates for all endpoints, assets, components, software, and other procured goods that are part of the SuC (including all firmware and embedded software components).



- 4.5.2 The TSCC Contractor shall obtain and document the vendor's lifecycle and support policy for each procured product, including security patching cadence, notice periods for EoL announcements, and process for extended support agreements.
- 4.5.3 EoS refers to the date when the vendor or developer of an item stops producing updates, security patches, or provides technical support for that item; meaning vulnerabilities that are present on the system after the EoS date will remain vulnerable indefinitely.
- 4.5.4 EoL refers to the last day when the product is being produced and sold by the vendor or developer; meaning replacement parts are no longer available.
- 4.5.5 EoL and EoS dates shall be available in the asset inventory for all entries, where applicable. The inventory must support automated queries and filtering based on support status.
- 4.5.6 Vendor support, prior to the EoS, shall include security updates and patches for vulnerabilities.
- 4.5.7 The TSCC Contractor shall ensure that all products procured under the contract shall have a minimum of ten years of declared support from the vendor; the end of support date shall be no sooner than ten years from the date of implementation. The vendor's EoS declaration must be available in writing or verified from official sources.
- 4.5.8 Any procured goods under the contract that have an EoL or EoS date within ten years of implementation shall not be allowed; where options are not available that fulfill this requirement, the TSCC Contractor must provide a detailed written justification to the Authority for review and acceptance.
- 4.5.9 The TSCC Contractor must implement a solution, either as part of the asset management system or an interfacing system that alerts the TSCC Contractor and Authority, twelve, six, and three months prior to the EoS or EoL date.
- 4.5.10 Where the TSCC Contractor has procured goods that are approaching EoL or EoS, the TSCC Contractor must develop a mitigation plan which outlines steps to either replace the item or procure extended support for the item for a reasonable period until the item can be replaced. The mitigation plan must include a strategy for replacement or upgrade, evaluation of extended support options, a risk assessment aligned to contract-specific frameworks and estimated costs and timelines. The plan must be submitted to the Authority for review and approval.
- 4.5.11 **All software components must be reviewed to identify hardcoded dependencies on EoL software platforms (e.g., outdated runtime libraries, unsupported operating systems, deprecated APIs).**
- 4.5.12 **The TSCC Contractor shall maintain a lifecycle roadmap that identifies support timelines and planned upgrade windows for all major SuC components, aligned to maintenance access windows and Authority deployment plans.**
- 4.5.13 **Product lifecycle risks shall be tracked in the cybersecurity risk registers and cross-referenced in the Assurance Case.**
- 4.5.14 The TSCC Contractor shall maintain a rolling 5-year product transition or replacement roadmap for all critical SuC components that have anticipated End of Support (EoS) or End of Life (EoL) risk. This roadmap shall be reviewed and updated annually with the Authority.
- 4.5.15 The use of grey-market, refurbished, or unsupported hardware or software components is prohibited unless explicitly approved by the Authority through a formal risk-based justification and documented exception process.



- 4.5.16 If a product within the SuC becomes subject to an unplanned EoS or EoL event, the TSCC Contractor must notify the Authority within ten (10) business days of becoming aware. A revised risk assessment and mitigation plan must be submitted within thirty (30) business days.



5 CYBERSECURITY RISK MANAGEMENT

5.1 Risk Assessment Activities

- 5.1.1 The TSCC Contractor must follow a formal process for cybersecurity risk assessments; the process must be reviewed and approved by the Authority and relevant senior stakeholders. This process must align with the Authority's contract-specific risk standards, as well as NIST, CENELEC TS 50701, TSA, and other applicable federal and program guidance. The process must demonstrate traceability from threat modelling to SL-T assignment, control definition, and risk treatment.
- 5.1.2 The TSCC Contractor must use a risk matrix during risk assessments that must be approved by the Authority and relevant senior stakeholders.
- 5.1.3 The TSCC Contractor must use documented likelihood and consequence descriptions during risk assessments that directly align with the risk matrix and are not ambiguous. These definitions must be traceable to the risk appetite and consequence levels defined by the Authority.
- 5.1.4 The TSCC Contractor shall work with the Authority to determine risk acceptance levels.
- 5.1.5 The TSCC Contractor shall define risk scenarios based on credible threats.
- 5.1.6 The TSCC Contractor shall perform threat modelling exercises to identify risk scenarios, threat modelling exercises must, at a minimum, include:
- Threats outlined in this specification
 - Threats from industry standards
 - Advisories from ENISA, TSA, and NIST
 - MITRE ATT&CK for ICS and current TTPs from threat intelligence sources
 - Program-specific threat guidance issued by the Authority or U.S. federal agencies (e.g., CISA).
 - Threat modelling activities must be completed multiple levels of decomposition, including:
 - At the architectural level – modelling threats at the SuC boundary and overall system
 - At the zone level – modelling threats between zones or conduits
 - At the asset or functional level – modelling risks to individual components or services
- 5.1.7 Each threat model must define the assets in scope, entry points, trust boundaries, communication flows, and attacker objectives.
- 5.1.8 The TSCC Contractor shall use the output of vulnerability assessments to inform threat modelling and risk analysis. Findings must be documented and mapped to known threat scenarios.
- 5.1.9 Risk assessment and threat modelling activities must include relevant subject matter experts and stakeholders from engineering, maintenance, cybersecurity, rail operations, the Authority, suppliers, and other relevant teams. The System Owner shall be responsible for ensuring that the right resources are in attendance.
- 5.1.10 The TSCC Contractor must create formal documentation for all risk assessments; the risk assessment documentation must include all relevant evidence and activities.
- 5.1.11 Each System Owner shall be accountable and responsible for maintaining a risk register that contains all cybersecurity risks associated with their system, subsystem, or asset. The System Owner may delegate this responsibility to an appropriate member of personnel that reports directly to the System Owner. The Risk Register shall be kept current and contain the required information as agreed with the Cybersecurity Lead.



- 5.1.12 The Cybersecurity Lead must produce and maintain a formal, version-controlled centralized cybersecurity risk register. The register must support filtering and categorization by zone, conduit, system, threat type, asset class, and responsible party. Each entry must include a unique identifier, risk owner, risk scenario, affected systems, impact category, risk rating, treatment plan, and status.
- 5.1.13 The TSCC Contractor shall work with relevant senior stakeholders, including the Lead Engineer and Authority to determine risk treatment options once initial security level targets, security controls, and risk ratings have been defined from the options below:
- **Accept:** If the risk is within appetite or tolerance and no security controls will reduce the risk further, the risk shall be accepted by an authorized party.
 - **Mitigate:** Mitigating risks involves defining additional controls to reduce the risk rating, primarily by implementing controls to reduce the likelihood of occurrence.
 - **Avoid:** Avoiding risks is the process of removing the source of the risk where risks can't be mitigated, this is usually achieved by changing the architecture or de-scoping the risk source.
 - **Transfer:** Transferring risks is the process of moving the responsibility of managing a risk to a third party, an example of risk transference is the usage of cloud-based email instead of hosting a local email server.
 - The TSCC Contractor shall have an independent contractor verify the risk assessment process has been followed and identified risks align with the justification and analysis provided.

5.2 Risk Assessments

5.2.1 The TSCC Contractor must at a minimum complete the risk assessments outlined in this section.

5.2.2 High Level Risk Assessment

- 5.2.2.1 The TSCC Contractor must perform a high-level risk assessment during the System definition and Operational Context phase,
- 5.2.2.2 The high-level risk assessment shall align with the objectives of the high-level risk assessment described in CENELEC TS 50701.
- 5.2.2.3 The high-level risk assessment shall primarily be an impact assessment, determining the consequences of individual components of the SuC being compromised.
- 5.2.2.4 The TSCC Contractor shall perform the high-level risk assessment under the assumption that there are no security controls in place to reduce the likelihood or consequence of any risks or threat scenarios identified during high-level risk assessment activities.
- 5.2.2.5 Risk ratings assigned to risk scenarios as an outcome of the high-level risk assessment shall be documented as inherent risk ratings for traceability throughout the contract scope of works to demonstrate risk mitigation efforts
- 5.2.2.6 As an outcome of the high-level risk assessment, the TSCC Contractor shall map risk scenarios to worst case consequence descriptions to prioritize risks and inform the SL-Ts as detailed in section 3.10.
- 5.2.2.7 The TSCC Contractor shall determine if changes to the conceptual zone and conduit model is required to mitigate or avoid risks
- 5.2.2.8 The outcomes of the high-level risk assessment and any changes to the zone and conduit model must be used to inform design decisions of the network and asset interfaces
- 5.2.2.9 The Cybersecurity Lead must sign the relevant architectural and design documentation to verify that cybersecurity controls and mitigating actions have been adequately included and referenced.



- 5.2.2.10 The high-level risk assessment shall be reviewed and signed off by the Authority and Operator (where applicable) to ensure operational and transitional risks are captured early.
- 5.2.2.11 The high-level risk assessment shall include the Lead Engineer, Authority, and be facilitated by the Cybersecurity Lead.
- 5.2.3 Detailed risk assessment**
- 5.2.3.1 The TSCC Contractor must conduct a detailed risk assessment during the risk analysis and evaluation stage.
- 5.2.3.2 The detailed risk assessment shall expand upon the high-level risk assessment using additional system context, such as protocols used for communication and interface requirements.
- 5.2.3.3 The detailed risk assessment shall be completed at multiple levels of detail, including a system-wide assessment, a zone level assessment, and an asset level assessment; each assessment shall be performed with staff appropriate for the level of detail (such as strategic resources for system-wide, technical SMEs delegated by the System Owners for lower level).
- 5.2.3.4 A risk rating shall be determined during the detailed risk assessment; this risk rating shall be based on the controls that are planned to be implemented by performing a likelihood assessment.
- 5.2.3.5 The TSCC Contractor shall ensure that detailed risk assessments are coordinated with safety, RAMS, and human factors engineering to ensure a cross-domain understanding of residual system risk.
- 5.2.3.6 All detailed risk assessments must trace individual risks to applicable security requirements, zones, and interface specifications and identify responsible System Owners.
- 5.2.3.7 A list of risk treatment selections shall be produced as an outcome of the detailed risk assessment, the treatment selections shall be co-engineered by the Cybersecurity Lead, System Owners, and their delegates
- 5.2.3.8 Where a decision has been made to mitigate a risk, a detailed list of security controls and mitigating actions shall be listed against the risk scenario.
- 5.2.3.9 Where the controls defined throughout this specification and the SL-T requirements don't reduce risks to an acceptable level, the TSCC Contractor may choose to implement additional countermeasures.
- 5.2.3.10 Policy or procedural processes required to mitigate risks to acceptable levels shall be communicated to the Operator.
- 5.2.3.11 All assumptions made during the detailed risk assessment must be documented, including details of how they may affect the risk rating.



6 CYBERSECURITY SYSTEM REQUIREMENTS

6.1 Network Segmentation

- 6.1.1 The TSCC Contractor must segment the SuC from all external networks; this includes physical, logical, and functional segmentation of safety, operations, and enterprise zones in accordance with the defined zone and conduit model. Traffic between the SuC and interfacing networks must be monitored, analyzed, and controlled.
- 6.1.2 The network in this section refers to the DCN and other communications networks that carry operational data, voice data, video data, and other data required to achieve the objectives of the technical specifications, such as cybersecurity logging data.
- 6.1.3 The TSCC Contractor shall limit network traffic to only what is required to enable the operation of the CHSR system and facilitate the required interfaces.
- 6.1.4 The network must not be dependent on external networks, if there is an outage of IT, ticketing, public wi-fi, or other networks, the operational network must still be functional.
- 6.1.5 The network must be capable of fail-secure modes of communication, where communication between zones is restricted to mitigate an incident while also considering safety implications; fail-secure and fail-safe modes must be analyzed for incident containment activities.
- 6.1.6 The TSCC Contractor shall implement a DMZ between the SuC's boundary and external networks.
- 6.1.7 The DMZ shall host all services that require communication between networks and centralized services, traffic shall be controlled so that two networks never directly communicate with each other. Inbound and outbound traffic from the DMZ must be strictly limited and monitored.
- 6.1.8 The TSCC Contractor shall implement a combination of physical segmentation and logical segmentation wherever feasible to protect critical systems; physical segmentation refers to using different networking infrastructure for different zones or systems, meaning they are "air-gapped" and have no logical method of communicating with each other.
- 6.1.9 The TSCC Contractor should consider using data diodes, which are dedicated communication devices only capable of unidirectional communication, where critical networks are required to send data to non-critical networks or where traffic is not required to be bi-directional. Where data diodes are used, the TSCC Contractor must consider requirements such as bi-directional protocols (TCP) and procure diodes or supporting technology capable of managing these connections.
- 6.1.10 The SuC network must be segmented in alignment with the zone and conduit model, each zone shall be logically segmented from other zones, communication between segments shall be controlled and compliant with the conduit requirements. Zoning shall also reflect functional and safety boundaries, including SIL, RAMS, and SL-T requirements.
- 6.1.11 The TSCC Contractor shall procure appropriate networking devices capable of restricting all communications between segments unless explicit allow rules are defined and implemented. The use of deny-by-default and explicit allowlists shall be enforced at all network boundaries.
- 6.1.12 Network Management Systems shall be on an isolated out-of-band management network with dedicated communication paths. Shared management/data planes are not permitted without documented justification and approval.
- 6.1.13 All network management traffic should use dedicated network interfaces that are physically and logically isolated from regular network traffic.



- 6.1.14 Where data, files, or updates need to be downloaded from the internet, strict rules must be enforced. The TSCC Contractor should consider configuring rulesets on network boundary devices that can be enabled and disabled to open or close communications with update servers in the DMZ when required to limit the attack surface.
- 6.1.15 DNS, DHCP, Authentication Services, Directory Services, Timing Servers, and other critical networking servers must be segmented and protected from unauthorized access. These services shall reside in hardened security zones with restricted access control. Secure versions of protocols shall be used over default protocols.
- 6.1.16 The TSCC Contractor should consider the use of virtualization technologies to enforce zone boundaries, such as virtual switches, virtual routing (VRF), virtual firewalls, and software-defined networking.
- 6.1.17 The TSCC Contractor shall ensure that all traffic between zones at the same physical location traverses the firewall or virtual firewalls to enforce micro segmentation and ensure traffic traverses secure conduits.
- 6.1.18 Network communication rules, such as ACLs, firewall rules, VLANs, subnets, and other information must be documented and updated on a regular basis with version control. Configuration changes must follow formal change control procedures and be reviewed for cybersecurity impact prior to implementation. The TSCC Contractor shall validate segmentation controls through formal testing (e.g., port scans, ACL enforcement checks) during design, commissioning, and whenever network changes occur. Periodic reviews must be undertaken to confirm segmentation remains effective and aligned with design intent.

6.2 Network Security

- 6.2.1 The Cybersecurity Services Lead shall be responsible for configuring network devices that have been procured for the purpose of cybersecurity, such as IDS, IPS, and Firewalls. The Cybersecurity Services Lead shall work closely with the networking team to identify roles and responsibilities for individual devices and co-engineer all connectivity rules.
- 6.2.2 The TSCC Contractor must implement technical mechanisms, such as Network Management Systems, to enable the implementation and monitoring of network configuration and security settings.
- 6.2.3 The TSCC Contractor shall ensure that traffic within the boundaries of and at the boundary of critical networks or zones is limited to exclusively required traffic and monitored for signs of compromise.
- 6.2.4 Deep Packet Inspection (DPI) and Intrusion Prevention Systems (IPS) shall be used at the boundary of networks and must detect where unexpected protocols or payload data are being transmitted.
- 6.2.5 TLS Termination points shall be considered to enable deep packet inspection or protocol analysis.
- 6.2.6 The TSCC Contractor shall consider all user access from external networks to be remote access; remote access must be managed, protected, and require secure authentication and defined authorization (Network Access Control). All remote access requirements must be documented by the System Owners and co-engineered by the System Owner, Cybersecurity Lead, Cybersecurity Services Lead, and the TSCC Contractor or subcontractor that requires remote access.
- 6.2.7 The TSCC Contractor shall procure networking, encryption, and security software and hardware to comply with the security requirements outlined in this specification, where devices are procured, their functionality should be clearly documented, as certain devices will be capable of multiple of the following, this list should be considered in addition to other solutions:
 - 6.2.7.1 Stateful Firewalls with advanced capabilities to manage and filter traffic, manage sessions, and enforce policies at the boundary or between network segments and zones.



- 6.2.7.2 Deep Packet Inspection, which performs analysis of packet payload data, can verify additional details to ensure that network traffic is using the expected protocols and communicating expected amounts or types of data.
- 6.2.7.3 Intrusion Detection and Prevention Systems, capable of either detecting and alerting potential intrusions (out-of-line) or stopping potential attacks (in-line)
- 6.2.7.4 Anti-DoS solutions, capable of detecting denial of service traffic and implementing countermeasures
- 6.2.7.5 Secure Remote Access solutions capable of enforcing policies, requiring strong authentication with complex passwords and MFA, making risk-based access decisions, maintaining session integrity, and allowing central management and monitoring of open sessions.
- 6.2.7.6 Secure, dedicated servers for remote access, such as a tightly controlled RDP server configured with secure hardening, least functionality, monitoring, and additional authentication requirements.
- 6.2.7.7 Routers, switches, and gateways with the capabilities to enforce zone and conduit SL-T requirements, such as communication confidentiality and integrity using modern protocols.
- 6.2.7.8 Proxies or Reverse Proxies capable of inspecting traffic for anomalies and enforcing policies (denying network communications if a device is not compliant)
- 6.2.7.9 Centralized identity, authentication, and access management, including directory services (such as Active Directory), and AAA services (such as RADIUS) in addition to other solutions that enable authentication and policy enforcement across devices communicating on the network.
- 6.2.8 Firewalls shall be deployed across the network and not only at the boundary of the network, network traffic shall follow deny-by-default rules when communicating between zones, ACLs shall be used but must be complemented by firewalls to enable packet filtering.
- 6.2.9 Network security devices that are enriched by cloud-based libraries or artificial intelligence may be used to complement network security objectives. Where these devices are used, they shall be deployed on an isolated network which receives logs using a data diode that only permits unidirectional traffic. These devices must be protected from unauthorized access and configured with deny-by-default firewalls, allowing only the minimum necessary connectivity to external services. Cloud-enabled network security devices shall forward high-value packets to the SIEM to enhance security incident detection. The TSCC Contractor shall determine whether this device is located on the same network as the SIEM or on a separate, dedicated network. Additionally, such devices must not introduce new threat vectors from external cloud APIs, enrichment feeds, or remote management interfaces. Their exposure to the internet shall be tightly controlled and reviewed regularly to ensure that threat intelligence feeds do not result in an expanded attack surface.
- 6.2.10 All network devices must have synchronized clocks and timestamps.
- 6.2.11 The TSCC Contractor may use a combination of hardware-based, embedded, host-based, and software-based firewall technologies to achieve network security objectives.
- 6.2.12 Network traffic between zones (within conduits) shall be encrypted for all communication within the SuC.
- 6.2.13 Network traffic between or within critical zones shall be analyzed for signs of intrusion or anomalous behavior.
- 6.2.14 The TSCC Contractor shall determine where intrusion detection shall be used over intrusion prevention using a risk-based approach; safety critical systems must not be interrupted by an intrusion prevention system unless a fail-safe state has been enforced.
- 6.2.15 Network devices must be configured to only allow connections from specified ports and protocols.



- 6.2.16 Port security and MAC Address binding shall be implemented for all physical interfaces; changes to the MAC Address connected to individual interfaces must be logged.
- 6.2.17 Network devices, including security solutions, must be patched periodically in accordance with their criticality and location on the network.
- 6.2.18 Patching timeframes for internet facing remote access solutions and firewalls must be in accordance with industry best practice.
- 6.2.19 Processes and procedures for limiting connectivity to internet facing devices or devices facing other external networks shall be defined to ensure that a secure state can be maintained if a patch for a critical vulnerability is not available.
- 6.2.20 Remote access solutions should limit remote access requests to specific IP ranges associated with a secure VPN or network where only security policy compliant devices can communicate.

6.3 Remote Access

- 6.3.1 Some systems, subsystems, and assets across the CHSR SuC will require remote access, it is the responsibility of the System Owner to ensure that all remote access requirements are identified early in the contract to ensure that the Cybersecurity Services Lead can facilitate the connectivity. Remote access activities may include maintenance work, patching, configuration, regulator access, vendor access, and performance monitoring. Where the remote access solution does not support the requirements of the TSCC Contractor, subcontractor, or vendor, the System Owner must work with the Cybersecurity Services Lead to design and co-engineer a solution that is fit for purpose while achieving the requirements of this specification. All remote access that does not fit the requirements of this specification must be documented, approved by the Cybersecurity Lead, Lead Engineer, and Authority, and disabled once the remote access is no longer required.
- 6.3.2 The System Owner shall be responsible for ensuring that no undocumented or insecure remote access connectivity is established, this shall include the identification of unauthorized devices being connected to on-site assets for the purpose of remote access. All instances of unauthorized connections or devices being discovered shall be reported to the Cybersecurity Lead, the Cybersecurity Lead shall ensure that appropriate action is taken as agreed with the Authority.
- 6.3.3 All activities that require remote access to any components of the SuC must be pre-approved:
 - System Acceptance Phase:
 - Pre-Handover (Pre-Operational Testing): Remote access is managed by the TSCC Contractor.
 - Pre-Handover (Operational Testing): Approval is granted by The Authority (Integrator).
 - Operation, Maintenance, and Performance Monitoring Phase:
 - Post-Handover (during the Defects Liability Period (DLP)): Approval is managed by The Authority (O&M).
 - Post-DLP: Approval is managed by The Authority (O&M).
- 6.3.4 Where subcontractors require remote access to the SuC, appropriate risk assessments and mitigation strategies must be defined and approved by The Authority.
- 6.3.5 Remote access to the SuC must be centralized, managed, controlled, monitored, and protected from unauthorized access.
 - **The TSCC Contractor shall be responsible for implementing and maintaining these controls Pre-Handover.**
 - **Post-Handover, the Operator and/or Maintainer shall take over full responsibility.**



- 6.3.6 Remote access to the SuC must be facilitated by a dedicated solution capable of session management.
- 6.3.7 Remote access to the SuC must use dedicated jump hosts that are hardened.
- 6.3.8 Remote access jump hosts shall be in the DMZ.
- 6.3.9 Jump hosts shall follow the least functionality principle.
- 6.3.10 Different jump hosts must be used for different levels of criticality, a dedicated jump host shall exist for the following categories at a minimum, each jump host shall have dedicated zones and conduits with appropriate security controls:
 - Safety-critical
 - Operations-critical (Other than safety)
 - Non-critical
 - Secondary Networks (testing, staging, non-production).
- 6.3.11 Remote access sessions shall be time limited and require a new session to be created once the time limit has been reached.
- 6.3.12 Remote access sessions' time to expire shall be defined during change management procedures.
- 6.3.13 All remote access sessions shall be mapped to work tickets, change management, or change control documentation.
- 6.3.14 Remote access changes shall be mapped to an individual and tied back to approved changes; any actions that deviate from change documentation shall be reviewed and appropriate steps shall be taken where fraud is discovered, or process and procedure has not been followed.
- 6.3.15 Remote access sessions must be logged; logged details shall include:
 - Remote Access User ID
 - Authentication details
 - Time
 - Duration
 - Systems accessed
 - Actions taken
 - Source IP
 - Other available information relevant to security event detection or audit activities.
- 6.3.16 Remote access sessions must have unique and random session identifiers.
- 6.3.17 Remote access sessions must be closed once the TCP or UDP session is closed, a new session must be opened for each individual connection.
- 6.3.18 Remote access communications shall be encrypted using the protocols permitted in this specification.
- 6.3.19 Connections to the remote access solution shall be limited to certain IP ranges, these IP ranges shall be associated with a secure network or authenticated VPN.
- 6.3.20 IP Ranges that are allowed to connect to the remote access solution must be approved by The Authority.
- 6.3.21 The TSCC Contractor shall ensure that the network and devices associated with the IP ranges permitted to connect remotely are adequately secure and comply with this technical specification.
- 6.3.22 All remote access connections shall use multi-factor authentication and strong passwords.



- 6.3.23 Remote access to critical systems shall be limited; where this connectivity is required, the connectivity shall be facilitated using temporary rulesets which are disabled once the work has been completed.
- 6.3.24 Authorized personnel shall have the capability to approve, deny, or close remote access sessions.
- 6.3.25 All remote access connectivity must pass through advanced firewalls and intrusion detection and prevention technologies.
- 6.3.26 The remote access solution may be configured to enable supervisor override, dual control, or similar technical controls that require a member of staff, located in the CSOC or OCC, to control the changes made by users connecting via the remote access solution; where this control is implemented, the authorized personnel in the CSOC or OCC shall be responsible for approving changes to systems accessed remotely, all actions by the approving user shall be logged.
- 6.3.27 Dual control, supervisor override, or similar controls must consider safety cases and incident response activities to ensure that the control does not inhibit staff from performing their duties during emergency procedures.
- 6.3.28 Remote Access to the SuC shall implement role-based access control and follow the least-privilege principle.
- 6.3.29 Remote access to the SuC shall use just-in-time access provisioning, remote access accounts shall not be active unless they require access; a remote access account that is active shall only have the permissions required to perform the change associated with the current session.

6.4 Wireless Security

- 6.4.1 This section shall apply to all wireless access within the SuC, including wi-fi leveraged by contractors, FRMCS, and other networks that the public does not have access to.
- 6.4.2 Wireless access points must authenticate all devices that connect to a network; authentication must permit unique identification of the device that has connected, tied back to an identifier in the asset inventory.
- 6.4.3 Wireless users must authenticate to wireless networks using unique credentials, keys, or certificates.
- 6.4.4 Wireless access shall be limited to authenticated, authorized, and managed devices.
- 6.4.5 Access control must be implemented for wireless networks in alignment with the access control requirements specified in this standard.
- 6.4.6 Wireless networks shall be capable of detecting unauthorized devices attempting to connect to the network and alert the central logging or SIEM platform when such attempts occur.
- 6.4.7 Wireless networks shall implement mitigation and/or prevention measures for, at a minimum, the following attack types:
 - Signal jamming (Denial of Service)
 - Fake or rogue Access Points
 - Spoofed wireless traffic (False Commands)
 - Wireless traffic sniffing (Capture and read wireless traffic)
 - Replay attacks (Repeating captured wireless signals)
- 6.4.8 Secure wireless protocols shall be used to ensure that wireless traffic is encrypted. The wireless protocol shall either be WPA3 or another protocol that complies with the encryption requirements defined in this technical specification.



- 6.4.9 Network security controls, such as logging and audit requirements, shall apply to wireless networks.

6.5 Endpoint Security

- 6.5.1 To support a defense-in-depth approach, the TSCC Contractor must implement security controls on endpoints as an **independent** layer of protection, complementing network and perimeter controls.
- 6.5.2 For this section, endpoints refer to all devices that communicate leveraging IP-based technology or run general purpose operating systems such as Linux or Windows. Many of the controls outlined in this section may not apply to other types of operating system, device, or communications technology, such as Real-time Operating Systems on embedded devices that use serial based hard-wired communications. The ability to protect these devices to the standard outlined in this specification must be considered when making procurement choices and equivalent countermeasures must be defined and implemented so far as reasonably practicable.
- 6.5.3 The Cybersecurity Services Lead shall be responsible for ensuring that centralized solutions for endpoint security (such as anti-malware) are available and consumable. The System Owners shall work with the Cybersecurity Services Lead to on-board all endpoints to these solutions.
- 6.5.4 System Owners shall be responsible for ensuring all endpoints within their scope of ownership are compliant with this specification, including working with the Cybersecurity Lead and Cybersecurity Services Lead to ensure that secure baseline images are used, secure images are created once configuration is completed, and appropriate security guidelines are selected.
- 6.5.5 Endpoints must be configured to provide only the essential functions required for their intended purpose and nothing more.
- 6.5.6 Endpoints must have the capability to detect and prevent the execution of malicious code from all sources.
- 6.5.7 Malicious code detection and prevention must at the minimum be signature-based detection and shall be complemented by behavior-based detection capabilities.
- 6.5.8 Malicious code detection and prevention technologies or techniques must be kept current by receiving updates to detection logic or the library of known malicious signatures.
- 6.5.9 Malicious code prevention technologies shall not interfere with safety integrity, where automated prevention introduces risk that a safety critical system may fail, countermeasures shall instead be defined and implemented.
- 6.5.10 Endpoints shall be capable of identifying and authenticating individual software and processes; where an endpoint hosts more than one process, each process must be uniquely identified and authenticated.
- 6.5.11 Security hardening measures for endpoints must include the blocking or disablement of unused services, ports, and protocols.
- 6.5.12 Vendor hardening guidelines or industry hardening guidelines, such as CIS benchmarks, must be implemented to securely harden endpoints.
- 6.5.13 Endpoints that users directly interact with shall be monitored by a configuration management solution that detects changes to baseline configurations.
- 6.5.14 Hardening shall be completed prior to configuring endpoints. Services, ports, and protocols that are required shall be re-enabled during configuration.



- 6.5.15 Applications and software executions shall be limited to an approved set by leveraging a combination of techniques, which include removing unused applications and software, verifying application signatures, application control or whitelisting, group policy rules, and access controls.
- 6.5.16 Endpoints must be configured to prevent autorun for removable media.
- 6.5.17 Endpoints shall automatically scan removable media for malicious code, in addition to scans that may occur prior to the removable media being inserted into the endpoint.
- 6.5.18 Endpoints that leverage applications or software with macro capabilities shall disable or limit this capability to only allow approved macros.
- 6.5.19 Each endpoint must be uniquely identifiable in an asset inventory, in directories, and when communicating with other endpoints.
- 6.5.20 Cryptographic measures shall be used to verify the authenticity of endpoints that are issuing commands or instructions to other endpoints or relaying safety critical data to safety systems.
- 6.5.21 Endpoints and endpoint security solutions shall have logging capabilities enabled in accordance with monitoring and auditing requirements.
- 6.5.22 Endpoints shall leverage technologies such as full disk encryption to protect data at rest while they are powered down and prior to authentication.
- 6.5.23 Endpoints that store data, such as database servers, shall use encryption to protect data at rest.
- 6.5.24 Virtualized endpoints within the SuC must not share infrastructure with endpoints that are part of external networks, such as IT systems.
- 6.5.25 Non-critical endpoints shall not share a hypervisor or hardware with critical endpoints.
- 6.5.26 Endpoints shall be enrolled into a centralized directory service that enforces security policies and hardening controls.
- 6.5.27 Endpoints shall be grouped in the directory service to ensure that consistent security policies are applied to all endpoints in the same zone.
- 6.5.28 Endpoints that are mobile (e.g., laptops, phones, tablets) shall have remote wipe capabilities.
- 6.5.29 PLCs, RTUs, and other low level endpoints configuration, code, or logic, shall be backed up in a secure location with integrity protection to enable incident response efforts.
- 6.5.30 The TSCC Contractor shall validate the configuration and operational status of endpoint controls through formal security testing during commissioning, system changes, and on a periodic basis. Results shall be documented and made available to the Authority.
- 6.5.31 Endpoint logs that are forwarded to the SIEM must include as the following events: user logins, authentication attempts configuration changes, application execution, new connections, new command executions, new files, files downloaded from external sources, and other security alerts. Logs must be time stamped, protected from tampering, and forwarded to the central logging system.
- 6.5.32 USB ports and other peripheral interfaces must be disabled by default. If access is required, device control software shall restrict permitted devices, and usage must be logged.
- 6.5.33 Engineering workstations, HMIs, and control servers must receive additional hardening specific to their function. This includes disabling internet access (unless explicitly justified), locking down user privileges, and implementing physical port protections.



- 6.5.34 The TSCC Contractor must ensure endpoint security documentation includes the rationale for selected controls, expected behavior, testing procedures, and rollback instructions.

6.6 Vulnerability and Patch Management

- 6.6.1 The TSCC Contractor shall take a risk-based approach to vulnerability and patch management.
- 6.6.2 Vulnerabilities shall be identified, analyzed, and prioritized for remediation.
- 6.6.3 The System Owners shall be responsible for vulnerability management for assets within their scope. Vulnerability management decisions shall be communicated to Cybersecurity Lead to ensure they align with the requirements of this technical specification. The System Owner is responsible for gathering evidence that the vulnerability and patch management requirements have been met throughout the contract.
- 6.6.4 Common vulnerabilities and exposures (CVEs) shall be identified on endpoints (assets, systems, workstations, maintenance laptops, networking devices, supporting infrastructure, and others within the SuC).
- 6.6.5 A combination of agent based, authenticated, unauthenticated, and passive vulnerability scanners shall be used.
- 6.6.6 The TSCC Contractor shall determine where vulnerability scanning may have adverse impacts. Where vulnerability scanning is not feasible due to operational or safety risks, alternative procedures for identifying vulnerabilities shall be established.
- 6.6.7 The TSCC Contractor shall ensure that any portable or mobile devices used to interact with SuC assets undergo vulnerability assessments and are included in patching and configuration baselines.
- 6.6.8 Mobile devices, such as maintenance tablets, shall be enrolled to a Mobile Device Management (MDM) system to enforce security policies and enable compliance with this technical specification.
- 6.6.9 Vulnerabilities shall be assessed in accordance with the approved risk assessment process to inform patching decisions. The patching decision must indicate whether to patch now (emergency or out-of-cycle), next (in the next patching cycle), or never (where patching risks outweigh the benefits). Installation of patches shall follow change management procedures to ensure that any risks associated with the installation of a patch are identified and mitigated.
- 6.6.10 Regular patching of Windows and Linux endpoints shall occur in alignment with patch release schedules; where patches may cause compatibility issues or asset failure, remediation actions must be taken to enable the installation of the patch.
- 6.6.11 Regular patching of other endpoints shall occur periodically based on the criticality of the endpoint and the complexity of patching. Patching procedures for individual endpoints shall be documented along with associated risks and complexities of patching, such as the requirement to re-flash read only memory or insert replacement media containing entire new versions.
- 6.6.12 Emergency and out-of-cycle patching procedures shall be defined for the duration of the contract, including deployment and maintenance, to ensure vulnerabilities are patched in a timely manner.
- 6.6.13 Endpoints shall be patched to the latest supported version at the time of handover to the Operator or Authority, all vulnerabilities that have an available patch must be patched, unpatched vulnerabilities must be detailed in handover documentation.
- 6.6.14 The TSCC Contractor shall define testing and rollback plans for all patches; the testing of patches shall include verification that a vulnerability has been patched.



- 6.6.15 Vulnerability assessments shall occur periodically throughout the course of the contract.
- 6.6.16 Vulnerability assessments shall follow a documented and approved procedure for identifying potential weaknesses in the system beyond those that are automatically detectable; vulnerabilities include weaknesses in how people, processes, and technology contribute to the operation of the rail system, such as single points of failure, access control weaknesses, or critical processes that are prone to human error or fraud.
- 6.6.17 Vulnerability assessment findings shall be translated into risk assessment findings, with associated risk ratings and mitigation plans; these risk assessments shall be facilitated by the Cybersecurity Lead and attended by System Owners and their delegates.
- 6.6.18 The TSCC Contractor shall procure independent penetration testing services at major milestones of the project.
- 6.6.19 Penetration testing services shall target prioritized endpoints according to their criticality and location on the network (e.g. devices on the boundary of other networks shall be prioritized regardless of their individual criticality).
- 6.6.20 Penetration testing activities shall be formally scoped, including safety and security precautions, objectives, scope, toolsets, tester qualification requirements, risks, finding evaluation criteria, communication plans, and other details that the TSCC Contractor deem to be necessary to ensure that penetration testing activities achieve the desired outcomes while not having adverse impacts on the deployment timelines or endpoint integrity.
- 6.6.21 Penetration testing shall be scoped by the Cybersecurity Lead; System Owners shall respond to queries raised by the Cybersecurity Lead during the scoping of penetration testing.
- 6.6.22 Penetration testing documentation, including scope documents and finding documents, shall be approved by relevant stakeholders.
- 6.6.23 Detailed findings of vulnerability assessments and penetration testing activities shall be protected and distributed on a need-to-know basis.
- 6.6.24 Vulnerability assessment and penetration testing finding mitigations shall be re-tested to provide assurance that the findings have been remediated.

6.7 Identity and Access Management

- 6.7.1 The TSCC Contractor shall define unique identifiers for all software, processes, entities, and endpoints; these identifiers shall follow a consistent naming scheme. An identifier is a unique name or label.
- 6.7.2 Identifiers shall be used consistently between directory services, asset inventories, and ticketing systems.
- 6.7.3 The TSCC Contractor shall implement authentication mechanisms to verify the identity of users, processes, and systems accessing the SuC. These mechanisms must align with the authentication requirements defined in this specification. Where standard methods cannot be used, compensating controls must be implemented to support identity verification and non-repudiation objectives. The authentication mechanisms shall be defined centrally by the Cybersecurity Services Lead and other relevant System Owners. Individual System Owners shall work with the Cybersecurity Services Lead to ensure their systems, subsystems, and assets are on-boarded to the authentication mechanism, including the creation and mapping of role-based access roles to directory service roles.



- 6.7.4 All authentication protocols shall leverage encryption that complies with the encryption requirements of this technical specification.
- 6.7.5 Authentication protocols that are known to be vulnerable must not be used.
- 6.7.6 Authentication shall involve multiple factors of authentication for all human users, including at least two of the following:
- Something a user knows (password or PIN)
 - Something a user has (Smart cards or hardware-based authentication device)
 - Something a user is (such as biometrics or physical identity verification)
- 6.7.7 The TSCC Contractor shall use centralized directory services to create unique identities for all users.
- 6.7.8 The TSCC Contractor shall be responsible for the management, governance, and configuration of directory services, identities, permissions, groups, roles, and policies to ensure they align with cybersecurity objectives.
- 6.7.9 Where passwords are used, the directory services shall be configured to enforce strong, unique passwords with defined complexity and length requirements for all users.
- 6.7.10 The system shall be able to enforce password rules when changing passwords. Password changes shall not be performed through insecure methods such as copying password hashes, modifying registry values, or editing configuration files directly. Secure self-service password changes or identity-governed password vault integrations shall be used.
- 6.7.11 Default credentials, including usernames and passwords, must be changed prior to configuration of endpoints.
- 6.7.12 Default credentials shall be securely documented and securely provided to the Authority or Operator at the time of handover.
- 6.7.13 Role-based access control shall be enforced; permissions shall be assigned to roles that are created in the directory service instead of permissions being assigned directly to individual accounts.
- 6.7.14 Where local accounts are used for access control due to technical or operational limitations, the System Owner is responsible for demonstrating that the role-based access permissions are compliant with this technical specification, role-based access control shall be synchronized with the directory services.
- 6.7.15 Permission assignments shall follow the least privilege principle; each role shall only have the permissions required to perform their duties, where an individual has multiple job functions, they shall be assigned multiple roles.
- 6.7.15.1 Where all users that have a certain role do not require the same permissions as a specific user with that role, additional roles shall be created and assigned to that user, rather than modifying the base role.
- 6.7.15.2 The TSCC Contractor shall assign roles to individual users or assign roles to groups and add appropriate users to those groups.
- 6.7.16 Roles shall follow a naming scheme consistent with the roles and responsibilities outlined in the Contract.
- 6.7.17 In instances where the TSCC Contractor demonstrates that directory services are unable to be used, local accounts must enforce password complexity and rotation rules, and additional controls must be implemented to verify the identity of users accessing the system.



- 6.7.18 Hardware-based authentication keys (such as Yubikeys) may be used to add an additional layer of security to laptops and workstations. These keys must be tightly controlled and have defined processes and procedures for key management, certificate management, installation guidance, and governance of personnel.
- 6.7.19 A 60 second delay between authentication attempts shall be enforced after three consecutive failed login attempts by a user.
- 6.7.20 The TSCC Contractor must have detailed provisioning and deprovisioning procedures with supporting processes and procedures.
- 6.7.21 Access provisioning shall follow an automated workflow or leverage a ticketing system to obtain formal approval.
- 6.7.22 Access provisioning decisions shall be documented and available for audit purposes and user access reviews.
- 6.7.23 The TSCC Contractor shall disable individual accounts and deprovision access once access is no longer required.
- 6.7.24 Local Administrator or Root accounts on endpoints shall be carefully controlled, disabled where practical, and managed; access to these accounts shall be limited to break-glass, safety incident or disaster recovery scenarios to avoid misuse.
- 6.7.24.1 Where administrative accounts in directory services or locally are created for the purpose of incident response or disaster recovery, the credentials for these accounts shall not be known by any individual and instead be stored in a physical safe or vault at an appropriate location that is readily accessible by authorized personnel using M-of-N or Dual control for the purpose of incident response. The credential shall be **rotated immediately after use**.
- 6.7.25 Privileged access must be logged and monitored for signs of misuse or compromise. Logs must be forwarded to a central security monitoring system (e.g., SIEM) and integrated into the CSOC for real-time analysis.
- 6.7.26 Privileged access shall be granted using just-in-time (JIT) principles where feasible and automatically revoked after task completion.
- 6.7.27 The System Owner is responsible for ensuring that privileged access requests are mapped to work orders in a ticketing system or equivalent.
- 6.7.28 Privileged accounts shall not have the ability to delete or modify logs.
- 6.7.29 All changes to identity and access configurations (e.g., new accounts, permissions changes, role assignments) shall be logged and auditable.
- 6.7.30 User access reviews must be conducted periodically throughout the contract to ensure that users have the correct level of access and dormant accounts are disabled.
- 6.7.31 User access reviews must include sampled checks of provisioning and de-provisioning documentation to ensure that processes are being followed.
- 6.7.32 User access review outcomes shall inform the Assurance Case.
- 6.7.33 Shared accounts are prohibited unless explicitly justified and approved by the Cybersecurity Lead and Authority. Where used, compensating controls such as session monitoring, user attribution, and access logging must be implemented.



- 6.7.34 All service accounts, API accounts, and other non-human identities shall be traceable to an accountable role or owner, documented in the asset inventory, and subject to the same provisioning, review, and least privilege requirements as human users.
- 6.7.35 Access provisioned for third parties, including vendors and contractors, shall be governed by time-bound and scope-bound access policies, and monitored continuously.

6.8 Cryptography and Key Management

- 6.8.1 Cryptographic controls must be implemented and shall support the security objectives of confidentiality, integrity, authenticity, and non-repudiation. These controls must align with the overall cybersecurity objectives for the SuC:
 - 6.8.1.1 **Confidentiality:** Encrypting data in-transit and at-rest using strong encryption algorithms to reduce the likelihood of unauthorized access.
 - 6.8.1.2 **Integrity:** Combining encryption and hashing cryptographic hash functions (e.g., SHA-256 or better) to detect tampering with messages, files, or configuration data.
 - 6.8.1.3 **Non-Repudiation:** Digital signatures and cryptographic authentication mechanisms to ensure that actions and transactions can be traced back to their origin and cannot be denied by the actor.
 - 6.8.1.4 **Authenticity:** Using certificate-based or key-based authentication mechanisms to verify the identity of users, devices, systems, or services performing actions or communications within the SuC.
- 6.8.2 The TSCC Contractor shall define and document processes and procedures for generation, distribution, storage, rotation, archival, revocation, and destruction of cryptographic keys, certificates, and secrets. These shall be reviewed and approved by the Authority.
- 6.8.3 The Cybersecurity Services Lead shall be the central point of contact to enable on-boarding to the centralized cryptographic services. System Owners shall reach out to the Cybersecurity Service Lead when certificates, secrets, keys, or other cryptographic material or services are required.
- 6.8.4 The TSCC Contractor shall store encryption keys and other secrets in validated Hardware Security Modules (HSMs) or Trusted Platform Modules (TPMs); where use of HSMs or TPMs is not feasible, a secure software-based vault that supports encryption, access control, and audit logging shall be used with Cybersecurity Lead and Authority approval.
- 6.8.5 All access to encryption keys and other secrets must be protected from unauthorized access using a combination of role-based access control, multi-factor authentication and approval workflows.
- 6.8.6 All access, generation, use, rotation, destruction, or other actions relating to encryption keys or other secrets must be fully logged to detect misuse, fraud, or compromise.
- 6.8.7 **The TSCC Contractor shall log all cryptographic events, including key generation, key access, key usage, certificate issuance and revocation, and cryptographic failure events. The logs must be protected from modification and retained in accordance with the logging and monitoring requirements.**
- 6.8.8 **The TSCC Contractor shall define key ownership and custodianship for all keys.**
- 6.8.9 All encryption keys and secrets shall be considered sensitive information; controls that protect the confidentiality of keys and secrets must be implemented in transit and at-rest.
- 6.8.10 **The TSCC Contractor shall maintain an inventory containing a list of all cryptographic keys, secrets, certificates, and their attributes with appropriate access control.**



- 6.8.11 Key and secrets rotation timeframes must be defined; the following factors shall be considered when determining rotation timeframes:
- Authority, regulatory, and industry standards
 - Risk of compromise
 - Complexity of key or secret (key-length, password length, password complexity rules)
 - Complexity of changing key or secret (Requires maintenance window vs regular BAU activity).
- 6.8.12 Only modern cryptographic algorithms and protocols shall be used; the following algorithms shall be used unless more secure protocols have been released and recommended by industry standards prior to the beginning of the contract:
- 6.8.12.1 TLS shall be used to protect data in transit
- 6.8.12.2 Where TLS is used, TLS 1.3 (or newer, if approved) must be used. All TLS 1.2 and earlier versions must be disabled unless justified and approved.
- 6.8.12.3 Known-vulnerable cipher suites must be disabled across all TLS implementations.
- 6.8.12.4 Procurement processes shall ensure that only cryptographic products supporting the approved protocols and algorithms are selected.
- 6.8.12.5 AES256 (Advanced Encryption Standard 256-bit) shall be used for all data in transit and data at rest encryption.
- 6.8.12.6 SHA256 or SHA512 shall be used for all hashing, including file hash checking and message integrity verification
- 6.8.12.7 Hash-based Message Authentication Code (HMAC) shall be used for message authentication and integrity verification.
- 6.8.12.8 ECDH, Diffie-Hellman (2048 bits or higher), RSA (2048 bits or higher) shall be used for asymmetric key exchange.
- 6.8.12.9 ECDSA (256 bits or higher), RSA (2048 bits or higher) shall be used for certificates and digital signatures.
- 6.8.12.10 IPsec may be used for VPNs or secure tunnels to achieve conduit requirements following the above guidance for selected algorithms.
- 6.8.12.11 GCM (Galois/Counter Mode) shall be used for symmetric encryption. Other cipher modes (e.g., ECB, CBC without padding) are not permitted.
- 6.8.12.12 A risk assessment should be conducted to determine if quantum computing based attacks need to be considered when selecting key exchange algorithms.
- 6.8.12.13 A risk assessment should be conducted to determine if quantum computer-based attacks need to be considered when determining certificate expiry requirements, up-to-date guidance should be considered for selecting key sizes.
- 6.8.12.14 Where proprietary cryptographic algorithms or protocols must be used (e.g., embedded in OEM devices), the TSCC Contractor must demonstrate compliance with Kerckhoffs' Principle and provide third-party verification or security validation evidence where available.
- 6.8.12.15 **The TSCC Contractor shall define incident response procedures to respond to compromise of secrets.**
- 6.8.13 **Public Key Infrastructure**



- 6.8.13.1 The TSCC Contractor must implement PKI (Public Key Infrastructure) to enable TLS and certificate-based authentication in compliance with ETCS Subset-137 and applicable national cybersecurity regulations.
- 6.8.13.2 The TSCC Contractor must harden the PKI in alignment with the requirements established in ETCS Subset-137 and follow cryptographic best practices including secure key lifecycle management and strict access controls.
- 6.8.13.3 Root Certificate Authorities (CAs) must be air-gapped and located in controlled physically secure, access-controlled environments with security logs and surveillance.
- 6.8.13.4 Root CAs must be designed to enforce M of N or Dual Control for certificate signing operations, ensuring no single individual can issue certificates.
- 6.8.13.5 Backups of Root CA keys and certificates shall be securely stored in a separate, physically secure location and protected to the same standard as the Root CA, for use solely in disaster recovery scenarios.
- 6.8.13.6 Intermediary CAs shall be deployed to support online certificate issuance and revocation. Their use shall align with SIL requirements and be segregated according to safety criticality.
- 6.8.13.7 The TSCC Contractor must implement a segregated PKI hierarchy at either the Root or Intermediary CA level to isolate safety critical certificate authorities from non-critical certificate authorities. This segregation shall be justified by a documented risk assessment.
- 6.8.13.8 Designated Registration Authorities (RAs) shall verify the identity of users, devices, and services requesting certificates before issuance.
- 6.8.13.9 All certificates must comply with the X.509 v3 standard and include relevant subject fields, key usage constraints, and validity periods as per system requirements.
- 6.8.13.10 Mutual TLS (mTLS) or equivalent mutual authentication mechanisms shall be used for critical/SIL network communications.
- 6.8.13.11 Payload data within TLS sessions must be encrypted where the content includes authentication material, cryptographic secrets, or other sensitive operational data.
- 6.8.13.12 Each TLS session must generate a new ephemeral session key using forward secrecy-capable key exchange mechanisms.
- 6.8.13.13 Session resumption (e.g. via session ID reuse or session tickets) must be disabled to prevent key reuse vulnerabilities.
- 6.8.13.14 TLS sessions shall be explicitly terminated when TCP connections are disconnected. Reuse of session keys across sessions is not permitted.
- 6.8.13.15 The TSCC Contractor must develop a risk-assessed and approved procedure for deploying the Root CA certificate to all required endpoints. This must include testing, rollback, and validation steps.
- 6.8.13.16 Certificate Revocation Lists (CRLs) shall be published and updated frequently, and distributed via secure, authenticated channels.
- 6.8.13.17 Online Certificate Status Protocol (OCSP) may be used to provide real-time revocation status.
- 6.8.13.18 Where OCSP is used, a fallback to CRLs shall be configured to ensure revocation checks are enforced if OCSP fails.
- 6.8.13.19 All TLS implementations must enforce revocation status checking using OCSP or CRLs before allowing a connection to proceed.



- 6.8.13.20 The PKI implementation must support emergency certificate revocation processes, including automated distribution of updated CRLs or OCSP responses.
- 6.8.13.21 TLS communication failure states must be defined and handled in a way that maintains both system safety and system security (e.g. safe failover with no data leakage).
- 6.8.13.22 TLS communication errors, including expired or invalid certificates, must generate alerts and be reported to the Cyber Security Operations Centre (CSOC) or relevant Operational Control Centre (OCC).
- 6.8.13.23 TLS certificate expiration periods must be informed by risk assessment and industry guidance, including considerations for quantum threats and operational impact, the initial expiry date for certificates shall be set to 825 days and later changed based on risk assessment outcomes.
- 6.8.13.24 The TSCC Contractor shall provide the Operator and/or Maintainer with formal PKI handover documentation, including step-by-step procedures for certificate issuance, revocation, renewal, and secure storage practices.

6.9 Cybersecurity Operations Centre (CSOC)

6.9.1 General Requirements

- 6.9.1.1 The TSCC Contractor shall establish a Cyber Security Operations Centre (CSOC) to perform proactive monitoring, detection, analysis, and response to cybersecurity incidents and events throughout the lifecycle of the contract.
- 6.9.1.2 The Cybersecurity Services Lead shall be the System Owner of the SIEM and CSOC devices, components of the CSOC shall be compliant with this technical specification.
- 6.9.1.3 The CSOC shall be physically located at or co-located within the OCC to enable close interfacing with operational and safety-critical staff.
- 6.9.1.4 The CSOC shall implement a Security Information and Event Management (SIEM) platform to ingest, aggregate, analyze, and correlate log data in near-real-time to detect cybersecurity events.
- 6.9.1.5 The SIEM solution must be scalable to support the phased expansion of the project, enabling the onboarding of additional systems and upgrades without service disruption.
- 6.9.1.6 The following sources shall generate logs in a standardized and normalized format compatible with the SIEM to ensure effective event correlation:
 - Critical Systems
 - Network Devices
 - Applications
 - Services
 - Security Tools
 - Endpoints
 - PLCs, RTUs, and other Control System components.
- 6.9.1.7 All log sources shall be time stamped using a centralized, authenticated time source, such as a secure NTP server, to ensure synchronization across all systems and consistency in event analysis.
- 6.9.1.8 The SIEM shall ingest logs from all environments, including secondary and non-production environments such as testing, staging, pre-production, and integration labs.



- 6.9.1.9 Secondary environments shall also use unidirectional communication following the deny-by-default principle to ensure that infections of any environment don't cross infect other environments.
- 6.9.1.10 Log collection shall use a combination of agent-based and agentless methods, selected based on performance, compatibility, and endpoint constraints, and must be documented with justifications.
- 6.9.1.11 The SIEM shall include pre-built and customizable dashboards that provide operational, security, and incident-related views tailored to the CSOC's responsibilities.
- 6.9.1.12 The TSCC Contractor shall document and provide step-by-step procedures for dashboard configuration and customization to the Authority or Operator.
- 6.9.1.13 The SIEM shall provide CSOC staff with the ability to query ingested log information using timestamps, filters, keywords, or identifiers.
- 6.9.1.14 The SIEM shall provide CSOC staff with the ability to manually correlate events across multiple systems.
- 6.9.1.15 The CSOC room shall have adequate equipment and connectivity to facilitate multiple levels of eyes-on-glass monitoring and other cybersecurity activities in alignment with the roles and responsibilities defined by the TSCC Contractor.
- 6.9.1.16 The CSOC shall be configured to receive automated alerts for high-risk or anomalous cybersecurity events, based on correlation rules, baselining, or anomaly detection.
- 6.9.1.17 Cybersecurity event detection rules shall be defined based on common use-cases (attack patterns and indicators of compromise (IoC's)) and threat intelligence sources (Tactics, Techniques and Procedures - TTPs).
- 6.9.1.18 The SIEM or threat intelligence solution shall provide CSOC staff with the ability to read more information about each IoC or TTP.
- 6.9.1.19 The SIEM shall automatically tag IoCs or information associated with TTPs.
- 6.9.1.20 The TSCC Contractor shall develop processes for reducing the number of false positives throughout the contract period.
- 6.9.1.21 Detection use-cases must use a combination of known indicators and behavior-based event detection mechanisms.
- 6.9.1.22 A combination of human-readable threat intelligence and machine-readable intelligence shall be used to define detection use-cases.
- 6.9.1.23 Cybersecurity events shall automatically be assigned severity levels which shall determine the priority and level of analysis required.
- 6.9.1.24 The SIEM shall be capable of automatically building a timeline of events that lead to the creation of the alert. The SIEM shall enable CSOC staff to drill down into the details of each individual alert of the timeline to gather context and perform analysis.
- 6.9.1.25 The SIEM should leverage MITRE ATT&CK for ICS or similar cybersecurity attack kill chains to map the timeline of events.
- 6.9.1.26 The SIEM shall integrate with the Cybersecurity Ticketing System to support full event-to-incident tracking and documentation, including:
 - Automatically create tickets or provide adequate information for rapid creating of tickets
 - Record steps taken by CSOC staff



- Record escalation paths followed during event or incident
 - Track event status
 - Include timestamps for decision making, such as transitioning from an event to an incident
 - Include details regarding the owner of the incident
 - Automatically produce a timeline of actions taken throughout the incident, additional events or alerts relating to the incident, and references to sources of information such as indicators of compromise, logs, and other information that can be used during lessons learned
 - Detail plans that were activated and teams that were contacted throughout the incident response process
 - Closure details and links to lessons learned
- 6.9.1.27 The SIEM solution shall enforce integrity protections for all log data, including the use of cryptographic hashes, immutable storage, and access controls, to maintain evidentiary value for incident investigations.
- 6.9.1.28 The TSCC Contractor shall provide adequate storage and infrastructure to enable archival and in-use storage of logs.
- 6.9.1.29 The TSCC Contractor shall store three months of logs in the in-use storage (storage where the SIEM is currently accessing data) to enable detection of security incidents that have occurred in the past three months.
- 6.9.1.30 Log files must be retained for a minimum of seven years, or as specified by an appropriate risk assessment or current regulatory requirements.
- 6.9.1.31 The SIEM shall be capable of generating daily, weekly, monthly, and annual reports that detail information relevant to senior stakeholders on the contract, these reports shall not contain detailed sensitive information and shall be shared as part of the assurance activities.
- 6.9.1.32 The SIEM shall provide CSOC staff with the ability to export information from the SIEM in multiple common formats, including CSV and PDF, for audit purposes.
- 6.9.1.33 The CSOC workstations and SIEM shall enforce Role-Based Access Control (RBAC), MFA, session timeouts, and central auditing for all access.
- 6.9.1.34 All access to the SIEM, including queries and configuration changes, must generate audit logs and be retained for forensic analysis.
- 6.9.1.35 A backup CSOC workstation, the BCSOC, shall be available.
- 6.9.1.36 The BCSOC shall be configured to enable rapid failover, using methods such as an active-active setup.
- 6.9.1.37 CSOC staff shall mobilize the BCSOC in the event of the primary CSOC failing, processes and procedures shall be defined by the TSCC Contractor for CSOC continuity.
- 6.9.1.38 The SIEM and CSOC shall use a dedicated network which receives unidirectional log traffic.
- 6.9.1.39 The boundary between the SuC networks and the CSOC network shall only allow traffic to traverse to the CSOC network, this connectivity should be facilitated by a unidirectional data diode.
- 6.9.1.40 Internet access from the CSOC network must be strictly controlled and filtered using a deny-by-default firewall configuration; only threat intelligence feeds, time synchronization, and approved update mechanisms may be permitted.
- 6.9.1.41 The SIEM and CSOC network shall be protected by dedicated network security products, including a boundary firewall to manage internet traffic.



- 6.9.1.42 The CSOC networks shall follow logging and monitoring controls established in this technical specification to detect anomalies and thwart attacks on monitoring infrastructure.
- 6.9.1.43 The SuC shall not have any functional or performance dependency on the CSOC network. Where unidirectional connectivity is not feasible, the interface must default to a fail-secure state upon failure and shall not propagate faults or vulnerabilities bi-directionally.
- 6.9.1.44 The networking infrastructure of the SuC and the CSOC network must both be designed to support the estimated amount of log traffic and scalable as the number of railway assets increases over time.
- 6.9.1.45 Estimated log traffic values shall be documented in the design documentation and should assume worst case scenarios.
- 6.9.1.46 CSOC staffing recommendations after handover shall be provided to the Authority or Operator, the staffing recommendations shall align with the design and layout of the CSOC.
- 6.9.1.47 The CSOC shall be staffed once core connectivity has been established and until handover to ensure cybersecurity events are detected and to continuously improve detection use-cases and remove false positives prior to handover.
- 6.9.1.48 The TSCC Contractor shall define and implement CSOC onboarding procedures to ensure staff are appropriately trained, cleared (if applicable), and familiar with systems, tools, and incident response procedures before assuming operational duties.
- 6.9.1.49 Incident response plans and playbooks shall include details regarding the roles and responsibilities of the CSOC staff.
- 6.9.1.50 The TSCC Contractor must define a process for quickly mapping asset identifiers associated with events to zones and conduits on a zone and conduit diagram to allow contextualization of security incidents.
- 6.9.1.51 The CSOC shall support simulation exercises, including red team/blue team testing or tabletop exercises, to validate incident response readiness and detection capability.

6.9.2 Cybersecurity Ticketing System

- 6.9.2.1 The TSCC Contractor shall deploy or expand an existing service used elsewhere in the contract, a dedicated platform to facilitate cybersecurity ticketing, which shall be integrated with the CSOC and SIEM.
- 6.9.2.2 The Cybersecurity Services Lead shall use the ticketing system to track all integration and onboarding activities and shall be the System Owner of the ticketing system if an independent cybersecurity ticketing system is procured, or if an existing ticketing system is used, the Cybersecurity Services Lead shall be the accountable entity approving cybersecurity integration and onboarding tickets or work-orders.
- 6.9.2.3 **Role-based access control shall be enforced on the ticketing system. All actions (create, update, close) shall be logged with user identity and timestamp for audit and forensic purposes.**
- 6.9.2.4 The TSCC Contractor shall provide a mechanism to report, track, and document cybersecurity incidents, concerns, findings, resolutions, vulnerabilities, deviations from policy, and other security-relevant issues.
- 6.9.2.5 The TSCC Contractor shall document and implement processes and procedures for managing cybersecurity tickets end-to-end, including logging, categorization, triage, analysis, resolution, closure, and post-incident review.



- 6.9.2.6 Cybersecurity ticket timestamps shall be synchronized with the centralized time source used across the SuC to support event correlation and forensic investigations.
- 6.9.2.7 Tickets shall be archived once they are closed, retained according to the applicable retention policy, and provided to the Operator or Authority at the time of handover.
- 6.9.2.8 **All open cybersecurity tickets shall be reviewed, resolved, or formally transferred prior to handover. Any unresolved tickets shall be documented with associated risk ratings, mitigation plans, and ownership transfer.**
- 6.9.2.9 Ticket system processes, escalation paths, configuration settings, workflows, and user access management procedures shall be documented and provided to the Operator or Authority at the time of handover.
- 6.9.2.10 Sensitive information, such as encryption keys, certificates, passwords, and other secrets, shall not be stored in tickets. A process shall be defined for redacting information deemed sensitive and instead referencing the secure location where the original data is stored.
- 6.9.2.11 Cybersecurity tickets shall be readily available to authorized parties upon request, with appropriate role-based access control and audit logging.
- 6.9.2.12 **Cybersecurity tickets that identify systemic issues, recurring vulnerabilities, or risks shall be referenced in the cybersecurity risk register and associated mitigation strategies.**
- 6.9.2.13 Cybersecurity ticket metadata, such as ticket volume, resolution time, recurring issues, and trends, shall be used to inform the Cybersecurity Assurance Case.

6.9.3 Logging and Monitoring

- 6.9.3.1 The TSCC Contractor shall design the SuC to enable logs to be collected, protected, and forwarded to a central location for analysis.
- 6.9.3.2 System Owners shall work with the Cybersecurity Services Lead to configure and on-board their devices to the logging solution, this includes the configuration of endpoints and network devices to collect necessary security logs and configuring communication paths, agents, and edge devices.
- 6.9.3.3 The TSCC Contractor must log all security relevant events; the following inconclusive list shall serve as a baseline:
- Authentication: Successful and failed login events, session opening/closing events, manual/automatic session closure
 - Configuration Changes: Network configuration, software configuration, OS configuration, registry/policy changes
 - Security Changes: Firewall rules changes, IDS/IPS changes, ACL changes, changes to conduits
 - Remote Access: New connections, session initiation/closure, actions taken, attempted connections (with assets from remote access solution), changes made, user details, connection source, connection duration.
 - Privileged Access: Privilege escalation attempts, privileged use, execution of privileged commands, account creation, deletion, or modification, permission changes
 - Critical Assets: All activities, changes, interactions, communications.
 - Systems: OS logs, application logs, failures, alerts, errors, process logs



- Logging Information: Creation, changes, access, reading, writing, disabling, modification, failures, time errors, log rotation errors, memory errors associated with logs
- Security Logs: Anti-malware, Intrusion (IDS/IPS), firewall, prevented executions, prevented connections, detected events

- 6.9.3.4 Additional logs as outlined in individual sections shall be collected and forwarded to the central location.
- 6.9.3.5 All logs must include relevant information, including timestamp, source, user ID, event type, event details, and asset identifier.
- 6.9.3.6 The TSCC Contractor must ensure no human users have permission to write, modify, or delete log files.
- 6.9.3.7 Log files and directories containing log files shall be monitored for unauthorized access or modifications. Intentional modification of log files must be recorded, and the TSCC Contractor shall work with the Authority to determine appropriate action.
- 6.9.3.8 The network, endpoints, components, systems, assets, and other parts of the SuC must be designed to facilitate the logging requirements, including the collection, storage, real-time communication, archival, analysis, time synchronization, integrity protection, authenticity, and confidentiality of information stored in sensitive logs.
- 6.9.3.9 Logs must be collected in a format that is compatible with the centralized log analysis solution (SIEM).
- 6.9.3.10 Logs shall be protected in transit using cryptographic mechanisms including encryption and hashing to protect the confidentiality and integrity of log information.
- 6.9.3.11 Log rotation periods shall be defined in accordance with individual endpoint capabilities.
- 6.9.3.12 Inherent log forwarding capabilities, agent-based log forwarders, or dedicated edge computing devices shall be used to automatically forward logs to the SIEM.
- 6.9.3.13 Logs must be forwarded frequently to enable detection of incidents within 15 minutes of the event occurring and within 5 minutes for safety or operationally critical networks.
- 6.9.3.14 Log retention periods must be defined by the TSCC Contractor and approved by the Authority in accordance with up-to-date regulatory requirements and the Authorities data retention standards.
- 6.9.3.15 Logs that are stored during their retention period must be protected from unauthorized access, deletion, or modification.
- 6.9.3.16 Logs that are stored during their retention period must be accessible if required for the purpose of an investigation.
- 6.9.3.17 The TSCC Contractor may choose to have multiple tiers of storage, such as hot storage for live SIEM data, cold storage for indexed searchable data, and immutable backup storage for long term archival purposes with slower potential search times.
- 6.9.3.18 Log storage solutions should leverage additional security mechanisms to prevent unauthorized modification, including write-once-read-many (WORM) storage, automatic hash verification to detect modifications, and digital signatures.
- 6.9.3.19 Logs must regularly be audited to detect signs of fraud, abuse, or compromise.
- 6.9.3.20 The TSCC Contractor shall develop a process for performing audits of logs which are approved by the Authority.



- 6.9.3.21 The TSCC Contractor shall document any findings of audits and document them as part of the Assurance Case.

6.9.4 Incident Response

- 6.9.4.1 The TSCC Contractor shall develop documented cybersecurity incident response plans, playbooks, and procedures that shall be used throughout the lifecycle of the contract. These documents must include interfaces with CSOC operations, the cybersecurity ticketing system, and asset management systems.
- 6.9.4.2 **The TSCC Contractor shall review and update the incident response plan at least annually or upon significant changes to the SuC, threat environment, regulations, or after a major incident.**
- 6.9.4.3 The TSCC Contractor shall define roles and responsibilities as part of the cybersecurity incident response plan to enable incident detection, classification, reporting, containment, investigation, evidence collection, and recovery.
- 6.9.4.4 The incident response plan shall detail how incidents are classified by severity, prioritized, escalated, and interfaced with other internal and external teams, including operational, engineering, legal, communications, and regulatory stakeholders.
- 6.9.4.5 **The incident response plan shall include predefined communication procedures, including contact details, internal and external communications channels, escalation contacts, and templated notifications for different incident types.**
- 6.9.4.6 **The TSCC Contractor shall coordinate with third parties, including suppliers, system integrators, and OEMs, during incident response, particularly where vendor support is required to contain or investigate an incident. Contact rosters must be maintained**
- 6.9.4.7 The TSCC Contractor shall consider the operation and integration of the CSOC, cybersecurity ticketing system, and SIEM for incident detection, triage, escalation, response, and lessons learned once implementation and integration phases have started.
- 6.9.4.8 **The TSCC Contractor shall perform post-incident reviews and root cause analysis for all major cybersecurity incidents. The analysis shall include contributing factors, control effectiveness, and specific corrective actions. The findings shall be shared with the Authority.**
- 6.9.4.9 **The incident response plan shall include containment and recovery procedures to isolate affected systems, re-establish safe operations, and document restoration actions. Recovery steps must be tested during drills.**
- 6.9.4.10 The TSCC Contractor shall be responsible for regularly testing their incident response processes, procedures, and documentation to ensure it allows an effective incident response effort. Tests shall include tabletop and technical simulation exercises. All lessons learned from real incidents or tests shall be documented and handed over to the Authority to inform the post-contract incident response activities.
- 6.9.4.11 All incidents must be reported to the Authority. Where regulation or legislation mandates incident reporting to a government or regulatory body, the TSCC Contractor must formally agree with the Authority which entity is responsible for undertaking this obligation and maintain traceable records of each report.
- 6.9.4.12 **The TSCC Contractor shall define performance metrics and KPIs for the incident response capability, including mean time to detect (MTTD), mean time to respond (MTTR), and incident closure rates. These metrics shall be reported to the Authority quarterly.**



- 6.9.4.13 **The TSCC Contractor shall include procedures for evidence preservation, forensic collection, and chain-of-custody tracking to support investigation, attribution, and possible legal or regulatory follow-up.**
- 6.9.4.14 **The Cybersecurity Lead shall be responsible for facilitating incident response plan exercises, either as an independent exercise or as part of broader incident response testing activities.**
- 6.9.4.15 **The Cybersecurity Lead shall be responsible for ensuring that lessons learned and improvement plans are developed and are documented in the Assurance Case.**

6.10 Backup and Restoration

- 6.10.1 The TSCC Contractor must develop a backup and restoration strategy that aligns with business continuity plans, disaster recovery plans, incident response plans, and service level agreements, as established in the contract. The strategy shall define ownership, scope, testing frequency, documentation structure, and responsible roles.
- 6.10.2 The Cybersecurity Services Lead shall be the System Owner for backup and restoration technologies and assist System Owners to onboard their systems, subsystems, and assets to the centralized service.
- 6.10.3 The Cybersecurity Services Lead and System Owners shall work with the Cybersecurity Lead to determine backup strategies for individual systems, subsystems, and assets.
- 6.10.4 The SuC shall be capable to recover to the most recent backup which has a known secure state, and the restoration process shall verify the integrity and security posture of the restored system to prevent reinfection or configuration drift, where:
- Security values and configurations are correct and reflect the intended security baseline.
 - Critical security patches are installed and validated post-restoration.
 - Applications and system software are installed and configured with secure settings that match the SuC design and cybersecurity requirements.
- 6.10.5 The backup and restoration strategy must cover the entire scope of the SuC, including systems managed by third-party vendors or external contractors.
- 6.10.6 The backup and restoration strategy must be approved by relevant stakeholders, including senior stakeholders or delegated resources from the Authority.
- 6.10.7 Dedicated backup infrastructure capable of supporting the requirements outlined in the backup and restoration strategy must be procured, hardened and deployed.
- 6.10.8 The following data must be backed up at a minimum:
- System configurations
 - Operating System Images (Hardened “golden images”)
 - Network Device Configurations
 - PLC, RTU, and other low-level endpoint configurations, logic, programs, and code
 - Security Device Rulesets and Configuration
 - User and Identity Management (Directory Services / AAA) data
 - License files
 - Secrets (keys, certificates)
 - Safety Integrity Logic



- 6.10.9 Backups must be validated and tested upon creation and on a periodic basis as defined in the strategy. Validation must include cryptographic hash comparison, integrity checks, and simulated restoration tests to verify system recoverability.
- 6.10.10 The TSCC Contractor shall maintain an inventory of all backup jobs, including systems backed up, schedule, storage location, and validation status.
- 6.10.11 Backups shall be taken after each change as part of the change management process; if a backup does not exist already, a backup must be created prior to the change to support a rollback plan and disaster recovery testing.
- 6.10.12 Backups must be replicated across multiple physically and logically separate locations. At minimum, one copy shall be maintained as an online backup and one as an offline or immutable backup, such as write once read many backups (WORM).
- 6.10.13 Where third-party platforms or cloud-based tools are used for backup or storage, the TSCC Contractor shall provide a documented risk assessment and controls map demonstrating compliance with this specification.
- 6.10.14 Online backup infrastructure shall be protected from unauthorized access using role-based access control, multi-factor authentication, network segmentation, strong encryption, and anomaly detection.
- 6.10.15 All backups must be encrypted at rest using AES256 encryption or equivalent protocols recommended by recognized national or state cybersecurity authorities at the time of contract execution. Backup encryption keys shall be managed, rotated, and stored securely.
- 6.10.16 The TSCC Contractor must demonstrate, through restoration drills and documented testing, that the SuC can recover from various incidents or disaster scenarios and return to a secure, safe, and functioning state within acceptable downtime thresholds.
- 6.10.17 The TSCC Contractor must demonstrate that both online and offline backups can be used to recover systems. This must include system-level and granular-level restorations.
- 6.10.18 The TSCC Contractor shall ensure that the end-to-end restoration process that shall be handed over to the Authority and Operator can return systems to a safe, secure, and functional state within anticipated service level agreement timeframes. Restoration instructions must be written, role-based, and validated for usability.
- 6.10.19 The TSCC Contractor shall provide the Operator and Authority with documented instructions and access credentials required to continue secure backup and restoration activities after handover.

6.11 Physical Security

- 6.11.1 The TSCC Contractor shall implement physical security measures to ensure that cybersecurity controls and system integrity cannot be bypassed through unauthorized physical access to any device, interface, or media connected to the rail system.
- 6.11.2 System Owners shall be responsible for ensuring that electronic access control to areas is aligned with the role-based access required to interact with their system, subsystem, or asset. Where physical access control cannot be reliably enforced in alignment with role-based access control, the System Owner must highlight this risk to the Cybersecurity Lead and implement a mitigation strategy.
- 6.11.3 Access to critical rail network systems and SuC infrastructure must be restricted to authorized personnel by implementing centralized, auditable physical access control systems with role-based access permissions.



- 6.11.4 Physical access control shall enforce two or more factors of authentication to verify the identity of individuals accessing any room or cabinet containing critical rail network systems, SuC infrastructure, or control system interfaces.
- 6.11.5 Physical access control systems and their associated access control lists shall undergo user access reviews.
- 6.11.6 Physical access shall be logged; access logs shall be timestamped using the same time source as cybersecurity logs across the network and retained in accordance with log retention policies.
- 6.11.7 Physical access logs shall be readily accessible and available for the SIEM to perform log correlation at the time of a cybersecurity incident.
- 6.11.8 Additional measures of verifying the physical location of personnel, such as smart cards or RFID tags shall be available for log correlation.
- 6.11.9 Visitor access shall be strictly governed, requiring registration, pre-approval, escort by authorized personnel, and justification of access purpose.
- 6.11.10 CCTV cameras shall be installed to monitor entrances to all equipment rooms, server rooms, data centers, and any areas containing critical infrastructure components of the rail network and SuC. Cameras shall support retention and secure access to footage.
- 6.11.11 Remote or unmanned facilities shall be physically secured with access restriction mechanisms, tamper detection, intrusion alarms, and integration with CSOC alerting systems.
- 6.11.12 Network cables, patch panels, and other communications infrastructure shall be protected from unauthorized physical access, tampering, or eavesdropping using cable locks, conduits, and secured enclosures.
- 6.11.13 Physical security perimeters for rooms containing critical rail network systems and SuC infrastructure must be defined, documented, and protected using structural and procedural controls such as reinforced doors, access zones, and intrusion-resistant walls.
- 6.11.14 Security perimeters shall have continuously monitored intrusion detection systems to detect unauthorized physical access attempts and generate alerts in real-time to the CSOC.
- 6.11.15 The TSCC Contractor shall design rooms containing critical rail network systems and SuC infrastructure to have appropriate environmental controls, including temperature, humidity, air quality, smoke detection, and other factors to protect the availability of the rail network.
- 6.11.16 The environmental controls shall account for increasing equipment density, variable power loads, redundancy requirements, and projected changes in regional climate conditions.
- 6.11.17 Physical controls shall complement logical controls to prevent unauthorized peripheral connections, including blocking unapproved devices from being plugged into networking equipment, serial interfaces, or USB ports.
- 6.11.18 Critical rail network systems, SuC infrastructure, and cybersecurity devices shall have redundant power sources that are both physically secured and logically segmented from other systems, with protections against unauthorized access and cyberattacks implemented as per the requirements in this specification.
- 6.11.19 The TSCC Contractor shall implement tamper-evident security seals or enclosures on racks, field cabinets, and patch panels in exposed or remote environments that contain critical rail network systems.
- 6.11.20 The TSCC Contractor shall ensure that physical security incident response plan exercises consider cybersecurity incidents to enable converged security incident drills.



6.12 Information Security

- 6.12.1 In the context of this section, information refers specifically to structured or unstructured data that is human-readable, meaning that an individual could derive meaning from reading it. This may include design documentation, asset management system entries, source code, networking information, personnel details, logs, and operational data.
- 6.12.2 The TSCC Contractor shall classify all information stored in the asset management system or enterprise systems that facilitate functionality or decision-making associated with the SuC.
- 6.12.3 Classification of information shall align across all CHSR scopes of work, the TSCC Contractor shall be responsible for ensuring that a common classification framework that is approved by the Authority has been adopted.
- 6.12.4 Logical metadata, machine-readable, and human-readable classification labels, security tags, or equivalent shall be implemented and standardized across IT systems.
- 6.12.5 Metadata and machine-readable labels and security tags shall be used to enforce technical security policies, controls, and monitor network boundaries and prevent data exfiltration.
- 6.12.6 Classification of information shall be based on the criticality of the information to either the business, operations, safety, or other CHSR functions.
- 6.12.7 When determining the criticality of information, documented and approved procedures, such as business impact assessments (BIA) shall be used.
- 6.12.8 Procedures used for information criticality assessments shall be aligned with the approved risk matrix to enable traceability and risk assessment activities.
- 6.12.9 The criticality of assets that store information of a higher criticality rating than the asset itself shall inherit the information's criticality rating.
- 6.12.10 The TSCC Contractor shall define appropriate policies and procedures for managing information, these policies and procedures shall be aligned with the ISO27001 standard.
- 6.12.11 Information handling processes, procedures, and training shall be defined to ensure that both logical and physical copies of information are controlled and protected from unauthorized access caused by human error.
- 6.12.12 Processes, procedures, and training shall include labelling practices, to ensure that human-readable and machine-readable labels or security tags are consistently demarked to enable appropriate handling procedures by personnel that aligns with the individual classification of information.
- 6.12.13 Information shall be protected using the access control and encryption requirements defined in this specification.
- 6.12.14 Access to information shall be implemented using a least privileged and need-to-know approach; an individual shall only have access to the information they require to perform their duties.
- 6.12.15 Collection of Personally Identifiable Information (PII) shall be limited to what is necessary, where there is no business justification for PII to be collected, the TSCC Contractor shall not collect it.
- 6.12.16 PII shall be stored exclusively in systems and locations where it is required, where PII is transferred to another system or location, only the fields required by the new system or location shall be transferred.
- 6.12.17 PII collection and usage shall comply with the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), as applicable.



- 6.12.18 Real information (i.e., information in the production environment) must not be used for functional application testing purposes, testing that requires the usage of real information must seek approval from appropriate stakeholders.
- 6.12.19 Information pertaining to previous incidents or that could be used to cause a future incident must be protected from unauthorized and unmonitored access.
- 6.12.20 Access and changes to information must be logged for all information where the compromise of integrity, confidentiality, or authenticity of the information could lead to negative impacts to people, process, technology, operations, safety, CHSR reputation, or other consequences defined in the approved risk matrix.
- 6.12.21 Access and change logs for information shall be monitored in alignment with the logging and monitoring requirements outlined in this specification. The TSCC Contractor shall perform assessments to determine if a separate ITSOC (Information Technology Security Operations Center) will be established and coordinate with the delivery team to ensure that appropriate logs are forwarded to the ITSOC SIEM.
- 6.12.22 Enterprise networks where information is stored shall be segmented and all network traffic between network segments shall be controlled and protected from unauthorized access or tampering.
- 6.12.23 A Zero-Trust Architecture (ZTA) should be implemented across the enterprise network. The ZTA shall enforce authentication and authorization decisions based on user identity, device posture (group policy compliance and security agents installed), application context (classification of information stored on application), and risk (calculated or perceived risk of access request, based on factors such as time, location, and threat intelligence).
- 6.12.24 Where a ZTA is used, it shall be designed in alignment with the NIST 800-207 publication, which describes the ZT Logical Components and decision points which are responsible for performing the decision making.
- 6.12.25 If a hybrid environment is used (on premise and cloud), the TSCC Contractor shall implement proxy or reverse proxy services, such as a Cloud Access Security Broker (CASB) solution to enforce security policies and manage access to cloud services.
- 6.12.26 Software as a Service (SaaS) and other cloud services shall have restricted access control consistent with the network security controls and identity and access management controls outlined in this specification; this may be enforced by the proxy.
- 6.12.27 The proxy shall be capable of ensuring sessions are authenticated and authorized, logging access details, and identifying instances where unsanctioned cloud applications are being used, such as external email services or file upload services that may be used to exfiltrate data.
- 6.12.28 Integrations between information systems, such as between the asset management system and a configuration database, must be encrypted and authenticated in accordance with this technical specification.
- 6.12.29 Information disposal procedures (as defined by quality management or applicable standards/regulation) must be defined to ensure that information is securely deleted and destroyed.
- 6.12.30 Information disposal procedures shall include physical and logical information disposal procedures and requirements, including shredding requirements, destruction requirements, and secure disk purging and declassification requirements.
- 6.12.31 Read, write, execute, modification, and other operations performed on information, systems that contain information, or applications that use information shall be logged and forwarded to a SIEM.



- 6.12.32 Information shall be backed up in accordance with the backup and restoration section of this technical specification.
- 6.12.33 Backup and archival periods of information shall be defined based on classification and regulatory requirements.

6.13 Application Programming Interfaces Security

- 6.13.1 Application Programming Interfaces (APIs) between applications and environments must be secured.
- 6.13.2 APIs must use HTTPS or equivalent TLS enabled protocol.
- 6.13.3 APIs shall use encryption to protect data in transit as outlined in this specification.
- 6.13.4 APIs shall use OAuth 2.0 and OpenID Connect for authentication and authorization of data access.
- 6.13.5 APIs shall use a combination of mechanisms to verify the authenticity of an API endpoint and API requests. The mechanisms may include network security rules (firewalls), mutual authentication, or digital signatures that assist in verifying the identity of the API endpoint or requestor.
- 6.13.6 All APIs shall be configured to deny all requests by default and only allow requests from specified IP addresses.
- 6.13.7 API keys shall only be used where bearer tokens (JWT/OAuth 2.0/OIDC) are not available for use due to technical constraints. Where the API supports OAuth 2.0 or OIDC, API keys must not be used. If API keys are used:
 - 6.13.7.1 The encryption requirements outlined in this specification must be implemented to protect the API key
 - 6.13.7.2 The API key must be rotated monthly with proper key management procedures
 - 6.13.7.3 The API key must not be exposed in documentation or code repositories
 - 6.13.7.4 Staff responsible for configuring APIs must undertake training to rotate keys and understand the risks associated with API keys
 - 6.13.7.5 Monitoring controls to detect potential leakage of the API key must be implemented.
- 6.13.8 All API requests must be sanitized, validated, and conform to a defined schema. Requests that do not fulfill these requirements must be rejected and a generic http response code must be provided; the response shall not provide any details as to why the request failed.
- 6.13.9 API request failures and rejections shall generate logs with additional details and forward them to a SIEM.



7 SECURITY VALIDATION, VERIFICATION, AND TESTING

- 7.1.1 The TSCC Contractor is responsible for ensuring that verification and validation (V&V) and cybersecurity testing is undertaken to demonstrate compliance with this Specification and inform the Assurance Case, which will be used to approve the cybersecurity works.
- 7.1.2 System Owners shall work with the Cybersecurity Lead to develop the Cybersecurity V&V activities for their individual systems, subsystems, and assets.
- 7.1.3 The TSCC Contractor shall develop a Cybersecurity V&V Plan that aligns with the outcomes described in CENELEC TS 50701 and is consistent with V&V plans in other safety, systems, and software domains.
- 7.1.4 The V&V plan shall include roles and responsibilities, methodologies, tools, acceptance criteria, and mapping templates that trace cybersecurity requirements to evidence items and verification activities.
- 7.1.5 V&V activities must be executed by a team independent from those responsible for the original design and implementation, to uphold the principle of separation of duties and avoid bias.
- 7.1.6 The V&V activities shall verify that all design documentation adequately addresses all cybersecurity requirements.
- 7.1.7 The V&V activities shall validate that the as-built operational environment meets the objectives of cybersecurity controls and verify that configurations are correctly implemented.
- 7.1.8 The V&V plan shall detail how Achieved Security Levels (SL-A) shall be measured, documented, reviewed, and approved, including acceptance thresholds.
- 7.1.9 The V&V Plan shall include references to penetration testing and vulnerability assessment activities and explain how they support and complement the broader cybersecurity V&V objectives.
- 7.1.10 The TSCC Contractor shall develop a Cybersecurity Testing Plan that outlines specific testing activities across the lifecycle stages of the contract, including unit, integration, system, and site acceptance testing.
- 7.1.11 The following types of cybersecurity testing shall be undertaken:
- Hardware configuration testing
 - Software configuration testing
 - Fail-secure mode testing
 - Network segmentation testing
 - Penetration testing
 - Input Testing/Fuzzing
 - Patch and rollback testing
 - Backup and recovery testing
 - Log-source and detection testing
- 7.1.12 All security test tools (e.g. fuzzers, scanners, simulators) used by the TSCC Contractor must be validated to ensure they are approved for use in safety-critical OT environments.
- 7.1.13 All testing shall include standard use-cases (unintentional harm) and abuse use-cases (intentional misuse or attack).
- 7.1.14 Penetration testing must be clearly scoped and must define objectives, in-scope systems, testing constraints, and exclusion zones.



- 7.1.15 All fail-secure modes must be tested to confirm that safety-related fail-safe states are preserved, and that fail-secure states achieve the intended cybersecurity protections.
- 7.1.16 Network segmentation testing shall verify all interfaces are aligned with the zone and conduit model and that no communication bypasses designated conduits.
- 7.1.17 Input testing must be performed for all user interfaces, such as Graphical User Interfaces (GUIs) to ensure that malformed or malicious input does not cause failures or expose vulnerabilities. This shall follow OWASP and other relevant secure coding/testing guidelines.
- 7.1.18 Configuration testing activities shall verify that configuration baselines are applied consistently across all deployed devices and environments.
- 7.1.19 Configuration testing activities shall verify that all devices have appropriate security agents and applications installed; all security agents and applications must be examined to ensure they are configured consistently.
- 7.1.20 Patch and rollback testing shall demonstrate that patches can be installed with low risk and, if needed, uninstalled through rollback procedures that restore the SuC to a secure baseline state.
- 7.1.21 Backup and recovery testing shall demonstrate recovery of systems from both online and offline backups within SLA timeframes and confirm systems return to a secure, operational state.
- 7.1.22 Testing environments shall be isolated from operational systems and must not impact live operations or safety during the execution of any V&V activity.
- 7.1.23 The TSCC Contractor shall repeat selected V&V and cybersecurity testing after major updates, reconfigurations, or software changes affecting the SuC, to ensure continued compliance.
- 7.1.24 The outcomes of testing shall be documented in formal testing reports and incorporated into the Assurance Case to support compliance verification.
- 7.1.25 The TSCC Contractor shall define traceability between test cases and the cybersecurity requirements they are validating or verifying, to demonstrate full coverage and identify any untested controls.



8 LIFECYCLE PHASE REQUIREMENTS & DELIVERABLES

8.1.1 The TSCC Contractor must define, detail and deliver the cybersecurity works throughout the lifecycle phases. This must include, but is not limited to:

- **Supply:** Define component selection criteria, vendor selection and assessment criteria, supply chain management processes, selection criteria for subcontractors, and supply chain, vendor, and subcontractor risk management throughout the contract
- **Delivery:** The SuC shall be delivered in compliance with the technical specification, including the implementation of all security controls, performing all relevant assessments, and producing all relevant documentation.
- **Maintenance:** Systems in the SuC shall be maintained throughout the contract and processes and procedures shall be defined to allow the Authority to continue maintenance to the same standard once handover has occurred.
- **Testing, Commissioning, Assurances, Compliance:** How systems within the SuC are tested, verified, and validated to be compliant with the security controls and principles outlined in this technical specification shall be defined and demonstrated by the TSCC Contractor.
- **Operation:** The TSCC Contractor shall ensure that the systems in the SuC are ready for operations, with detailed processes and procedures outlining operational requirements and activities to continue the secure state during operations after handover.
- **Training:** The TSCC Contractor shall outline a cybersecurity training plan or including cybersecurity training in a broader training plan with appropriate tracking mechanisms to ensure that relevant staff have completed general or targeted training.
- **Disposal:** The TSCC Contractor shall outline detailed requirements for the disposal of systems or data once they are no longer required or operable.

8.1.2 The TSCC Contractor shall complete the following activities and produce the deliverables outlined in the table below during the TS 50701 (EN 50126) Phases.

8.1.3 All deliverables below must be completed with adequate time to permit a review period and approval process for each delivery.

TS 50701 Phase	Cybersecurity Activities	Deliverables
Prerequisites	• Roles and Responsibilities agreed with Authority • Review legal and regulatory obligations • Review Authority Standards	• Produce and seek approval for scope, systems under consideration, context, objectives, principles, and other high-level sections of the Cybersecurity Management Plan
Concept	• Review current industry and global security context relevant to contract • Kick-off meeting to finalize cybersecurity objectives • Develop communications and cross-team collaboration plan • Complete all sections of the Cybersecurity Management Plan including reviews and approval	• Cybersecurity Management Plan



TS 50701 Phase	Cybersecurity Activities	Deliverables
System definition and Operational Context	- Review initial SuC boundaries, architecture documentation, network plans, and provide feedback from a cybersecurity perspective - Perform the initial risk assessment of the SuC	- Conceptual Zone and Conduit Diagram - Document containing details of each zone and conduit, including components, interfaces, and other characteristics - Initial Risk Assessment - Risk Register
Risk analysis and Evaluation	- Review initial set of functional requirements - Review technical specification threat library and update to include modern threats - Perform threat modelling workshops - Perform the detailed risk assessment	- Security Level Targets (SL-T) for all Zones and Conduits in the Zone and Conduit Diagram - Documented people, process, and technology compensating controls, countermeasures, and assumptions - Detailed Risk Assessment - Updated Risk Register
Specification of System Requirements	- Document all people, process, and technology cybersecurity requirements derived from this technical specification, up-to-date industry, regulatory, government, or authority standards - Review system requirements to ensure they align with cybersecurity requirements, objectives, controls, and outcomes - Deliver finalized list of cybersecurity requirements - Reviewed and approved overall system requirements - Write V&V and Testing plans for cybersecurity, detailing the high-level methodology, scope, and objectives; detailed activities shall be added in later phases to inform hands-on work.	- Rail System Cybersecurity requirements - Draft V&V and Testing Plans



TS 50701 Phase	Cybersecurity Activities	Deliverables
Architecture and apportionment of system requirements	• Define procurement assessment criteria for vendors, supply chain risks, security level capability (SL-C) procurement assessments, subcontractor assessments and risk management. • Define secure software development lifecycle requirements, including common vulnerability mitigation requirements, such as OWASP, and secure development training requirements • Deliver cybersecurity procurement requirements, activities, criteria, and plan and seek review and approval from Authority • Deliver SSDLC requirements where in house development shall be performed	• Secure software development requirements. • Vendor, supply chain, and manufacturer cybersecurity processes, procedures, and requirements. • Cybersecurity procurement processes, procedures, and requirements.



TS 50701 Phase	Cybersecurity Activities	Deliverables
Design	• Inform design using risk assessment to ensure that the design accounts for all threats, vulnerabilities, and other risks. • Ensure that the cybersecurity design principles are followed when designing the network and interfaces. • Ensure design is aligned with the up-to-date zone and conduit model, with appropriate design features at each zone boundary, SuC boundary; and within zones, including encryption infrastructure, logging and monitoring infrastructure, and security products. • Document an as-designed security architecture which includes all security devices and other networking or interfacing devices that contribute to cybersecurity objectives for the SuC. • Perform verification activities prior to design approval to ensure all security controls have been designed in all aspects of the design. • Ensure networking, power, and communications infrastructure has included adequate bandwidth for all security devices and traffic. • Develop the final version of Testing and V&V plans, detailing the planned activities with the independent team that shall be conducting the work.	• As-designed security architecture mapped to zone and conduit model • Cybersecurity requirements mapping • First version of Assurance Case • Refreshed risk register based on design • Cybersecurity testing activities • Cybersecurity V&V activities



TS 50701 Phase	Cybersecurity Activities	Deliverables
Implementation, Manufacture or Procurement	• Ensure all implementation personnel have completed appropriate awareness training, • Perform relevant assessments during procurement prior to implementation as per the criteria established in previous phases. • Oversee and govern implementation activities to ensure they are delivered in alignment with the security requirements, objectives, and are aligned with the design. • Work with networking and communications teams to develop firewall rules, ACLs, VLANs and other network segmentation requirements in alignment with the technical specification to ensure the implementation follows design principles. • Ensure all log sources are configured and forwarding logs to the SIEM. • Configure the SIEM and CSOC to enable automated detection of incidents and appropriate alerting. • Ensure processes and procedures are followed, including change management and configuration management documentation, to inform the security Assurance Case. • Verify SL-C of all devices to ensure they align with SL-T for each zone and define countermeasures if required to ensure Zone and Conduit model requirements are met. • Ensure asset inventory is populated with all procured items. • Harden all devices according to vendor guidelines or industry best practice. • Compare and remediate any cybersecurity control gaps between the design and as-built system.	• Processes and procedures for implementation, configuration, and on-going maintenance of cybersecurity systems and activities. • SL-C for each component • SL-A for each zone as per the as-built documentation and implementation activities • As-built security architecture • Identity and access management documentation, including account hierarchies, roles, groups, users, permissions mapping, and authentication requirements. • Supply chain, vendor management, and manufacturer cybersecurity management output • Backups of all implementation guidelines, configurations, images, logic, and other documentation. • Updated Assurance Case (steps taken during implementation & as-built requirements mapping) • Refreshed Risk Register



TS 50701 Phase	Cybersecurity Activities	Deliverables
Integration	- Perform integration testing to verify cybersecurity requirement implementation. - Perform vulnerability assessments and penetration testing. - Validate network segmentation aligns with design. - Validate log sources are all forwarding logs to the SIEM. - Test cybersecurity detection use-cases	- Vulnerability assessment report - Penetration testing report - Findings remediation plans - Updated Assurance Case (Testing outcomes, network segmentation verification, logging & monitoring)
System Validation	- Perform validation and verification activities for all cybersecurity controls. - Document SL-A for all zones and conduits - Performing remaining testing to demonstrate security control implementation.	- Assurance Case (Final version with evidence of all activities and compliance). - Final Zone and Conduit diagram (SL-A).
System Acceptance	Obtain sign-off from relevant senior authority stakeholders, responsible engineers, and SMEs.	- Signed Assurance Case - Final Risk Register
Operation, Maintenance, and Performance Monitoring	Perform handover activities and ensure the Authority has all information required for takeover maintenance.	Maintenance Security Procedures and Records

TABLE 4 - DELIVERABLES

9 HANDOVER

- 9.1.1 The TSCC Contractor shall be responsible for ensuring that all cybersecurity documentation, configurations processes, procedures, controls, and secrets are transferred to the Authority. A comprehensive handover index or register of all cybersecurity documentation must be provided, with each item traceable to a specific requirement or activity in this specification.
- 9.1.2 Risk documentation, including risk management plans, risk assessment procedure documentation, iterations of risk assessments, risk registers, risk ratings, risk scenarios, risk mitigations, risk actions, outstanding risk treatment plans, and other details resulting from cybersecurity risk management works shall be provided to the Authority. The TSCC Contractor shall ensure that the final risk documentation has been provided to the Authority with adequate time to respond to any queries or clarification requests.
- 9.1.3 Process and procedure documentation for the secure configuration of devices across the SuC shall be provided to the Authority. The documentation must contain adequate detail to continue managing the SuC in compliance with this technical specification. The TSCC Contractor shall be responsible for



ensuring that the Authority has adequate information to perform any action required to maintain the cybersecurity state at handover.

- 9.1.4 At the Authorities discretion, the TSCC Contractor shall be expected to produce process or procedure documentation for any cybersecurity component that has not been adequately documented. The TSCC Contractor shall provide process and procedure documentation to the Authority in due time to enable multiple iterations of review and clarification. The Authority shall review and formally approve these documents prior to final handover.
- 9.1.5 The TSCC Contractor shall conduct training sessions and technical walkthroughs with the Authority's cybersecurity, operations, and maintenance staff to review key handover documents, tools, and operational procedures. This shall include a Q&A session and confirmation that the Authority understands how to manage the SuC post-handover.
- 9.1.6 Baseline security documentation, including baseline configuration documentation, hardened disk images, vendor hardening guideline documentation, group policies, implementation and setup procedures, and other relevant information necessary for the Authority to securely configure new or restored systems.
- 9.1.7 SIEM documentation, logging configuration, logging requirements, monitoring, detection use-cases, alerting configurations, dashboard configuration procedures, staffing requirements, and other documentation that contains all the detail required to operate the CSOC and security monitoring function across the rail network.
- 9.1.8 Cybersecurity relevant asset inventory data, including identifiers mapped to IP addresses, VLANs, product versions, product details, MAC Addresses, software versions, network interface ports, and other information available and deemed necessary by the TSCC Contractor or the Authority to cybersecurity works.
- 9.1.9 Network and cybersecurity architecture documentation, including zone and conduit diagrams, network architecture diagrams, dataflow diagrams, security architecture diagrams that include security devices, and other architecture or design documentation that include all devices and endpoints throughout the rail system relevant to cybersecurity works.
- 9.1.10 The TSCC Contractor is responsible for ensuring that network configuration documentation is transferred to the Authority using a secure mechanism such as password protected encrypted file transfer. Network configuration documentation shall be complemented by adequate detail for each ruleset, to enable the Authority to continue allow by exception connectivity.
- 9.1.11 The TSCC Contractor shall work with the Authority to determine a secure mechanism for transferring secrets, including cryptographic keys, certificates, privileged credentials, and default passwords. The mechanism shall be cryptographically secure, protected from unauthorized access, and access shall be limited. Critical system secrets shall be separate from non-critical systems.
- 9.1.12 Cybersecurity verification, validation, and testing documentation, including the final assurance case, vulnerability assessments, vulnerability scan reports, patching history, penetration testing reports, control implementation verification documents and evidence, independent assessment reports, and other security activity documentation that demonstrate compliance with this technical specification.
- 9.1.13 The TSCC Contractor shall confirm that cybersecurity-related logs, assurance records, and evidence collected during the contract are archived and available to the Authority for the duration required by regulatory or contractual obligations.



- 9.1.14 The TSCC Contractor shall document and hand over a cybersecurity lessons learned report, identifying key challenges, successes, and recommendations for ongoing system protection and monitoring.
- 9.1.15 The TSCC Contractor shall demonstrate to the Authority that secure disposal mechanisms are defined, tested, and ready for use to remove all sensitive information once the handover activities have been completed.



Schedule 5(b)

Digital Communications Network

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0006 – Digital Communication Network (DCN)

Rev. 1.0

Authored:

A handwritten signature in black ink, appearing to read "Harshal Jadhav".

Harshal Jadhav, Telecom System Lead

12/23/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Thomas Newey".

Thomas Newey, Telecoms Lead

12/23/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Bruno Comperat".

Bruno Comperat, Deputy Director of Rail Engineering

12/23/2025

Date

Approved:

A handwritten signature in blue ink, appearing to read "Ryan Scott".

Ryan Scott, Director of Rail Engineering

12/23/2025

Date

Released:

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Amit Joshi, Configuration Manager

12/23/2025

Date



Document Revision History – DCN Specifications**Second Edition****December 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition
1.0	December 2025	Updated for Addendum 2



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION	5
2	REFERENCE STANDARDS AND DOCUMENTS	6
2.1	GENERAL	6
2.2	DESIGN GUIDELINES	6
2.3	STANDARDS	6
2.4	OTHER DOCUMENTS	11
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	12
4	SYSTEM DESCRIPTION	13
4.1	PURPOSE OF THE DCN	13
4.2	DCN SYSTEM DEFINITION	13
4.3	DCN SYSTEM OPERATIONAL CONTEXT	13
4.4	DESIGN LIFE	13
5	SYSTEM REQUIREMENTS	14
5.1	GENERAL REQUIREMENTS	14
5.2	ENVIRONMENTAL CONDITIONS REQUIREMENTS	14
5.3	OPERATIONAL REQUIREMENTS FOR DCN	14
5.4	FUNCTIONAL REQUIREMENTS FOR DCN	15
5.5	PERFORMANCE REQUIREMENTS FOR DCN	18
5.6	SAFETY REQUIREMENTS	22
5.7	RAM REQUIREMENTS	22
5.8	CYBERSECURITY AND SECURITY REQUIREMENTS	22
6	INTERFACES REQUIREMENTS	24
6.1	GENERAL REQUIREMENTS	24
6.2	THIRD PARTY INTERFACES	24
6.3	EXTERNAL INTERFACES – STATIONS CONTRACTOR	24
6.4	EXTERNAL INTERFACES – FACILITIES CONTRACTOR	25
6.5	INTERNAL INTERFACE FOR DCN	26
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS	28
7.1	GENERAL REQUIREMENTS	28
7.2	SOFTWARE AND HARDWARE REQUIREMENTS	28
7.3	EMC REQUIREMENTS	30
8	TOLERANCES	31
9	SCOPE OF SUPPLY AND DELIVERY	32
9.1	GENERAL REQUIREMENTS	32
9.2	SPECIFIC REQUIREMENTS	32



10	MANUFACTURING	33
10.1	GENERAL REQUIREMENTS	33
11	INSTALLATION AND INTEGRATION	34
11.1	GENERAL REQUIREMENTS	34
12	TESTING & ACCEPTANCE	35
12.1	GENERAL REQUIREMENTS	35
12.2	SPECIFIC REQUIREMENTS	35
13	SUBMITTALS	36
13.1	GENERAL REQUIREMENTS	36
14	QUALITY MANAGEMENT	37
14.1	GENERAL REQUIREMENTS	37
15	ADDITIONAL INFORMATION REQUESTED	38
15.1	GENERAL REQUIREMENTS	38
16	LOGISTICS	39
16.1	GENERAL REQUIREMENTS	39



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Digital Communication Network (DCN) system, hereinafter: DCN.
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of the DCN is presented in Appendix A.
- 1.1.4 The requirements are formulated using the following words and their meanings:
 - "Shall": Indicates a mandatory requirement that must be strictly implemented; a waiver from a mandatory requirement is permissible only with approval of a design variance.
 - "Should": Indicates a preferred course of action; a design variance is not required if it is not exercised.
 - "Must": Indicates an obligation or a mandatory requirement.
 - "May": Indicates a permissible course of action within the limits of the standards; a design variance is not required if it is not exercised.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines, and specifications provided in this chapter for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, and training, operations and maintenance.

2.2 Design Guidelines

- 2.2.1 The latest version of the following Design Guidelines shall be applied:

ID	Code	Title
[R1]	Design Criteria Manual	Chapter 12 – Communication Systems and Train Control
[R2]	AREMA Standards	Chapter 17 – High-Speed Rail Systems

TABLE 5 - DESIGN GUIDELINES

2.3 Standards

- 2.3.1 The TSCC Contractor shall fully consider and apply the following standards, the in-force standards shall be applied.

ID	Standard	Title
[R3]	ANSI/TIA-568-B.1-5	Telecommunications Cabling Standard Part 1: General Requirements Addendum 5 - Telecommunications Cabling for Telecommunications Enclosures
[R4]	ANSI/TIA-568-B.2-6	Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 6: Category 6 Related Component Test Procedures
[R5]	ANSI/TIA-758-A	Customer-Owned Outside Plant Telecommunications Standard
[R6]	EIA-TIA-455	Standard Test Procedure for Fiber Optic Fibers, Cables, Transducers, Sensors, Connecting and Terminating Devices, and Other Fiber Optic Components
[R7]	EN 300 386	Telecommunication network equipment; Electromagnetic Compatibility (EMC) requirements; Harmonized Standard covering the essential requirements of the Directive 2014/30/EU
[R8]	EN 50121	Railway Applications – Electromagnetic compatibility (All Parts)
[R9]	EN 50121-3-2	Railway applications - Electromagnetic compatibility - Part 3-2: Rolling stock – Apparatus
[R10]	EN 50121-4	Railway applications - Electromagnetic compatibility - Part 4: Emission and immunity of the signaling and telecommunications apparatus
[R11]	EN 50121-5	Railway applications - Electromagnetic compatibility Emission and immunity of fixed power supply installations and apparatus
[R12]	EN 50122	Railway Applications – Fixed Installations, Electrical Safety (All Parts)
[R13]	EN 50122-1	Railway applications - Fixed installations - Electrical safety, earthing and the return circuit - Part 1: Protective provisions against electric shock
[R14]	EN 50124	Railway applications - Insulation coordination



ID	Standard	Title
[R15]	EN 50125	Railway applications - Environmental conditions for equipment (All parts)
[R16]	EN 50125-2	Railway applications - Environmental conditions for equipment - Part 2: Fixed electrical installations
[R17]	EN 50125-3	Railway applications - Environmental conditions for equipment - Part 3: Equipment for signaling and telecommunications
[R18]	EN 50126	Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) (All parts)
[R19]	EN 50126-1	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
[R20]	EN 50126-2	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
[R21]	EN 50128	Railway Applications – Communications, signaling and processing systems – Software for railway control and protection systems
[R22]	EN 50129	Railway Applications – Communication, signaling and processing systems – Safety-related electronic systems for signaling
[R23]	EN 50155	Railway Applications – Electronic equipment used on rolling stock
[R24]	EN 50159	Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems
[R25]	EN 50164	Lightning Protection Components
[R26]	EN 50164-3	Lightning Protection Components (LPC) -- Part 3: Requirements for isolating spark gaps
[R27]	EN 50173	Information technology - Generic cabling systems
[R28]	EN 50174	Information technology - Cabling installation
[R29]	EN 50289-1-6	Communication cables - Specifications for test methods - Part 1-6: electrical test methods - Electromagnetic performance
[R30]	EN 50310	Application of equipotential bonding and earthing in buildings with information technology equipment
[R31]	EN 50600-2-4	Information technology - Data center facilities and infrastructures - Part 2-4: telecommunications cabling infrastructure
[R32]	EN 55024	Information technology equipment. Immunity characteristics. Limits and methods of measurement
[R33]	EN 60297-3	Mechanical structures for electronic equipment - Dimensions of mechanical structures of the 482,6 mm (19 in) series - Part 3-100: basic dimensions of front panels, sub racks, chassis, racks and cabinets
[R34]	EN 60332-1	Tests on electric and optical fiber cables under fire conditions
[R35]	EN 60529	Degrees of protection provided by enclosures (IP Code)



ID	Standard	Title
[R36]	EN 60664-1	Insulation coordination for equipment within low-voltage systems -- Part 1: Principles, requirements and tests
[R37]	EN 60754-2	Test on gases evolved during combustion of materials from cables – Part 2: Determination of acidity (by pH measurement) and conductivity
[R38]	EN 61000-6	Electromagnetic compatibility (EMC) - generic standards (All parts)
[R39]	EN 61000-6-2	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity standard for industrial environments
[R40]	EN 61000-6-4	Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments
[R41]	EN 61034	Measurement of smoke density of cables burning under defined conditions
[R42]	EN 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
[R43]	EN 61643-11	Low-voltage surge protective devices - Part 11: Surge protective devices connected to low-voltage power systems - Requirements and tests methods
[R44]	EN 61643-21	Low voltage surge protective devices - Part 21: Surge protective devices connected to telecommunications and signaling networks – Performance requirements and test methods
[R45]	EN 62305	Protection against lightning (All parts)
[R46]	EN 62305-1	Protection against lightning - Part 1: General principles
[R47]	EN 62305-2	Protection against lightning - Part 2: Risk management
[R48]	EN 62305-3	Protection against lightning - Part 3: Physical damage to structures and life hazard
[R49]	IEC 60068	Environmental testing
[R50]	IEC 60304	Standard colors for insulation for low-frequency cables and wires
[R51]	IEC 60331	Tests for electric cables under fire conditions
[R52]	IEC 60364	Low-voltage electrical installations (equivalent to HD 384 series)
[R53]	IEC 60794-1-21	Optical fiber cables - Part 1-21: Generic specification - Basic optical cable test procedures
[R54]	IEC 60794-3	Optical fiber cables - Part 3: Outdoor cables - Sectional specification
[R55]	IEC 61000-3-6	Electromagnetic compatibility (EMC) - Part 3: Limits - Section 6: Assessment of emission limits for distorting loads in MV and HV power systems - Basic EMC publication
[R56]	IEC 61000-3-7	Electromagnetic compatibility (EMC) - Part 3-7: Limits - Assessment of emission limits for the connection of fluctuating installations to MV, HV and EHV power systems
[R57]	IEC 61000-5-2	Electromagnetic compatibility (EMC) - Part 5: Installation and mitigation guidelines - Section 2: Earthing and cabling



ID	Standard	Title
[R58]	IEC 61156-5	Multicore and symmetrical pair/quad cables for digital communications – Part 5: Symmetrical pair/quad cables with transmission characteristics up to 1 000 MHz – Horizontal floor wiring – Sectional specification
[R59]	IEC 61643	Low-voltage surge protective devices
[R60]	IEC 61850	Communication networks and systems for power utility automation - ALL PARTS
[R61]	IEC 62305-4	Protection against lightning - Part 4: Electrical and electronic systems within structures
[R62]	IEC/EN 60793-1-1	Optical fibers - Part 1-1: Measurement methods and test procedures - General and guidance
[R63]	IEC/EN 60793-1-20	Optical fibers - Part 1-20: Measurement methods and test procedures - Fiber geometry
[R64]	IEC/EN 60793-1-21	Optical fibers - Part 1-21: Measurement methods and test procedures - Coating geometry
[R65]	IEC/EN 60793-1-22	Optical fibers - Part 1-22: Measurement methods and test procedures - Length measurement
[R66]	IEC/EN 60793-1-30	Optical fibers -- Part 1-30: Measurement methods and test procedures - Fibre proof test
[R67]	IEC/EN 60793-1-32	Optical fibers - Part 1-32: Measurement methods and test procedures - Coating strippability
[R68]	IEC/EN 60793-1-33	Optical fibers - Part 1-33: Measurement methods and test procedures - Stress corrosion susceptibility
[R69]	IEC/EN 60793-1-40	Optical fibers - Part 1-40: Attenuation measurement methods
[R70]	IEC/EN 60793-1-45	Optical fibers - Part 1-45: Measurement methods and test procedures - Mode field diameter
[R71]	IEC/EN 60793-1-47	Optical fibers - Part 1-47: Measurement methods and test procedures - Macrobending loss
[R72]	IEC/EN 60793-1-48	Optical fibers - Part 1-48: Measurement methods and test procedures - Polarization mode dispersion
[R73]	IEC/EN 60793-2-50	Optical fibers - Part 2-50: Product specifications - Sectional specification for class B single-mode fibers
[R74]	IEC/ISA 62443 (ISA/99)	Security for industrial automation and control systems.
[R75]	IEEE 1220	IEEE Standard for Application and Management of the Systems Engineering Process
[R76]	IEEE 802.1AE	IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security
[R77]	IEEE 802.1p	CoS Prioritization



ID	Standard	Title
[R78]	IEEE 802.1Q	IEEE Standard For Local and Metropolitan Area Networks--Bridges And Bridged Networks
[R79]	IEEE 802.1q	VLAN
[R80]	IEEE 802.3ae	10 Gb Ethernet over Fiber; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW
[R81]	IEEE 802.3af	Power over Ethernet (PoE)
[R82]	IEEE 802.3an	10GBASE-T 10 Gb Ethernet over Unshielded Twisted Pair (UTP)
[R83]	IEEE 802.3at	Power over Ethernet Plus
[R84]	IEEE 802.3u	100BASE-TX specification
[R85]	IEEE 802.3x	Ethernet flow control
[R86]	IEEE 802.3z	1000BASE-X specification
[R87]	IEEE 802.ax	Local and Metropolitan Area Networks Link Aggregation
[R88]	ISO 11064	Ergonomic design of control centers
[R89]	ISO 7240-16:2007	Fire detection and alarm systems — Part 16: Sound system control and indicating equipment
[R90]	ISO/CEI 15288	Systems engineering - Systems life cycle processes
[R91]	ISO/IEC 11801	Information technology — Generic cabling for customer premises
[R92]	ITU-T E. 408	Telecommunication Networks Security Requirements
[R93]	ITU-T E. 409	Incident Organization and Security Incident Handling
[R94]	ITU-T G.652/G.655/G.656	Fiber Optic Cable Specification
[R95]	ITU-T G.8010	Architecture of Ethernet layer networks
[R96]	ITU-T G.8110	MPLS layer network architecture
[R97]	ITU-T G.8262	Timing characteristics of a synchronous equipment slave clock
[R98]	ITU-T G.8271/Y.1366	Time and phase synchronization aspects of telecommunication networks
[R99]	ITU-T G.8273.2/Y.1368.2	Timing characteristics of telecom boundary clocks and telecom time slave clocks for use with full timing support from the network
[R100]	ITU-T G.8275/Y.1369.2	Architecture and requirements for packet-based time and phase distribution
[R101]	ITU-T X. 805	Security Architecture for Systems Providing End-to-End Communications
[R102]	ITU-T Y.1540	Internet protocol data communication service - IP packet transfer and availability performance parameters
[R103]	ITU-T Y.1541	Network performance objectives for IP-based services



ID	Standard	Title
[R104]	NFPA 780	Standard for the Installation of Lightning Protection Systems
[R105]	RFC 2030	Simple Network Time Protocol (SNTP) Version 4
[R106]	TIA/EIA-568-B/C	Telecommunications Cabling Standards
[R107]	TIA/EIA-606-A	Administration Standard for Commercial Telecommunications Infrastructure
[R108]	TIA/EIA-607-A	Grounding and Bonding Requirements for Telecommunications
[R109]	TIA-526-7 (OFSTP-7)	Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant
[R110]	TIA-569-B	Standards for Telecommunications Pathways and Spaces

TABLE 6 – STANDARDS

2.4 Other Documents

2.4.1 The following documents shall be referred:

ID	Document	Title
[R111]	Schedule 1	Safety, Security and RAM Requirements
[R113]	Schedule 16	Scope of Work
[R114]	Schedule 5a SPEC-0005	Cyber Security Technical Specification

TABLE 3 - OTHER DOCUMENTS

3 TERMS, DEFINITIONS, AND ABBREVIATIONS

- 3.1.1 All the terms, definitions, and abbreviations are provided in the Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of the DCN

- 4.1.1 The purpose of the Digital Communication Network (DCN) system is to provide a robust, reliable, redundant, and high-capacity communication infrastructure to support all the requirements of the California High-Speed-Rail system.
- 4.1.2 The purpose of the DCN shall be the primary telecommunications infrastructure for California High-Speed-Rail. It shall provide connectivity between different locations and facilities.

4.2 DCN System Definition

- 4.2.1 The DCN system is a distributed network designed to manage communication between various facilities, trackside equipment, and the control center.
- 4.2.2 The DCN system shall be provided by the TSCC Contractor, including both active and passive components of the system.

4.3 DCN System Operational Context

- 4.3.1 The mission of the DCN system is to facilitate clear and reliable communication between the various stakeholders involved in CHSR operations in compliance with the operational needs.

4.4 Design Life

- 4.4.1 The design life shall be 15 years.
- 4.4.2 The design life requirements for the DCN system shall allow for the pertinent evolution and technological change of the DCN system throughout its life.
- 4.4.3 The TSCC Contractor shall ensure that the DCN components with shorter design lifespans shall be managed by scheduled technology refresh strategies and spares management plans.
- 4.4.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce DCN system components (with equal or compatible technical specifications) for the entire design life required.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

- 5.1.1 The DCN shall be designed in accordance with the requirements described in this specification.
- 5.1.2 The TSCC Contractor's scope shall include all phases, including design, supply, deployment, installation, configuration, testing, and commissioning for the DCN system.
- 5.1.3 The TSCC Contractor shall provide all necessary DCN equipment, cabling, software, and licenses required to design, supply, deploy, install, configure, test, and commission the system at all locations.
- 5.1.4 The DCN shall transport all required video, voice, and data between OCC, Stations, Facilities, Traction power substations, solar sites, and wayside facilities along the California high-speed line.
- 5.1.5 The DCN shall include advanced network management features, which will provide control, monitoring, and configuration of the network system, maintain configuration database for all network elements, gather and log alarm events from these elements, and generate performance statistics reports, including availability and performance. With the proposed network management system, it shall be possible to completely reconfigure the transmission network in case of a failure.
- 5.1.6 DCN equipment shall be backed up with Uninterruptible Power Supplies that provide localized battery backup for at least 12 hours in the event of mains power failure at DCN sites.
- 5.1.7 Buildings containing DCN equipment shall be provided with an external connection point for a backup generator.
- 5.1.8 The DCN equipment shall have a service life of not less than 15 years.

5.2 Environmental Conditions Requirements

- 5.2.1 The TSCC Contractor's DCN system design shall respect local climatic conditions.
- 5.2.2 All equipment shall be protected from damage or degradation in performance due to shock or vibration as experienced in the railway environment.
- 5.2.3 The TSCC Contractor's design for the DCN system shall comply with the following telecom-related environmental requirements (list non-exhaustive):
 - 5.2.3.1 The equipment provided and installation-related material shall be adapted to the special local environmental conditions, e.g., stainless-steel fixations, housing, etc.
 - 5.2.3.2 Based on the different installation sites, the different ingress protection (IP) requirements shall be specified.
 - 5.2.3.3 Air conditioning calculation and air conditioning systems shall be provided for the different required technical rooms in and outside of technical buildings provided by the TSCC Contractor.
 - 5.2.3.4 The equipment provided shall be protected from damage or degradation in performance due to shock or vibration as experienced in the railway environment.

5.3 Operational Requirements for DCN

- 5.3.1 The TSCC Contractor's DCN design shall ensure compliance with the California HSR planned operations and shall allow the operation and maintenance of the main line and related local facilities.



5.4 Functional Requirements for DCN

5.4.1 General requirements

- 5.4.1.1 The DCN shall be a digital transmission network that provides the following functions:
- Transmit data, voice, and video from the various subsystems.
 - Continuously monitor the network status and inform operator(s) in real time.
 - Automatically reconfigure the network in case of failure.
- 5.4.1.2 For the CHSR railway, the DCN shall be based in a fully redundant self-healing backbone transmission network. MPLS (Multi-Protocol Label Switching) or other options may be proposed with appropriate justification.
- 5.4.1.3 The DCN data-link layer (layer-2) shall be preferably based on IP-MPLS technology and properly justified. If GMPLS, MPLS-TP, or any other technologies are considered by the TSCC Contractor as an alternative to the IP-MPLS preferred solution, it shall be properly justified. Only solutions based on technologies successfully deployed in high-speed railway infrastructures shall be proposed by the TSCC Contractor and subject to Authority approval.
- 5.4.1.4 As a minimum, the DCN system shall consist of the following components:
- Access: consisting of switches and different interfaces to manage all field and end equipment.
 - Backbone and Distribution: to supply redundant connectivity to switches located in the stations and sites.
 - Connectivity through the optical fiber cable network connecting stations, depot, OCC, distributed sites, and maintenance facilities.
 - Compliance with Cybersecurity Project requirements to avoid malicious intrusions.
 - Network Management System for the DCN.
 - A state-of-the-art architecture and connectivity solution shall be provided to the OCC data center infrastructure.
- 5.4.1.5 The TSCC Contractor's design shall consider at least two redundant DCNs, one for carrying the critical operational services and another for the non-critical operational services, aligned with the cybersecurity policies designed for this project, with redundancy regarding to:
- nodes within the network.
 - redundant DCN power supply equipment.
 - interconnection topology considering the optical fiber cable network.
 - and any other requirement within this specification.
- 5.4.1.6 The allocation of operational services into critical and non-critical should be as follows (non-exhaustive, to be refined during the design phase):
- 5.4.1.7 Critical operational services:
- ETCS
 - Interlocking
 - Traffic Management System
 - Wireless Communication Systems.
 - Network Timing System.



- Telephony System.
- Integrated Control and Supervision System.
- Power SCADA
- Intrusion Detection

5.4.1.8 Non-critical operational services:

- Public Address and Customer Information System.
- CCTV System.
- Automated Fare Collection System.
- Fire Protection System
- Electronic Access Control Systems.
- Asset Management.
- Hazard Detection and Early Warning System
- Stations equipment's (as per 6.3)
- Facilities equipment's (as per 6.4)
- Asset Management System.

5.4.1.9 The DCN must be based on packet switching and routing as a major evolution of backbone technologies.

5.4.1.10 Each DCN node shall be fully redundant, and single points of failure shall be avoided.

5.4.1.11 The TSCC Contractor's DCN design shall provide routing between the nodes based on an optimal configuration within the optical fiber cables.

5.4.1.12 The optical fiber cables shall be connected to the stations (and other facilities) along the high-speed line. The topologies may be proposed and properly justified by the TSCC Contractor upon approval by the Authority.

5.4.1.13 The network shall be dimensioned to interface and interconnect the critical and non-critical sub-systems for operational purposes.

5.4.1.14 QoS assurance shall be supported by the network nodes.

5.4.1.15 QoS management shall utilize (not limited to):

- Classification and marking tools shall be used for DCN Core, Distribution, and Access nodes to differentiate between applications and sort packets into different traffic types.
- Congestion management tools to determine which queue to place the packets into include priority queuing, first-in, first-out, and low-latency queuing.
- Congestion avoidance tools to drop low-priority packets when congestion occurs.
- Shaping and load balancing tools to manipulate DCN traffic prioritization and policies for real-time applications over less time-sensitive applications.
- The TSCC Contractor's solution for the DCN shall support the following features (not limited to):
 - Network segmentation functionalities.
 - Layer 2-4 switching capabilities.
 - Multicast and Unicast transport with IPv4 and IPv6 packets.



- Multicast through IGMP.
- Loop prevention technology.

- 5.4.1.16 The TSCC Contractor shall describe the configuration, operation, interoperability, and synchronization of the network, including its operation during different possible fault scenarios.
- 5.4.1.17 The TSCC Contractor's design for DCN shall respect special country-related requirements and regulations (e.g., local governmental laws concerning subscriber information and database sharing, etc.).
- 5.4.1.18 The DCN shall be equipped with facilities for high security of data and protection from external sources via suitable firewalls to ensure the security and integrity of the rail systems.
- 5.4.1.19 Firewall/proxy server appliances shall be provided at the point of interconnection with the Internet and as a gateway to the DCN network.
- 5.4.1.20 Access to the operating system software for maintenance purposes shall be segregated on an administration and management network through a dedicated MPLS VPN connectivity.
- 5.4.1.21 Access to the operating system software for maintenance purposes shall be password protected to allow access by appropriately qualified levels of personnel for maintenance.

5.4.2 Network Management System (NMS)

- 5.4.2.1 The NMS solution designed by the TSCC Contractor shall include a comprehensive network management system (NMS) for the entire DCN's components and devices.
- 5.4.2.2 All DCN shall be managed and monitored by NMS to be located at the OCC.
- 5.4.2.3 The NMS shall include system monitoring tools, configuration tools, traffic controlling, service planning, and activation tools that shall be used by operation and maintenance personnel.
- 5.4.2.4 The NMS shall incorporate a real-time optical fiber monitoring and assurance system that can, at least, identify degradations, localize failures, and provide root-cause analysis. These monitoring features shall be carried out by the network equipment itself or by means of external dedicated devices.

5.4.3 Optical Fiber

- 5.4.3.1 The TSCC Contractor shall install a single-mode fiber optic cable in a duct, on one side of the track, for the entire length of the Right-of-Way. The Optical fiber cables shall consist of a minimum of 192 fibers each distributed in multiple tubes.
- 5.4.3.2 The TSCC Contractor's design shall ensure, for the optical fiber cable, protection against impact, crush, and rodent damage at any point of the optical networks. This protection against impact, crush, and rodents shall be provided by the multi-ducts, micro-ducts, and any other solutions.
- 5.4.3.3 The TSCC Contractor's design shall ensure external additional protection against rodents, especially in the manholes, extract points, and where micro-ducts do not provide enough protection or are not recommended. Those specific solutions regarding rodent protection shall be properly described and justified by the TSCC Contractor and approved by the Authority.
- 5.4.3.4 In general, the TSCC Contractor's design shall ensure and provide the proper continuity of enough multi-ducts/micro-ducts all along the cableways both in open line and in stations or any other facility even for undertrack crossings to maintain the protection when fiber cross from the opposite side of the track to the equipment location, station building or any trackside equipment. The main reason is that the multi-ducts/micro-ducts shall provide protection against impact, crush, and rodents to the fibers to avoid the fiber being unprotected in any section of the cableways.



- 5.4.3.5 Optical fiber cable shall be deployed to support routing between the nodes.
- 5.4.3.6 The Optical Fiber system shall be duly documented, using a software tool, allowing the identification of every FO in use for each service and for every section of the fiber path, as well as the reserve FO, allowing potential changes to be made graphically.

5.5 Performance Requirements for DCN

5.5.1 General requirements

- 5.5.1.1 The DCN's design shall be based on state-of-the-art technology for high-speed railways.
- 5.5.1.2 DCN's design shall be compliant with the norms and standards listed in 2.3 (not limited to), but especially to:
 - EN 50128 Railway Applications – Communications, signaling and processing systems – Software for railway control and protection systems.
 - EN 50129 Railway Applications – Communication, signaling and processing systems – Safety related electronic systems for signaling.
 - EN 50159 Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems.
 - EN 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems (SIL)(certification).
- 5.5.1.3 The TSCC Contractor shall provide expected data traffic analysis as part of the Design to include overhead management and expandability.
- 5.5.1.4 The DCN shall use optical fibers as the physical transmission layer (high bandwidth, not sensitive to electromagnetic interference, extendibility, etc.).
- 5.5.1.5 The TSCC Contractor shall dimension the provided DCN according to the required network services and the number of different network users.
- 5.5.1.6 The TSCC Contractor shall be responsible for providing a solution with adequate requirements, in terms of throughput and latency, to fulfil the most demanding needs for all the operational applications to be served (to ensure non-blocking service provision and avoid bottlenecks in data throughput).
- 5.5.1.7 For the network topology design, the number of rings and the number of nodes per ring shall be dimensioned considering aspects such as the latency, time synchronization, delivery, and others to ensure the redundancy and optimal performance of the whole DCN.
- 5.5.1.8 The DCN shall enable the convergence of multiple applications/subsystems within the same infrastructure, considering that each of these applications/subsystems has unique network requirements, priorities, security restrictions, bandwidth capacity, latency, QoS, etc.
- 5.5.1.9 To ensure a high level of security for transmission and to offer efficient traffic management, the DCN shall support application segment routing, resource reservation, encryption, traffic differentiation, and isolation (for example, based on VLANs, VXLAN, VPNs, IPVPN, EVPNs, wavelength separation, and DWDM / CWDM, or other similar approaches).
- 5.5.1.10 The DCN shall be able to allocate bandwidth as per request from any of the sub-systems and shall provide the ability to reserve bandwidth for some of the sub-systems and applications that require guaranteed bandwidth.



- 5.5.1.11 To get the best optimization of network resources, the DCN shall support QoS (Quality of Service) and Traffic Engineering. Additionally, it is recommended that the DCN be capable of supporting wavelength multiplexing to increase traffic capacity as needed for future extensions.
- 5.5.1.12 The TSCC Contractor shall define and deploy the specific Traffic Engineering configuration compliant with DCN operational, functional, and performance specifications and Cybersecurity project requirements.
- 5.5.1.13 The TSCC Contractor's design for DCN shall specify target convergence times after a disconnection within the DCN WAN for critical services, non-critical services, and end-to-end services.
- 5.5.1.14 The network equipment carrying synchronization information shall be compliant with IEEE 1588v2 Precision Time Protocol (PTP), G.8271, G.8275.1&2, G.8273.1&2 (not limited to) to provide time accuracy expressed in terms of time error with respect to a common reference, that allows the synchronization of the most demanding systems like FRMCS.
- 5.5.1.15 The network equipment carrying synchronization information shall be compliant with Network Time Protocol to provide time synchronization for systems.
- 5.5.1.16 The TSCC Contractor's design for the DCN shall comply with ITU-T G.8010, ITU-T G.8110, RFC 3031, RFC 3032, and any other relevant standards applicable.
- 5.5.1.17 The access strategy of the different subsystem and field equipment (CCTV cameras, PACIS end devices, etc.) to the DCN shall be assessed by the TSCC Contractor to provide the most optimal solution in terms of performance, use of network devices, and cybersecurity considerations.
- 5.5.1.18 DCN network devices shall support MACsec (IEEE 802.1AE) encryption. Vendor's proprietary encryption features (layer 2 or layer 3) may be proposed subject to Authority approval.
- 5.5.1.19 Prior to the detailed design and manufacturing of the DCN, the TSCC Contractor shall:
- Assess the data rates, bandwidth requirements, and usage level of each individual system that the DCN is required to support and shall estimate total loading and submit such details for the approval of the Authority.
 - Compile and submit an expected performance report to the Authority that includes details of the required DCN capabilities, network throughput, worst-case transmission delay times, availability, including MTTR.

5.5.2 Network Management System

- 5.5.2.1 The NMS for DCN main components shall include (not limited to):
- Managing entities.
 - Managed devices.
 - Agents.
 - Standard network management protocols.
 - Monitoring, configuration, and setup tools.
 - Network traffic engineering, monitoring & control.
 - Resource utilization (CPU, RAM memory, IOPS, etc.).
 - HMI, GUI, and dashboards.
- 5.5.2.2 The Network Management System (NMS) for DCN main functions shall include (not limited to):
- Automatic network discovery tools for all equipment types and services.



- Automatic network mapping tool.
- Element management for each networking sub-system, including web interface.
- Asset inventory monitoring and reporting.
- Creation, configuration and deletion of users and roles.
- IP address management.
- Performance alarms triggered by thresholds parameters defined by the operators.
- Troubleshooting capabilities.
- Reporting tools.

5.5.2.3 The NMS for DCN shall be (not limited to):

- Scalable to manage all networking and information systems elements within a single system.
- Virtualized solution capability.
- Capable of managing network elements from different vendors within a single system, with the monitoring of alarms and performance.
- Based on the latest version of network management protocol and shall support the latest versions of SNMP.
- Support the addition of new and specific Management Information Base(s) (MIBs) easily and with a user-friendly procedure.
- Aligned with cybersecurity policies to implement security features to prevent unauthorized users from gaining access to critical network resources.
- Provided with an embedded performance tool to manage the overall performance of all network and information systems components.
- Able to perform network planning, traffic engineering, remote configuration, installation, maintenance, expansion, restoration, and disaster recovery.
- Provided with features for security and accountability and shall generate a log file for any user access to configuration or platform changes.

5.5.2.4 All analyzed Quality of Service (QoS) performance parameters shall be monitored by the NMS for DCN:

- Bandwidth: Core, Distribution, and Access switches/routers and port allocation.
- Latency: Video, Voice (to include Mean Opinion Score (MOS)), Data, Metadata, including Firewalls.
- Jitter: variation in packet delays, including Firewalls.
- Packet Loss: Packet delivery percentage of packets that are dropped within the DCN Network as per a predefined period.
- Throughput and IOPS: for all systems interfacing the DCN.
- Bit Error Rate (BER).
- Connected link optical fiber loss profile monitoring (attenuation levels and location of events and failures).
- Disaster Recovery response times.
- All performance levels shall be end-to-end.



- 5.5.2.5 The NMS's graphical user interface (GUI) shall be well-designed, agile, easy to use, and intuitive and shall include (not limited to):
- Access control and profiling functionalities aligned with the project's cybersecurity policies.
 - Network admission control.
 - Dashboard Human-Machine Interface (HMI) and GUI to the OCC operators.
 - Network map and topology view for each network layer.
 - Services map view for each service type.
 - Drill-down capabilities from network map to specific device or specific service.
 - Configuration wizard tools.
 - Automatic discovery and configuration of new components.
 - Capability of configuring multiple devices at a same time.
 - Capability of Command Line Interface (CLI) support.
 - Outstanding alarms.
 - Troubleshooting features.
- 5.5.2.6 The NMS shall forward the selected events to the ICSS system.
- 5.5.2.7 The NMS system shall support (not limited to):
- 802.1Q VLAN, IEEE 802.1P, IEEE 802.1w, IEEE 802.3x Ethernet Flow Control, RMON, TFTP/FTP, CLI MAC, etc.
 - Load balancing, QoS, bandwidth, latency, response time, and errors, real-time and ad-hoc monitoring.
 - Monitoring, management, and allocation of bandwidth.
 - Automated and/or manual scripts setup.
 - Monitoring and reporting of all equipment.
- 5.5.2.8 Monitoring capabilities shall support Management Information Base (MIB), Simple Network Management Protocol (SNMP v3 and associated security features), traps reporting, and Internet Control Message Protocol (ICMP), including packets containing error, control, and informational messages.
- 5.5.3 Optical Fiber**
- 5.5.3.1 The TSCC Contractor shall specify and justify the number of fiber optic cables and the number of fibers inside those cables to ensure the provision of adequate fiber optic cores to service the designed DCN (spare and dark fibers shall be considered in the dimensioning).
- 5.5.3.2 The TSCC Contractor shall design for the minimum requirements for fiber optic materials:
- Fibre optic cables shall be, at least, compliant with the following standards: ITU-T Recommendation G.652D, G.655, G.657, IEC/EN 60793-1-20/21/22/30/32/33/40/42/45/47/48, IEC/EN 60793-2-50 Category B-652.D, EIA/TIA 455, IEC 60794-1-2, IEC 60794-3, EIA/TIA 568-C, EN 50173-1, ISO/IEC 11801.
 - Single-mode fiber optic cable shall be compatible with CWDM, DWDM, and non-DWDM technologies.
 - Fiber optic color coding shall be as per IEC 60304.



- Single-mode Fiber optic insertion loss shall be $\leq 0.35\text{dB/km}$.
- Fiber optic splice fusions insertion loss shall be $\leq 0.05\text{dB}$.
- Testing shall be in accordance with TIA/EIA-455, IEC/EN 60793-1 and IEC/EN 60794-1-2x.
- Drop-off fiber optic cables shall be halogen-free (HFFR), flame retardant, and shall comply with IEC-60332-1.
- Multimode Fiber optic (if additionally provided) shall be at least OM3 50/125 μm .

- 5.5.3.3 At least one meter of fiber shall be stored without twists or kinks within optical fiber splice organizers at joints and terminations.
- 5.5.3.4 Optical fiber splice organizers shall accommodate individual strain relief for each splice and allow for future maintenance or modification without damage to the cable or splices.
- 5.5.3.5 The number of fibers shall be calculated considering all the sub-systems to interface with (in conjunction with the TSCC Contractor), plus a 50% excess, and another percentage reserved for dark fiber to be confirmed by the Authority.
- 5.5.3.6 The estimation of the number of cables and fibers per cable shall be the most efficient possible to avoid unnecessary/in excess splices and intermediate points of failure. This estimation shall be done in conjunction with the Authority, who may involve third-party users.
- 5.5.3.7 The TSCC Contractor shall reserve a dedicated fiber optic pair (dark fiber) for the Power Supply & MV/LV Distribution Systems along the CHSR alignment.

5.6 Safety Requirements

- 5.6.1 DCN shall comply with the safety requirements defined in Schedule 1.

5.7 RAM Requirements

- 5.7.1 The TSCC Contractor shall be responsible for performing all the activities as specified in Schedule 1.
- 5.7.2 The availability of DCN at circuit level shall be defined as the availability of the circuit between both end points of the DCN where the required bandwidth is available for access.
- 5.7.3 Any circuit of the DCN shall be considered unavailable when:
- There is a loss of communication between the end points of the circuit, or
 - The quality of signal transmission within the circuit is below the performance standards.

5.8 Cybersecurity and Security Requirements

- 5.8.1 The TSCC Contractor's design for DCN shall be in full compliance with the CHSR Cybersecurity Technical Specification.
- 5.8.2 The DCN network shall be designed in compliance with the network security and network segmentation requirements defined in the cybersecurity specification and enable the implementation of the zone and conduit model.
- 5.8.3 The DCN shall have a System Owner who shall be accountable for cybersecurity risk ownership and mitigation.
- 5.8.4 The DCN team shall work closely with the Cybersecurity Lead and Cybersecurity Services Lead to procure and configure network devices in compliance with the cybersecurity technical specification, specifically,



switches, routers, firewalls, and other devices that are configured to allow/disallow communications across the network.

- 5.8.5 The DCN network shall be designed to facilitate the logging information required to be transmitted from devices to the SIEM, also considering future log sources being on-boarded during later phases of the CHSR works.
- 5.8.6 The DCN team shall facilitate cybersecurity requirements and objectives by attending risk assessments, attending threat modelling exercises, designing network layer controls such as tunnel mode VPNs to facilitate encryption between devices that may not support encryption, configuring the NMS in compliance with the cybersecurity technical specification to maintain the integrity of network configurations and security, and other activities as requested by cybersecurity teams.
- 5.8.7 DCN boundaries must be protected by a deny-by-default firewall with intrusion prevention capabilities, boundaries include all locations where the DCN interfaces with another network.
- 5.8.8 DCN boundary devices must have an appropriate vulnerability and patch management plan.
- 5.8.9 Firewalls shall be placed appropriately across the DCN to enable east-west traffic filtering; a firewall shall be located at each equipment room or other room containing computing equipment at a minimum.



6 INTERFACES REQUIREMENTS

6.1 General Requirements

6.1.1 Interfaces are classified as below:

- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR contractors);
- External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors);
- Internal interfaces between systems within the TSCC scope.

6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.

6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification. Third Partys Interfaces

6.2 Third Party Interfaces

6.2.1 The DCN shall provide interfaces with external networks such as Internet Service Provider (ISP) networks, Transit Agency networks, First Responder Networks, and Utility Company networks as necessary to meet the Contract Requirements.

6.2.2 The TSCC Contractor shall coordinate with the Supplier for the optical fiber cable. The TSCC Contractor shall provide the design inputs related to optical fiber cable to the Supplier.

6.3 External Interfaces – stations contractor

6.3.1 Stations DCN connectivity

6.3.1.1 The stations contractor shall supply, install, terminate, label, and test all data infrastructure cabling throughout the stations, excluding :

- Telecommunications equipment rooms
- Wayside in stations areas

6.3.1.2 The stations contractor shall provide all associated containment, patch panels, outlets, and related passive components required to deliver a fully functional structured cabling system up to the designated DCN switch connection points.

6.3.1.3 The stations contract shall coordinate with the TSCC Contractor to ensure compatibility of cable terminations and interface points with the DCN switching equipment.

6.3.1.4 The TSCC Contractor shall supply, install, configure, and commission all the DCN network switches to which the data infrastructure cabling provided by the stations contractor shall connect.

6.3.1.5 The TSCC Contractor shall supply, install, terminate, and test all data infrastructure cabling located within telecommunication equipment room and wayside areas, including connections between switches, servers, storage, and other active equipment.

6.3.1.6 The TSCC Contractor shall ensure all DCN switch ports are appropriately configured and operational for the services and systems requiring connectivity.

6.3.1.7 The TSCC Contractor shall provide integration testing of switches with the stations contractor's cabling infrastructure to confirm end-to-end performance and compliance.

6.3.2 DCN equipment integration in stations



- 6.3.2.1 The TSCC Contractor shall install all DCN network equipment in the station communication rooms being provided by stations contractors.
- 6.3.2.2 The TSCC Contractor shall provide to stations contractors:
- Equipment dimensions
 - Equipment clearances requirements
 - Equipment mounting and fixings requirements
 - Cable routes/containment requirements
 - Equipment loadings
 - Installation and maintenance requirements
 - Equipment heating loads
 - Equipment cooling loads
 - Equipment hydraulic requirements
- 6.3.2.3 The TSCC Contractor shall provide the following information to stations contractors to accommodate DCN equipment installation and operations and maintenance:
- Room dimensions and layouts
 - Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
 - Room raised floor system
 - Delivery access routes.

6.4 External Interfaces – facilities contractor

6.4.1 Facilities DCN connectivity

- 6.4.1.1 The facilities contractor shall supply, install, terminate, label, and test all data infrastructure cabling throughout the stations, excluding :
- OCC equipment rooms and OCC desks in OCC control rooms
 - Wayside in facilities areas
- 6.4.1.2 The facilities contractor shall provide all associated containment, patch panels, outlets, and related passive components required to deliver a fully functional structured cabling system up to the designated DCN switch connection points.
- 6.4.1.3 The facilities contract coordinate with the TSCC Contractor to ensure compatibility of cable terminations and interface points with the DCN switching equipment.
- 6.4.1.4 The TSCC Contractor shall supply, install, configure, and commission all the DCN network switches to which the data infrastructure cabling provided by the facilities contractor shall connect.
- 6.4.1.5 The TSCC Contractor shall supply, install, terminate, and test all data infrastructure cabling located within OCC equipment's rooms and wayside areas, including connections between switches, servers, storage, and other active equipment.
- 6.4.1.6 The TSCC Contractor shall ensure all DCN switch ports are appropriately configured and operational for the services and systems requiring connectivity.
- 6.4.1.7 The TSCC Contractor shall provide integration testing of switches with the facilities contractor's cabling infrastructure to confirm end-to-end performance and compliance.



6.4.2 DCN equipment integration in Facilities

6.4.2.1 The TSCC Contractor shall install all DCN network equipment in the OCC and facility buildings being constructed by the facilities contractor.

6.4.2.2 The TSCC Contractor shall provide to the facilities contractor:

- Equipment dimensions
- Equipment clearances requirements
- Equipment mounting and fixings requirements
- Cable routes/containment requirements
- Equipment loadings
- Installation and maintenance requirements
- Equipment heating loads
- Equipment cooling loads
- Equipment hydraulic requirements

6.4.2.3 The TSCC Contractor shall provide the following information to the facility building contractor to facilitate the DCN equipment installation and operational/maintenance requirements:

- Room dimensions and layouts
- Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
- Room raised floor system
- Delivery access routes.

6.5 Internal Interface for DCN

6.5.1 Interfaces with TSCC Systems – data connectivity

6.5.1.1 The DCN shall have an interface with the following Critical services sub-systems to provide them with a robust, reliable, redundant, and high-capacity communication transport infrastructure.

- Telephony system
- Network Timing system
- ETCS
- Interlocking
- Traffic Management System
- Power SCADA
- Wireless Communication Systems
- Integrated Control and Supervision System

6.5.1.2 The DCN shall have an interface with the following non-critical services sub-systems to provide them with a robust, reliable, redundant, and high-capacity communication transport infrastructure.

- Hazard Detection and Early Warning System
- CCTV system.
- Automatic Fair Collection System.
- Public Address and Customer Information System.



- Fire Protection system.
- Electronic Access Control Systems.
- Asset Management System.
- Technical Buildings (Shelters/Containers) and related MEP system.

6.5.2 Interface with Integrated Control and Supervision Systems

6.5.2.1 The ICSS shall monitor status and operational alarms from DCN.

6.5.3 Interface with Asset Management System (EAMS)

6.5.3.1 The DCN System shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied by the TSCC Contractor shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards. Refer to 2.3.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the design life requirements.

7.2 Software and Hardware Requirements

- 7.2.1 Single-mode (SM) optical fiber cables shall be considered for the backbone transmission network in open line and network uplinks (preferably OS2 type).
- 7.2.2 Fibers shall comply with the instructions ITU-T G.652/G.655/G.656/G.657. However, the TSCC Contractor may propose any other optical fiber technology if there are objective and demonstrable improvements for the system.
- 7.2.3 For structured cabling inside buildings and data centers, Single Mode optical fiber shall be preferred, but Multimode fiber (preferably OM4) may be considered upon the TSCC Contractor's assurance of no impact on performance and the avoidance of potential bottlenecks and allowing for future developments.
- 7.2.4 In addition, all the elements required for an optimal optical connectivity shall be considered, such as connectors and ODF/patch panels for backbone, terminating and interconnecting equipment, including Termination Protection Devices, SM optical patch cords, MM optical patch cords (if needed), latching connectors, racks, shelves and trays, cabinets, termination, and distribution boxes.
- 7.2.5 All cables shall be fire and flame retardant, halogen-free, non-corrosive, etc., in accordance with local applicable Laws.
- 7.2.6 Fiber optic splice enclosures shall be installed with 50% spare capacity.
- 7.2.7 Detailed cable routing and labeling plans shall be delivered by the TSCC Contractor.
- 7.2.8 The TSCC Contractor's design for all central servers shall be on-premises, either physical, virtualized, or cloud-based, to facilitate system evolution and comply with cybersecurity requirements.
- 7.2.9 Network equipment for open-line trackside locations (Technical Buildings, Cabinets, TPS, Radio sites, etc.) shall preferably be fan-less. Fan cooling may be accepted upon the TSCC Contractor's evidence that reliability figures are equivalent to the fan-less solution.
- 7.2.10 The DCN components shall be fully redundant in hardware, power supply, cabling, and software so that the provided services survive during any one failure of hardware, cabling, and software.
- 7.2.11 The DCN and NMS components shall incorporate a hot-swappable power supply.
- 7.2.12 The DCN equipment provided shall be extendable without requiring the replacement of existing equipment.
- 7.2.13 Hot-swappable elements, such as fans and power supplies, should be swappable without tools.
- 7.2.14 Hardware, software, firmware, or data changes required to support future extensions or expansions on-line shall be accomplished without performance or functionality degradation or availability to the operational systems.
- 7.2.15 A 50% spare capacity for each subsystem shall be provided for the DCN design.
- 7.2.16 DCN shall be adapted for electric power systems using IEC-61850 protocols (GOOSE, SV messaging).



- 7.2.17 Copper cable shall be avoided whenever possible in favor of optical connections.
- 7.2.18 If copper cable is not avoidable, CAT6A/CAT7A cable compliant with IEC 11801, TIA/EIA-568-b-2, IEC60332-1, IEEE 802.3, 10GBASE-T, EN50288-5-1 and other relevant standards shall be used.
- 7.2.19 Structured cabling inside stations and other facilities for Telecom system operational purposes shall be provided by the TSCC Contractor as part of access to the DCN.
- 7.2.20 The structured cabling shall be certified according to the latest applicable standards in this regard.
- 7.2.21 The structured cabling cables shall be compliant with (not limited to):
- CAT6A cables shall comply with IEC 61156-5 CAT6A.
 - CAT7A cables shall comply with IEC 61156-5 CAT7A.
 - Cables' flame retardancy shall comply with IEC 60332-1. Indoor cables shall withstand 120 minutes.
 - Cables shall be halogen-free (HFFR) and shall comply with IEC 60754-2.
 - Cables evaporated smoke density under burning conditions shall comply with IEC 61034.
 - CAT6A/CAT7A patch cords shall be shielded.
 - CAT6A/CAT7A patch cords shall be earthed and bonded.
 - RJ45 molded connectors shall comply with IEC 11801.
- 7.2.22 Regarding the terminating and interconnecting equipment of the structured cabling, it shall include (not limited to):
- termination protection devices.
 - distribution cabinets.
 - cross-connects.
 - cable trays and hangers.
 - CAT6A/CAT7A patch cords.
- 7.2.23 The core routers/switches shall be delivered with extra 50% spare ports with respect to the final number of active ports and supported bandwidth and shall be scalable by 50% more without changing supervisors, CPU's, power supplies, chassis (if modular design considered by the TSCC Contractor), etc.
- 7.2.24 The distribution routers/switches shall be delivered with an extra 50% spare ports with respect to the final number of active ports and supported bandwidth.
- 7.2.25 The access switches shall be delivered with an extra 50% spare ports with respect to the final number of active ports and supported bandwidth.
- 7.2.26 Equipment Interfaces shall operate under IP with Ethernet RJ-45 and fiber connections.
- 7.2.27 The TSCC Contractor shall provide technical racks to allocate all the equipment. Standard EIA 483 mm or ETSI compatible 19" racks at least 42U of height shall be installed and shall support both EIA-310 and OCP racks.
- 7.2.28 The NMS shall be based on COTS software and hardware (cloud, on-premises, or virtualized).
- 7.2.29 Any upgrade or intervention made on the NMS shall not impact the operational functioning of the network.



7.3 EMC Requirements

- 7.3.1 The DCN shall be fully immune and protected from any Electromagnetic Interference (EMI) with traction power, multi-tubular cabling, and Radio Frequency Interference (RFI). The EMI emissions shall be mitigated in accordance with applicable standards (EN 50122 or equivalent).



8 TOLERANCES

Not applicable to DCN System.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

- 9.1.1 The TSCC Contractor shall supply and deliver all components related to the DCN system scope of work, except where the Authority furnishes the main optical fiber cable to the TSCC Contractor.
- 9.1.2 The TSCC Contractor shall supply and deliver all passive components related to the optical fiber cable.

9.2 Specific Requirements

- 9.2.1 The DCN scope of supply and delivery shall include (not limited to):
- Network devices for backbone and LAN networks (routers, switches, etc.).
 - Cabling and connectors.
 - Racks.
 - Software architecture, including full definition of protocols used.
 - Network Management System for the DCN.
 - Central servers.
 - Workstations/HMIs.
 - All HW/SW licenses covering the duration of the Agreement.
 - Auxiliary elements and gear for DCN (connectors, patch panels, tools, etc.).
 - Spare parts.
 - Maintenance laptops.
- 9.2.2 The Optical fiber cable scope of supply and delivery shall include (not limited to):
- Optical Fiber cables (Except main FO furnished by the Authority).
 - Protection against impacts, crush, and rodents for FO, especially in the manholes and extract points.
 - FO management software solution.
 - FO measurements and testing equipment.
 - Auxiliary elements and gear for FO (including connectors, ODFs, patch panels, FO tools, FO blowing machines, etc.).
 - Optical fiber splice organizers.
 - Spare parts.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Contract.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in Schedule 16 Scope of Work and Schedule 3.



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in Schedule 16 Scope of Work and in Schedule 3.

12.2 Specific Requirements

12.2.1 Specifically, to check the condition of the optical fiber cables following splicing and connection, but before implementation of an optical link, optical tests and measurements shall be performed by the TSCC Contractor. Each fiber shall be fully tested (including spare ones) according to OTDR tests (Optical Time Domain Reflectometer). Testing shall comply with TIA/EIA-526-7 standard, and the following information (not limited to) shall be recorded and reported during the test procedure:

- Type of test equipment used (manufacturer, model, and serial number).
- Date of test.
- Date of last test equipment calibration.
- Optical source wavelength, spectral width, and for multi-mode, the coupled power ratio (CPR).
- Fiber identification.
- End point locations.
- Test direction.
- Reference power measurement (when not using a power meter with a Relative Power Measurement Mode).
- Measured attenuation of the link segment.
- The measurement curve shall be attached to the report.



13 SUBMITTALS

13.1 General Requirements

13.1.1 General submittal requirements are defined in Schedule 16 Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor and Supplier information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence DCN subsystem reliability, availability, and maintainability characteristics.



16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are specified in the Agreement.



Schedule 5(c)

Electronic Access Control System (EACS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0007 – Electronic Access Control System (EACS)

Rev. 0.0

A handwritten signature in black ink, appearing to read "Harshal".

Authored:

Harshal Jadhav, Telecom System Lead

23 December 2025

Date

A handwritten signature in black ink, appearing to read "Thomas".

Checked:

Thomas Newey, Telecoms Lead

12/23/2025

Date

A handwritten signature in black ink, appearing to read "Bruno".

Checked:

Bruno Comperat, Deputy Director of Rail Engineering

12/12/2025

Date

A handwritten signature in blue ink, appearing to read "Ryan Scott".

Approved:

Ryan Scott, Director of Rail Engineering

12/23/2025

Date

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Released:

Amit Joshi, Configuration Manager

12/23/2025

Date



Document Revision History – EACS Specifications**Second Edition****December 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition
1.0	December 2025	Second edition for Addendum 2



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION.....	5
2	REFERENCE STANDARDS AND DOCUMENTS	6
2.1	GENERAL	6
2.2	DESIGN GUIDELINES	6
2.3	TSI	6
2.4	STANDARDS	6
2.5	OTHER DOCUMENTS	7
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	8
3.1	TERMS, DEFINITIONS AND ABBREVIATIONS	8
4	SYSTEM DESCRIPTION	9
4.1	PURPOSE OF THE EACS	9
4.2	EACS SYSTEM DEFINITION	9
4.3	EACS SYSTEM OPERATIONAL CONTEXT.....	9
4.4	DESIGN LIFE	9
5	SYSTEM REQUIREMENTS.....	11
5.1	GENERAL REQUIREMENTS.....	11
5.2	ENVIRONMENTAL CONDITIONS REQUIREMENTS	12
5.3	OPERATIONAL REQUIREMENTS FOR EACS	13
5.4	FUNCTIONAL REQUIREMENTS FOR EACS	13
5.5	PERFORMANCE REQUIREMENTS FOR EACS	16
5.6	CYBERSECURITY AND SECURITY REQUIREMENTS.....	17
6	INTERFACES REQUIREMENTS	19
6.1	GENERAL REQUIREMENTS.....	19
6.2	EXTERNAL INTERFACE – STATIONS CONTRACTORS	19
6.3	EXTERNAL INTERFACE – FACILITIES CONTRACTORS.....	19
6.4	INTERNAL INTERFACE.....	20
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS.....	21
7.1	GENERAL REQUIREMENTS.....	21
7.2	SW AND HW REQUIREMENTS.....	21
7.3	EMC REQUIREMENTS.....	23
8	TOLERANCES.....	24
9	SCOPE OF SUPPLY AND DELIVERY	25
9.1	GENERAL REQUIREMENTS.....	25
9.2	SPECIFIC REQUIREMENTS	25
10	MANUFACTURING	26
10.1	GENERAL REQUIREMENTS.....	26
11	INSTALLATION AND INTEGRATION	27



11.1	GENERAL REQUIREMENTS.....	27
11.2	SYSTEM INTEGRATION REQUIREMENTS	27
12	TESTING & ACCEPTANCE	28
12.1	GENERAL REQUIREMENTS.....	28
12.2	SPECIFIC REQUIREMENTS	28
13	SUBMITTALS	29
13.1	GENERAL REQUIREMENTS.....	29
14	QUALITY MANAGEMENT	30
14.1	GENERAL REQUIREMENTS.....	30
15	ADDITIONAL INFORMATION REQUESTED	31
15.1	GENERAL REQUIREMENTS.....	31
16	LOGISTICS	32
16.1	GENERAL REQUIREMENTS.....	32



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Electronic Access Control System (EACS) system, hereinafter: EACS.
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of the EACS is presented in Appendix A.
 - **"Shall"**: Indicates a mandatory requirement that must be strictly implemented; a waiver from a mandatory requirement is permissible only with approval of a design variance.
 - **"Should"**: Indicates a preferred course of action; a design variance is not required if it is not exercised.
 - **"Must"**: Indicates an obligation or a mandatory requirement.
 - **"May"**: Indicates a permissible course of action within the limits of the standards; a design variance is not required if it is not exercised.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the standards, guidelines, and specifications provided in this chapter for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, and training.

2.2 Design Guidelines

- 2.2.1 The latest version of the following Design Guidelines shall be applied:

ID	Code	Title
[R1]	Design Criteria Manual	Chapter 5 – Safety and Security
[R2]	Design Criteria Manual	Chapter 12 – Communication Systems and Train Control
[R3]	Design Criteria Manual	Chapter 25 – Intrusion Detection
[R4]	AREMA Standards	Chapter 17 – High-Speed Rail Systems

TABLE 8 DESIGN GUIDELINES

2.3 TSI

- 2.3.1 Not applicable for the EACS

2.4 Standards

- 2.4.1 The TSCC Contractor shall fully take into account and apply the following standards.

ID	Code	Title
[R5]	TR 16705	Perimeter protection - Performance classification methodology
[R6]	EN300386	Telecommunication network equipment; Electromagnetic Compatibility (EMC) requirements; Harmonized Standard covering the essential requirements of the Directive 2014/30/EU
[R7]	EN 50121	Railway Applications – Electromagnetic Compatibility
[R8]	EN 50122-1	Railway applications - Fixed installations - Electrical safety, earthing and the return circuit - Part 1: Protective provisions against electric shock
[R9]	EN 50124	Railway Applications - Insulation Coordination
[R10]	EN 50125	Railway Applications - Environmental Conditions for Equipment
[R11]	EN 50130	Alarm systems. General requirements
[R12]	EN 50131	Alarm systems – Intrusion and hold-up systems
[R13]	EN 50133	Alarm systems - Access control systems for use in security applications
[R14]	EN 50136	Alarm systems - Alarm transmission systems and equipment



ID	Code	Title
[R15]	EN 50173	Information technology - Generic cabling systems
[R16]	EN 50174	Information technology - Cabling installation
[R17]	EN 50346	Information technology -Cabling installation -Testing of installed cabling
[R18]	EN 50398	Alarm systems - Combined and integrated alarm systems
[R19]	TR 50456	Alarm systems - Guidelines to achieving compliance with EC directives for equipment of alarm systems
[R20]	TR 50531	Alarm systems - Terms and definitions
[R21]	TS 50661	Alarm systems - External perimeter security systems
[R22]	EN 60839	Electronic access control systems
[R23]	IEC 61000	Electromagnetic compatibility (EMC)
[R24]	EN 61034	Measurement of smoke density of cables burning under defined conditions
[R25]	IEC 60529	Degrees of protection provided by enclosures (IP Code)
[R26]	IEC62443	Security for Industrial Automation and Control Systems
[R27]	ISO/IEC 27001	Information Security Management Systems requirements
[R28]	NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security
[R29]	NIST Cybersecurity Framework (CSF)	Framework for Improving Critical Infrastructure Cybersecurity
[R30]	NFPA 72	National Fire Alarm and Signaling Code
[R31]	NFPA 101	Life Safety Code
[R32]	ANSI/BHMA A156.1	Electromechanical locks and latches
[R33]	UL 294	Standard for Access Control System Units
[R34]	CBC 1604.10	California Building Code (CBC) § 1604.10 – Seismic design requirements for critical infrastructure
[R35]	CPUC General Orders & Safety Regulations	CPUC General Orders & Safety Regulations – California Public Utilities Commission requirements for railroad infrastructure
[R36]	FRA and FTA Regulations	Federal Railroad Administration and Federal Transit Administration rules
[R37]	FCC Part 15	EMC requirements for unintentional radiators
[R38]	California Public Records Act & CCPA	Transparency, privacy, and data-protection requirements

TABLE 9 LIST OF APPLICABLE STANDARDS

2.5 Other Documents

2.5.1 The following other documents shall be referred:



ID	Document	Title
[R39]	Schedule 16	Scope of Work
[R40]	Schedule 5(a) SPEC-0005	Cybersecurity specification
[R41]	Schedule 1	Safety, Security and RAM Requirements

TABLE 10 OTHER DOCUMENTS

3 TERMS, DEFINITIONS, AND ABBREVIATIONS

3.1 Terms, Definitions and Abbreviations

- 3.1.1 All the terms, definitions, and abbreviations are provided in schedule 5(t) – Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of the EACS

- 4.1.1 The TSCC Contractor shall supply an Electronic Access Control System (EACS) that provides centralized, secure, and auditable control of physical access to all CHSR-managed facilities and assets, supporting NFPA 72 and NFPA 101 life-safety egress requirements during emergency evacuations.
- 4.1.2 The TSCC Contractor shall supply the EACS to deter and detect unauthorized entry by combining credential-based authentication with intrusion detection and alarm management, in alignment with the CHSR Operational Concept Document.
- 4.1.3 The TSCC Contractor shall supply the EACS to deliver real-time monitoring and reporting of all access and intrusion events, enabling timely response to security incidents.
- 4.1.4 The TSCC Contractor shall supply the EACS to support peak-load scenarios—such as simultaneous badge presentations during shift changes—with credential-validation latency and event-throughput performance as defined in Section 5.5 of this document

4.2 EACS System Definition

- 4.2.1 The EACS is a networked security solution that provides centralized management, monitoring, intrusion detection, and control of physical access to CHSR infrastructure and facilities designated as EACS Protected Areas. The EACS comprises electronic locks, access control devices (e.g. RFID readers, keypads, biometric scanners), control panels, communication interfaces, and a central management platform. It authenticates personnel, logs all access events, generates alarms and integrates with security and operational systems to support asset protection, regulatory compliance, and safe railway operations.
- 4.2.2 The EACS shall be a state-of-the-art microprocessor-based, software-controlled automatic system with necessary programming functions, annunciation, self-test, and controls.

4.3 EACS System Operational Context

- 4.3.1 The TSCC Contractor shall supply the EACS to operate continuously, 24 hours per day, 7 days per week, across all CHSR facilities, including stations, depots, shelters, train control rooms, trackside cabinets, and control center—and to integrate with the CHSR Asset Management System for maintenance workflows.
- 4.3.2 The TSCC Contractor shall supply the EACS to enforce access policies autonomously at field controllers if central communications are interrupted, queuing all events locally for later synchronization.
- 4.3.3 The TSCC Contractor shall demonstrate the EACS's functionality through the following operational scenarios:
 - Routine Access: A valid credential presented at a field reader is authenticated by the local controller (even if offline), the door unlocks, and the event is logged centrally upon reconnection.
 - Tailgating Prevention: A second credential presented at a dual-reader portal without a corresponding egress event triggers a local alarm and immediate notification to the Security Operator console.
 - Emergency Evacuation: Upon receipt of a verified fire-alarm signal, the EACS automatically releases all egress doors, inhibits entry devices, and logs evacuation-mode activations in accordance with NFPA 101 and NFPA 72.
- 4.3.4 The TSCC Contractor shall supply the EACS to support phased roll-out and incremental commissioning, enabling new sites to be commissioned without impacting existing operations.
- 4.3.5 The TSCC Contractor shall supply integration details for other systems (e.g., Asset Management System, CCTV, Fire Protection) in Section 6 of this document.

4.4 Design Life

- 4.4.1 The design life for the EACS shall be 30 years.



- 4.4.2 The design life requirements of the EACS shall allow for the pertinent evolution and technological change of the EACS throughout its life to ensure it remains fit for purpose.
- 4.4.3 The TSCC Contractor shall ensure EACS components with shorter design lifespans shall be managed by scheduled technology refresh strategies and spares management plans.
- 4.4.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce EACS system components (with equal or compatible technical specifications) for the entire design life required.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

5.1.1 Scope of Contractor's Responsibility

- 5.1.1.1 The TSCC Contractor shall be responsible for all components, systems, interfaces, and activities necessary to fully design, deliver, integrate, test, and operationalize the EACS to the standard required for high-speed rail operations and for CHSR to enter revenue service. This includes design, procurement, sourcing, construction, installation, configuration, integration, verification, validation, training, documentation, operations, maintenance, and handover of all EACS subsystems, in accordance with this and other specifications, and subject to acceptance by the Authority.

5.1.2 Risk Assessment for Protected Areas

- 5.1.2.1 The TSCC Contractor shall perform an EACS Risk Assessment to identify all areas to be designated as EACS Protected Areas and define the appropriate level of protection for each based on local circumstances, hazards, and risk. The assessment shall, at a minimum, evaluate:

- Wayside access.
- Access to structures.
- Maintenance of Way Facilities and Sidings.
- Operations Control Facilities.
- Station Platforms.
- Equipment Cabinets and Shelters.
- Vehicle access.
- Pedestrian Access.
- Rolling Stock maintenance facilities.
- Access from neighbor, connected railroads, and facilities.

- 5.1.2.2 The TSCC Contractor shall submit the EACS Risk Assessment report to the Authority for review and approval prior to procurement.

5.1.3 Control & Monitoring Workstations

- 5.1.3.1 The TSCC Contractor shall use the Integrated Control and Supervision System (ICSS) Workstation as the primary console for all routine EACS control and real-time monitoring functions.
- 5.1.3.2 The TSCC Contractor shall ensure compatibility and integration of the EACS with the ICSS Workstation to provide the full feature set of control and monitoring functionality.
- 5.1.3.3 The TSCC Contractor shall supply a dedicated Administrative Workstation—physically and logically separated from ICSS and Security Operator consoles—through which O&M personnel may add, modify, or remove user accounts and credentials following defined, multi-level approval workflows.



5.1.4 Physical Access Control of Protected Areas

- 5.1.4.1 The TSCC Contractor shall lock and control, via the EACS, every access gate along the CHSR right-of-way, including maintenance-and-service personnel (pedestrian) and vehicular gates. The TSCC Contractor's EACS Risk Assessment shall cover all such gates and define appropriate protection levels.
- 5.1.4.2 The TSCC Contractor shall install the EACS at every designated EACS Protected Area to manage authorized access for routine operations, task-specific activities, and emergency egress.
- 5.1.4.3 The TSCC Contractor shall protect any system assets located off the right-of-way with EACS, in accordance with the approved risk assessment.
- 5.1.4.4 The TSCC Contractor shall equip each protected door, window, or opening within EACS Protected Areas with a surface-electromagnetic lock operated by the local EACS control unit.
- 5.1.4.5 The TSCC Contractor shall ensure all protected doors remain locked when not in use and are monitored by motion-and-request-to-exit sensor circuits that incorporate multiple sensing technologies (not solely passive infrared).
- 5.1.4.6 The TSCC Contractor shall deploy local EACS control units within each Protected Area, including OCC buildings, stations, depots, maintenance and train-care facilities, traction-power and solar sites, and wayside locations.

5.1.5 Power and data Resilience

- 5.1.5.1 The TSCC Contractor shall support each local EACS control unit with a battery backup sufficient for at least 30 minutes of continuous operation during a power outage and generate alarm notifications to the ICSS Operator when operating on backup.
- 5.1.5.2 The TSCC Contractor shall provide automatic data-backup functionality so that data and event logs are backed up before being overwritten. Log-file storage capacity shall cover at least one month of events, with a notification issued to the ICSS Operator when storage utilization reaches 90 percent.

5.1.6 Server Redundancy & Cybersecurity Compliance

- 5.1.6.1 The TSCC Contractor shall design all central servers with on-premises redundancy—whether physical, virtualized, or cloud-based—to facilitate system evolution and comply with cybersecurity requirements defined in Section 5.6 of this document and Schedule 5(a).

5.2 Environmental Conditions Requirements

5.2.1 Environmental Resilience

- 5.2.1.1 The TSCC Contractor shall design and supply the EACS to be resilient to the full range of local environmental and climatic conditions at each installation site, as defined in the CHSR Environmental Specification, including temperature extremes, solar exposure, humidity variations, and salt spray (where applicable).
- 5.2.1.2 The TSCC Contractor shall ensure all EACS equipment operates satisfactorily under normal usage conditions, including diurnal and seasonal fluctuations.

5.2.2 Ingress protection

- 5.2.2.1 The TSCC Contractor shall supply outdoor EACS enclosures with a minimum ingress-protection rating of IP66.
- 5.2.2.2 The TSCC Contractor shall supply any equipment directly exposed to weather—such as wayside controllers, readers, and sensors—with a minimum ingress-protection rating of IP67.

5.2.3 Mechanical Durability

- 5.2.3.1 The TSCC Contractor shall protect all EACS components from shock and vibration loads typical of the railway environment, in compliance with EN 50155, EN 61373, and the CHSR Environmental Specification.



- 5.2.3.2 The TSCC Contractor shall mount equipment on vibration-isolating hardware or include internal damping as required to maintain performance over the design life.

5.3 Operational Requirements for EACS

5.3.1 Operational Compliance

- 5.3.1.1 The TSCC Contractor shall ensure the EACS design fully complies with the CHSR Planned Operations schedule and the CHSR Operational Concept, enabling uninterrupted operation of the main line and all associated local facilities.

5.3.2 Operational Modes and Availability

- 5.3.2.1 The TSCC Contractor shall supply the EACS with configurable operational modes:

- Normal
- Off-Hours
- Lockdown
- Maintenance.

These modes can be triggered by schedule or by authorized operator command via the ICSS Workstation.

- 5.3.2.2 The TSCC Contractor shall ensure each operational mode transition occurs within 10 seconds of its trigger event, with all mode changes logged in the central server.

- 5.3.2.3 The TSCC Contractor shall support scheduled maintenance windows without degrading core EACS functions, allowing maintenance-mode activation at predefined times.

5.3.3 Remote Monitoring and Control

- 5.3.3.1 The TSCC Contractor shall provide remote monitoring and control capabilities via the ICSS Workstation, enabling authorized personnel to view system status, acknowledge alarms, and execute overrides from the operation center.

- 5.3.3.2 The TSCC Contractor shall ensure secure, low-latency connectivity (≤ 200 ms round-trip) between remote consoles and field controllers under normal network conditions.

5.3.4 Maintenance Access Support

- 5.3.4.1 The TSCC Contractor shall supply the EACS to facilitate maintenance access, allowing O&M personnel to enter Protected Areas in Maintenance Mode without triggering intrusion alarms, and shall automatically revert to the prior mode upon session timeout or manual exit.

- 5.3.4.2 The TSCC Contractor shall log all Maintenance Mode activations, including user identity, start/end times, and areas accessed.

5.3.5 Security Continuity and Failover

- 5.3.5.1 The TSCC Contractor shall design the EACS so that a failure of any single component—field controller, network link, or server—does not interrupt overall system operation, with automatic failover to redundant components in ≤ 5 s.

- 5.3.5.2 The TSCC Contractor shall provide documented procedures for manual intervention and recovery in the event of multiple concurrent failures or disaster scenarios.

5.4 Functional Requirements for EACS

5.4.1 General System Functions

- 5.4.1.1 The TSCC Contractor shall supply the EACS to timestamp all events and alarms using the CHSR Network Timing System.



- 5.4.1.2 The TSCC Contractor shall supply the EACS to detect and report the status (open/closed) of every protected door.
- 5.4.1.3 The TSCC Contractor shall supply the EACS to uniquely address and identify every sensor and device.
- 5.4.1.4 The TSCC Contractor shall supply the EACS to provide comprehensive reporting in multiple formats (Word, Excel, PDF) with user-defined filters. Example reports shall include, but not be limited to:
- **Daily Access Summary:** Total number of granted and denied entries per door, per credential type, and per user group.
 - **Unauthorized Access Log:** Detailed list of all access-denied events, forced-door activations, tailgating incidents, and tamper alarms.
 - **User Activity Report:** Individual credential usage history over a specified period, showing access times, locations, and authentication devices.
 - **Blacklist Report:** Current list of revoked, expired, or stolen credentials, including revocation timestamps and responsible administrator.
 - **Maintenance Mode Audit:** Record of all Maintenance Mode activations, including user identity, start/end times, and affected areas.
 - **Alarm Trend Analysis:** Aggregated alarm counts by severity and type, with time-series charts to identify hotspots and peak periods.
 - **User Provisioning & Deprovisioning Audit:** Monthly tally of user adds, moves, and drops, including special-role assignments (admins, emergency responders), to verify adherence to least-privilege principles.
 - **Credential Lifecycle Report:** Summary of credential enrolments, expirations, revocations, and role-based assignments over the past month, highlighting any abnormal spikes (e.g. mass expirations).
 - **Incident Response Activity Report:** Details of all security incidents simulated or real (e.g., tailgating events, forced-door alarms), response times, actions taken, and closure status.
 - **Configuration Change Log:** Chronological record of all approved configuration changes (who changed what, when, and why), tied back to the Change Request IDs and approval signatures.
- 5.4.1.5 The TSCC Contractor shall supply the EACS to notify the ICSS Operator of any loss or recovery of communications between local control units and the ICSS (including control-unit failures).
- 5.4.1.6 The TSCC Contractor shall supply the EACS so that, when in local maintenance mode, all other system functions remain fully operational.
- 5.4.1.7 The TSCC Contractor shall supply the EACS to provide comprehensive reporting—Access, Event, Activity, and Blacklist Reports—in multiple formats (Word, Excel, PDF) with user-defined filters.
- 5.4.1.8 The TSCC Contractor shall supply the EACS with an optional time-attendance module for selected doors, subject to the Authority's approval.
- 5.4.1.9 The TSCC Contractor shall supply central servers with fully redundant master/secondary configurations, ensuring automatic failover of the secondary server upon primary-server malfunction.
- 5.4.2 **Access Control Functions**
- 5.4.2.1 The TSCC Contractor shall supply the EACS to grant access to EACS Protected Areas only to authorized personnel.
- 5.4.2.2 The TSCC Contractor shall supply the EACS to restrict and deny access to unauthorized personnel.
- 5.4.2.3 The TSCC Contractor shall supply the EACS to monitor in real time all access attempts—both authorized and unauthorized—to EACS Protected Areas.
- 5.4.2.4 The TSCC Contractor shall supply the EACS to generate alarms for any unauthorized access attempts.



- 5.4.2.5 The TSCC Contractor shall supply the EACS to detect and report fraudulent access events, including forced-door openings, held-open doors, tampering, and credential-denied presentations.
- 5.4.2.6 The TSCC Contractor shall ensure each access-control event or alarm record includes:
- Date and time of the event
 - Event type
 - Event location
 - Credential or user reference
 - Authentication device used
 - Authorization result (and cause if denied)
 - Failure type (if applicable)
 - Alarm severity
 - Acknowledgement state.
- 5.4.2.7 The TSCC Contractor shall supply the EACS to log all personnel access to Protected Areas, including:
- Identity of the individual(s) gaining access
 - Relationship of the individual(s) to the equipment accessed
 - Identity of any person granting or escorting access, including third-party contractors
- 5.4.2.8 The TSCC Contractor shall supply the EACS so that, once authenticated, personnel must pass through the protected door within a configurable timeout; otherwise, the door shall re-lock.
- 5.4.2.9 The TSCC Contractor shall supply the EACS to provide manual override, lock, and unlock capabilities for protected doors, including scheduled override times.
- 5.4.2.10 The TSCC Contractor shall supply the EACS to continuously supervise lock and reader health and report any device failures.
- 5.4.2.11 The TSCC Contractor shall supply the EACS so that, in the event of a local control-unit failure:
- No new authentications are accepted
 - Controlled doors remain locked.
- 5.4.2.12 The TSCC Contractor shall supply the EACS so that, in the event of a power outage, local control units continue operating on battery backup for at least 30 minutes.
- 5.4.2.13 The TSCC Contractor shall supply the EACS so that, in the event of communications loss between readers and the local control unit, no new authentications are accepted.
- 5.4.2.14 The TSCC Contractor shall supply the EACS so that, in the event of a reader failure:
- Controlled doors remain locked
 - Other readers and functions are unaffected
- 5.4.2.15 The TSCC Contractor shall supply the EACS so that local control units automatically reconnect and upload locally logged events once normal communications resume.
- 5.4.2.16 The TSCC Contractor shall supply the EACS readers to automatically reconnect and forward buffered logs when communications are restored.
- 5.4.2.17 The TSCC Contractor shall supply each protected door with an emergency-door-release mechanism (inside the Protected Area) to manually unlock the door in case of emergency.
- 5.4.2.18 The TSCC Contractor shall supply each local control unit with sufficient I/O and reader ports to manage all protected doors within its Protected Area.
- 5.4.3 Intrusion Detection Functions**
- 5.4.3.1 The TSCC Contractor shall supply the EACS to monitor intrusion sensors within each Protected Area.



- 5.4.3.2 The TSCC Contractor shall supply the EACS to report any intrusion alarms in real time.
- 5.4.3.3 The TSCC Contractor shall supply the EACS to detect and alert on unauthorized attempts to breach doors, windows, fences, or interior motion—bookmarking events for OCC staff.
- 5.4.3.4 The TSCC Contractor shall ensure each intrusion event or alarm record includes:
- Date and time of the event
 - Event type
 - Event location
 - Sensor reference
 - Failure type (if applicable)
 - Alarm severity
 - Acknowledgement state
- 5.4.3.5 The TSCC Contractor shall supply the EACS so that intrusion-sensor inputs to local control units use dry contacts or I/O relays.

5.5 Performance Requirements for EACS

5.5.1 General Performance Requirements

- 5.5.1.1 The TSCC Contractor shall supply local EACS control units sized to manage the number of intrusion and access points determined by the approved EACS Risk Assessment for each facility type (OCC buildings, stations, depots, maintenance and train-care facilities, traction-power facilities and solar sites, wayside facilities, and related fenced areas).
- 5.5.1.2 The TSCC Contractor shall assess the proposed subsystem architecture and define a local-archiving retention period that meets the Authority's audit and operational needs and shall configure each local control unit to archive the requisite volume of events without data loss.
- 5.5.1.3 The TSCC Contractor shall supply credential-reader hardware and firmware such that the access-card response time does not exceed 300 ms, measured from card presentation in the reader field to the grant/deny indication.
- 5.5.1.4 The TSCC Contractor shall install and configure credential readers to reliably detect cards placed no more than 50 mm from the reader surface. The magnetic or mechanical door sensors shall operate correctly with an actual door-gap of 5 mm $\pm$ 2 mm.
- 5.5.1.5 The electromagnetic locks and strike plates shall be installed with an alignment tolerance of $\pm$ 2 mm in two axes to maintain proper holding force.

5.5.2 Peak Concurrency

- 5.5.2.1 The TSCC Contractor shall demonstrate support for at least 500 simultaneous badge presentations per station without performance degradation.

5.5.3 Event-Processing Throughput

- 5.5.3.1 The TSCC Contractor shall verify that the Central Server can sustain 1,000 events/sec for logging and alarm processing over a continuous 10-minute interval.

5.5.4 Local-Archive Capacity & RTO/RPO

- 5.5.4.1 The TSCC Contractor shall provision local-event storage for a minimum of 30 days at average peak event rates, and shall define and meet a Recovery Time Objective (RTO) of 1 hour and a Recovery Point Objective (RPO) of 15 minutes for local-archive restoration (covered in the TCS System Scope of Work Disaster Recovery Plan).

5.5.5 System-Health Monitoring Under Load



- 5.5.5.1 The TSCC Contractor shall supply health-monitoring metrics—including CPU, memory, and I/O utilization thresholds—for controllers and servers under full-load conditions, generating alarms if utilization exceeds 75 %.

5.5.6 Failover & Recovery Drills

- 5.5.6.1 The TSCC Contractor shall conduct quarterly failover and archive-recovery exercises to validate automatic switchover of control units and restoration of local archives, with reports submitted to the Authority.

5.5.7 Safety Requirements

- 5.5.7.1 The TSCC Contractor shall ensure the EACS design and implementation comply with all safety requirements defined in the System Safety Plan.

5.5.8 RAM Requirements

- 5.5.8.1 The TSCC Contractor shall supply the EACS to operate continuously, 24×7 throughout the CHSR operational service period, excluding planned maintenance windows where EACS maintenance is required. O&M procedures must define alternative arrangements for controlled access during those planned maintenance windows.

- 5.5.8.2 The TSCC Contractor shall put in place strategies to reduce the operational impact of EACS maintenance activities—such as patching, firmware updates, and system reboots—including but not limited to:

- Rolling-upgrade deployments on clustered servers and controllers to ensure continuous service.
- Hot-swap replacement of field controllers and reader modules using pre-configured spare units.
- Condition-based maintenance scheduling driven by real-time health monitoring to defer non-critical work until low-traffic periods.

- 5.5.8.3 The TSCC Contractor shall define and document fallback arrangements during EACS maintenance, such as:

- Local offline validation at field controllers with cached credential data to permit authorized access even if central servers are unavailable.
- Temporary mechanical override (e.g., secure break-glass keys) or pre-issued PIN codes for emergency egress or critical maintenance access.
- Alternate communication paths (e.g., secondary network links or cellular backup) for remote monitoring and remote patch orchestration.
- Manual access logs to be maintained by O&M staff and imported back into the EACS once normal operations resume.

- 5.5.8.4 The TSCC Contractor shall include these maintenance-impact mitigation strategies and fallback procedures in the Operations & Maintenance Manual and validate them during Site Acceptance Testing.

5.6 Cybersecurity and Security Requirements

5.6.1 General Requirement

- 5.6.1.1 The TSCC Contractor's EACS design shall be in full compliance with the Authority's cybersecurity policies and Cybersecurity Technical Specification.

5.6.2 EACS- Specific Security Controls

Unless otherwise specified in the Cybersecurity Technical Specification, the EACS shall additionally implement the following controls:

5.6.3 Encrypted Reader–Panel Communications:



- 5.6.3.1 All reader–controller links shall use a supervised protocol (e.g., OSDP Secure Channel v2 or equivalent), with session keys rotated at least daily.
- 5.6.4 **Network Encryption**
 - 5.6.4.1 All IP-based traffic (controllers↔servers, workstations↔servers, mobile-credential interfaces) shall employ TLS 1.3, with certificates issued and managed by the CHSR OT PKI in accordance with FIPS 140-2/ISO 27001.
- 5.6.5 **Credential Lifecycle Audit**
 - 5.6.5.1 All credential operations (enrollment, renewal, suspension, revocation) shall be logged in real time and forwarded in a standardized format (CEF or JSON) to the OT SIEM.
- 5.6.6 **Firmware Integrity**
 - 5.6.6.1 All firmware images for controllers, readers, and sensors shall be digitally signed; the system shall verify each signature before installation.
- 5.6.7 **Key Management**
 - 5.6.7.1 All cryptographic keys shall be generated, stored, and used within a FIPS 140-2 Level 2+ HSM (or equivalent), with at least annual key rotation and formal emergency-revocation procedures.
- 5.6.8 **Automated Isolation**
 - 5.6.8.1 Upon detection of a high-severity security event (e.g., panel compromise, credential theft), the EACS shall automatically isolate affected field controllers through configurable OT-zone firewall rules.
- 5.6.9 **Extended Log Retention**
 - 5.6.9.1 Audit-log retention shall meet or exceed the Cybersecurity Technical Specification, with access-control and intrusion logs retained for a minimum of three years per The Authority's Records Management Plan.
- 5.6.10 **Reporting and Assurance**
 - 5.6.10.1 The TSCC Contractor shall submit quarterly Security Assurance Reports for the EACS, detailing patch status, vulnerability-scan results, key-rotation logs, and incident metrics.
 - 5.6.10.2 The TSCC Contractor shall arrange an annual independent security audit—addressing encrypted channels, HSM usage, log integrity, and credential workflows—with findings and corrective-action plans delivered to the Authority.
- 5.6.11 **Integration with OT Cybersecurity Platform**
 - 5.6.11.1 The EACS shall forward all security events, system-health alarms, and audit logs to the CHSR OT cybersecurity platform over encrypted channels for correlation, alerting, and long-term archival.
 - 5.6.11.2 The EACS shall consume threat-intelligence feeds (e.g., blacklisted credential IDs, revoked certificates) via secure REST APIs and automatically quarantine or revoke affected credentials or panels.



6 INTERFACES REQUIREMENTS

6.1 General Requirements

6.1.1 Interfaces are classified as below:

- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR contractors);
- External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors);
- Internal interfaces between systems within the TSCC scope.

6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.

6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification. Third Partys Interfaces

6.2 External Interface – stations contractors

6.2.1 TSCC EACS equipment integration in stations

6.2.1.1 The TSCC Contractor shall provide to the station contractors:

- Equipment dimensions
- Equipment clearances requirements
- Equipment mounting and fixings requirements
- Cable routes/containment requirements
- Installation and maintenance requirements
- Electronics locks specifications
- Intrusion sensors type and location
- Control panel location

6.2.1.2 To be provided by the stations contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:

- Door locations and types
- Detailed plans and elevations indicating walls, fences, windows, and entry points
- Door frames
- Specific door dimensions and materials.

6.2.2 External Interface – facilities FPS system

6.2.2.1 EACS interfaces with the Fire Protection System (FPS) so that verified fire alarms automatically release locks on designated egress doors controlled by local EACS units.

6.3 External Interface – facilities contractors

6.3.1 EACS equipment integration in facilities

6.3.1.1 The TSCC Contractor shall provide to the facilities contractor:

- Equipment dimensions
- Equipment clearances requirements
- Equipment mounting and fixings requirements
- Cable routes/containment requirements



- Installation and maintenance requirements
- Electronics locks specifications
- Intrusion sensors type and location
- Control panel location

6.3.1.2 To be provided by the stations contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:

- Door locations and types
- Detailed plans and elevations indicating walls, fences, windows, and entry points
- Door frames
- Specific door dimensions and materials.

6.3.2 **External Interface – facilities FPS system**

6.3.2.1 EACS interfaces with the Fire Protection System (FPS) so that verified fire alarms automatically release locks on designated egress doors controlled by local EACS units.

6.4 Internal Interface

6.4.1 **Interface with Network Timing System (NTS)**

6.4.1.1 EACS shall have an interface to the Network Timing System (NTS) to retrieve a time reference for timestamping all events and logs.

6.4.2 **Interface with Digital Communications Network (DCN)**

6.4.2.1 EACS shall have an interface to the Digital Communications Network (DCN) to get connectivity.

6.4.3 **Interface with Integrated Control and Supervision System (ICSS)**

6.4.3.1 EACS shall interface with the ICSS to provide information related to access control and intrusion detection to the ICSS workstation.

6.4.3.2 EACS shall interface with the Fire Protection System (FPS) so that verified fire alarms automatically release locks on designated egress doors controlled by local EACS units.

6.4.4 **Interface with CCTV System**

6.4.4.1 EACS shall be interconnected with the CCTV System at the central level, and in case of unauthorized access or intrusion alarm, the video related to the area where such event is generated shall be highlighted to the Operator in the Station/OCC.

6.4.5 **Interface with traction substations and shelters**

6.4.5.1 The TSCC Contractor shall coordinate all EACS cabling routes with the approved cableway designs, providing pathway fill calculations, bend radii, and segregation from power circuits as required.

6.4.5.2 EACS shall interface to the Traction Substations and Shelter sites to ensure necessary space, environmental conditions, etc.

6.4.6 **Interface with Enterprise Asset Management Systems (EAMS)**

6.4.6.1 The EACS shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.

6.4.7 **Interface with Low Voltage Power System**

6.4.7.1 The EACS shall interface with an Uninterruptible Power Supply (UPS) to get the required power to feed the EACS System equipment.



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied by the TSCC Contractor shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards. Refer to 2.4.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the design life requirements.
- 7.1.3 The TSCC Contractor shall supply all power- and signal-distribution cabling as low-toxicity, low-smoke, zero-halogen, fire-retardant construction.
- 7.1.4 The EACS shall be complete with all equipment, supporting structures, hardware, licenses, software, cabling, and ancillary services which are useful for efficient operation of the EACS components. Such accessories and materials shall be deemed to be within the scope of this specification, whether specifically mentioned or not.
- 7.1.5 All special tools and test equipment intended for configuration of the EACS shall be deemed to be within the scope of this specification, whether specifically mentioned or not.

7.2 SW and HW Requirements

7.2.1 Hardware requirements

- 7.2.1.1 All cables shall be fire and flame retardant, halogen-free, non-corrosive, etc., in accordance with local applicable Laws.
- 7.2.1.2 Detailed cable routing and labelling plans shall be delivered by the TSCC Contractor.
- 7.2.1.3 The TSCC Contractor's design for all central servers shall be on-premises, either physical, virtualized, or cloud-based, to facilitate system evolution and comply with cybersecurity requirements.
- 7.2.1.4 Hardware, software, firmware, or data changes required to support future extensions or expansions on-line shall be accomplished without performance or functionality degradation or availability to the operational systems.
- 7.2.1.5 The structured cabling shall be certified according to the latest applicable standards in this regard.
- 7.2.1.6 The structured cabling cables shall be compliant with (not limited to):
 - CAT6A cables shall comply with IEC 61156-5 CAT6A.
 - CAT7A cables shall comply with IEC 61156-5 CAT7A.
 - Cables' flame retardancy shall comply with IEC 60332-1. Indoor cables shall withstand 120 minutes.
 - Cables shall be halogen-free (HFFR) and shall comply with IEC 60754-2.
 - Cables evaporated smoke density under burning conditions shall comply with IEC 61034.
 - CAT6A/CAT7A patch cords shall be shielded.
 - CAT6A/CAT7A patch cords shall be earthed and bonded.
 - RJ45 molded connectors shall comply with IEC 11801.
- 7.2.1.7 Regarding the terminating and interconnecting equipment of the structured cabling it shall include (not limited to):
 - termination protection devices
 - distribution cabinets
 - cross-connects
 - cable trays and hangers
 - CAT6A/CAT7A patch cords



- 7.2.1.8 Equipment Interfaces shall operate under IP with Ethernet RJ-45 and fiber connections.
- 7.2.1.9 LV electrical cables, control and communication cables for EACS shall be fire-rated.
- 7.2.1.10 The EACS equipment provided shall be expandable without requiring the replacement of existing equipment.
- 7.2.1.11 Hot-swappable elements, such as fans and power supplies, should be swappable without tools.

7.2.2 Software Requirements

- 7.2.2.1 The Operating of all the EACS devices shall be provided with the latest stable release.
- 7.2.2.2 All application software shall be upgraded to the latest stable release and shall support all the requirements specified. All software licenses shall be provided.
- 7.2.2.3 The EACS shall have an interface with the ICSS system (Integrated Control and Supervision System) for the functions dedicated to the control and monitoring of the EACS, i.e., Intrusion Detection, Access Control, and Archiving.
- 7.2.2.4 The TSCC Contractor shall provide the EACS software, which shall be a full-featured Security Management System software package.
- 7.2.2.5 The EACS software shall provide the administration function of the software, i.e., the creation, deletion, and configuration of accounts, sites, and Operators.
- 7.2.2.6 The EACS software configuration features shall gather all the functions dedicated to the creation and the configuration of the items related to the EACS: accounts, sites, schedules, readers, sensors, events archiving, dashboards, etc.
- 7.2.2.7 The EACS software shall provide an administration function for database management, including synchronization with local EACS control units and other functions such as edit, add, delete, search, sort, and print for EACS records and reports.
- 7.2.2.8 The EACS software shall be provided for the user administration responsible to ensure functionality related the user and user groups (for example, safety and security operator, head of security, IT administrator, users administrator, users, etc.) administration and management including levels of access rights by access location, time (day, time), user enrolment, user credentials (access cards, code keys, biometrics) management, i.e. their creation, configuration (including their credentials) or suspension; card personalization, etc.
- 7.2.2.9 User creation/suspension /deletion, modification of user credentials, activation/suspension /deactivation of the identification means associated with a user, and user profile assignment shall be performed at a central level.
- 7.2.2.10 EACS statuses (alarms and events) and modes of the EACS equipment shall be transmitted to the EACS software.
- 7.2.2.11 The EACS software shall display alarms and events in a list format and a graphical user interface (GUI), with the ability to export in multiple file types.
- 7.2.2.12 Control and monitoring of the EACS devices shall be provided (opening of EACS protected doors, arming or disarming an area, etc...) from the EACS software.
- 7.2.2.13 Control of the EACS device mode (operational, inhibition and maintenance) shall be provided from the EACS software.
- 7.2.2.14 Display of the operational status of any EACS device (in maintenance, inhibited, operational, out of service, etc.) shall be provided by the EACS software.
- 7.2.2.15 Display of the technical status of any EACS device (in service, isolated, in failure...) shall be provided by the EACS software.
- 7.2.2.16 Events archiving and reports yielding shall be provided by the EACS software.
- 7.2.2.17 Searching of the events or alarms history shall be ensured at least according to the following criteria:



- A credential reference or a group of credentials,
- A user or a group of users,
- An EACS Protected Area or a group of EACS Protected Areas,
- A type of event,
- A severity of alarm,
- An acknowledgement state of alarm,
- A cause of deny (for access control events),
- A time and date.

- 7.2.2.18 The Operator shall be able to release an EACS protected door (temporary/permanently) from the EACS software.
- 7.2.2.19 The Operator shall be able to lock an EACS protected door (temporarily/permanently) from the EACS software.
- 7.2.2.20 The Operator shall be able to visualize the technical status of the EACS equipment from the EACS software.
- 7.2.2.21 The Operator shall be able to visualize and change the operational mode of the EACS equipment from the EACS software.
- 7.2.2.22 The Operator shall be able to visualize and acknowledge EACS alarms from the EACS software.
- 7.2.2.23 The Operator shall be able to visualize the EACS Protected Area layout in at least four levels: room, floor, perimeter, and railroad section.
- 7.2.2.24 The Operator shall be able to remotely arm/disarm an EACS Protected Area (or group of Protected Areas) from the EACS software.
- 7.2.2.25 The Operator shall receive an alarm when the emergency door release mechanism, if any, has been used (emergency exit is activated) on the EACS software.
- 7.2.2.26 The Operator shall be able to re-arm the emergency door release mechanism, if any, to reactivate the door lock.
- 7.2.2.27 The quantity of users allowed by the EACS software shall be agreed with the Authority.

7.3 EMC Requirements

- 7.3.1 The TSCC Contractor shall supply all EACS equipment to be fully immune to and compliant with EMI/RFI requirements, per EN 50121-4 (railway electromagnetic compatibility) and FCC Part 15 for unintentional radiators.
- 7.3.2 The TSCC Contractor shall mitigate emissions and susceptibility through appropriate shielding, filtering, and grounding.



8 TOLERANCES

Not applicable to EACS.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

- 9.1.1 The TSCC Contractor shall supply and deliver all components related to the EACS System as per Schedule 16 Scope of Work.

9.2 Specific Requirements

- 9.2.1 The TSCC Contractor shall supply, deliver, and install all hardware, software, firmware, and ancillary items necessary to implement the complete EACS solution in accordance with this specification.
- 9.2.2 All supplied items shall be factory-new (unless otherwise agreed), fully compatible, factory-configured for plug-and-play deployment, and delivered with required licenses, certificates, and documentation.
- 9.2.3 The TSCC Contractor shall submit a detailed Bill of Materials for Authority review, covering quantities, part numbers, revisions, and supplier information, and shall update it to reflect any approved changes.
- 9.2.4 The EACS scope of supply and delivery shall include (not limited to):
- Central server(s) with database
 - Local EACS control units.
 - Software.
 - Smart cards.
 - Card reader
 - Combined authentication devices (biometric + card + code key).
 - Intrusion detection sensors (passive infrared, glass-break, vibration, door-position).
 - Request-to-exit push buttons.
 - Electromagnetic locks, strike plates.
 - Emergency Door Release mechanisms
 - Cabling and connectors.
 - Racks.
 - Full-featured Security Management System software suite, including Administration, Monitoring, Reporting, and Archiving modules
 - Software architecture documentation, including a full definition of protocols used.
 - Software licenses.
 - Auxiliary elements, supporting structures, special tools and test equipment.
 - Spare parts.
 - Maintenance laptops.
 - Dedicated Administrative workstation for user/credential management.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Contract.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in Schedule 16 and Schedule 3.

11.2 System Integration Requirements

- 11.2.1 The TSCC Contractor shall integrate local controllers, central servers, and workstations into the CHSR OT network, enforcing VLAN segmentation, mutual-TLS, and OSDP Secure Channel.
- 11.2.2 The TSCC Contractor shall configure time synchronization (NTP/PTP) so that all EACS devices maintain clock drift within ± 1 ms per 24 hours.
- 11.2.3 The TSCC Contractor shall import credential and user-group data via the Administrative Workstation, verify replication to all controllers within 5 minutes, and test login/logout workflows.
- 11.2.4 The TSCC Contractor shall integrate intrusion and access-control events with the ICSS Workstation, CCTV, Fire Protection, and OT SIEM, executing positive and negative test cases.
- 11.2.5 The TSCC Contractor shall implement tamper-detection and chain-of-custody procedures for cryptographic keys and HSM modules during installation, in line with the Cybersecurity Technical Specification.



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in Schedule 16 and in Schedule 3.

12.2 Specific Requirements

12.2.1 Failure event test cases, Interface test cases and the following information (not limited to) shall be recorded and reported during the test procedure:

- Power outage; aims to test the time duration of battery backup and the alarm raised. Also, the door functions during the battery backup period, and the door lock's release function after the battery backup period.
- Network communication lost between the EACS control unit and the authentication device failure; aims to test the door function (standalone mode).
- EACS control unit failure; aims to test the door function (standalone mode).
- Authentication device failure; aims to test the door lock's release function.

12.2.2 To ensure full coverage, the TSCC Contractor shall also include the following test categories, referencing the applicable sections of this specification:

- Environmental Stress Tests- Verify equipment operation at temperature, humidity, and ingress extremes.
- Performance Benchmarks- Credential-response latency and peak-load concurrency tests.
- Cybersecurity Validation- Vulnerability scans, penetration tests, and secure-channel verification.
- Interface Testing- End-to-end message-flow checks with NTS, DCN, FPS, CCTV, etc.



13 SUBMITTALS

13.1 General Requirements

13.1.1 General submittal requirements are defined in the Agreement and Schedule 16.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence EACS subsystem reliability, availability, and maintainability characteristics.



16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.



Schedule 5(d)

Enterprise Asset Management System (EAMS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0008 – Enterprise Asset Management System (EAMS)

Rev. 1.0

A handwritten signature in blue ink, appearing to read "V. Decanter".

Authored:

Vincent Decanter, TCS Engineer

12/22/2025

Date

A handwritten signature in black ink, appearing to read "Tom Newey".

Checked:

Thomas Newey, Telecom Lead

12/22/2025

Date

A handwritten signature in black ink, appearing to read "Bruno Comperat".

Checked:

Bruno Comperat, Deputy Director of Rail Engineering

12/23/2025

Date

A handwritten signature in blue ink, appearing to read "Ryan Scott".

Approved:

Ryan Scott, Director of Rail Engineering

12/23/2025

Date

Released:

12/23/2025





Amit Joshi, Configuration Manager

Date

Document Revision History – EAMS Specifications**Second Edition****December 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition
1.0	December 2025	Second edition for Addendum 2



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION	5
2	REFERENCE STANDARDS AND DOCUMENTS	6
2.1	GENERAL	6
2.2	STANDARDS	6
3	TERMS, DEFINITION, AND ABBREVIATION	7
4	SYSTEM DESCRIPTION	8
4.1	PURPOSE OF THE EAMS	8
4.2	EAMS DEFINITION.....	8
4.3	EAMS OPERATIONAL CONTEXT	8
4.4	DESIGN LIFE	9
5	SYSTEM REQUIREMENT	10
5.1	GENERAL REQUIREMENTS.....	10
5.2	ENVIRONMENTAL REQUIREMENTS.....	13
5.3	OPERATIONAL REQUIREMENTS	14
5.4	FUNCTIONAL REQUIREMENTS.....	15
5.5	PERFORMANCE REQUIREMENTS FOR EAMS.....	36
5.6	CYBERSECURITY AND SECURITY REQUIREMENTS.....	37
6	INTERFACE REQUIREMENTS	39
6.1	GENERAL REQUIREMENTS.....	39
6.2	THIRD PARTIES INTERFACES.....	41
6.3	EXTERNAL INTERFACES.....	41
6.4	INTERNAL INTERFACES.....	42
7	MATERIALS, PRODUCTS AND COMPONENTS REQUIREMENTS	46
7.1	GENERAL REQUIREMENTS.....	46
7.2	SOFTWARE AND HARDWARE SPECIFIC REQUIREMENTS.....	46
8	TOLERANCES	49
9	SCOPE OF SUPPLY AND DELIVERY	50
9.2	SPECIFIC REQUIREMENTS	50
10	MANUFACTURING.....	52
10.1	GENERAL REQUIREMENTS.....	52
11	INSTALLATION AND INTEGRATION.....	53
11.1	GENERAL REQUIREMENTS.....	53
12	TESTING, VALIDATION AND ACCEPTANCE	54
12.1	GENERAL REQUIREMENTS.....	54
12.2	SPECIFIC REQUIREMENTS FACTORY ACCEPTANCE TESTING (FAT).....	54



12.3	SPECIFIC REQUIREMENTS SITE ACCEPTANCE TESTING (SAT).....	54
12.4	SPECIFIC REQUIREMENTS PERFORMANCE BENCHMARK TESTING.....	54
12.5	SPECIFIC REQUIREMENTS CYBERSECURITY	55
13	SUBMITTALS.....	56
13.1	GENERAL REQUIREMENTS.....	56
14	QUALITY MANAGEMENT.....	57
14.1	GENERAL REQUIREMENTS.....	57
15	ADDITIONAL INFORMATION REQUESTED	58
15.1	GENERAL REQUIREMENTS.....	58
16	LOGISTICS	59
16.1	GENERAL REQUIREMENTS.....	59



1 INTRODUCTION

1.1 Scope of the technical specification

- 1.1.1 The scope of this Technical Specification is to define The Authority's Requirements for the Enterprise Asset Management System, hereinafter: **EAMS**.
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of the EAMS is presented in Appendix A.
- 1.1.4 The requirements are formulated using the following words and their meanings:
 - **"Shall"**: Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure).
 - **"Should"**: Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents.
 - **"Must"**: Indicates an obligation or a mandatory requirement.
 - **"May"**: Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines and specifications provided in this technical specification for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, training, operations and maintenance.
- 2.1.2 All generic standards to be used are provided in: Contract Technical Requirements – Scope of Work.

2.2 Standards

- 2.2.1 The TSCC Contractor shall fully consider and apply the following specific UIC Recommendations and Standards to be used for EAMS listed below.

ID	Code	Title
[R1]	UIC Railway Application Guide	Practical implementation of Asset Management through ISO 55001
[R2]	ISO 55000	Overview, principles and terminology for Asset Management Systems
[R3]	ISO 55001	Requirements for an Asset Management System
[R4]	ISO 55002	Guidelines for the application of ISO 55001
[R5]	Asset Inventory Guidance for Owners and Operators	Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators

TABLE 1 - LIST OF APPLICABLE STANDARDS

- 2.2.2 The EAMS shall support the California HSR program's alignment with ISO 55001 principles and UIC best practices for asset management. These principles include value realization, leadership and accountability, risk-based decision making, and continual improvement across the asset lifecycle. The EAMS shall also support The Authority's strategic asset objectives and enable evidence-based decision making.
- 2.2.3 In the event of any conflict, inconsistency, or ambiguity between the requirements set out in this specification and those in other applicable documents or standards, the resolution of such conflicts shall be determined by the Authority. The TSCC Contractor shall seek clarification in writing and shall not proceed on assumptions. The Authority's determination shall be final and binding



3 TERMS, DEFINITION, AND ABBREVIATION

- 3.1.1 All the terms, definitions, and abbreviations are provided in Schedule 5(t) SPEC-0024 – Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of the EAMS

- 4.1.1 The EAMS shall be a requirement-driven and standards-aligned solution whose aim is to effectively track and monitor the Authority's physical or digital assets across their entire lifecycle, in accordance with ISO 55001 principles (including asset value realization, risk-based decision making, and continual improvement), with appropriate configuration management processes.
- 4.1.2 The EAMS shall provide mechanisms to measure alignment between asset performance and organizational objectives, enabling data-driven governance and strategic asset planning.

4.2 EAMS Definition

- 4.2.1 The California High Speed Rail (CHSR) Authority's EAMS shall be a systematic management framework for the governance of the assets value, with the purpose of establishing the asset management plan and asset management objectives.
- 4.2.2 The EAMS shall apply to both tangible items that have potential or actual value, such as buildings, equipment or human resources, and intangible assets, such as digital twins, configuration baselines, human capital, intellectual property, goodwill, financial assets, or software licenses.
- 4.2.3 Intangible assets (e.g., configuration baselines, software licenses, digital twins, human capital) shall be modeled as metadata entries or linked data objects, integrated with relevant systems such:
- Building Information Model (BIM)
 - Geographic Information System (GIS)
 - Electronic Document Management System (EDMS)
 - Enterprise Resource Planning (ERP)
 - Traffic Management System (TMS)
 - Integrated Control and Supervision System (ICSS)
 - Power SCADA System
 - Monitoring and configuration systems of the various CHSR systems
 - Building Management Systems
 - HR platforms
 - Cybersecurity systems
 - Financial systems
- 4.2.4 The EAMS shall support the setting and monitoring of asset management objectives, risk-based decision support, and continual improvement, as part of the CHSR's broader asset management plan framework.
- 4.2.5 The internal processes and activities conducted within the EAMS shall be associated with the organizational strategy, relying on the entire organization, regardless of the hierarchy level.
- 4.2.6 The EAMS shall identify and maintain the relationships between assets and their associated documentation, configurations, version history, and dependency structures, particularly for modular or software-intensive systems.

4.3 EAMS Operational Context

- 4.3.1 The EAMS shall be used by multiple stakeholders across the CHSR program, including but not limited to those involved in asset governance, planning, operations, and lifecycle management.



- 4.3.2 EAMS shall provide the ability to manage assets in such a way that they contribute to the successful operation of CHSR, by delivering the expected level of operational performance reliably, efficiently, and sustainably. The main EAMS stakeholders are the operators and maintenance staff.
- 4.3.3 The EAMS shall support secure, role-based interaction across all relevant stakeholders, including operators, maintenance contractors, the Authority, suppliers, and the wider supply chain.
- 4.3.4 The EAMS architecture shall be designed with clearly defined functional boundaries and responsibilities for data ownership and exchange with adjacent systems. These definitions shall include documented integration mechanisms, and interface specifications.
- 4.3.5 The EAMS shall define and document its functional boundaries relative to external systems.
- 4.3.6 The EAMS shall include multi-role support with configurable user access levels, ensuring that operators, maintenance contractors, and the Authority have appropriate permissions and role-based workflows. Generic or shared user accounts shall not be permitted; each user shall authenticate using unique credentials and be granted the minimum necessary privileges. Access control measures shall be implemented in full compliance with the *TSCC System Technical Specification - Cybersecurity*.

4.4 Design Life

- 4.4.1 The Design Life requirements of the Asset Management System shall be 15 years, aligned with the lifecycle expectations of California HSR infrastructure systems
- 4.4.2 The TSCC Contractor shall ensure that the manufacturers shall be able to supply EAMS components with equal or better technical specifications, throughout the required operational lifetime, recognizing the potential for successive generations and evolving sensor technology.
- 4.4.3 The EAMS design shall include a long-term support and evolution roadmap, demonstrating how hardware and software components will be maintained, upgraded, or replaced over the design life. This shall include:
- Plans for ongoing software and hardware support, data continuity, backward compatibility, and migration paths
 - Scheduled refresh strategies and spares management plans for components with shorter inherent lifespans (e.g., field devices, handhelds)
 - The ability to integrate any replacement components with equal or better technical specifications elements into the existing EAMS architecture and dependent subsystems without requiring modifications aside from the item being replaced.
- 4.4.4 The design life shall be supported through a combination of hardware refresh planning, software version upgradeability, vendor support agreements, obsolescence management, and data migration strategies. Static system configurations shall not be assumed beyond five years without formal review and validation by the Authority.
- 4.4.5 The TSCC Contractor shall ensure that software and data formats remain interoperable with future technologies and shall provide backward compatibility or migration tools as part of system upgrades.
- 4.4.6 End-of-life planning shall be incorporated into the EAMS architecture, including secure data archiving, handover protocols, and licensing continuity provisions.



5 SYSTEM REQUIREMENT

5.1 General Requirements

- 5.1.1 The Enterprise Asset Management System shall be designed in accordance with the requirements described in this specification, and other relevant documents listed in Section 2 and the Scope of Work.
- 5.1.2 The EAMS architecture shall be designed to support maintenance, repair workflows, decision-making, data analysis, system resilience, scalability and to manage costs. The TSCC Contractor shall ensure that the EAMS is properly integrated with all CHSR systems.
- 5.1.3 The EAMS shall be available in English. Multilingual support, including Spanish, should be considered based on operational and regulatory requirements defined by the Authority.
- 5.1.4 The EAMS software shall be tailored to workflow specified in *Figure 1*. The process shall be reviewed, developed, and improved to enhance the EAMS performance over time. Workflow configurations shall be customizable, version-controlled, and traceable within the EAMS to support lifecycle assurance, auditability, and maintainability.

Note: Data Driven maintenance the EAMS workflow main stages shall be defined and developed as illustrated in *Figure 1*.

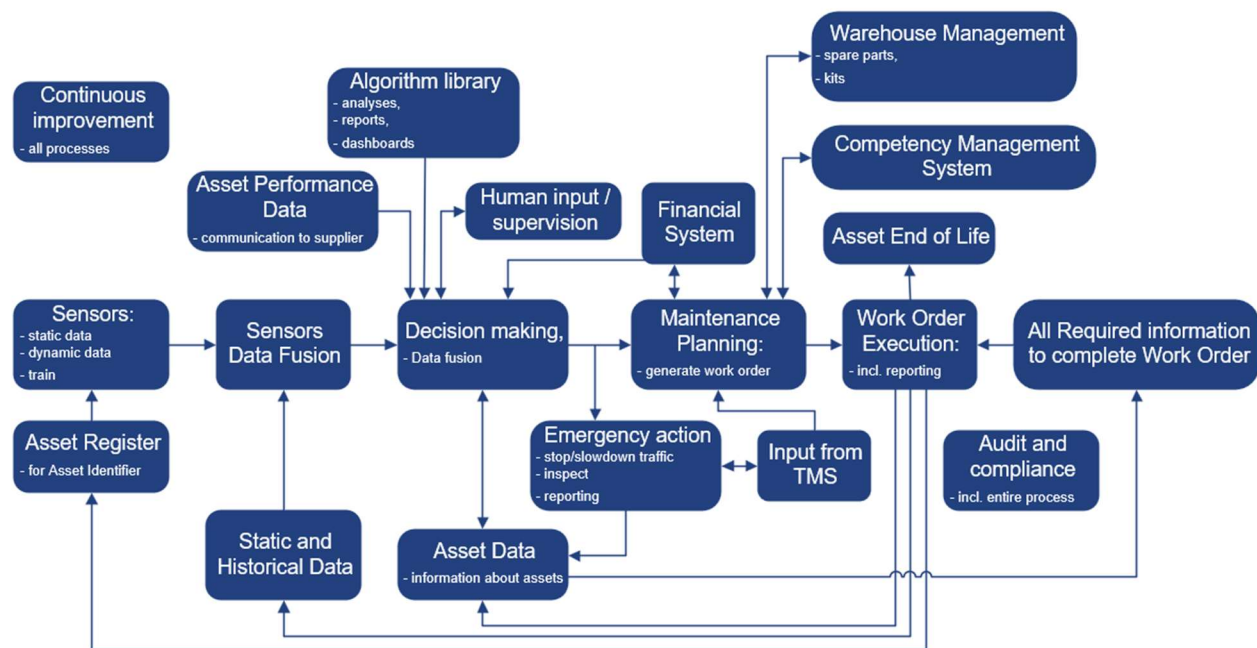


FIGURE 1 - EAMS DATA EXCHANGE WORKFLOW DIAGRAM

5.1.5 Data Collection:

5.1.5.1 Sensors shall provide:

- Static Asset Information data (GIS, etc.),
- Dynamic Asset Information data,
- Train data.

5.1.6 Sensors Data Fusion



5.1.6.1 The EAMS shall integrate static, historical, and real-time sensor data for analysis and contextualization.

5.1.7 Decision-Making

5.1.7.1 The EAMS shall support decision-making using:

- Fused sensor data,
- Algorithms and analysis libraries,
- Asset and performance data (including supplier information),
- Financial system inputs (e.g., lifecycle cost),
- **Human-in-the-loop oversight and validation.**

5.1.8 Maintenance Task Planning

5.1.8.1 The EAMS shall generate work orders based on decisions and financial data.

5.1.9 Work Order Execution and Reporting

5.1.9.1 Scheduled tasks shall be executed and reported. Asset data shall be used to complete and log work orders, including potential lifecycle impacts

5.1.10 Asset Register

5.1.10.1 The EAMS shall maintain an authoritative asset identifier register.

5.1.10.2 No constraints shall be imposed on data ownership, schema access, or protocol use by the TSCC Contractor or any system supplier.

5.1.11 All data ingested by the EAMS shall be validated for format, schema, source, and timestamp accuracy. Invalid or duplicate records shall be flagged for inspection or rejected by the system.

5.1.12 All ingested or generated data shall include metadata (e.g., source ID, timestamp, version ID) to support traceability, audit logging, and change history across the asset lifecycle.

5.1.13 Communication Protocols

5.1.13.1 The protocols used for data exchange shall be fully documented, including schema definitions. Documentation shall be provided in both human- and machine-readable formats.

5.1.13.2 The implemented protocols shall include, at a minimum:

- Message namespace definitions,
- Version control schemes,
- Sensor node status messages,
- Change-of-state messaging (e.g., value, event, threshold breach notifications).

5.1.13.3 The EAMS **shall** support seamless integration through a defined set of communication protocols. Other open protocols **may** be proposed with justification. Protocols **shall** be categorized as either:

- **Primary protocols** for system-wide interaction, or
- **Secondary protocols** for use within subsystems.

5.1.13.4 EAMS primary protocols are used for system-wide interaction and integration. These shall include, but are not limited to:

- OPC Unified Architecture (OPC UA)



- MQTT and MQTT Sparkplug
- EULYNX.

5.1.13.5 EAMS secondary protocols are used only within specific subsystems. These shall include, but are not limited to:

- IEC 60870-5
- IEC 61850
- SNMP V3
- BACnet
- Profibus
- Profinet
- Profisafe.

5.1.13.6 Other open protocols may be proposed by the TSCC Contractor, subject to approval by the Authority. Proposed protocols shall comply with the open standard requirements defined in **Clause 5.1.23**.

5.1.13.7 The EAMS shall support a wide range of network types and connections, including 5G FRMCS private networks, without technical limitations on expansion or integration.

5.1.13.8 The selected protocols shall comply with the TSCC System Technical Specification -Cybersecurity, including authentication, authorization, and encryption of all external interfaces.

5.1.13.9 Open standard shall not include proprietary or undocumented protocol.

5.1.13.10 The protocol implementations shall be documented in both human and machine-readable formats and delivered with test articles.

5.1.13.11 Ingested data shall be processed through a streaming data pipeline that correlates and consolidates event information across subsystems to support unified user interfaces, analytics, and lifecycle intelligence.

5.1.13.12 Any protocol suggested shall be based on a public open specification (e.g., EN, ISO, IETF RFC) or another unencumbered and publicly available standard accepted by the Authority.

5.1.13.13 The EAMS shall be modular and scalable, allowing additional assets, data sources, or subsystems to be integrated without fundamental redesign. This includes support for containerization, microservices, and distributed deployments.

5.1.13.14 The EAMS shall maintain versioning and lifecycle support for protocols, APIs, and integration modules. Deprecated protocols shall be phased out in coordination with the Authority and with backward compatibility maintained as needed.

5.1.13.15 The EAMS shall support an extensible network architecture, with no imposed constraints on physical or logical connections. This shall include compatibility with high-bandwidth, low-latency platforms such as private 5G (FRMCS) networks and modern edge-based telemetry platforms.

5.1.14 Asset Information

5.1.14.1 The EAMS shall process the following types of dynamic Asset Information at a minimum:

- Alarm data (tag, timestamp, severity, description)
- Event data (equipment ID, location, priority, date/time, type)
- Operational metrics (cycle counts, runtime, energy usage, voltage/load levels).



- 5.1.14.2 The EAMS shall provide dashboards and reports on performance metrics such as uptime, response time, integration status, and data freshness, supporting SLA monitoring and operational diagnostics.
- 5.1.14.3 The EAMS shall provide user-configurable functions to filter, prioritize, and escalate alarms, enabling operators to automatically trigger service requests for specified asset classes or alarm types.
- 5.1.14.4 The EAMS shall update usage and operational metrics for all relevant assets and subassemblies.
- 5.1.14.5 The EAMS shall also be capable of transmitting relevant operational status data (e.g., maintenance status, asset availability) to maintain synchronization.

5.2 Environmental Requirements

- 5.2.1 The EAMS equipment shall meet the environmental requirements defined in Section 7 and any applicable standards listed in Section 2, including IEC 60068 for environmental testing, and local regulatory requirements applicable to railway infrastructure in California.
- 5.2.2 The EAMS hardware (including servers, workstations, network devices, and field equipment) shall comply with defined environmental performance parameters including, but not limited to:
 - Operating temperature range: –20°C to +55°C (unless otherwise specified by installation location)
 - Storage temperature: –40°C to +70°C
 - Relative humidity tolerance: 5% to 95% non-condensing
 - Vibration resistance compliant with IEC 61373
 - Shock resistance and mechanical durability for mobile/portable devices.
- 5.2.3 All EAMS equipment intended for outdoor or harsh environments shall have a minimum ingress protection rating of IP65 (per IEC 60529), and enclosures shall be resistant to dust, moisture, corrosion, and UV exposure.
- 5.2.4 EAMS components installed in passenger-accessible or safety-critical areas shall comply with EN 45545-2 fire protection standards, including limits on flammability, smoke emission, and toxicity of fumes.
- 5.2.5 The TSCC Contractor shall categorize EAMS hardware by installation environment (e.g., OCC, wayside, on-vehicle, depot, mobile/field) and apply environmental requirements accordingly, subject to review and approval by the Authority.
- 5.2.6 All EAMS devices and infrastructures shall maintain performance during its design life under defined environmental conditions, including resistance to thermal cycling, condensation, and vibration fatigue.
- 5.2.7 All EAMS hardware and associated components shall comply with environmental sustainability directives, including RoHS (Restriction of Hazardous Substances) and WEEE (Waste Electrical and Electronic Equipment) where applicable.
- 5.2.8 All EAMS-related equipment, including servers, handheld devices, network hardware, and embedded systems, shall comply with Electromagnetic Compatibility (EMC) requirements and meet the environmental requirements defined in Section 5.2. Compliance shall be demonstrated in accordance with applicable standards, including but not limited to:
 - IEC 61000-6-2 (Immunity for industrial environments)
 - IEC 61000-6-4 (Emission for industrial environments)
 - EN 50121 series (Railway applications – EMC)
 - FCC Part 15, Subpart B (for digital devices in the United States).



EMC compliance shall be validated by testing conducted at accredited laboratories and shall be documented in compliance reports submitted to The Authority prior to commissioning.

- 5.2.9 All EAMS hardware components, including third-party integrations, shall conform to both emissions and immunity standards applicable to their installation environment (e.g., OCC, field cabinets, trainsets interfaces).
- 5.2.10 Where multiple standards apply (e.g., FCC and EN 50121), the more stringent requirement shall prevail unless otherwise agreed with The Authority.
- 5.2.11 The TSCC Contractor shall provide evidence of EMC compliance via certified lab test reports and declarations of conformity. Testing shall include both conducted and radiated emissions and immunity, verified under representative operating conditions.

5.3 Operational Requirements

- 5.3.1 The TSCC Contractor shall provide or support a maintenance organization, incorporating all required elements to enable condition-based and predictive maintenance strategies using EAMS data and workflows.
- 5.3.2 The TSCC Contractor shall determine the required EAMS capacity, and performance parameters, based on defined maintenance processes and system load expectations (e.g. number of assets, sensor inputs per second, user sessions, storage requirements). These capacity requirements shall be validated against the predictive maintenance strategy and future expansion scenarios.
- 5.3.3 The EAMS shall support continuous 24/7 operation and enable timely execution of all core system functions without degradation.
- 5.3.4 The TSCC Contractor shall define and implement the necessary redundancy, failover, and disaster recovery (DR) mechanisms—covering Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)—to satisfy these targets.
- 5.3.5 The EAMS shall minimize manual data entry by integrating data from sensors, Internal Interfaces, External Interfaces, and structured external sources. Where manual input is necessary, field validation and error reduction techniques shall be applied.
- 5.3.6 The EAMS shall include a monitoring dashboard displaying system status, uptime, data flows, fault conditions, integration status, and performance KPIs. The system shall support automated alerts and logs to assist operators in fault detection and recovery.
- 5.3.7 The EAMS shall integrate with existing support systems, including the IT Service Desk, and field maintenance teams. A clearly defined incident response and escalation procedure shall be documented for EAMS-related faults or failures.
- 5.3.8 The TSCC Contractor shall perform usability testing with representative users during HMI development to validate interface design, task efficiency, accessibility, and overall user experience.
- 5.3.9 The EAMS shall provide role-based HMI views and configurable dashboards tailored to different user profiles (e.g. maintenance engineer, operator, asset manager), with appropriate access controls as per the *TSCC System Technical Specification - Cybersecurity*.
- 5.3.10 The EAMS user interface (HMI) shall be designed in accordance with ISO 9241-210:2019 Ergonomics of human-system interaction, ensuring usability, efficiency, and accessibility. The interface shall comply with WCAG 2.1 Level AA accessibility standards and adopt best practices from the U.S. Web Design System



(USWDS) where applicable. The design shall prioritize intuitive navigation, minimal interaction steps, responsive layout across devices, and support for user role customization.

5.4 Functional Requirements

5.4.1 General Requirements

- 5.4.1.1 The EAMS shall embed a customizable logic and calculation engine, based on proven solutions from other railway projects. This engine shall support the configuration of user-defined rules, formulas, diagnostic workflows, and asset-specific models, enabling the development of:
- Specialized condition and performance monitoring logic
 - Tools aligned with RAM (Reliability, Availability, Maintainability), RCM (Reliability-Centred Maintenance), FRACAS ((Failure Reporting, Analysis, and Corrective Action System), and lifecycle cost models.
- 5.4.1.2 A web-based HMI solution shall be implemented using scalable, standards-based web technologies (e.g. HTML5, RESTful APIs, JSON). Web servers shall host modular clients optimized for browser compatibility, responsive design, and centralized administration.
- 5.4.1.3 The EAMS shall support all required protocols for integration with alarm, telemetry, condition monitoring, and operational datasets across CHSR systems and third-party systems. It shall handle both real-time and historical data sources, with built-in support for timestamp validation, schema conformity, buffering, and event prioritization.
- 5.4.1.4 The EAMS shall allow authorized users to configure, test, and validate logical rules and workflows in a secure sandbox or test environment before production deployment. This environment shall support simulation with sample asset data.
- 5.4.1.5 All user-defined logic, dashboards, and HMI (Human Machine Interface) configurations shall be version-controlled and include audit logs for changes. Changes shall require approval or validation workflows defined by the Authority.
- 5.4.1.6 The EAMS HMI shall be accessible on desktops, tablets, and ruggedized field devices, and shall offer configurable role-based views for maintenance personnel, operators, engineers, and administrators.
- 5.4.1.7 The EAMS shall include Application Programming Interfaces (APIs) and plug-in frameworks to allow future extension of system functions, analytics, and third-party integrations. The API documentation shall be published, version-controlled, and accessible via a developer portal or equivalent interface.
- 5.4.1.8 The EAMS shall provide detailed system and data ingestion logs, including protocol status, data quality issues, event drops, and latency metrics. These logs shall be available for analysis, alerting, and troubleshooting.

5.4.2 EAMS Data Store

- 5.4.2.1 The EAMS Data Store shall be an organized, scalable, and secure collection of structured data and documentation for all CHRS assets.
- 5.4.2.2 The EAMS Data Store shall track, organize, and maintain asset-related information throughout the lifecycle, from acquisition and commissioning to decommissioning and disposal.
- 5.4.2.3 The EAMS Data Store shall ensure high-quality, highly available Asset Information to support performance, safety, maintenance, and analytical operations across all functional areas of the California High-Speed Rail system.



- 5.4.2.4 Each asset shall be assigned a unique identifier by the Asset Register. The EAMS shall interface with the Asset Register through a secure and synchronized API or data exchange process, ensuring up-to-date and consistent asset IDs and Asset Information.
- 5.4.2.5 The EAMS shall incorporate and organize all CHSR assets in a structure identical to the System Breakdown Structure (PBS) and corresponding maintenance plans, from the top system level to individual components.
- 5.4.2.6 Asset Information data structures and metadata models shall be standardized across asset types to enable consistent reporting, lifecycle analysis, and decision support across all EAMS modules.
- 5.4.2.7 The EAMS shall support import and export of structured data using formats compatible with commonly used text, presentation, and analytics software (e.g. CSV, XML, JSON, Excel, PDF).
- 5.4.2.8 The TSCC Contractor shall ensure real-time and batch-mode integration of the EAMS Data Store with CHSR systems, including support for automated data validation and error handling.
- 5.4.2.9 The EAMS Data Store shall include, but not be limited to, the following content types:
- Spare parts catalogues
 - Product acceptance certificates
 - As-built drawings and BIM models (linked to GIS)
 - Direct linkages to California HSR GIS System
 - RAM, RCM and FMEA
 - Maintenance and repair history
 - Installation and O&M manuals
 - System identifiers
 - Related documentation required for asset governance, operations, and assurance.
- 5.4.2.10 The EAMS Data Store shall retain and generate asset-related reports, including automatic and scheduled reports. The system shall support time-based queries and enable users to retrieve historic reports based on asset ID, report type, or time range.
- 5.4.2.11 All real-time and historical data shall be logically structured by asset and stored in a way that enables analysis at system, subsystem, or component levels. Data ingestion shall be timestamped and source tracked.
- 5.4.2.12 Information maintained in the EAMS Data Store shall include, but not be limited to:
- Static Asset Information Metadata, such as:
 - Unique asset ID
 - Asset type and classification
 - Asset name and description
 - Manufacturer and model
 - Serial number
 - Technical specifications
 - Acquisition date and cost
 - Warranty or guarantee terms
 - Asset condition/status (e.g., active, under repair, retired)
 - Physical location (coordinates, section ID, facility name)
 - Ownership and custodian information



Lifecycle stage (e.g., installed, commissioned, decommissioned)
Maintenance records,
Work orders and task assignments,
Integration-related data (APIs, mappings),
Inventory and procurement data,
Asset tracking and location history,
Documentation (manuals, images, certificates),

- Dynamic Asset Information data
 - Real-time sensor and condition monitoring data,
 - User access logs and audit records,
 - Security-related events and metadata,
- Reports and analysis,
- Risk and compliance records,
- Data schemas and definitions for consistency.

- 5.4.2.13 The EAMS shall utilize a combination of relational, time-series, and unstructured data storage technologies, chosen based on the nature of the data (e.g., operational telemetry, documents, logs, structured records).
- 5.4.2.14 The EAMS Data Store shall include configurable data retention policies based on asset type, criticality, and regulatory requirements. These policies shall support both short-term operational use and long-term archiving (e.g., 25–30 years for critical infrastructure records).
- 5.4.2.15 The EAMS Data Store shall implement routine, automated backup and recovery mechanisms, with clearly defined recovery time objectives (RTO) and recovery point objectives (RPO). Backup status shall be monitored, and failures reported to operations teams.
- 5.4.2.16 The EAMS shall support tamper detection, version control, and cryptographic integrity checks (e.g., checksums, hash validation) for all stored data and documents. All changes shall be audit-logged and traceable.
- 5.4.2.17 The EAMS shall maintain bi-directional synchronization with external authoritative systems (e.g., GIS, Asset Register, EDMS) and resolve discrepancies using configurable reconciliation rules. Changes shall not result in silent data overwrites.
- 5.4.2.18 The EAMS Data Store shall be designed for performance at scale, supporting high-volume concurrent queries, indexing, and low-latency access for real-time data ingestion and dashboard displays.

5.4.3 Data Acquisition and Categorization

- 5.4.3.1 The EAMS shall acquire and integrate structured and unstructured data not only from subsystems but also from all CHSR assets as illustrated in Figure 2. The EAMS shall support multiple ingestion modes including real-time streaming, scheduled batch uploads, and API-based pull mechanisms. Integration security shall comply with the TSCC System Technical Specification - Cybersecurity.
- 5.4.3.2 The EAMS shall receive structured notifications from connected systems to generate dynamic Asset Information and alerts, with each notification containing, at a minimum:
- A unique registration number generated by EAMS or inherited from the source system
 - Status (e.g., created, enriched, closed)
 - Identification of the originating system (name or ID)
 - A full timestamp (date, hour, minutes, and seconds)



- A description of the alert (preformatted where possible)
- Cause of degradation or failure (coded where available, free text only as fallback)
- Event or metric that triggered the alert
- State of the system before alert generation
- Linked media or data (e.g., photos, videos, raw sensor data)
- Notification settings (e.g., priority, user assignment)
- Associated supply chain events or disruptions.

5.4.3.3 The EAMS shall process alerts and notifications from monitoring systems into structured records used to drive data mining routines, asset diagnostics, and predictive maintenance models. Data source authentication, event logging, and ingest validation shall align with the *TSCC System Technical Specification - Cybersecurity*.

5.4.3.4 EAMS-generated reports and outputs shall include the following, at a minimum:

- Metrics (sensor values, KPIs),
- Status updates,
- Associated multimedia (photos, videos),
- Raw maintenance or inspection data,
- Links to external media storage or embedded attachments.

5.4.3.5 The EAMS shall be capable of querying asset telemetry and performance indicators, such as energy consumption, uptime, cycle counts, and temperature, from all connected systems using defined protocols.

5.4.3.6 The EAMS shall classify and structure assets according to the PBS (Product Breakdown Structure), ensuring consistent tagging and archiving across all asset types and lifecycle phases.

5.4.3.7 During physical asset data acquisition, the EAMS shall apply AutoID principles (e.g., RFID, barcodes, QR codes) where it is practical to minimize manual input, reduce errors, and support accurate traceability.

5.4.3.8 The EAMS shall distinguish between real-time, near-real-time, and historical data, with support for configurable thresholds, time-windowed data retention, and alert suppression rules based on operational context.

5.4.3.9 All inbound data shall be authenticated, validated, and subject to integrity checks, including source identity verification, timestamp validation, and schema conformance. Integration must comply with the *TSCC System Technical Specification - Cybersecurity*.

5.4.3.10 The EAMS shall normalize data received from external systems, translating units, terminology, and status codes into standardized formats using configurable mapping logic or a harmonization engine.

5.4.3.11 Where structured codes exist (e.g., for cause of failure, degradation type), the EAMS shall use controlled vocabularies. Free-text fields should be limited to secondary or supporting commentary to enable automated processing.

5.4.3.12 The EAMS shall support alert visualization on dashboards, using configurable severity levels, color coding, geospatial markers (if location-tagged), and escalations based on asset class or impact.

5.4.4 Human Resources System data

5.4.4.1 The EAMS shall interface securely with the Operator Human Resource System (HRS) and a Competency Management System to support staff assignment, work planning, and compliance with



labor constraints. Access control, data protection, and audit logging shall comply with the TSCC System Technical Specification - Cybersecurity. This integration shall enable real-time data exchange and shall support the following functions:

- Automated assignment of work orders to maintenance teams or individuals with the required technical skills, certifications, and competencies. Assignment logic shall validate qualification currency and training status.
- Workforce scheduling based on team availability, personnel shift patterns, and track possession windows. The system shall enforce maximum working time per technician and flag scheduling conflicts or overloads.

- 5.4.4.2 Integration between the EAMS and HR systems shall use secure, standards-based APIs or data exchange interfaces, and enforce role-based access control to restrict access to sensitive personnel data in accordance with the TSCC System Technical Specification - Cybersecurity and applicable privacy regulations.
- 5.4.4.3 The EAMS shall incorporate shift calendars, approved leave, overtime limits, and applicable labor or union rules into the scheduling engine to ensure compliance with workplace agreements and personnel availability.
- 5.4.4.4 All staff assignment and scheduling decisions shall be logged, timestamped, and auditable, including override actions, system-suggested reassignments, and approvals by supervisory personnel.
- 5.4.4.5 The EAMS shall restrict the assignment of work orders to personnel with expired certifications, pending medical restrictions, or insufficient qualification levels, and alert supervisors to any such conflicts.
- 5.4.4.6 The EAMS shall support dynamic reassignment of tasks in real-time, enabling planners to respond to unavailability, shift changes, or emergency conditions without compromising compliance rules.
- 5.4.4.7 The system shall include dashboards and reporting tools to allow resource managers to monitor workload distribution, technician utilization, qualification coverage, and forecasted gaps.

5.4.5 Mapping and 3D

- 5.4.5.1 The EAMS shall integrate geographic and infrastructure data with the CHSR GIS and associated BIM models. This integration shall support visualization of infrastructure geometry, location-based asset data, and the graphical display of asset condition. The EAMS shall link to or embed BIM and GIS layers using open standards such as Industry Foundation Classes (IFC) for BIM and OGC-compliant formats (e.g., WMS, GeoJSON) for GIS.
- 5.4.5.2 The EAMS shall support interactive 2D/3D map views, including the ability to zoom, pan, filter, and select infrastructure elements or assets from within a GIS or BIM interface embedded in the EAMS HMI.
- 5.4.5.3 The EAMS shall support live overlay of asset condition data (e.g., alarms, health status, maintenance state) on the GIS/BIM display, using color-coded icons, heatmaps, or similar graphical representations.
- 5.4.5.4 Users shall be able to search for assets by location, facility, or map zone and filter displayed assets based on status, system, or priority.
- 5.4.5.5 The GIS and BIM integration shall comply with Schedule 4 – Digital Engineering Requirements and related interface requirements within this document suite.
- 5.4.5.6 The EAMS shall enforce secure access and user-specific permissions to GIS and BIM data layers in accordance with the TSCC System Technical Specification - Cybersecurity, especially for infrastructure locations that are operationally or security-sensitive.



5.4.6 Electronic Document Management System

- 5.4.6.1 The EAMS shall integrate an Electronic Document Management System (EDMS) module, either internal or external, to manage all asset-related documents. The EDMS shall support centralized storage, structured access, and lifecycle control for the following document types:
- Maintenance manuals
 - Technical manuals
 - Training materials
 - Procedures and work instructions
 - Engineering drawings and schematics
 - Spare parts catalogs
 - Operational rules and regulatory instructions
 - Job aids and task checklists
 - Safety instructions and incident response documents
 - Regulatory compliance documents
 - Work orders and associated reports
 - Communication logs related to asset operations
 - BIM models and linked GIS documents.
- 5.4.6.2 The EDMS shall be fully accessible through the EAMS interface and support contextual linking of documents to assets, systems, components, work orders, and maintenance records.
- 5.4.6.3 The EAMS shall provide configurable dashboards and user-specific views that enable users to retrieve linked documents based on asset, task, or system context. Information security controls, including role-based document access and action auditing, shall be implemented in accordance with the TSCC System Technical Specification - Cybersecurity.
- 5.4.6.4 The EDMS shall support document lifecycle management, including draft, approval, revision control, archive, and expiration status. Version metadata shall include document owner, version number, status, date modified, and approval history.
- 5.4.6.5 The EDMS shall enforce role-based access controls (RBAC) and document classification levels (e.g., public, internal, confidential). All document access and edits shall be logged with user ID, timestamp, and action.
- 5.4.6.6 The EDMS shall support advanced search and retrieval functions, including full-text indexing, filtering by metadata (e.g., asset ID, document type), and real-time query performance suitable for field operations.
- 5.4.6.7 The EDMS shall integrate with the EAMS Data Store, Asset Register, and BIM/GIS platforms to enable cross-referencing of documents to spatial models and asset hierarchies.
- 5.4.6.8 The EDMS shall support long-term archiving and retention of documents in accordance with applicable federal and California state regulations (e.g., FRA, CPUC) and shall support open file formats including PDF/A, DOCX, DWG, and IFC.
- 5.4.6.9 The EDMS shall support optional features including digital watermarking, document expiration dates, read-only distribution, and encryption of sensitive documents, particularly those related to physical security or restricted assets.



5.4.7 Maintenance History and Regulation

- 5.4.7.1 The EAMS shall record, store, and present the full maintenance history of each asset, including past interventions, planned activities, and ongoing tasks. Maintenance history shall be categorized using configurable parameters such as EAMS asset ID, system type, maintenance type, materials used, and work outcome. Categorization requirements shall be confirmed during implementation workshops.
- 5.4.7.2 The configuration of maintenance history categories and filters shall be user-driven, based on a library of available metadata fields, and shall not require involvement from the EAMS supplier after commissioning.
- 5.4.7.3 The EAMS shall maintain a tamper-evident, time-stamped audit trail of all maintenance activities, including system-generated events and user interactions. Audit logs shall be stored in a secure, append-only format and protected in accordance with the TSCC System Technical Specification - Cybersecurity.
- 5.4.7.4 In the event of an incident, investigation, or insurance claim, authorized personnel shall be able to verify the maintenance status of any asset. All user actions, approvals, and changes related to maintenance activities shall be recorded with timestamps, user ID, and action type to support full traceability.
- 5.4.7.5 The EAMS shall maintain centralized maintenance history data in a format suitable for regulatory and certification use, including compliance with ISO 55001, ISO 9001, and the standards referenced in Section 2.1. Records shall be readily exportable in support of third-party audits or internal reviews.
- 5.4.7.6 The EAMS shall link each historical maintenance record to the corresponding work order, technician, asset condition, and applicable maintenance plan, allowing comparison between planned and executed tasks.
- 5.4.7.7 The EAMS shall support filtering and reporting of maintenance history by asset, location, date range, task type, maintenance outcome, and responsible team or technician.
- 5.4.7.8 Maintenance history records shall include, where available:
- Fault or failure codes
 - Root cause indicators
 - Corrective actions taken
 - Component(s) replaced
 - Downtime and restoration time
 - Post-maintenance test results or technician notes.
- 5.4.7.9 Maintenance history data shall be retained for a period defined by applicable regulatory obligations (e.g., 10 years minimum for general systems; up to 30 years for critical assets) and managed in accordance with the EAMS Data Retention Policy and cybersecurity protocols.
- 5.4.7.10 Access to maintenance history and audit logs shall be role-restricted, with configurable permission and real-time monitoring of access attempts. Controls shall comply with the TSCC System Technical Specification - Cybersecurity.

5.4.8 Data Corruption

- 5.4.8.1 The EAMS shall implement protection mechanisms against data corruption and unauthorized modification. The system shall ensure data integrity during reading, writing, storage, transmission, and processing by applying automated validation, structured input controls, and error handling protocols. At a minimum, the following measures shall be implemented:



- Real-time and scheduled data validation routines using configurable rules for required fields, data types, ranges, and domain constraints
- Referential integrity enforcement across linked data sets
- Audit logs to track all Create, Read, Update, Delete (CRUD) operations with timestamps, user ID, and operation type
- Automated detection of:
 - Duplicate or redundant entries
 - Structural conflicts (e.g. broken hierarchies, misaligned formats)
 - Naming conflicts and inconsistent terminology
 - Contradictory values
 - Misspellings and malformed inputs
 - Aggregation inconsistencies or outdated calculations
 - Temporal inconsistencies (e.g., future dates or overlapping time windows)
- Standardized error-handling workflows and recovery routines
- Ongoing system health monitoring and integrity testing routines.

5.4.8.2 The EAMS shall minimize the need for manual data entry and duplication by automating data ingestion, enforcing pre-filled templates, and enabling integration with external systems wherever feasible. Manual entry fields shall include input validation, formatting rules, and auto-suggestions to reduce errors.

5.4.8.3 Data integrity, audit logging, and access control for critical data operations shall comply with the TSCC System Technical Specification - Cybersecurity. This includes enforcing role-based controls and validating data against authorized schemas.

5.4.8.4 The EAMS shall maintain a centralized and version-controlled data schema, including a data dictionary that defines field-level requirements, units, naming conventions, and validation rules. Any schema changes shall be logged and subject to approval by the Authority.

5.4.8.5 The EAMS shall implement cryptographic methods such as hashing or digital signatures to detect and prevent unauthorized or accidental data corruption in critical datasets and audit trails.

5.4.8.6 The EAMS shall include automated alerting for corruption or validation failures, with configurable thresholds and escalation levels. These alerts shall be viewable in dashboards and sent to designated system administrators.

5.4.8.7 The EAMS shall support point-in-time recovery, including restoration from backup in the event of partial or full data corruption. Data recovery procedures shall be documented and tested periodically in accordance with the system backup and disaster recovery strategy.

5.4.9 Evidence and Cause Analysis

5.4.9.1 The EAMS shall incorporate Root Cause Analysis (RCA) methodologies to update existing clauses (in bold for changes) and add additional clauses for considerations.

5.4.9.2 The TSCC Contractor shall implement machine learning (ML) and artificial intelligence (AI) capabilities to enhance RCA performance. These capabilities shall assist in identifying root causes based on historical data, real-time asset conditions, and maintenance records and shall include transparent logic or explainability functions.

5.4.9.3 The TSCC Contractor shall define, develop, and integrate appropriate RCA workflows into the EAMS, incorporating both manual and automated analysis pathways to support technical decision-making.



RCA functions shall be accessible via the EAMS HMI and support traceable user input, evidence links, and recommendation outputs.

- 5.4.9.4 All verified root cause analyses and associated logic, models, or rules shall be added to a version-controlled algorithm library for future reuse and optimization. This library shall be accessible to authorized EAMS users and integrated into broader decision support tools.
- 5.4.9.5 The EAMS shall trigger RCA automatically based on configurable conditions, such as repeat failures, unplanned downtime events, asset unavailability, or failed maintenance outcomes. RCA initiation criteria shall be defined during system configuration in consultation with the Authority.
- 5.4.9.6 RCA functionality shall draw from all relevant EAMS modules, including FRACAS records, sensor data, fault codes, maintenance history, operator reports, and inspection logs to form a comprehensive diagnostic base.
- 5.4.9.7 RCA outputs generated by AI/ML components shall be subject to human validation. The system shall present supporting evidence, reasoning pathways, and confidence indicators. RCA decisions shall include review logs, timestamps, and user approvals.
- 5.4.9.8 The EAMS shall track the effectiveness of RCA results through closed-loop monitoring, using indicators such as recurrence rate, downtime reduction, or mean time between failures (MTBF) to validate root cause recommendations.
- 5.4.9.9 RCA modules shall interface with fault management, condition monitoring, and configuration management tools to support holistic asset diagnostics and avoid duplication of analysis functions across systems.

5.4.10 Maintenance Plan

- 5.4.10.1 The EAMS shall support the execution, scheduling, tracking, and completion of all tasks defined in the maintenance plan developed during the design and commissioning phases, in accordance with California HSR maintenance and asset management guidelines. The EAMS shall accommodate various maintenance types, including preventive, corrective, predictive, and condition-based strategies.
- 5.4.10.2 The EAMS architecture shall support the creation, editing, and validation of unscheduled or ad hoc work orders in response to real-time events, sensor alerts, operator requests, or asset failures.
- 5.4.10.3 The EAMS shall allow a long-term maintenance planning module capable of simulating workload demand, resource utilization, spare parts consumption, and technician availability over multi-year time horizons.
- 5.4.10.4 Predictive maintenance functionality shall be based on parameters derived from the RAM Analysis Report, including failure rates, meantime between failures (MTBF), and lifecycle cost (LCC) models. These calculations shall be supplemented by Reliability-Centered Maintenance (RCM) logic, data captured in FRACAS, and inputs from the fault management system.
- 5.4.10.5 The TSCC Contractor, in collaboration with The Authority, shall define and map key diagnostic data points—such as sensor readings, performance thresholds, and fault codes—to equipment-specific diagnostic tables to guide condition-based and reliability-based maintenance interventions.
- 5.4.10.6 The TSCC Contractor shall evaluate and, where approved by The Authority, implement artificial intelligence (AI) and machine learning (ML) capabilities to support maintenance decision-making. These capabilities shall align with the asset management plan and enhance predictive maintenance, RCM, and CBM functionality. All AI-driven recommendations shall include traceability and human validation before execution.



- 5.4.10.7 The EAMS shall support version control and approval workflows for maintenance plans. Historical versions shall be retained and auditable to support safety, quality, and regulatory traceability.
- 5.4.10.8 Maintenance plan execution data—such as early failures, deferrals, and corrective interventions—shall be used to continuously optimize future cycles. The EAMS shall provide a closed-loop feedback mechanism between maintenance outcomes and plan adjustments.
- 5.4.10.9 The EAMS shall include a visual simulation interface for maintenance forecasting, allowing users to model asset condition projections, workload peaks, technician capacity constraints, and spare part demand.
- 5.4.10.10 AI/ML models used in predictive maintenance shall be explainable, regularly validated, and monitored for performance drift. Decisions based on AI shall be logged with algorithm version, confidence score, and approval status.
- 5.4.10.11 This section shall be read in conjunction with the RAM Analysis Report, the RCM/CBM Implementation Plan, and the TSCC System Technical Specification - Cybersecurity where predictive algorithms and sensitive operational data are used.

5.4.11 Maintenance Analysis Tool

- 5.4.11.1 The EAMS shall include a Maintenance Analysis Tool that integrates a diagnostic function defined by the TSCC Contractor and approved by The Authority. The diagnostic function shall include structured tools such as diagnostic tables, fault trees, logic diagrams, and related analysis methods, and shall be aligned with data from FRACAS, condition monitoring, and maintenance history modules.
- 5.4.11.2 A diagnostic table shall be a structured representation of failure-related information used to assess the health, performance, and operational condition of assets. Diagnostic tables shall be maintained in a centralized and modifiable format.
- 5.4.11.3 Each diagnostic table shall consolidate relevant parameters, sensor readings, historical events, and calculated thresholds associated with specific asset types or systems.
- 5.4.11.4 Diagnostic tools shall support operational and maintenance decision-making by generating actionable insights into asset conditions, failure cause, and recommended actions.
- 5.4.11.5 The EAMS shall include, at a minimum, the following diagnostic and reference tables:
- Symptom/Evidence tables
 - Fault tables
 - Cause tables
 - Remedy tables (including Mean Time to Repair – MTTR)
 - Maintenance log tables
 - Sensor signal mapping tables
 - Diagnostic records (including analysis outcomes and decisions taken).
- 5.4.11.6 Predefined diagnostic workflows shall be developed to guide maintainers through fault analysis procedures. These workflows shall include decision steps, data checks, recommended actions, and approval logic where required. Workflows shall be user-role-specific, traceable, and linked to associated tables, sensor data, and work order processes.
- 5.4.11.7 Inspections findings shall be recorded in the EAMS and evaluated against baseline and live asset monitoring data. This may include comparisons of recorded symptoms to sensor values, dynamic thresholds, or failure signatures. Diagnostic logic shall adapt to evolving operational conditions.



- 5.4.11.8 The TSCC Contractor shall develop and maintain an algorithm library within the EAMS, containing all logic, diagnostic models, and analytical tools used in fault identification and asset condition evaluation.
- 5.4.11.9 The TSCC Contractor shall develop and maintain an algorithm library within the EAMS, containing all logic, diagnostic models, and analytical tools used in fault identification and asset condition evaluation.
- 5.4.11.10 The algorithm library shall include metadata such as version number, author, approval status, and model type. Access to the library shall be controlled by user roles and audit logged. The library shall support continuous improvement, subject to validation, review, and approval by The Authority.
- 5.4.11.11 The Maintenance Analysis Tool shall interface with the FRACAS module, Maintenance History, and Sensor Data Store to correlate events, failure causes, and performance degradation across operational timelines.
- 5.4.11.12 Diagnostic recommendations and AI-generated outputs shall include supporting rationale, source data references, and confidence scores where applicable. All automated or assisted decisions shall be recorded in a traceable diagnostic log.
- 5.4.11.13 The EAMS shall support validation and performance testing of diagnostic models (both rule-based and ML-driven) using metrics such as detection accuracy, false positive rate, and time-to-diagnosis.
- 5.4.11.14 The algorithm library shall include deprecation and rollback controls for outdated or underperforming models. Updates to algorithms shall be logged, versioned, and subject to approval workflows.
- 5.4.11.15 Access to diagnostic tools and the algorithm library shall comply with the TSCC System Technical Specification - Cybersecurity, including authentication, role-based permissions, and tamper protection of logic and model data.

5.4.12 Work Orders

- 5.4.12.1 The EAMS shall support automatic generation of work orders based on time-based schedules, mileage, usage thresholds, or triggered events from condition monitoring systems. Preventive and predictive maintenance modules shall generate work orders in alignment with defined maintenance plans.
- 5.4.12.2 The EAMS shall ingest real-time data from connected sensor systems and generate corresponding work orders without delay. Trigger thresholds, escalation conditions, and data mappings shall be configurable by The Authority.
- 5.4.12.3 The EAMS shall include a comprehensive work order management module with calendar-based visualization and reporting. This module shall interface with other EAMS functions including maintenance planning, documentation, spare parts, tools, human resources, and task libraries defined by The Authority.
- 5.4.12.4 The work order management module shall support work packaging—organizing and sequencing multiple work orders to minimize downtime, optimize resource allocation, and align with possession windows. The TSCC Contractor shall define detailed packaging procedures for approval by The Authority.
- 5.4.12.5 The EAMS shall allow authorized users to manually create ad hoc work orders via the EAMS HMI or mobile interface, with appropriate input validation, status tracking, and audit logging.
- 5.4.12.6 Each work order shall include the required competencies, certifications, and skills for execution, and the EAMS shall validate assigned personnel against these requirements before confirmation.
- 5.4.12.7 Maintenance personnel shall be required to scan their ID or equivalent credentials (e.g., NFC card, QR code) before accessing trackside areas, restricted zones, or initiating safety-critical work orders.



5.4.12.8 Each work order shall include, at a minimum, the following details:

- Required tools and equipment
- Required skills and certifications
- Spare parts and quantities
- Safety documents and procedures
- Relevant maintenance documentation and schematics
- Estimated labor effort and task duration.

5.4.12.9 The EAMS shall support both automatic and manual generation of work orders. All work orders shall follow a consistent lifecycle model and include metadata such as type, priority, origin, and associated asset ID.

5.4.12.10 The EAMS shall provide real-time tracking of work order status, from creation through completion. Status changes shall be logged and visible through dashboards and reports. Configurable prioritization rules shall enable dynamic task scheduling based on asset criticality and service impact.

5.4.12.11 The EAMS shall track work order-related costs including labor, materials, services, and overhead. This data shall be integrated with The Authority's financial and accounting systems for budgeting and forecasting purposes.

5.4.12.12 The EAMS shall support the creation and management of configurable work order templates and task libraries to standardize repeatable maintenance routines. The Authority shall be able to modify templates to reflect asset-specific variations or approved procedure changes.

5.4.12.13 The EAMS shall include an integrated module (internal or external) that interfaces with The Authority's supply chain system for the real-time coordination of maintenance tasks, parts requisitions, delivery tracking, and work order status updates.

5.4.12.14 The EAMS shall support the full lifecycle of a work order, including the following statuses:

- **Draft** – Initial creation of the work order record, with editable fields
- **Submitted** – Ready for review by supervisors or planners
- **Pre-Authorized** (optional) – Under technical, safety, or cybersecurity review prior to formal approval
- **Approved** – Work order formally approved for execution based on scope, risk, and resource checks
- **Scheduled** – Assigned to a time window, location, and workforce
- **Issued** (optional) – Officially dispatched or handed over to the responsible team (often coincides with permit-to-work)
- **In Progress** – Execution is underway by the assigned maintenance crew
- **On-Hold** – Temporarily paused due to external factors (e.g., weather, parts delay, access restrictions)
- **Completed** – All physical work completed on site
- **Verified/Quality Checked** (optional) – Work is inspected or validated for completeness, compliance, or QA requirements
- **Closed** – Work order is archived after successful verification and documentation
- **Cancelled** – Work order is invalidated prior to or during execution
- **Failed/Rejected** (optional) – Work order execution was unsuccessful or did not meet acceptance criteria and requires reissue or escalation.



- 5.4.12.15 Transitions between statuses shall be governed by configurable workflows, approval conditions, and user roles as defined by The Authority.
- 5.4.12.16 Work orders exceeding SLA thresholds for response or completion shall trigger automatic alerts, escalation to supervisors, and inclusion in compliance dashboards.
- 5.4.12.17 Field technicians shall be able to access, update, and close work orders via mobile or tablet devices. Offline functionality shall be supported for remote locations, with data synced when connectivity is restored.
- 5.4.12.18 The EAMS shall log all actions taken on a work order (e.g., assignment, reassignment, edit, cancellation, closure) along with user ID, timestamp, and device used, in accordance with the TSCC System Technical Specification - Cybersecurity.
- 5.4.12.19 Completed work orders shall feed directly into maintenance history, FRACAS, and asset condition records. Work order outcomes shall be evaluated against planned scope and used to improve future maintenance planning.

5.4.13 Spare parts management, kits, and tools

- 5.4.13.1 The EAMS shall include an interface module to integrate with The Authority's supply chain and inventory management systems. This module shall enable seamless coordination between asset management functions and procurement, stock control, and reporting workflows.
- 5.4.13.2 The EAMS interface module shall provide the following core functions:
- Inventory visibility across all relevant stock locations and storage types
 - Distribution, issue, and reclamation of parts for maintenance tasks
 - Repair management workflows for tools and equipment across storage areas, depots, and mobile units
 - Supplier management and linking of spare parts to approved vendors
 - Inventory cost tracking, including acquisition, restocking, mobilization, and demobilization costs.
- 5.4.13.3 The EAMS shall support identification and labeling of packaged maintenance kits, including contents, part numbers, quantities, shelf-life (if applicable), and linked asset types. AutoID technologies (e.g., RFID, barcode) shall be used where practicable.
- 5.4.13.4 Spare parts modelling within the EAMS shall support the following attributes, at a minimum:
- Number in stock (initial and max holding quantity)
 - Mobilization time (time from withdrawal to usage)
 - Restocking thresholds and reorder points
 - Restocking time (lead time to replenish)
 - California refurbishment time (turnaround time for reusable items)
 - Cost data (unit cost, overhead, and logistical costs)
- 5.4.13.5 The EAMS shall process all types of labeling used in California HSR using AutoID principles where feasible. Manual override methods shall be allowed only in defined exception cases and tracked by user ID and timestamp.
- 5.4.13.6 The EAMS shall support creation, assignment, and tracking of maintenance kits and tools within work orders. Kits may be predefined or assembled dynamically based on asset type, fault, or required maintenance action.



- 5.4.13.7 The EAMS shall manage tool inventory by tracking tool type, location, availability, calibration status, maintenance records, costs, responsible users, check-out/check-in events, and condition.
- 5.4.13.8 The EAMS shall support tool auditing and reporting functions to support forecasting, procurement decisions, and tool utilization analysis. Safety-critical tools shall include tamper alerts, loss prevention features, and usage thresholds.
- 5.4.13.9 The EAMS shall automate the ordering, restocking, quality assurance, issue, and return processes for spare parts and consumables. Minimum stock thresholds and alert levels shall be configurable by The Authority.
- 5.4.13.10 The EAMS shall integrate with software inventory and license management systems for tools and equipment with embedded firmware or software. Version control, patch history, and access to associated configuration files shall be supported.
- 5.4.13.11 Files such as configuration settings, digital certificates, and calibration files shall not be stored within the EAMS itself but may be referenced by link. The EAMS shall maintain metadata and provide secure version-controlled access to these external files.
- 5.4.13.12 The EAMS shall support classification of stock by criticality, type (e.g., serialized, consumable, refurbished), and location (e.g., central warehouse, depot, mobile unit), enabling precise inventory control and safety stock planning.
- 5.4.13.13 The EAMS shall track the lifecycle of spare parts and tools, including shelf life, expiration, warranty, and obsolescence. Alerts shall be generated for items nearing end-of-life, expiring calibration, or superseded part status.
- 5.4.13.14 Calibration tracking shall include calibration intervals, due dates, traceability to standards, and certification storage. Non-compliant tools shall trigger hold status and alert the responsible team.
- 5.4.13.15 The EAMS shall support predictive inventory forecasting based on historical usage trends, maintenance schedules, and seasonal demand patterns. Forecast data shall be used to support budgeting and supply chain planning.
- 5.4.13.16 Spare parts shall be linked to asset-specific Bills of Materials (BOMs), including compatible and alternative parts. The EAMS shall support automated part suggestions based on fault type and asset configuration.
- 5.4.13.17 All spare parts, tools, and consumables associated with critical assets shall comply with access control, audit logging, and integrity monitoring requirements as defined in the TSCC System Technical Specification - Cybersecurity.

5.4.14 FRACAS

- 5.4.14.1 The EAMS shall include an integrated FRACAS (Failure Reporting, Analysis and Corrective Action System) module to track, analyze, and close out asset failures, incidents, and corrective actions.
- 5.4.14.2 The FRACAS module shall enhance The Authority's ability to manage asset reliability, minimize downtime, and improve operational performance. By systematically tracking and analyzing failures, the FRACAS shall support optimization of maintenance strategies, resource planning, and long-term asset lifecycle decisions.
- 5.4.14.3 FRACAS module shall reference asset hierarchies and physical locations within the EAMS to accurately log failures and incidents and link them to individual assets or systems.
- 5.4.14.4 The work order module shall be integrated with the FRACAS module so that all incidents can be linked to the associated maintenance tasks and executed actions.



- 5.4.14.5 The FRACAS module shall be configured to capture detailed contextual information to support root cause analysis (RCA), including environmental conditions, operating parameters, maintenance history, inspection reports, and user comments.
- 5.4.14.6 The FRACAS module shall enable lifecycle tracking and performance measurement of affected assets using dashboards, KPIs, and start centers linked to work orders. Key indicators such as MTBF, MTTR, failure rate, and incident recurrence shall be supported.
- 5.4.14.7 Each failure or incident shall follow a defined lifecycle within the FRACAS module, including status stages such as Reported, Under Review, RCA Complete, Corrective Action Assigned, Verified, and Closed. Status changes shall be workflow-driven, timestamped, and role-governed.
- 5.4.14.8 The maintenance data associated with FRACAS records shall include, at a minimum:
- Work order ID
 - Maintenance task ID and procedure reference
 - Affected asset ID
 - Task interval (scheduled frequency)
 - Due date and actual completion date
 - Total downtime and labor hours
 - Parts and materials used
 - Inspection and test results
 - Description of discovered faults
 - Summary of corrective actions taken.
- 5.4.14.9 FRACAS reports shall be used to identify opportunities for maintenance strategy optimization, risk reduction, and service performance improvements, while preserving safety and compliance objectives.
- 5.4.14.10 The EAMS shall support extraction and export of FRACAS records and reports for analysis by maintenance engineers, safety personnel, and asset managers.
- 5.4.14.11 The EAMS shall be capable of generating FRACAS records automatically when defined fault codes, alerts, or failure criteria are detected by the system.
- 5.4.14.12 The FRACAS module shall include incident classification features to assign severity levels, impact types (e.g., safety, reliability, operational), and root cause categories. These classifications shall be used for triage, prioritization, and escalation workflows.
- 5.4.14.13 The FRACAS module shall support continuous improvement processes by enabling tracking of recurring failures, monitoring of action effectiveness, and generation of feedback into preventive maintenance plans and decision support tools.
- 5.4.14.14 The FRACAS module shall integrate with the Evidence and Cause Analysis tools (see Section 5.4.8), allowing incident records to be linked to root cause trees, diagnostic outputs, and algorithm library references.
- 5.4.14.15 The FRACAS module shall include configurable alerting for overdue corrective actions, incomplete RCA tasks, or repeated incidents on the same asset.
- 5.4.14.16 All FRACAS actions, decisions, and edits shall be logged and traceable to the initiating user, with timestamped records and role-based access controls as defined in the TSCC System Technical Specification - Cybersecurity.



- 5.4.14.17 The FRACAS module shall provide a closed-loop feedback mechanism to the EAMS maintenance planning module, allowing confirmed root causes and repeated incident data to influence task intervals, procedures, or asset replacement strategies.
- 5.4.14.18 The FRACAS module shall support periodic safety and compliance reviews, and provide configurable reports for regulatory submissions, insurance claims, and internal audits.
- 5.4.14.19 The FRACAS module shall support the classification and tracking of **defects** as a specific failure event type. Defects may include installation errors, manufacturing non-conformances, punch list items, or anomalies detected during inspection, commissioning, or handover. Each defect shall be linked to the affected asset, severity level, and related warranty, quality, or supplier documentation where applicable.

5.4.15 Asset Management Plan

- 5.4.15.1 The TSCC Contractor, in agreement with the Authority, shall develop an Asset Management Plan that provides sufficient information to support lifecycle investment decisions. The plan shall guide decisions relating to:
- Trade-off analysis for ageing assets
 - Optimization of maintenance strategies
 - Replacement or investment in new equipment scenarios
- 5.4.15.2 The Asset Management Plan shall be structured and categorized according to major asset groups, including at minimum: track systems, civil works, and major electromechanical systems (e.g., power, signaling, ventilation, control systems).
- 5.4.15.3 The TSCC Contractor shall provide periodic forecast reports identifying planned obsolescence and decommissioning of parts, subassemblies, or complete subsystems. These forecasts shall support proactive investment planning and maintenance schedule adjustments.
- 5.4.15.4 The Asset Management Plan shall be driven by Reliability-Centered Maintenance (RCM) and/or Condition-Based Maintenance (CBM) principles, with a focus on minimizing lifecycle cost, unplanned outages, and safety risks.
- 5.4.15.5 The TSCC Contractor shall prepare and submit the Asset Management Plan to The Authority for review and approval prior to implementation.
- 5.4.15.6 The Asset Management Plan shall be evidence-based, using best practices and supporting models to justify recommendations. These models shall include reliability analysis, FRACAS trends, lifecycle cost (LCC) analysis, and relevant performance indicators.
- 5.4.15.7 The Asset Management Plan shall align with the principles of ISO 55001 (Asset Management – Management Systems – Requirements) or equivalent industry-standard frameworks to ensure traceability, risk-based planning, and value optimization across the asset lifecycle.
- 5.4.15.8 The Asset Management Plan shall define governance roles and responsibilities, including designation of a plan owner, revision approver, and implementation oversight by The Authority.
- 5.4.15.9 The plan shall be reviewed and updated at least once every year, or following any significant change to asset class performance, maintenance strategy, or service level requirements.
- 5.4.15.10 The plan shall be traceable to EAMS modules including the asset register, maintenance planning, FRACAS, and predictive analytics. Changes in asset condition or failure rates shall be reflected in its planning assumptions and recommendations.



- 5.4.15.11 Capital investment recommendations within the plan shall be supported by cost-benefit analyses, residual life estimation, risk impact scores, and service performance projections.

5.4.16 Asset Condition Survey and Monitoring

- 5.4.16.1 The TSCC Contractor shall establish periodic asset condition surveys and audits to assess asset degradation and deterioration using industry best practices. The proposed methodology and frequency shall be submitted to The Authority for approval.
- 5.4.16.2 Condition audits shall support the projection of asset degradation, identification of failure trends, and modeling of remaining useful life in short-, medium-, and long-term horizons to inform investment planning and replacement strategies.
- 5.4.16.3 The TSCC Contractor shall prepare and submit an Asset Condition Survey Management Plan that outlines the methodology for collecting, assessing, and reporting on asset conditions. The plan shall present a structured, data-driven approach to maximize asset life while maintaining required levels of availability, performance, and safety.
- 5.4.16.4 The EAMS shall support condition assessments through the analysis of available data sets, including inspection data, sensor readings, historical work orders, and operational performance metrics. Condition audits may be initiated manually or triggered automatically based on threshold values.
- 5.4.16.5 The TSCC Contractor shall propose an audit frequency for each major asset class, based on criticality, risk, and degradation profiles. This shall be reviewed and approved by The Authority.
- 5.4.16.6 The EAMS shall host all asset-related data necessary for maintenance contractor operations, including condition records, inspection logs, usage data, and access to the current Asset Register and maintenance history.
- 5.4.16.7 If maintenance contractors maintain separate data systems, the transfer of operational and condition data into the EAMS shall be mandatory. The EAMS shall serve as the authoritative master system and the single source of truth for all operational data, asset condition, competencies, required equipment, and maintenance activities across the California High-Speed Rail program.
- 5.4.16.8 The EAMS shall maintain the master copy of all condition monitoring and inspection data. TSCC Contractor internal systems may only serve as temporary or read-only repositories and must synchronize with the EAMS per defined data transfer protocols.
- 5.4.16.9 The EAMS shall support periodic reporting of asset condition to original equipment manufacturers (OEMs), suppliers, or The Authority. Reports shall be auto generated or scheduled based on configured time intervals or events.
- 5.4.16.10 The Asset Condition Survey Management Plan shall define the types of condition evaluation used (e.g., visual inspection, structural assessment, sensor-derived metrics), condition scoring scales (e.g., 1–5 or health index), and asset-specific thresholds for concern or replacement.
- 5.4.16.11 The EAMS shall support geospatial tagging and photographic or video evidence collection during surveys. Condition data shall be linked to the GIS/BIM representation of each asset.
- 5.4.16.12 Condition data collected from maintenance contractors shall be subject to validation rules, version control, and audit logging. Only verified data shall influence planning, reporting, or investment recommendations.
- 5.4.16.13 The EAMS shall differentiate between condition surveys (manual, planned evaluations), monitoring (continuous, sensor-based tracking), and inspections (event- or schedule-based assessments) for traceability and reporting clarity.



- 5.4.16.14 All condition data shall comply with the TSCC System Technical Specification - Cybersecurity, including data integrity validation, encryption in transit/storage, and user-based access controls.
- 5.4.16.15 Outputs of the asset condition survey shall feed directly into the Asset Management Plan (see Section 5.4.15), maintenance strategy optimization, and capital investment prioritization modules.

5.4.17 Obsolescence Management

- 5.4.17.1 The TSCC Contractor shall develop and maintain an Obsolescence Management Plan (OMP), to be approved by the Authority and integrated into the EAMS as a functional module with associated reporting and data tracking capabilities.
- 5.4.17.2 The Obsolescence Management Plan shall describe processes and strategies to manage and mitigate obsolescence risk to preserve operational performance, safety, and maintainability. It shall include, at a minimum:
- Guidelines for identifying and replacing obsolete components and equipment, with specific focus on electronic and software-dependent systems.
 - Replacement strategies based on modular and open architectures to support partial upgrades. Any deviations from modular/open architecture shall require prior written approval by The Authority.
 - Software update strategies to address compatibility, patching, and end-of-support risks, with preference for modular and decoupled implementations.
 - Inventory plans for strategic and non-strategic spare parts.
 - Management of tool obsolescence, including identification of new tool requirements and secure disposal of outdated equipment.
 - Processes to proactively monitor vulnerable components and subsystems using EAMS analytics and supplier lifecycle data.
- 5.4.17.3 The EAMS shall provide functionality to monitor component development roadmaps, supply chain availability, and commercial lifecycle status of all software and hardware components. Alerts shall be generated for components approaching end-of-life.
- 5.4.17.4 Maintenance engineering staff shall ensure that all spare parts contracts include up-to-date obsolescence condition information for critical components, including manufacturer support status, last-time-buy notifications, and replacement part references.
- 5.4.17.5 Upon identifying an obsolete component, the TSCC Contractor shall initiate actions to identify, evaluate, test, and gain all required internal and external approvals for replacement, refurbishment, or adaptation of equivalent components.
- 5.4.17.6 For each obsolete component replaced, the TSCC Contractor shall provide full documentation covering testing, installation procedures, operational validation, and configuration control for hardware and/or software.
- 5.4.17.7 Obsolescence shall be considered during the equipment specification and design phase. Systems shall prioritize the use of open, modular architectures to facilitate partial redesigns, interface updates, and integration of new technologies.
- 5.4.17.8 Selected architectures shall conform to recognized or emerging market standards (e.g., software languages, interface protocols). Any deviation shall be justified and is subject to written approval by The Authority.



- 5.4.17.9 The TSCC Contractor shall provide a list of anticipated obsolete equipment on an annual basis and upon request via the EAMS. This list shall project the upcoming period and support advanced scheduling of replacement or mitigation actions.
- 5.4.17.10 At contract close-out and during the maintenance handover process, the TSCC Contractor shall demonstrate that no critical system or component will become obsolete for a minimum period after handover to be approved by The Authority.
- 5.4.17.11 If the TSCC Contractor is unable to demonstrate continued operability of the system due to foreseeable obsolescence, they shall remain liable for renewal, reengineering, or replacement costs required to sustain asset functionality.
- 5.4.17.12 The Obsolescence Management Plan shall be aligned with the principles of IEC 62402 – Obsolescence Management – Application Guide or equivalent international standards. The plan shall include structured risk assessment, monitoring, mitigation, and resolution processes.
- 5.4.17.13 Obsolescence risk shall be assessed using a criticality-based scoring model considering component impact, system function, vendor dependency, and lifecycle support. High-risk items shall be prioritized in the OMP with defined mitigation strategies.
- 5.4.17.14 The EAMS shall integrate obsolescence tracking with the Asset Register, Maintenance Planning, Spare Parts Inventory, and FRACAS modules to ensure full traceability and proactive planning.
- 5.4.17.15 Supplier monitoring shall be included in the obsolescence strategy, including tracking of OEM lifecycle notifications, end-of-sale/end-of-support announcements, and coordinated last-time-buy actions.
- 5.4.17.16 The TSCC System Technical Specification - Cybersecurity shall be applied to all software and firmware obsolescence cases. Unsupported software versions shall be risk assessed, patched, or replaced as part of the security maintenance lifecycle.
- 5.4.17.17 The TSCC Contractor shall define an obsolescence change control workflow, including review, validation, and approval stages involving engineering, cybersecurity, and system safety representatives.

5.4.18 Lifecycle Management

- 5.4.18.1 The EAMS shall include a Lifecycle Management Tool that supports data-driven decision-making throughout the asset lifecycle. This tool shall be used to assess the total cost of ownership, performance, and timing of asset renewal or refurbishment.
- 5.4.18.2 The EAMS shall calculate the Lifecycle Cost (LCC) for each individual asset registered in the EAMS at intervals defined by The Authority, and upon key trigger events such as major repair, cost deviation, or condition change.
- 5.4.18.3 The EAMS shall calculate the mean LCC by asset class or equipment type, using aggregated operational and maintenance data stored in the EAMS. These calculations shall be performed at intervals defined by The Authority or as required for planning and investment analysis.
- 5.4.18.4 LCC analysis results shall be stored in a structured format within the EAMS and used as input to other EAMS modules, including:
- Asset Management Plan (AMP)
 - Obsolescence Management
 - Maintenance Strategy Optimization
 - Capital Investment Forecasting.



- 5.4.18.5 Common LCC models and reference analyses for California HSR assets shall be developed by the TSCC Contractor and stored in a reusable library within the EAMS. The models shall be version-controlled and subject to review and approval by The Authority.
- 5.4.18.6 All LCC analyses shall follow a recognized international standard such as ISO 15686-5, EN 60300-3-3, or an equivalent framework approved by The Authority. The selected methodology shall ensure repeatability, transparency, and defensibility of results.
- 5.4.18.7 The EAMS shall require LCC models to incorporate, at a minimum: initial capital cost, installation, preventive and corrective maintenance, energy consumption, downtime cost, obsolescence, and end-of-life decommissioning.
- 5.4.18.8 LCC calculation logic shall be fully integrated with EAMS modules including Work Orders, FRACAS, Spare Parts Inventory, Asset Condition, and Obsolescence data to maintain accuracy and real-time cost reflection.
- 5.4.18.9 The Lifecycle Management Tool shall support scenario-based and sensitivity analysis, allowing The Authority to evaluate cost and risk across multiple operational or funding assumptions (e.g., varying failure rates, inflation, discount rates).
- 5.4.18.10 LCC outputs shall be used as input into decision support tools for asset renewal planning, budgeting, risk-based prioritization, and maintenance strategy justification.

5.4.19 Building Information Modelling and Digital Twins

- 5.4.19.1 The EAMS shall be fully compatible with Building Information Modeling (BIM) data structures and Digital Twin applications, and shall implement integration protocols that allow seamless communication, synchronization, and management of asset lifecycle information. The EAMS shall be designed to integrate with BIM and Digital Twins in a way that is compatible with BIM's representation of assets and information contained within BIM models and the California HSR GIS geodatabase.
- 5.4.19.2 The EAMS shall enable two-way integration with Digital Twins, allowing asset performance data, condition monitoring, and maintenance status to be visualized and analyzed in real time within the digital twin environment.
- 5.4.19.3 Digital Twin shall support functions such as real-time simulation, predictive diagnostics, spatial analytics, and 3D visualization of asset condition and interventions. Integration with FRACAS, LCC, and Asset Condition modules shall be supported.
- 5.4.19.4 The EAMS shall track BIM model versions, distinguish between "as-designed," "as-built," and "as-maintained" states, and store update history in compliance with the system's configuration management plan.
- 5.4.19.5 Access to BIM and Digital Twin data shall be governed by role-based permissions and logged for audit purposes. Integration shall align with the TSCC System Technical Specification - Cybersecurity, and data exchanges shall be encrypted and validated.

5.4.20 Reporting, Analysis and auditing

- 5.4.20.1 The EAMS shall generate reports across all relevant maintenance and asset management categories to support operational decision-making and performance analysis. At a minimum, the reporting functionality shall cover:
- Asset availability and downtime tracking
 - Materials usage and consumption trends
 - Labor and material cost reporting, including cost per task and per asset



- MRO (maintenance, repair, and overhaul) inventory optimization
- Supplier performance assessments (e.g., delivery times, quality metrics)
- Condition monitoring summaries and alerts
- Asset performance trend analysis over time.

- 5.4.20.2 Reports shall support business intelligence functions, be visualized via dashboards, and provide insights to optimize maintenance planning and investment decisions.
- 5.4.20.3 The EAMS system shall support seamless scalability, enabling integration of new equipment, subsystems, or modules without the need for architectural redesign or server infrastructure overhaul. Reporting functionality shall accommodate new data streams and equipment classes dynamically.
- 5.4.20.4 The EAMS shall provide a fully documented and license-free interface (e.g., REST API, ODBC/JDBC) to support the integration of third-party analytics, visualization, and reporting tools. The interface shall allow read/write access to defined datasets, including historical logs, real-time data, and master records, as approved by The Authority.
- 5.4.20.5 The EAMS reporting engine shall support full lifecycle coverage, from asset acquisition through retirement. Reports shall include inputs/outputs from integrated systems, compliance with audit requirements, configuration change logs, and lifecycle-based risk assessments. All reporting functions shall align with The Authority's cybersecurity and auditability requirements.
- 5.4.20.6 The EAMS shall support export of reports in multiple standard formats (e.g., CSV, PDF, XLSX, JSON, XML), and allow automated report scheduling, email delivery, and user-defined distribution lists.
- 5.4.20.7 The EAMS shall support configurable role-based access to reports, dashboards, and analytics modules. Users shall only view and access information within their assigned scope of responsibility.
- 5.4.20.8 The EAMS shall include time-series analytics tools for evaluating trends over configurable historical ranges (e.g., 7-day, 30-day, 12-month). These tools shall support anomaly detection, forecasting, and seasonal comparison of asset behavior.
- 5.4.20.9 The EAMS shall maintain an immutable audit log of all system activity, including user actions, data imports/exports, asset configuration changes, and system access events. Audit logs shall be exportable, queryable, and retained in accordance with the TSCC System Technical Specification - Cybersecurity.
- 5.4.20.10 The EAMS shall support the definition and tracking of custom KPIs and performance indicators. Users shall be able to configure KPIs using system data fields, define thresholds, and visualize them within dashboards or reports.
- 5.4.20.11 The EAMS shall generate cybersecurity-related operational reports, including access violation summaries, failed login attempts, system event logs, and patch status compliance, to support CSOC and regulatory reporting.

5.4.21 Mobile EAMS Devices

- 5.4.21.1 The EAMS-FRMCS integration shall support communication with handheld mobile devices (e.g., Android, iOS, rugged tablets) for:
- Viewing and updating work orders:
 - Logging faults, alarms, or asset condition data
 - Uploading photos, audio notes, and GPS location



- Receiving push notifications or escalations
The user interface shall be adapted for mobile use with offline data caching and sync capabilities.

5.4.21.2 All handheld devices accessing the EAMS via FRMCS shall:

- Be enrolled in a Mobile Device Management (MDM) system
- Authenticate using multifactor authentication (MFA) or digital certificates
- Encrypt all data transmissions using TLS 1.3 or FRMCS-approved VPN tunnels
- Be remotely wipeable in case of loss or compromise.

5.4.21.3 EAMS traffic over FRMCS shall be classified and routed based on Quality of Service (QoS) requirements. Maintenance-critical messages (e.g., safety-related work orders) shall be flagged for high-priority delivery with retry logic if transmission fails.

5.4.21.4 The EAMS shall provide:

- Reliable sync of work order updates within a maximum delay (e.g., 10 seconds) of submission, agreed with The Authority
- Message retry logic with configurable thresholds
- Local caching of work order data during FRMCS outages
- Status indicators on handhelds for connectivity and sync state.

5.4.21.5 The EAMS-FRMCS interface shall be described in a dedicated Interface Control Document (ICD) compliant with the 3GPP standards governing FRMCS. The ICD shall define:

- Protocols used (e.g., REST, MQTT)
- Message structure
- Retry and queueing behavior
- Device identification and access control methods.

5.4.21.6 Integration of FRMCS with EAMS shall be validated during Factory and Site Acceptance Testing using simulated and real handheld devices in various connectivity scenarios.

5.5 Performance Requirements for EAMS

5.5.1 The EAMS shall meet the following minimum performance response times under normal load conditions, agreed with The Authority (e.g., the indicative values below):

- System initialization time (real-time data servers): not greater than two (2) minutes
- Display of any image, dialog box, or UI component following user interaction: not greater than 0.5 seconds
- Web-based dashboard loading: not greater than 2 seconds
- API response time (95th percentile): not greater than 1.0 second for standard data queries.

5.5.2 The EAMS shall be designed for futureproofing and retrofit upgradeability, including the ability to:

- Install new functional modules and adopt new technologies without re-engineering the system
- Modify, upgrade, or replace individual features or services independently
- Support long-term vendor and platform independence
- Implement version control, rollback procedures, and staged deployment strategies as part of change management.



- 5.5.3 The EAMS shall integrate a performance monitoring module to track and report on system quality metrics, including at minimum:
- System availability and uptime
 - Scheduled vs. unscheduled downtime
 - Service and data accuracy levels
 - User experience (latency, failed interactions, responsiveness)
 - Integration latency with connected systems
 - These KPIs shall be presented via configurable dashboards and exported for SLA and compliance tracking.
- 5.5.4 The EAMS system shall support full customization and shall be based on a modular architecture to ensure separation of services, flexibility in future development, and the ability to isolate system components for independent scaling and maintenance.
- 5.5.5 The failure of any single EAMS node, hardware component, or service endpoint shall not disrupt overall EAMS operations. Redundant system elements shall take over seamlessly to maintain availability.
- 5.5.6 In the event of a communications failure between peripheral equipment and the systems in the OCC, BOCC, or Local Control Rooms, the EAMS and peripheral equipment shall continue operating in a standalone, degraded-but-safe mode until communications are restored.
- 5.5.7 The EAMS shall comply with all safety-related performance and fail-safety requirements as defined in the Contract including any Safety Integrity Level (SIL) classifications applicable to EAMS-controlled functions.
- 5.5.8 The EAMS shall meet the RAM targets defined in Schedule 1 – Safety, Security and RAM Requirements, including specified targets for MTBF (Mean Time Between Failures), MTTR (Mean Time to Repair), and system availability. These metrics shall be validated during system performance testing and monitored continuously in operation.
- 5.5.9 The EAMS shall implement system-wide load balancing and horizontal scaling mechanisms to optimize performance under peak conditions. Clustering of application services and failover configurations shall be tested during system acceptance.
- 5.5.10 The performance of security controls (e.g., encryption, multifactor authentication, intrusion detection) shall be validated to ensure no degradation of user experience or system responsiveness.
- 5.5.11 All EAMS performance data, including response times and user load metrics, shall be captured and stored for analysis and compliance verification for a minimum period (e.g., at least 24 months), agreed with The Authority.
- 5.5.12 EAMS modules related to safety, security, or system integrity shall include built-in performance self-checks and watchdog mechanisms that trigger alerts on delay thresholds or degraded processing speed.
- 5.5.13 The EAMS shall provide a continuous performance dashboard accessible by The Authority, with color-coded SLA compliance indicators, trend analysis, and custom threshold alerts.

5.6 Cybersecurity and Security Requirements

- 5.6.1 The EAMS design, configuration, and operation shall be fully compliant with the *CHSR Cybersecurity Technical Specification*. All EAMS components (including IT, OT, cloud, and edge elements) shall implement the security controls, roles, logging, and assurance measures defined in the *CHSR Cybersecurity Technical Specification*.



5.6.2 The EAMS shall include cybersecurity-relevant assets in its asset management scope and record detailed metadata for each asset. The TSCC Contractor shall review CISA's *Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators* as guidance. At a minimum, the EAMS shall store and manage the following attributes for cybersecurity-relevant assets:

- Device name and logical identifier
- Manufacturer and model
- Hardware type and serial number
- Operating system name and version
- Firmware version and release date
- Installed software and patch levels
- Known vulnerabilities (e.g., CVE identifiers)
- Network interface details (e.g., MAC address, IP address, port status)
- Associated criticality or security classification (if defined)
- Link to cybersecurity risk assessments and controls applied.

This information shall be exportable and used to support threat detection, vulnerability management, and incident response activities in accordance with the *CHSR Cybersecurity Technical Specification*.

5.6.3 The EAMS shall implement a mapping table demonstrating how each EAMS subsystem complies with applicable sections of the *CHSR Cybersecurity Technical Specification*. This mapping shall be submitted to The Authority and reviewed during system acceptance.

5.6.4 The EAMS shall be integrated with a SIEM platform compliant with the *CHSR Cybersecurity Technical Specification*. The EAMS shall send logs, alerts, and key cybersecurity telemetry to the SIEM.

5.6.5 All EAMS user authentication and authorization functions shall use an Identity and Access Management solution compliant with the *CHSR Cybersecurity Technical Specification*.

5.6.6 All APIs used by the EAMS shall be secured in compliance with industry standards (e.g., OWASP) and compliant with the API section of the *CHSR Cybersecurity Technical Specification*.

5.6.7 The asset inventory shall have the capability to label assets according to their criticality.

5.6.8 Information security controls shall be designed and implemented in compliance with the information security section of the *CHSR Cybersecurity Technical Specification*, the EAMS shall have functionality that facilitates compliance with the ISO27001.

5.6.9 Role-based access control (RBAC) shall be enforced consistently across all EAMS modules and interfaces.

5.6.10 The EAMS shall support cybersecurity vulnerability and patch tracking for all managed hardware, firmware, and software components, in alignment with the Vulnerability and Patch Management section of the *CHSR Cybersecurity Technical Specification*.

5.6.11 The EAMS shall enforce secure communications protocols for all internal and external system integrations and shall block or document the use of insecure or deprecated protocols, communications protocols shall be compliant with the *CHSR Cybersecurity Technical Specification*.

5.6.12 Any system event, user activity, or data access attempt affecting critical EAMS functionality shall be logged with timestamps, user IDs, and event descriptions in accordance with the *CHSR Cybersecurity Technical Specification* Section Logging and Monitoring. These logs shall be retained for a minimum period as agreed with The Authority.



- 5.6.13 EAMS components shall be hardened in accordance with applicable industry standards and the *CHSR Cybersecurity Technical Specification*. Any deviation shall require written approval from the Cybersecurity Lead and other appropriate senior stakeholders.
- 5.6.14 The EAMS shall support automated security health checks, with alerts generated for misconfiguration, outdated software components, or integrity check failures.
- 5.6.15 The EAMS shall have a nominated System Owner who shall be accountable for cybersecurity risk ownership and mitigation.
- 5.6.16 The EAMS System Owner shall be responsible for ensuring that appropriate resources are present at cybersecurity threat modelling and risk assessment activities.

6 INTERFACE REQUIREMENTS

6.1 General Requirements

- 6.1.1 Interfaces are classified as below:
- Third Party interfaces: interfaces between systems and systems provided by Third Party (excluding CHSR contractors)
 - External interfaces: interface between systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors)
 - Interfaces between systems within the TSCC Contract.
- 6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.
- 6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.
- 6.1.4 All EAMS interfaces shall support structured, standards-based data formats such as JSON, XML, OPC UA, or CSV, and comply with any semantic or schema constraints.
- 6.1.5 All EAMS interfaces shall be protected by cybersecurity controls including encryption (e.g., TLS 1.3), message authentication, endpoint validation, and compliance with the *TSCC System Technical Specification - Cybersecurity*.
- 6.1.6 Interfaces that support high-frequency data exchanges (e.g., condition monitoring, telemetry) shall meet the defined performance requirements for message latency, throughput, and system responsiveness.
- 6.1.7 All interfaces that exchange sensitive or operational data (e.g., financial, TPS, security telemetry) shall implement secure communication protocols such as TLS 1.3, mutual certificate authentication, and VPN tunneling where required.
- 6.1.8 Each interface shall include fault handling logic, including:
- Retry strategies
 - Alert generation on failed communication
 - Data integrity checks
 - Logging of malformed or incomplete messages.
- 6.1.9 All active interfaces shall be monitored for status, latency, error rates, and availability. EAMS shall present this information in a health dashboard and expose logs to the central monitoring system.



- 6.1.10 All interfaces shall comply with the *TSCC System Technical Specification - Cybersecurity*, including:
- Access control enforcement
 - Endpoint authentication
 - Encrypted communication
 - Logging of interface activity and failures.
- 6.1.11 All raw data received by the EAMS shall be mapped to a normalized internal data model defined in an EAMS Data Dictionary. Inconsistent or unstructured input formats shall be rejected or quarantined for validation.
- 6.1.12 Monitoring interfaces shall use open and widely adopted protocols such as OPC UA, MQTT, or RESTful APIs. Data payloads shall be structured using standard formats (e.g., JSON, XML) and comply with an EAMS schema registry.
- 6.1.13 The EAMS shall provide a feedback mechanism to source systems indicating data reception status, validation success/failure, and any generated events or anomalies triggered by the received data.
- 6.1.14 All monitoring data interfaces shall include:
- Endpoint authentication
 - Data integrity checks (e.g., checksums or digital signatures)
 - Encryption during transit (e.g., TLS 1.3)
 - Role-based access restrictions
in accordance with the *TSCC System Technical Specification - Cybersecurity*.
- 6.1.15 Monitoring data shall be processed and stored within the EAMS to support:
- Trend analysis and dashboards
 - Predictive maintenance (via ML/AI modules)
 - FRACAS root cause analysis
 - Lifecycle cost modeling (LCC)
 - Condition-based maintenance (CBM) routines.
- 6.1.16 Additional metering and telemetry data may be transmitted to the EAMS from subsystems, including but not limited to energy consumption, voltage/current fluctuations, pressure, temperature, and vibration metrics. The TSCC Contractor shall identify the relevant data sources and ensure the EAMS can ingest and process these values at the required frequency.
- 6.1.17 The EAMS shall interface with existing subsystems to automatically gather available operational data including, but not limited to:
- Time-of-use data (e.g., ON/OFF sequences, cycle counts, power-up frequency) for each device and sub-component
 - Non-emergency fault or warning events
 - Alarms and condition-based alerts with associated metadata (e.g., location, priority, asset ID).
- 6.1.18 Security appliances and platforms (e.g., intrusion detection, endpoint protection) shall be integrated with the EAMS for telemetry, configuration monitoring, and operational coordination, subject to approval and alignment with the *TSCC System Technical Specification - Cybersecurity*.



6.2 Third Parties Interfaces

- 6.2.1 Where the EAMS exposes APIs or open interfaces for integration with Third Parties systems, such interfaces shall be secure and standards-based, supporting structured and interoperable data formats such as ISO 10303 (STEP), Industry Foundation Classes (IFC), JSON, XML, or OPC UA.

6.3 External Interfaces

6.3.1 Interfaces with operator systems

- 6.3.1.1 The EAMS shall include a finance interface module to exchange procurement and accounting data with external financial systems from the operator. This interface shall manage, at a minimum:

- Creation and status updates for purchase requisitions and purchase orders
- Inventory updates for received goods
- Cost and budget modifications
- Currency and tax rate changes
- Asset depreciation tracking and reporting.

- 6.3.1.2 The EAMS shall include a human resources interface module to exchange staff data with external system from the operator to support staff assignment, work planning, and compliance with labor constraints.

- 6.3.1.3 The EAMS shall support integration with standard email and messaging services (e.g., SMTP, SMS gateway, REST-based messaging APIs) to notify external suppliers of service requests, shipment updates, and material requirements.

- 6.3.1.4 The EAMS shall support communication with external systems using open, industry-standard protocols such as REST, SOAP, OPC UA, MQTT, or others as approved by The Authority. All interface protocols shall ensure reliable data exchange for asset monitoring, lifecycle tracking, and infrastructure planning.

6.3.2 Interfaces with stations contractors

- 6.3.2.1 The EAMS shall interface with station contractor systems to integrate static Asset Information data dynamic Asset Information including:

- Stations building elements, civil structures, concourse, platforms, waiting areas, offices, architectural elements, cable routes, restrooms, fencing, emergency equipment's, etc.
- Stations Mechanical and Electrica assets: Lighting, Medium Power Voltage Systems, Elevators, Escalators, Drainage and Hydraulics Systems, Fire Protection Systems, Heating Ventilation and Air Conditioning Systems.

6.3.3 Interfaces with facilities contractors

- 6.3.3.1 The EAMS shall interface with facilities contractor systems to integrate static Asset Information data dynamic Asset Information including:

- Facilities building elements, civil structures, concourse, areas, offices, architectural elements, cable routes
- Facilities Mechanical and Electrica assets: Lighting, Medium Power Voltage Systems, Elevators, Drainage and Hydraulics Systems, Fire Protection Systems, Heating Ventilation and Air Conditioning Systems.
- Trains Maintenance equipment

6.3.4 Interfaces with civil contractors



6.3.4.1 The EAMS shall interface with facilities contractor systems to integrate static Asset Information data dynamic Asset Information including:

- Civil structures: bridges, viaducts, tunnels

6.3.5 **Interfaces with trainsets contractor**

6.3.5.1 The EAMS shall interface with facilities contractor systems to integrate static Asset Information data dynamic Asset Information including:

- Near Real-Time Operational Data: speed and acceleration, deceleration, power usage
- Condition Monitoring data: vibration levels, temperature of critical components, brake performance, doors operations
- Fault and alarm

6.3.6 **Interfaces with Solar PV and Battery Electrical Storage System (BESS) contractors**

6.3.6.1 The EAMS shall provide for future interfaces with Solar PV and BESS contractor systems to integrate static Asset Information data dynamic Asset Information including:

- Solar PV production
- Battery Electrical Storage System

6.4 **Internal interfaces**

6.4.1 **TSCC Subsystems static and dynamic Asset Information**

6.4.1.1 The EAMS shall interface with TSCC Subsystems to integrate static Asset Information data and dynamic Asset Information data of TSCC Subsystems assets, including:

- Integrated Control and Supervision System (ICSS)
- Network Timing System (NTS)
- Traffic Management Systems (TMS)
- Digital Communication Network (DCN)
- Wireless Communication Systems (WCN)
- Telephony System
- Public Address and Customer Information Systems (PACIS)
- Electronic Access Control System (EACS)
- CCTV System
- Hazard Detection and Early Warning Systems
- Overhead Catenary System (OCS)
- Traction Power System
- Power SCADA System
- Low Voltage Power Distribution
- Fire Protection System
- Cybersecurity System

6.4.2 Interface with Network Timing System (NTS)



- 6.4.2.1 The EAMS shall interface with NTS systems to integrate static Asset Information data and exchange real-time, near-real-time, and historical data of NTS as described in the NTS Technical Specification.
- 6.4.2.2 The EAMS shall interface with the Network Timing System to synchronize the timestamps across all EAMS components and subsystems.
- 6.4.2.3 Time synchronization shall include fallback mechanisms and periodic drift detection. All logs and transactions within the EAMS shall include synchronized timestamps for traceability and event reconstruction.
- 6.4.3 Interface with Traffic Management System (TMS)
 - 6.4.3.1 The EAMS shall interface with the TMS to receive structured data regarding the status of engineering possessions, including start/end times, affected sections, and operational constraints. This data shall be used to suppress or adjust maintenance scheduling during affected periods.
 - 6.4.3.2 The EAMS shall receive incident and delay information from TMS, including root cause classification, location, impacted assets, and timestamp. This information shall be used to generate corrective maintenance work orders, flag affected assets for condition reassessment and correlate with FRACAS records.
- 6.4.4 Interface with Integrated Control and Supervision Systems (ICSS)
 - 6.4.4.1 Where overlaps exist between ICSS and other CHSR subsystems, a single, normalized data structure and processing logic shall be applied to avoid duplication and maintain consistency in alarm and event processing.
- 6.4.5 Interface with Digital Communication Network (DCN)
 - 6.4.5.1 The EAMS equipment shall be connected to the DNC via a dual-redundant physical and logical path to ensure continuous availability.
 - 6.4.5.2 The TSCC Contractor shall ensure that all data transmitted between the EAMS and the DCN is protected using secure communication protocols, including encryption (e.g., TLS 1.3, IPsec, or MACsec), mutual authentication, and integrity validation. All network transmission security shall comply with the *TSCC System Technical Specification - Cybersecurity*.
 - 6.4.5.3 The EAMS shall operate within the DCN delivered network infrastructure using a defined subnet or VLAN segment. The network configuration shall support logical separation of services, role-based access controls, and zoning for IT/OT isolation as required by the California HSR Network Architecture Guidelines and *TSCC System Technical Specification - Cybersecurity*.
 - 6.4.5.4 All EAMS communication over the Digital Communication Network shall use encrypted transport protocols (TLS 1.3, MACsec, or equivalent) and enforce endpoint authentication. Credentials and keys used shall be rotated in accordance with the Public Key Infrastructure (PKI) requirements of the *TSCC System Technical Specification - Cybersecurity*.
 - 6.4.5.5 EAMS network interfaces shall be logically segmented using VLANs or software-defined networking (SDN) constructs to separate functional domains (e.g., asset telemetry, maintenance data, admin access). Segmentation shall align with security zones defined in the *TSCC System Technical Specification - Cybersecurity*.
 - 6.4.5.6 The EAMS shall continuously monitor the health of its connection to the DCN.
- 6.4.6 **Internal with Wireless Communication Systems (WCS)**



- 6.4.6.1 The EAMS shall be capable of seamless integration with the Future Railway Mobile Communication System (FRMCS) to support secure, real-time data exchange with authorized handheld devices used by maintenance, inspection, and operations personnel. This integration shall enable two-way communication for activities such as work order updates, fault logging, asset status reporting, and field notifications, in compliance with the *TSCC System Technical Specification - Cybersecurity*.

6.4.7 Interfaces with Medium and Low Voltage Power System

- 6.4.7.1 The EAMS shall establish a dual-redundant interface with the Medium Voltage Power Supply System to receive power availability status, fault indicators, and performance telemetry. UPS and battery systems shall be provided by the Medium Voltage Power Supply System but shall expose monitoring data to the EAMS, including operational status, alarms, and switchover events. The interface shall comply with performance, redundancy, and cybersecurity requirements defined in the *TSCC System Technical Specification - Cybersecurity*.

- 6.4.7.2 The EAMS shall receive the following data from the Medium and Low Voltage Power Distribution System:

- Power source status (utility, generator, UPS)
- Fault and alarm codes
- Voltage and frequency levels
- Switchover events and durations
- Real-time and historical load metrics.

- 6.4.7.3 The EAMS shall monitor UPS and battery systems for:

- Battery health and charge level
- Estimated runtime remaining
- Number of discharge cycles
- Alert conditions (e.g., low charge, overload, maintenance due).

6.4.8 Interface with Cybersecurity

- 6.4.8.1 The EAMS shall interface with cybersecurity systems as defined in the *TSCC System Technical Specification - Cybersecurity*. This shall include real-time and scheduled data exchange with systems such as the Security Information and Event Management (SIEM) platform, Public Key Infrastructure (PKI), Endpoint Detection and Response (EDR), Vulnerability Management platform, Identity and Access Management (IAM) systems and the Security Control Room in the OCC. The EAMS shall support secure, bidirectional communication to enable threat detection, incident response, and continuous security monitoring.

- 6.4.8.2 The EAMS shall integrate with the following cybersecurity systems:

- SIEM for event log forwarding (e.g., login attempts, permission changes, failed API calls)
- OCC for real-time incident notifications, asset threat status, and compliance reporting
- IAM for user provisioning, role-based access control (RBAC), and audit trails
- PKI for certificate-based authentication of users and system interfaces
- EDR/Antivirus platforms for endpoint telemetry and security posture of EAMS nodes
- Vulnerability Management Systems for status of patches, CVEs, and system hardening metrics.
- The EAMS shall forward all relevant security events, audit logs, and system alerts to the SIEM using structured, timestamped, and integrity-verified log formats (e.g., syslog, CEF, JSON).



Logs shall be classified by sensitivity and retained according to California HSR retention policies.

- The EAMS shall be capable of receiving threat intelligence updates (e.g., IOCs, IP blocklists) and automated response commands (e.g., isolate device, disable user) from the OCC or cybersecurity automation platform.

6.4.8.3 The cybersecurity interface requirements shall be traceable to the relevant sections of the TSCC System Technical Specification - Cybersecurity, including:

- Section Vulnerability and Patch Management
- Section Identity and Access Management
- Section Cybersecurity Operations Center
- Section Logging and Monitoring.



7 MATERIALS, PRODUCTS AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied by the TSCC Contractor shall comply with applicable United States standards (e.g., ASTM, ANSI, IEEE, NFPA). Where no equivalent U.S. standard exists, relevant EN, ISO, or other internationally recognized standards may be used, as approved by The Authority and defined in *Section 2.2*.
- 7.1.2 All materials supplied shall be of sufficient quality to meet the designed service life requirements defined in the California HSR RAM and LCC strategies, and shall be verified through applicable certification, documentation, and testing protocols.
- 7.1.3 All materials shall be supported by certificates of compliance (e.g., mill test certificates, manufacturer declarations) indicating conformity with applicable standards. Where third-party certifications are required (e.g., UL, FM, NSF), copies shall be provided prior to installation.
- 7.1.4 A hierarchy of applicable standards shall be followed in this order of preference:
- California HSR-specific standards
 - U.S. national standards (e.g., ASTM, ANSI, AASHTO, IEEE)
 - ISO/IEC or other international standards
 - EN standards (when justified and accepted by The Authority).
 - All materials shall be selected with consideration for:
 - Long-term availability and resistance to obsolescence
 - Use of environmentally sustainable or recyclable materials
 - Avoidance of restricted substances (e.g., per REACH, RoHS).
- 7.1.5 For materials or components with embedded software (e.g., smart sensors), the following shall apply:
- Firmware version shall be documented and tracked
 - Components shall be assessed for known vulnerabilities (e.g., CVEs)
 - Software updates shall follow secure patch management
 - Unauthorized remote access features shall be prohibited.

7.2 Software and Hardware specific requirements

- 7.2.1 The EAMS design shall be based on Commercial Off-The-Shelf (COTS) components, open architecture, and modular system architecture, using industry-standard, non-proprietary interfaces.
- 7.2.2 The TSCC Contractor's design for all central servers shall be on-premises, either physical, virtualized, or cloud-based, to support storage and data exchange. All solutions shall comply with the *TSCC System Technical Specification - Cybersecurity*. Containerized infrastructure may also be considered, provided it meets operational and security requirements.
- 7.2.3 The EAMS handheld devices shall be fanless and ergonomically designed to improve user comfort in field conditions.
- 7.2.4 EAMS handheld devices shall demonstrate optimal performance and scalability to support growing data volumes and concurrent users. Devices shall maintain responsive performance under varying load conditions and be compatible with future EAMS database and feature expansions.



- 7.2.5 EAMS handheld devices shall support at least a minimum period of active use (e.g., 12 hours), agreed with The Authority, with the EAMS application and shall feature rapid charging capabilities.
- 7.2.6 The EAMS system shall include redundant power supply to prevent single points of failure.
- 7.2.7 EAMS devices shall be connected to the Uninterruptible Power Supply (UPS) infrastructure of the OCC or other critical facilities where installed.
- 7.2.8 The EAMS shall support future scalability and modular expansion while meeting or exceeding its REAMS targets, including support for degraded modes and failover conditions.
- 7.2.9 The TSCC Contractor shall provide EAMS workstations at each maintenance facility and within the OCC.
- 7.2.10 EAMS shall be provided with all required software licenses to support full lifecycle use.
- 7.2.11 License utilization shall be analyzed by the TSCC Contractor, and the most cost-effective solution proposed (e.g., subscription-based or perpetual), with the number of licenses minimized to meet operational needs.
- 7.2.12 The EAMS shall support the use of handheld or portable smart devices by field engineers and technicians for maintenance and inventory purposes, including wireless EAMS access and automatic asset identification using embedded tags (e.g., RFID or NFC).
- 7.2.13 The EAMS shall maintain and update all records in real time. Its architecture shall prevent data loss from single points of failure and shall include automated failure detection with corresponding alarms.
- 7.2.14 The EAMS system shall include:
- Servers located at the OCC
 - Operating system platforms based on modern, industry-standard technologies (e.g., Linux or Windows)
 - Local storage and analysis infrastructure, including container-based applications, where applicable.
- 7.2.15 The EAMS software shall be fully web-architected using modern development frameworks and technologies.
- 7.2.16 The EAMS shall support integration with Common Data Environment (CDE) servers and related services.
- 7.2.17 EAMS software shall be accessible to mobile maintenance staff via handheld terminals. Offline mode support shall be provided, allowing access to essential functions when network connectivity is unavailable.
- 7.2.18 All general-purpose software (e.g., operating systems, data stores, process control, networking, telecoms, and cloud infrastructure) shall be proven industrial-grade solutions widely used in commercial and critical infrastructure applications.
- 7.2.19 The EAMS interface shall be responsive and optimized for multiple user roles (e.g., operators, engineers, managers), and adaptable to devices such as PCs, tablets, and smartphones. AR/VR technologies may be used to support asset data visualization during maintenance activities.
- 7.2.20 The TSCC Contractor shall define, in conjunction with The Authority, the data-driven maintenance strategy and required EAMS modules to optimize asset performance.
- 7.2.21 Access to EAMS archives shall be controlled via strong authentication mechanisms. Access to sensitive repositories shall be restricted, logged, and protected with password policies that align with the *TSCC System Technical Specification - Cybersecurity*.



- 7.2.22 The EAMS server operating environment shall support lightweight client HMI architecture and multi-session support. Cybersecurity requirements for deployment shall be confirmed and integrated through formal workshops with The Authority.
- 7.2.23 The TSCC Contractor shall specify a web-based EAMS HMI using modern server and webserver architectures, including virtual machine and container support for scalability and simplified administration.
- 7.2.24 The TSCC Contractor shall provide a dedicated handheld application for field maintenance staff.
- 7.2.25 The processing capabilities of EAMS servers, workstations, and peripherals shall be sufficient to handle all operational events and include automatic backup and restoration functions for software and data.
- 7.2.26 The EAMS hardware and software components shall be optimized to support fast data visualization, minimal latency, and high-resolution display quality under all system loads.
- 7.2.27 Hardware scaling for the EAMS system shall primarily support horizontal expansion by adding servers and modular computers or storage elements.
- 7.2.28 The TSCC Contractor shall provide full version control records for all EAMS firmware, software, and handheld applications. Updates shall follow patch management and vulnerability scanning procedures defined in the *TSCC System Technical Specification - Cybersecurity*.
- 7.2.29 All operating systems and third-party software shall be hardened in accordance with CIS Benchmarks or equivalent standards.
- 7.2.30 All EAMS handheld devices shall be ruggedized and managed through Mobile Device Management (MDM). Devices shall support remote wipe, full disk encryption, and secure login methods.
- 7.2.31 The TSCC Contractor shall demonstrate that EAMS hardware and software will remain serviceable for a minimum of 15 years. Upgrade paths, component interchangeability, and modularity shall be documented and maintained.
- 7.2.32 All EAMS hardware and software components shall undergo Factory and Site Acceptance Testing, including:
- Performance under full system load
 - Failure/recovery validation
 - Backup and restoration functionality.
- 7.2.33 The TSCC Contractor shall deliver full installation, configuration, operation, and maintenance manuals for all software and hardware components, including interface specifications.



8 TOLERANCES

Not applicable to EAMS



9 SCOPE OF SUPPLY AND DELIVERY

- 9.1.1 The TSCC Contractor shall be responsible for the complete delivery, installation, configuration, testing, commissioning, and handover of the EAMS solution. The scope shall include all hardware, software, documentation, tools, training, and services necessary to ensure full functionality, maintainability, and compliance with the requirements of this specification.

9.2 Specific Requirements

9.2.1 Hardware and Infrastructure

- 9.2.1.1 The TSCC Contractor shall supply all central, backup, redundant, and edge servers necessary to support the EAMS architecture.
- 9.2.1.2 The TSCC Contractor shall supply and install EAMS operator workstations and Human-Machine Interfaces (HMI) at the Operations Control Center (OCC), Backup OCC (BOCC), and Infrastructure Maintenance Facilities.
- 9.2.1.3 All EAMS hardware components shall support horizontal and modular scalability and include redundant power supplies, local storage, and UPS integration.

9.2.2 Software and Licenses

- 9.2.2.1 The TSCC Contractor shall provide and install all required EAMS software, including database engines, analytics modules, handheld apps, mobile interfaces, and web-based HMI platforms.
- 9.2.2.2 The EAMS software architecture shall include full documentation of the system structure, communication protocols, interfaces, API definitions, and integration points with other systems.
- 9.2.2.3 The TSCC Contractor shall supply all required software licenses and subscriptions for the full lifecycle of the EAMS. Licenses must be transferrable to The Authority at the time of handover and shall not impose vendor lock-in.
- 9.2.2.4 A license register shall be maintained by the TSCC Contractor and delivered to The Authority, including type, scope, expiry dates, renewal conditions, and terms of use.

9.2.3 Tools, Spares and Auxiliary Equipment

- 9.2.3.1 The TSCC Contractor shall deliver all specialized test tools and diagnostic equipment necessary to validate, operate, and maintain the EAMS.
- 9.2.3.2 An initial set of spare parts for critical EAMS components shall be provided and documented in the asset register, including part numbers, expected replacement intervals, and storage requirements.
- 9.2.3.3 The TSCC Contractor shall supply all auxiliary equipment required for installation and protection of EAMS assets, including but not limited to mounting brackets, cases, cable bindings, and field accessories for handheld devices.

9.2.4 Training and Knowledge Transfer

- 9.2.4.1 The TSCC Contractor shall deliver training to OCC operators, field technicians, cybersecurity personnel, and maintenance planners. Training shall be delivered in both classroom and hands-on formats.
- 9.2.4.2 Training materials, including user guides, quick reference sheets, and safety instructions, shall be included as part of the documentation deliverables.

9.2.5 Support and Handover



- 9.2.5.1 The TSCC Contractor shall provide post-delivery support, including patches, software updates, and maintenance for the full design life of the EAMS, in accordance with REAMS and cybersecurity requirements.
- 9.2.5.2 At the time of project handover, the TSCC Contractor shall deliver a final transfer package including:
- Final system configuration
 - Complete and validated backups
 - Password vault or credential record
 - Software license keys and certificates
 - Confirmation of transfer of ownership and IP rights where applicable.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in Schedule 16 the Scope of Work.



12 TESTING, VALIDATION AND ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.

12.2 Specific Requirements Factory Acceptance Testing (FAT)

12.2.1 The TSCC Contractor shall conduct Factory Acceptance Testing (FAT) at the TSCC Contractor's facility, or another approved site, to verify that EAMS hardware, software, and configurations meet the contractual requirements before delivery to the project site.

12.2.2 FAT shall include functional testing of:

- EAMS user interface and data workflows
- Core software modules (e.g., work order generation, asset registry, reporting)
- API and protocol communication (e.g., OPC UA, MQTT, REST)
- System redundancy and failover
- Alarm and event processing logic.

12.2.3 All FAT results shall be formally documented and submitted to The Authority, including identified issues and corrective actions taken.

12.3 Specific Requirements Site Acceptance Testing (SAT)

12.3.1 The TSCC Contractor shall perform Site Acceptance Testing (SAT) after the EAMS has been delivered, installed, and configured in the operational environment.

12.3.2 SAT shall validate the correct integration of the EAMS with external systems (e.g., ICSS, TMS) and include:

- Connectivity and interface verification
- Data exchange and synchronization
- Alarm/event generation from live sources
- User role access control
- Redundancy and failover behavior under live conditions.

12.3.3 The SAT plan and procedure shall be approved by The Authority before execution. SAT shall be witnessed by The Authority or its representative.

12.3.4 All SAT results, test logs, and issue resolutions shall be submitted as part of the final Acceptance Test Report.

12.4 Specific Requirements Performance Benchmark Testing

12.4.1 The EAMS shall be subject to performance testing during FAT and SAT to ensure that the system meets response time, throughput, and availability benchmarks.

12.4.2 The TSCC Contractor shall simulate peak operational load conditions, including concurrent user access, real-time data ingestion, and reporting activity, to validate sustained performance.



12.5 Specific Requirements Cybersecurity

12.5.1 The EAMS shall be subject to cybersecurity validation as defined in the *CHSR Cybersecurity Technical Specification*

12.5.2 Cybersecurity testing shall include, but not be limited to:

- Authentication and access control testing
- Logging and monitoring verification
- Security misconfiguration and privilege escalation attempts
- Vulnerability scanning (e.g., CVEs, default credentials, open ports)
- Penetration testing of EAMS web interface and APIs.

12.5.3 Penetration testing shall be conducted by an independent, certified cybersecurity specialist and documented in a detailed report including findings, severity levels, and remediation actions.

12.5.4 The system shall not be accepted until all high and medium severity cybersecurity vulnerabilities have been resolved or mitigated to the satisfaction of The Authority.



13 SUBMITTALS

13.1 General Requirements

13.1.1 The submittals required for the Interlocking system are defined in Schedule 16 Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor and related Suppliers, information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence Interlocking system reliability, availability and maintainability characteristics.



16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.



Schedule 5(e)

European Train Control System (ETCS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specification

SPEC-0009 – European Train Control System (ETCS)

Rev. 1.0

A blue ink signature of Francois Pignard, consisting of a stylized 'F' followed by a horizontal line and a small flourish.

Authored:

Francois Pignard, TCS Engineer

10/15/2025

Date

A blue ink signature of Andrew Clapham, featuring a stylized 'A' and 'C'.

Checked:

Andrew Clapham, Train Control Lead

10/15/2025

Date

A blue ink signature of Bruno Comperat, featuring a stylized 'B' and 'C'.

Checked:

Bruno Comperat, Deputy Director of Rail Engineering

10/16/2025

Date

A blue ink signature of Ryan Scott, featuring a stylized 'R' and 'S'.

Approved:

Ryan Scott, Director of Rail Engineering

10/16/2025

Date

A blue ink signature of Amit Joshi, featuring a stylized 'A' and 'J'.

Released:

Amit Joshi, Configuration Manager

10/16/2025

Date



Document Revision History – ETCS Specifications**Second Edition****February 2026**

Revision	Date	Revision Description
0.0	September 2025	First edition
1.0	February 2026	Second Edition – Updated for TSCC Addendum 4



TABLE OF CONTENT

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION.....	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
1.1	GENERAL	6
2.2	ENGINEERING RULES GUIDELINES.....	6
2.3	TECHNICAL SPECIFICATIONS FOR INTEROPERABILITY	6
2.4	EULYNX.....	7
2.5	EUROPEAN AND OTHER INTERNATIONAL STANDARDS	7
2.6	EUG/ERTMS ENGINEERING GUIDELINES	7
2.7	TSCC DOCUMENTS	8
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	9
4	SYSTEM DESCRIPTION	10
4.1	PURPOSE OF ERTMS/ETCS.....	10
4.2	ERTMS/ETCS DEFINITION.....	10
4.3	ERTMS/ETCS OPERATIONAL CONTEXT	11
4.4	DESIGN LIFE	12
5	SYSTEM REQUIREMENTS.....	13
5.1	GENERAL REQUIREMENTS.....	13
5.2	ENVIRONMENTAL REQUIREMENTS.....	14
5.3	OPERATIONAL REQUIREMENTS	14
5.4	FUNCTIONAL REQUIREMENTS.....	19
5.5	PERFORMANCE REQUIREMENTS.....	29
5.6	REQUIREMENTS FOR EUROBALISES	30
5.7	CYBERSECURITY REQUIREMENTS.....	31
6	INTERFACES.....	32
6.1	GENERAL REQUIREMENTS.....	32
6.2	THIRD PARTIES INTERFACES.....	32
6.3	EXTERNAL INTERFACES - TRAINSETS CONTRACTOR.....	32
1.2	EXTERNAL INTERFACES – FACILITIES CONTRACTOR	33
6.4	INTERNAL INTERFACES	33
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS	37
8	TOLERANCES	38
9	SCOPE OF SUPPLY AND DELIVERY	39
9.1	GENERAL REQUIREMENTS.....	39
9.2	SPECIFIC REQUIREMENTS	39
10	MANUFACTURING.....	40
10.1	GENERAL REQUIREMENTS.....	40
11	INSTALLATION AND INTEGRATION.....	41



11.1	GENERAL REQUIREMENTS.....	41
11.2	SPECIFIC REQUIREMENTS	41
11.3	INSTALLATION REQUIREMENTS FOR BALISES.....	41
11.4	INSTALLATION REQUIREMENTS FOR TRACKSIDE MARKER BOARDS.....	42
11.5	MOUNTING REQUIREMENTS FOR INDOOR EQUIPMENT	43
12	TESTING & ACCEPTANCE	44
12.1	GENERAL REQUIREMENTS.....	44
12.2	SPECIFIC REQUIREMENTS	44
13	SUBMITTALS.....	45
13.1	GENERAL REQUIREMENTS.....	45
14	QUALITY MANAGEMENT.....	46
14.1	GENERAL REQUIREMENTS.....	46
15	ADDITIONAL INFORMATION REQUESTED	47
16	LOGISTICS	48



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the CHSR Authority's Requirements for the European Railway Train Management System / European Railway Train Control System (ERTMS/ETCS).
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of ETCS alongside other Train Control Systems is presented in Appendix A.
- 1.1.4 The requirements are formulated in accordance with using the following words and their meanings:
 - **"Shall"**: Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure).
 - **"Should"**: Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents.
 - **"Must"**: Indicates an obligation or a mandatory requirement.
 - **"May"**: Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines and specifications provided in this chapter for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, and training.
- 2.1.2 All generic standards to be used are provided in: Technical Contract Requirements – Scope of Work.

2.2 Engineering Rules Guidelines

- 2.2.1 Engineering Rules shall be considered as a guideline that has been used for reference design purpose and can be adjusted by the TSCC Contractor if necessary.
- 2.2.2 The latest version of the following Engineering Rules shall be applied:

ID	Code	Title
[R1]	19_STS	Signalling Engineering Rules
[R2]	DCM_01	Design Criteria Manual Chapter 1: Overview
[R3]	DCM_12	Design Criteria Manual Chapter 12: Communication Systems and Train Control
[R4]	AREMA_17	AREMA Standards Chapter 17 – High-Speed Rail Systems

TABLE 12 - ENGINEERING RULES

2.3 Technical Specifications for Interoperability

- 2.3.1 The following TSI and the related Application Guide applies to the Control-Command and Signalling (TCS) subsystems of the rail system in the European Union, including the HSR.
- 2.3.2 The Guide for the application of the TCS TSI is of voluntary application, as it does not mandate any requirement or specification in addition to those set out in the TCS TSI which instead are an essential part of the definition of the basic parameters and therefore mandatory.

ID	TSI	Title
[R5]	[TCS TSI 2023]	COMMISSION IMPLEMENTING REGULATION (EU) 2023/1695 of 10 August 2023 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union and repealing Regulation (EU) 2016/919
[R6]	[TCS TSI AG]	Guide for the application of the TCS TSI. In accordance with Article 19(3) of Regulation (EU) 2016/796 of the European Parliament and of the Council of 11 May 2016

TABLE 13 - LIST OF TSI AND REGULATIONS



2.4 EULYNX

- 2.4.1 The EULYNX Baseline Set 4 Release 4 shall apply to the Interlocking system of HSR, including its standard common interface with ETCS.

	Standard	Title
[R7]	[EULYNX Baseline Set 4 Release 4]	All documents listed in "EULYNX Documentation plan Eu.Doc.11 v4.1.pdf"

TABLE 14 - EULYNX SET OF SPECIFICATIONS

2.5 European and Other International Standards

- 2.5.1 The relevant standards to be used for ERTMS/ETCS are listed in the Scope of works document.
- 2.5.2 The latest in-force standards shall be applied, and if the standard is directly quoted in Annex A of the TCS TSI (list of mandatory standards) the version referenced in the TSI shall always prevail.

2.6 EUG/ERTMS Engineering Guidelines

- 2.6.1 The following ERTMS Users Group (EUG) guidelines can be applied to the ERTMS/ETCS of HSR where applicable.
- 2.6.2 As the current ERTMS guidelines refer to ETCS Baseline 2 and Baseline 3, the TSCC Contractor shall be able to reflect the engineering approach recommended by EUG in the new TCS TSI introducing ETCS Baseline 4.

	Guideline	Title
[R8]	EUG/ERTMS Engineering Guideline #23	Balise Engineering L2 and L3
[R9]	EUG/ERTMS Engineering Guideline #28	Gradients Segmentation
[R10]	EUG/ERTMS Engineering Guideline #66	Transition from SV 1.Y to SV 2.Y L1/2/3 with NTC Fallback
[R11]	EUG/ERTMS Engineering Guideline #67	Level Transition from LNTC to L1 SV2.Y
[R12]	EUG/ERTMS Engineering Guideline #68	Start of Mission B3
[R13]	EUG/ERTMS Engineering Guideline #69	Automatic Track Ahead Free (ATAF) B3
[R14]	EUG/ERTMS Engineering Guideline #70	Transition from L1 to STM
[R15]	EUG/ERTMS Engineering Guideline #71	Transition from L2 to LSTM
[R16]	EUG/ERTMS Engineering Guideline #72	Level Transition from level STM to L1
[R17]	EUG/ERTMS Engineering Guideline #74	RBC-RBC Handover
[R18]	EUG/ERTMS Engineering Guideline #75	Management of Shunting Activities
[R19]	EUG/ERTMS Engineering Guideline #76	Border Crossings
[R20]	EUG/ERTMS Engineering Guideline #77	Level Transition from LNTC to L2
[R21]	EUG/ERTMS Engineering Guideline #78	Level Transition from L2 to LNTC
[R22]	EUG/ERTMS Engineering Guideline #79	Baseline 2 Trackside for Baseline 3 Trains
[R23]	EUG/ERTMS Engineering Guideline #80	Hybrid Train Detection Engineering



	Guideline	Title
[R24]	EUG/ERTMS Engineering Guideline #81	Extension Key Request Function
[R25]	EUG/ERTMS Engineering Guideline #82	B2 to B3 RBC handover – under development
[R26]	EUG/ERTMS Engineering Guideline #83	Lost Connections – under development
[R27]	EUG/ERTMS Engineering Guideline #84	Overall ETCS (Compendium) – under development
[R28]	EUG/ERTMS Guideline 23E064-1A	KMS Guideline

TABLE 15 - LIST OF EUG GUIDELINES

2.7 TSCC Documents

2.7.1 The following documents shall be referred to:

ID	Document	Title
[R29]	Technical Contract Requirements	Scope of Work
[R30]		Wireless Communication System Specification
[R31]		Cybersecurity Technical Specification
[R32]		Hazard Detection and Early Warning System Specification
[R33]		Medium Voltage/Low Voltage Power Supply Technical Specification
[R34]		Network Timing System Technical Specification
[R35]		Digital Communication Network Technical Specification

TABLE 5 – TSCC DOCUMENTS

3 TERMS, DEFINITIONS, AND ABBREVIATIONS

- 3.1.1 All the terms, definitions, and abbreviations are provided in the Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of ERTMS/ETCS

- 4.1.1 The purpose of the ERTMS/ETCS is to ensure safe and technically interoperable train operation across the HSR Railway.

4.2 ERTMS/ETCS Definition

- 4.2.1 In this Technical Specification, the ERTMS/ETCS (hereinafter ETCS) shall be understood as part of the ERTMS system consisting of the standardised ETCS components and the Wireless Communication Systems component as specified in [R30].
- 4.2.2 Focusing on the regulatory framework of TCS TSI, the ETCS is expected to operate within the technical context set out below.

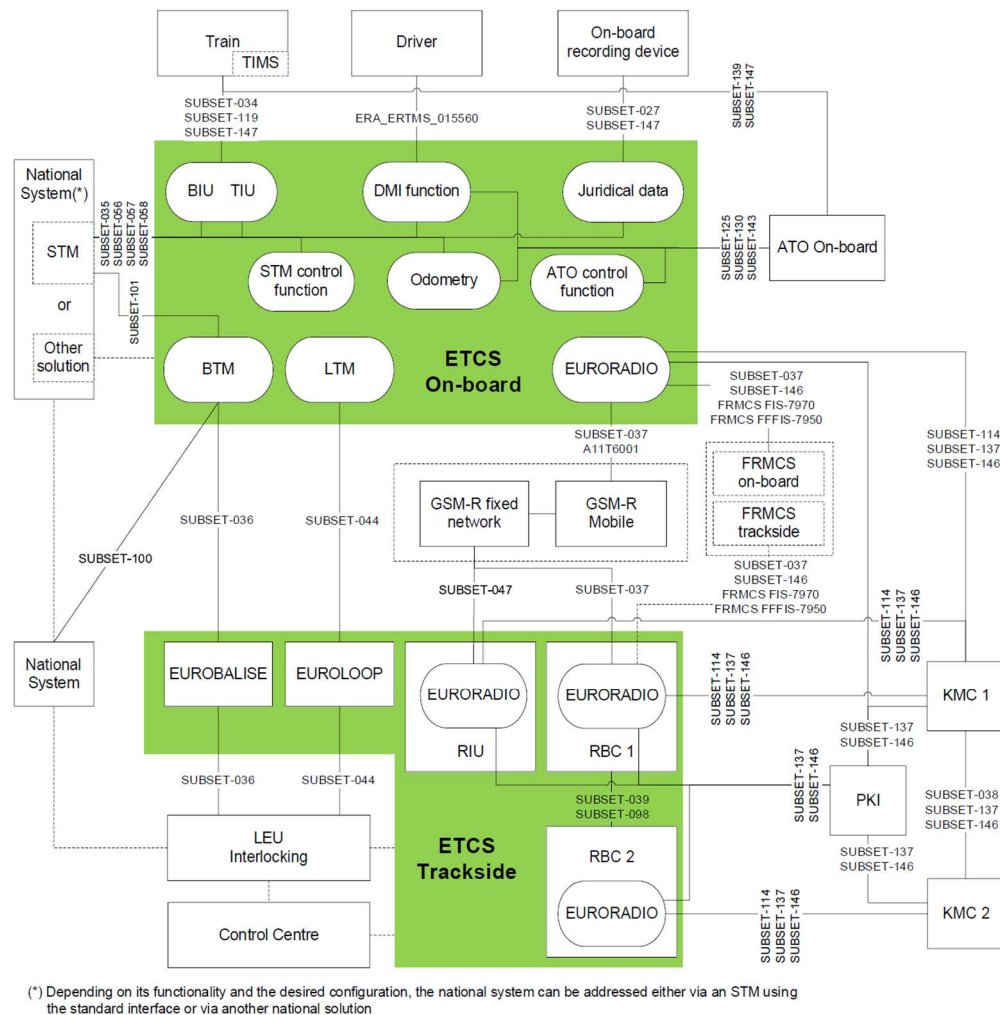


FIGURE 1 - ETCS TECHNICAL CONTEXT



- 4.2.3 The ETCS is composed of ETCS Trackside (ETCS-TS) and ETCS On-Board (ETCS-OB) which communicate via balises or radio messages.
- 4.2.4 This Technical Specification deals with the ETCS trackside part of TCS Subsystem, consisting of:
- Radio Block Centre (RBC), to enable ERTMS Level 2 train operations.
 - Eurobalises, mainly for location referencing.
 - Offline Key Management System (KMS), to secure Euroradio messages via the cryptographic keys. (Note: inputs and outputs provisions shall be made to enable future interface with Online KMS, which would eventually replace the Offline KMS)
 - Harmonized trackside marker boards, mainly to support driver operations when running close to the end of authorities or during on-sight train operations.
 - Non-harmonized trackside boards, mainly consisting of fixed signs supporting shunting operations, geographical reference, and other operational purposes.
 - Data recording, diagnostic and maintenance support.
 - Technical and functional interfaces internal to ETCS.
 - Technical and functional interfaces between ETCS and the other Systems of TSCC Subsystem.
 - Technical and functional interfaces between ETCS and the other Subsystems: Trainsets which are designed in accordance with the relevant TSIs.
- 4.2.5 All items listed above shall be within the scope of supply and delivery of the TSCC Contractor.
- 4.2.6 Balise groups shall consist of one or two balises.
- 4.2.7 KMS shall be an Offline KMS developed in accordance with Subset 114 of [TCS TSI 2023]. This Offline KMS shall be capable of being replaced with Online KMS when the number of keys required to be managed increases to a level where this Online feature becomes necessary.
- 4.2.8 Harmonized marker boards are designed according to the relevant TSI; non-harmonized signs shall be proposed by Contractor and agreed by CHSR Authority during the generic design phase. The TSCC Contractor shall provide information on materials, dimensions, optical properties, and operational purpose.
- 4.2.9 Additional non-harmonized signs may be necessary to identify other specific locations on the track:
- Wireless Communication Systems area;
 - RBC borders;
 - Start/end of interlocked areas;
 - Start/end of reversing areas, if any;
 - Safe areas, if any;
 - Station platforms: start/end of platform, normal stopping points;
 - At road overpasses when protected by vehicle fall detectors, etc...

4.3 ERTMS/ETCS Operational Context

- 4.3.1 In the operational context of TCS Subsystem, ETCS is one System of the whole HSR Train Control System which also includes the Wireless Communication System (Future Railway Mobile Communication System), CBI (Computer Based Interlocking) or IXL, TMS (Traffic Management System), and other TSCC supporting systems (Network Timing System, Hazard Detection and Early Warning System, Low Voltage Power System, Enterprise Asset Management System, etc.).
- 4.3.2 The architecture enveloping the TCS TSI and EULYNX domains described in Figure 1 and EULYNX System Definition Appendix A1 – EULYNX System Architecture Version 4.2 shall be taken as a reference for the implementation of ERTMS on the HSR Railway.



- 4.3.3 Looking at the organizational context of HSR railway operations, the main stakeholders involved in the use of ETCS, and in general of the whole TSCC system, are Train Operators and Maintainers of CAHSR, who are responsible for establishing the procedures for operating and maintaining the System.

4.4 Design Life

- 4.4.1 The design life of the ETCS shall be 30 years.
- 4.4.2 TSCC Contractor shall ensure that the manufacturers will be able to produce ETCS system components (with equal or compatible technical specifications) for the entire lifetime required.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

- 5.1.1 The ETCS shall fulfil the TCS TSI requirements, ensuring the technical interoperability of the HSR Railway and the compliance with the essential requirements set out in Interoperability Directive (EU) 2016/797 regarding: safety, reliability and availability, health, environmental protection, and technical compatibility.
- 5.1.2 The ETCS shall be based ETCS Baseline 4 Release 1 and System Version 2.1 according to TCS TSI 2023 and the necessary error correction available at the time of designing the system.
- 5.1.3 The ETCS train operations shall be based on ETCS Level 2, using RBC for radio messages, Wireless Communication Systems as radio bearer, fixed Eurobalises for location referencing, Marker Boards and fixed block sectioning based on axle counters for track vacancy detection.
- 5.1.4 The ETCS shall support train operations on HSR Railway under normal, degraded and emergency conditions:
 - Train and shunting movements on the HSR main line and related Facilities under the supervision of RBC (no line side signals);
 - Transitions between HSR main line and Facilities outside the supervision of RBC (line side signals may be required);
 - Transitions between HSR main line and other railway network (in the future)
- 5.1.5 The ETCS shall ensure that the expected safety and operational performances of HSR main line are achieved, both in open line and in local facilities under the supervision of RBC.
- 5.1.6 The ETCS shall ensure easy scalability to support the commissioning of TSCC system according to HSR implementation schedule.
- 5.1.7 The ETCS shall be based on Commercial Off The Shelf (COTS), open and modular system architecture, reducing the use of proprietary interfaces.
- 5.1.8 The SIL 4 certification process of ETCS shall comply with the relevant CENELEC safety standards: EN50126, EN50716, EN50129 and EN50159 (refer to 2.4).
- 5.1.9 The Interoperability Constituents of TSCC Subsystem shall be provided with an 'EC' declaration of conformity to the relevant basic parameters set out in the TCS TSI.
- 5.1.10 [Note to: 5.1.9: the compliance with the basic parameters ensures the fulfilment of the essential requirements set out in the Directive. For TSCC HSR project this requirement shall refer to the following trackside components: RBC, Eurobalise, Axle Counter, Marker Board]
- 5.1.11 Only Systems with service proven records of at least 2 years for application on railway infrastructure should be proposed by the TSCC Contractor, unless properly justified by the required ETCS application and agreed by the CHSR Authority.
- 5.1.12 The ETCS design shall tend to minimize the Environmental Impact of the TSCC subsystem and of the entire railway operation during O&M phase.
- 5.1.13 The correct functioning and performances of ETCS hardware, electronic and software components shall not be affected by the action of environmental conditions of the geographical area.
- 5.1.14 The ETCS shall comply with the HSR cybersecurity policies and main standards for cybersecurity in safety-related applications.
- 5.1.15 The ETCS design shall be aligned with the overall RAM and Safety target required for HSR.
- 5.1.16 Following requirement 5.1.15, the hazard mitigation shall be part of the ERTMS/ETCS design phase of TSCC Contractor covering all specific scenarios of HSR project and the generic scenarios set out in UNISIG standard SS-113 (ETCS Hazard Log).



5.2 Environmental Requirements

- 5.2.1 Refer to the Contract for general environmental requirements.
- 5.2.2 The ETCS equipment shall be compliant with EN50125-3 and the generic International Standards (refer to 2.4).
- 5.2.3 Outdoor ETCS components shall be aligned with the relevant parameters related to the following environmental conditions:
- Atmospheric pressure / Altitude;
 - Temperature;
 - Humidity;
 - Wind;
 - Surrounding air;
 - Rain ;
 - Solar Radiation;
 - Lightning;
 - Pollution;
 - Vibration and shocks
- 5.2.4 The ETCS equipment located in external ambient and in cubicle/shelter/building shall be compliant to the Climatic Class T2 defined in EN 50125-3 according to environmental classification provided by 60721-2-1, concerning Temperature and Humidity (refer to 2.4 and 2.2).
- 5.2.5 The Eurobalises shall comply with the specific environmental conditions defined in UNISIG standard SS-036 (FFFIS for Eurobalise) related to:
- Operational Temperature;
 - Storage;
 - Sealing, dust, and moisture;
 - Mechanical stress;
 - Meteorological conditions;
 - Lightning;
 - Chemical conditions;
 - Biological conditions;
 - Debris.
- 5.2.6 The Eurobalises shall be compliant with Debris Class A balises and related environmental parameters.
- 5.2.7 Marker Boards and Eurobalises shall be designed to be durable in railway environments, adequately protected from weathering and vandalism to preserve their physical, optical, and mechanical properties.
- 5.2.8 ERTMS/ETCS equipment shall be compliant to CENELEC standard 50121 Railway applications - Electromagnetic compatibility.
- 5.2.9 The TSCC Contractor shall include in the project the identification, analysis, and mitigation of environmental hazard risks.

5.3 Operational Requirements

- 5.3.1 The ETCS design shall ensure that the expected headway, capacity, and traffic volume on HSR main line are achieved.
- 5.3.2 The ETCS shall support train operations according to the HSR Operational Concept.



- 5.3.3 The ETCS shall ensure train operations at the design speed and maximum operational speed of 220mph.
- 5.3.4 The ETCS shall allow bidirectional train operations on all station tracks and in open line.
- 5.3.5 The ETCS trackside shall grant Movement Authorities (MAs) via radio according to the routes set by CBI and the status of the relevant trackside elements.
- 5.3.6 Harmonized ETCS marker boards, namely Stop Marker and Location Marker, shall be located at the end of the movement authorities where the driver requires supplementary information to identify the exact stopping location in addition to the display on the DMI.
- 5.3.7 Stop Markers and Location Markers may also be sub-located within an MA section to identify a specific location that shall be observed by the driver during degraded train operations. In this case they do not necessarily have to contribute to the spacing between trains.
- 5.3.8 Stop Markers shall be used where it is necessary to protect one or a group of safety-critical locations. The train must not overpass the Stop Marker at the end of authority or while running without MA, unless the driver has received a specific authorization by the signaller.
- 5.3.9 Location Markers should be preferred in case there is no safety-critical location to be protected. The train may overpass the Location Marker at the end of authority or while running without MA, under the responsibility of the driver. In general, it is up to Infrastructure Manager to decide whether a Location Marker can be used instead of a Stop Marker where no safety critical location needs to be protected.
- 5.3.10 [Note to 5.3.6, 5.3.8 and 5.3.9: an example of deployment of Stop markers and Location markers based on requirements is shown in the figure below.

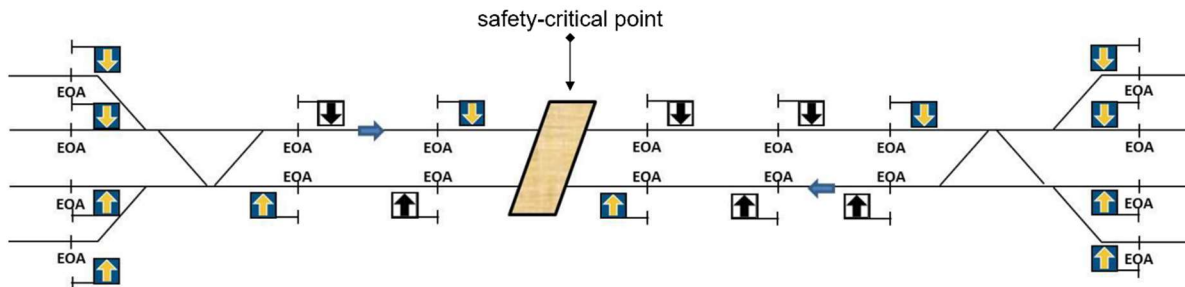


FIGURE 2 - STOP MARKERS AND LOCATION MARKERS EXAMPLE

- 5.3.11 In the operational context of HSR, the term “safety-critical location” shall be understood as any element on the track located between the TVP limits of an MA section (switch, fouling point of conflicting routes, entry of station, junction, vehicle intrusion at road overpass, other critical locations of rail infrastructure) that requires major protection via an ETCS Stop Marker, as the driver cannot pass it without specific authorization when the MA is not available
- 5.3.12 Since the operational purpose of Stop Markers and Location Markers may often coincide, the priority defined in the TCS TSI (reference document 21E089) shall apply to determine which type of marker must prevail.
- 5.3.13 Non-harmonized trackside boards shall be used to provide supplementary information, or to clearly identify those specific operational points where harmonized ETCS marker boards would not be able to fit the intended operational purpose.
- 5.3.14 The MA segmentation constitutes the basis for the spacing between trains, therefore it shall respect the HSR approach on block sectioning which shall be optimized by TSCC Contractor with the aim of achieving the performance of HSR operations.
- 5.3.15 All features of HSR railway line related to Tracks and Civils Subsystem (line speeds, slopes, curves, switches, bridges, tunnels, platforms, big metal masses, etc.), Traction Power Subsystem (traction system

voltage, etc.) and Trainset Subsystem (train categories, axle load, brake position, etc.) shall be reflected in ETCS data.

- 5.3.16 The ETCS may provide a safe response to the alarms triggered via direct interface, CBI or TMS by the detectors of the Hazard Detection and Early Warning System (HDEWS) that are specified in Schedule 5(g) – HDEWS Specification.
- 5.3.17 The engineering of movement authorities and of balises shall allow passenger trains to approach fluently and accurately to the operational stopping points.
- 5.3.18 The trains approaching the end of authority shall be prevented from overrunning the Supervised Location (hazard ETCS H-0001 of ETCS Hazard Log – subset 113).
- 5.3.19 The fixed release speed should be the main option to provide driving consistency.
- 5.3.20 TSCC Contractor shall evaluate which release speed among fixed is the most suitable option for HSR operations, considering that the nominal length of the overlap in station area is 70 m and that this value can change in some places. Note that 15km/h is expected to meet both safety and operational needs but that shall be validated during design.
- 5.3.21 In the case of conditional overlap (e.g., when overlap is too short) indicated to the RBC by the CBI, the RBC may authorize entry into the section in restrictive conditions (e.g., OS mode or Lower Release Speed).
- 5.3.22 When a switch is included in the overlap, the interlocking system may release the overlap immediately if the train is safely proven at stop before the marker. The overlap release can be requested by the RBC or can be determined by the interlocking system, using a timer, considering the lowest train speed and the stopping conditions.
- 5.3.23 ETCS trains shall be able to start or end a mission in any location of HSR mainline, including the facilities partially supervised by RBC.
- 5.3.24 The RBC shall allow trains to run on the mainline using the following ETCS modes: Full Supervision (FS), On-Sight (OS), Staff Responsible (SR), Reversing (RV).
- 5.3.25 Train movements under normal trackside conditions shall be performed in FS mode.
- 5.3.26 ETCS shall support joining and splitting of trains at station tracks.
- 5.3.27 Train movements under degraded trackside conditions shall be performed in OS or SR mode.
- 5.3.28 The RBC shall authorize OS mode to allow a train to move under the partial responsibility of the train driver, for example in a track which may be occupied by another train or other obstacles.
- 5.3.29 The RBC shall authorize SR mode to allow a train to move under the full responsibility of the train driver.
- 5.3.30 The balise engineering shall prevent trains in SR mode from passing critical locations.
- 5.3.31 The RBC should authorize RV mode to allow the trains to reverse to a safe location or to fit the train at station platforms in case of “long overshooting” of the stop location. Shunting (SH) and Isolation (IS) are other possible ETCS modes for reversing the movement direction.
- 5.3.32 Long tunnels and bridges are considered typical locations where it should be possible to reverse the train movement direction in case of emergency. RV mode shall require a careful recognition of the potential reversing areas during design phase of TSCC Contractor.
- 5.3.33 ETCS shall support shunting operations on all tracks equipped with ETCS.
- 5.3.34 The RBC shall authorize the SH mode for shunting operations in those facilities under the RBC supervision with scheduling of frequent shunting.
- 5.3.35 The RBC shall authorize the SH modes for shunting operations in those local facilities under the RBC supervision where shunting is occasional (e.g., passenger stations):
 - Shunting operations in SH mode shall be carried out within a safe envelope (shunting area) to increase the safety level of the overall train operations.



- The balise engineering shall prevent trains in SH mode from overrunning the shunting area limits.
- Shunting in the large rail yards outside the HSR mainline and the RBC supervision, shall be allowed by shunting signals and ETCS-OB shall be set to Level 0 SH mode.
- Shunting in non-signalled areas (e.g., infrastructure maintenance facilities) shall be carried out under the supervision and full responsibility of the local staff.
- ETCS shall allow smooth and harmonized train transitions with any interfaced railway network
- Handover and level transitions shall not affect the train operations in terms of speed, safety, and regularity.

5.3.36 ETCS National Values are a set of parameters usually defined by the Infrastructure Managers to ensure coherency between the onboard system behaviour and the rules and regulations in different countries. Since national values are only provided as example for the current project, the TSCC Contractor shall submit to the CHSR Authority a proposal compliant with the performance and safety requirements of HSR.

5.3.37 The following National Values shall be taken as examples:

Variable	Value	Note
V_NVSHUNT	30 km/h	-
V_NVSTFF	30 km/h	-
V_NVONSIGHT	30 km/h	-
V_NVLIMSUPERV	0 km/h	Limited Supervision mode is not authorized.
V_NVUNFIT	30 km/h	-
V_NVREL	15 km/h	-
D_NVROLL	5 m	-
Q_NVSBTSMPerm	1 (Yes)	-
Q_NVEMRRLS	0 (Apply emergency brake until standstill)	-
Q_NVGUIPERM	1 (Yes)	-
Q_NVSBFBPerm	0 (No)	Using the service brake feedback could cause unexpected brake interventions.
Q_NVINHSMICPerm	0 (No)	consider the speed measurement inaccuracy in the calculation of the braking curves.
V_NVALLOWOVTRP	0 km/h	Override to be selected only when the train is at standstill.
V_NVSUPOVTRP	30 km/h	Override speed limit shall be equal to the default Staff Responsible speed limit.
D_NV OVTRP	100 m	100 m is considered a suitable distance limit for the validity of train trip override



Variable	Value	Note
T_NVOVTRP	60 s	60s is considered a suitable time window for train trip override
D_NVPOTRP	0 m	It is not permitted to undertake reverse movements in Post Trip mode.
M_NVCONTACT	00 (Train Trip)	Value to be confirmed by risk Assessment
T_NVCONTACT	20s	Value to be confirmed by risk Assessment
M_NVDERUN	0 (No)	
D_NVSTFF	32767 (∞)	To facilitate operation in SR in case of degradation
Q_NVDRIVERADHES	1 (Allowed).	
A_NVMAXREADADH1	1.0 m/s ²	Default value
A_NVMAXREADADH2	0.7 m/s ²	Default value
A_NVMAXREADADH3	0.7 m/s ²	Default value
Q_NVLOCACC	12 m	Default value.
M_NVAVADH	0	Default value.
M_NVEBCL	9 (99.9999999%)	Highest confidence level for emergency brakes.
Q_NVKINT	1 (Integrated correction factors follow)	Only Gamma trains are allowed to operate. A preventive correction factor is applied to restrict any Lambda train from operating normally on the line.
Q_NVKVINTSET	01 (Conventional passenger trains)	Set of values below applicable to passenger trains
A_NVP12	0.5 m/s ²	1st Pivot value for 'Lower deceleration limit to determine the set of Kv'. (Kv = Correction factor)
A_NVP23	0.55 m/s ²	2nd Pivot value for 'Upper deceleration limit to determine the set of Kv'. As close as possible to the 1st pivot is used to ensure that the correction factor applies to all deceleration range
V_NVKVINT	0 km/h	Fixed value which starts the Kv speed dependant profile
M_NVKVINT	0	Integrated correction factor Kv applicable for any speed above V_NVKVINT (0 km/h) if the maximum train deceleration is below
A_NVP12	(0.5 m/s ²).	Most permissive value '0' selected to ensure Lambda trains cannot operate with ETCS normally on the line.



Variable	Value	Note
M_NVKVINT	0	Integrated correction factor Kv applicable for any speed above V_NVKVINT (0 km/h) if the maximum train deceleration above A_NVP23 (0.55 m/s ²). Most permissive value '0' selected to ensure Lambda trains cannot operate with ETCS normally on the line.
N_ITER	0	No further speed step iterations for the Kv correction factor provided.
Q_NVKVINTSET	00 (Freight trains)	Set of values below applicable to freight trains
V_NVKVINT	0 km/h	Fixed value which starts the Kv speed dependent profile
M_NVKVINT	0	Integrated correction factor Kv applicable for any speed above V_NVKVINT (0 km/h). Most permissive value '0' selected to ensure Lambda trains (which are not authorized to operate with ETCS on the line the Irish Network) will be enforced to calculate extremely conservative braking curves, leading to operation below release speed.
N_ITER	0	No further speed step iterations for the Kv correction factor provided.
L_NVKRINT	0 m	Fixed value which starts the Kr train length
M_NVRINT	0	Integrated correction factor Kr applicable for any train length above L_NVKRINT (0 m). Most permissive value '0' selected to ensure Lambda trains (which are not authorized to operate with ETCS on the line) will be enforced to calculate extremely conservative braking curves, leading to operation below release speed.
N_ITER	0	No further train length step iterations for the Kr correction factor provided.
M_NVKTINT	1	The Kt correction factor brake build-up time for Lambda trains is unchanged, as the chosen Kv and Kr correction factors can enforce the operation of Lambda trains under very conservative braking curve

TABLE 5 – NATIONAL VALUES EXAMPLES

5.4 Functional Requirements

- 5.4.1 Functional requirements refer to the functions specified in UNISIG standard SS-026, or any other expected functionality for maintenance supporting and data recording to carry out ETCS train operations on HSR railway line according to the high-level operational requirements defined in 5.3.



5.4.2 ETCS train operations shall be related to functions and processes managed by ETCS-TS and ETCS-OB for the safe supervision of train and shunting movements on HSR railway line, including but not limited to:

- Euroradio and Eurobalise messages.
- Movement authorities.
- Fixed and temporary speed restrictions, gradient, track conditions, and other profile data.
- ETCS modes for train and shunting operations, mode transitions.
- Supervision of the radio contact.
- Start of mission / End of mission.
- Level transitions.
- Handover RBC/RBC.
- Emergency messages.
- Text messages.
- National Values.
- Shunting areas management.
- Protection of working areas and other safety-related locations.
- HSR Territory Entering/leaving.

5.4.3 Euroradio messages

- 5.4.3.1 The bidirectional communication between RBC and ETCS-OB shall be based on the Euroradio protocol specified in UNISIG standard SS-037.
- 5.4.3.2 Euroradio messages shall contain packets and variables in accordance with UNISIG standards SS-026-7 and SS-026-8.
- 5.4.3.3 The maximum time interval between two consecutive messages sent by RBC to the same train shall not exceed the reference time given by the national value T_NVCONTACT.
- 5.4.3.4 The risk that a train may enter a not protected route after a loss of radio communication shall be mitigated.

5.4.4 Eurobalise message

- 5.4.4.1 Balise messages shall contain packets and variables in accordance with UNISIG standard, SS-026-7 and SS-026-8.
- 5.4.4.2 Balise groups shall ensure accurate relocation of the trains running close to operational stopping points (platform, stop marker, location marker, buffer stop, etc.), level transition areas, handover areas, any other relevant location.
- 5.4.4.3 Balise groups shall update the national values at cross borders, depots, and other relevant local facilities, with the aim preventing trains from moving with wrong values stored on-board.
- 5.4.4.4 Balise groups shall provide the “big metal masses” information.
- 5.4.4.5 Balise groups shall prevent trains in SR mode from overrunning critical locations.
- 5.4.4.6 Balise groups shall prevent trains in SH mode from overrunning the shunting area limits.
- 5.4.4.7 Balise groups shall support level transitions and handover RBC/RBC via immediate transition orders and announcements where not transmitted via radio.
- 5.4.4.8 Balise groups shall prevent trains from entering the ETCS Level 2 area with ETCS Level 0 erroneously selected and stored on board.
- 5.4.4.9 The balise engineering should be based on the approach defined in EUG Engineering Guideline #23 - Balise Engineering L2 and L3 (refer to 2.6), adapted to the requirements of the new ETCS Baseline 4 and related system versions, where necessary.



5.4.5 Movement Authorities for train operations and related modes

5.4.5.1 The ETCS operating modes allowed to be used by the RBC are within the HSL are:

- Full Supervision,
- On-sight
- Shunting
- Reversing

5.4.5.2 The Movement Authority shall contain all information necessary for the trains to run safely, preventing derailments, collisions and other dangerous situations which may cause harm to people (passengers and railway staff), loss of goods and damage to railway assets.

5.4.5.3 Before granting movement authorities, RBC shall evaluate the status of route elements and other wayside conditions transmitted by CBI: switches, TVP sections, asset alarms, working areas under engineering possession, any other element to be supervised on the MA.

5.4.5.4 RBC shall supervise the integrity of the safe connection with CBI and revoke all MAs in the area controlled by CBI when the communication is lost or corrupted.

5.4.5.5 The MA shall provide ETCS-OB with the following information: permission and distance to run, the track description, the linking information, when available, and the mode profile when required.

5.4.5.6 The track description shall define all permanent and temporary speed restrictions, the gradient profile, the track conditions, the areas where reversing is permitted, and the areas with reduced adhesion factor.

5.4.5.7 Where RBC detects that the distance to run includes a temporary speed restrictions area, the TSR's parameters shall be incorporated in the MA message.

5.4.5.8 Where RBC detects that the distance to run includes the handover area between adjacent RBCs, the RBC transition announcement shall be incorporated in the MA message.

5.4.5.9 Where RBC detects that the distance to run includes a level transition area, the level transition announcement shall be incorporated in the MA message.

5.4.5.10 Where RBC detects that the distance to run includes an area where different national values apply, the new values shall be incorporated in the MA message.

5.4.5.11 No movement authority shall be granted if RBC does not know the route or the TVP status.

5.4.5.12 No movement authority shall be granted if the route, or any portion of the route, has already been granted to another train (conflicting MA).

5.4.5.13 No movement authority shall be granted by RBC on the areas under engineering possession.

5.4.5.14 RBC shall supervise the position of the train in the MA and extend or shorten the authorized distance relying on the most updated information provided by CBI.

5.4.5.15 RBC shall ensure continuous supervision of the safety conditions received from CBI, and the loss of such conditions in the existing MA shall result in an immediate restriction on the affected portion of the track. Depending on the hazard and on the train position known by RBC, a new MA shorter than the previous one, or an emergency stop message, or a speed restriction, shall be sent to the train.

5.4.5.16 Note: for each hazard, TSCC Contractor shall evaluate the influence of T_NVCONTACT and the consequences of a possible emergency brake activation by train

5.4.5.17 The cooperative shortening of MA between RBC and ETCS-OB shall be used to increase the overall safety level of the train operation, for example to manage the approach locking function carried out by the interlocking during route cancellation/release (RBC-CBI interworking is required).

5.4.5.18 RBC shall be able to shift the MA location reference in case a slave engine becomes the leading engine after changing the train orientation or the running direction.

5.4.5.19 RBC shall manage the overlap, Danger Point and release speed at the End Of Authority (EOA).



- 5.4.5.20 The EOA locations shall allow passenger running under normal conditions to reach fluently their operational stopping point according to HSR timetable.
- 5.4.5.21 The Danger Point shall be located no further than the entry point of an occupied TVP section (axle counter limit), or the fouling point of a switch conflicting with other routes, or any other dangerous location specified beyond the EOA.
- 5.4.5.22 The Overlap should be used to improve the efficiency of the braking supervision during ETCS train operations.
- 5.4.5.23 The Overlap location shall be consistent with the portion of the track that CBI may add as a safety margin beyond the end of authority.
- 5.4.5.24 If CBI use a timer to release the overlap, the corresponding Overlap time-out of ETCS shall reflect the Interlocking behaviour.
- 5.4.5.25 Both overlap timers (CBI and ETCS) shall not expire before the train has come to a standstill.
- 5.4.5.26 RBC should inform CBI that the train has come to a standstill and permit the overlap to be released before the interlocking timer has expired (timer normalization).
- 5.4.5.27 The release speed shall enable ETCS trains performing with insufficient odometer accuracy to approach the EOA location.
- 5.4.5.28 The release speed shall ensure acceptable driving at the EOA location.
- 5.4.5.29 The RBC shall grant MA in FS mode for train operations only when all safety conditions within the permitted distance to run are fulfilled: switches shall be locked in the right position, TVP sections shall be vacant, any other expected conditions monitored in real time by CBI which would directly impact the MA shall be safe.
- 5.4.5.30 The RBC shall be able to grant OS mode to trains entering a TVP section that is not vacant under specific conditions, for example after a trackside failure or a previous axle counting error. The driver is responsible for checking the track vacancy.
- 5.4.5.31 The OS mode may also be used to allow the train to overrun, under the responsibility of the train driver, a location which may be interfered by peoples, vehicles, or any kind of obstacle, for example a vehicle intrusion reported by the Hazard Detection and Early Warning System at road overpasses, or other similar situations.
- 5.4.5.32 Since most often OS mode requires compliance with specific protocols to be followed before being granted, the TSCC Contractor shall evaluate when OS mode can be activated automatically by RBC and when it should require authorization by the traffic operator via TMS HMI (TMS Human Machine Interface) using special/double commands capable of overrunning the restriction.
- 5.4.5.33 Note: use cases for OS mode authorization by the traffic operator may relate to requirement 5.4.5.30
- 5.4.5.34 For operational needs (platform sharing/joining of trains) RBC shall allow a train to enter a platform partially occupied by another train in FS (or AD mode in case of automatic GoA2 operation), and switch to OS mode before reaching the occupied location.
- 5.4.5.35 Note: this kind of train operations should require the track to be divided in at least two TVP sections and may require the movement permission to be granted via a special/double command from TMS HMI
- 5.4.5.36 In OS mode the permitted speed shall be defined by the National Value; different values may be adopted for exceptional cases.
- 5.4.5.37 The location where the OS mode is requested by RBC shall be, at the latest, the entry point of the occupied track.
- 5.4.5.38 OS mode shall require the driver acknowledgment, with an acknowledgement area of at least 100 m in rear of the location where the transition to OS is requested by RBC.



- 5.4.5.39 If after a trackside failure (e.g., a loss of the radio contact) RBC is not able to grant MA in FS or OS, the train can move in SR mode after the Override procedure has been triggered by the train driver. The driver shall coordinate with the traffic controller and observe the specific instructions received (check if the track is clear, if switches are correctly positioned, etc.).
- 5.4.5.40 Trains are authorized to move in SR mode within fixed limits of speed and distance given by the relevant national values. Trackside balises giving the order "Stop if in SR" shall be deployed at each Stop Marker location to protect turnout areas and other specific locations from SR mode in case of driver misconduct.

5.4.6 Permanent speed restrictions

- 5.4.6.1 The SSP shall define all fixed speed restrictions imposed by HSR infrastructure (maximum line speed, curves, switches, bridges, tunnels, etc.), and one or more specific SSPs related to the international train categories which apply to HSR project. Train categorization shall be done during the design phase of TSCC Contractor.
- 5.4.6.2 SSP shall be evaluated as a safe segmentation that incorporates all speed changes as a sequence of static speeds.
- 5.4.6.3 Each SSP segment shall correspond to one value of the basic speed. Where it is acceptable to join more speed variations in a same SSP segment, the speed rate applied in that segment shall be the lowest of all values.
- 5.4.6.4 Any speed increase resulting from SSP shall be controlled by ETCS-OB including the train length delay.
- 5.4.6.5 Any speed changes resulting from ASP shall be controlled by ETCS-OB including the train length delay.

5.4.7 Temporary speed restrictions

- 5.4.7.1 RBC shall ensure centralized management of Temporary Speed Restrictions (TSRs).
- 5.4.7.2 TSRs shall be communicated by RBC to ETCS trains via MA.
- 5.4.7.3 Any speed changes resulting from TSR profile shall be controlled by ETCS-OB including the train length delay.
- 5.4.7.4 TSRs shall be activated either by the traffic operator via TMS/TSR HMI or automatically by RBC as a safe response to specific dangerous situations.
- 5.4.7.5 Along working areas, the TMS and/or RBC shall automatically reduce the speed of the trains running on the adjacent tracks. The automatic TSR shall be made SIL4 and shall cover at least the entire projection of the working area on the tracks kept in service for train operations.
- 5.4.7.6 Along temporary shunting areas, RBC shall automatically reduce the speed of the trains running on the adjacent tracks. The automatic TSR shall achieve SIL4 and cover at minimum the entire projection of the shunting area on the tracks kept in service for train operations.
- 5.4.7.7 Automatic TSRs shall rely on default TSRs that are automatically transmitted by RBC under predefined conditions. Additionally, the TSR parameters shall be configurable to allow operators to customize automatic TSRs for specific scenarios, especially in case of temporary possession in a working area.
- 5.4.7.8 Where TSR data are set and stored in a dedicated TSR server, ETCS shall ensure safe synchronization between RBC and TSR server, and any restart of equipment after a shutdown shall not result in a loss of TSR data or in a dangerous mismatch between servers.
- 5.4.7.9 The traffic operator shall be allowed to activate TSRs with default data (predefined TSRs), as well as to modify the existing ones, or plan new TSRs entering identity, start point, end point and speed rate via HMI, with a granularity of 10 meters and 5 km/h.
- 5.4.7.10 The traffic operator shall be proposed whether to activate the TSR immediately or schedule it for a given time.



- 5.4.7.11 The TSR time scheduling shall be done entering via HMI any time slot within the 24 hours of the day.
- 5.4.7.12 It shall also be possible to set the validity period of that time slot: daily, weekly, monthly, or any other date interval.
- 5.4.7.13 For operational needs, it shall be possible for the operator to revoke a TSR that has been set automatically by RBC.
- 5.4.7.14 For TSRs generated by the Hazard Detection and Early Warning System, RBC shall be able to revoke the TSR as soon as the alarm is reset.
- 5.4.7.15 [Note: regarding the speed rates of automatic TSRs in the above-mentioned scenarios, a safety study shall be necessary at system level, through benchmarking and alignment with Shadow Operator and IMs]
- 5.4.8 Other static speed restrictions**
- 5.4.8.1 The RBC may transmit the Permitted Braking Distance (PBD) information to allow ETCS-OB to calculate a speed restriction based on the PBD and the applicable National Values to ensure that the train can stop within the maximum permitted stopping distance.
- 5.4.9 Gradient profile**
- 5.4.9.1 Each segment shall correspond to one gradient value. Where it is acceptable to join more slope changes in a same segment, the gradient rate applied in that segment shall be the safest of all values.
- 5.4.9.2 As ETCS manages gradient values with a minimum resolution of 1‰, decimal numbers in uphill shall be rounded by defect, decimals in downhill shall be rounded by excess.
- 5.4.9.3 Gradient data collection and gradient segmentation should be carried out according to the EUG Engineering Guideline #28 - Gradients Segmentation (refer to 2.6).
- 5.4.10 Linking information**
- 5.4.10.1 The linking information shall link all relevant balise groups that will be passed by the train.
- 5.4.10.2 The linking information shall ensure that ETCS-OB applies a safe reaction (train trip or service braking) if a linked balise group containing vital information in FS or OS is not found or the transmitted data are inconsistent.
- 5.4.10.3 TSCC Contractor shall provide adequate balise engineering and ensure that the linking information is available on board in due course.
- 5.4.10.4 Track conditions
- 5.4.10.5 The Track Conditions information shall be incorporated in the MA message as soon as RBC detects that the train movement authority involves a HSR location where one or more track conditions apply.
- 5.4.10.6 RBC shall be able to manage at least the following types of track conditions as per SS-026:
- Non stopping area;
 - Air tightness;
 - Switch off regenerative brakes;
 - Big metal masses;
 - Radio hole;
 - Station platform.
- 5.4.10.7 For track conditions Air tightness, and Switch off regenerative brake, the latest transmission of the announcement in rear of the start location shall fulfil the time requirements defined in UNISIG standard SS-040.
- 5.4.10.8 The track condition "non-stopping area" should be set, railway bridges, tunnels, viaducts, or other locations according to the specific operational needs of HSR.



- 5.4.10.9 The TSCC Contractor shall include in the project the identification of metal object locations (turnouts, guard rails, big metal masses, etc.) with the aim of establishing the balise locations according to requirements defined in UNISIG standard SS-036.
- 5.4.10.10 If required, the track condition “big metal masses” shall be transmitted via balises at freight yards, depots, and other locations of HSR, to allow ETCS-OB to ignore the “integrity check” alarms of the onboard balise-reading system which may be triggered by big metal objects exceeding the limits given in UNISIG standard SS-036.
- 5.4.11 Start of Mission**
- 5.4.11.1 RBC shall support the Start of Mission (SoM) of ETCS trains according to the procedure defined in UNISIG standard SS-026-5.
- 5.4.11.2 Departure/arrival tracks of passenger and freight stations of HSR main line, as well as the exchange tracks of Facilities partially supervised by RBC, shall be considered as planned locations where it is possible to start a mission in ETCS Level 2.
- 5.4.11.3 It shall also be possible to start a new mission in any track section of HSR, including the open line areas, in case ETCS-OB is restarted after a system failure.
- 5.4.11.4 The SoM shall be designed to achieve FS mode as soon as possible, while ensuring transparent and predictable behaviour and procedures as well.
- 5.4.11.5 The ETCS trackside configuration should follow the basic principles defined in EUG Engineering Guideline #68 - Start of mission in Level 2/3, B3 (refer to 2.6), adapted to the requirements of the new ETCS Baseline 4 and related system versions, where necessary.
- 5.4.11.6 TSCC Contractor shall ensure adequate balise engineering and interworking between RBC, CBI and TMS, to reduce the occurrence of start of missions with invalid or ambiguous position.
- 5.4.11.7 Note: according to Regulation (EU) 2023/1695 (refer to 2.3) the ETCS on-board equipment shall be fitted with a Cold Movement Detection (CMD) to determine if a vehicle has been moved during the power off phase
- 5.4.11.8 If available, information from interlocking, TVP system and TMS shall enable RBC to (re)validate a position reported as invalid by onboard.
- 5.4.11.9 When the train position is valid and deemed unambiguous by RBC and the route conditions for MA are fulfilled, RBC shall allow the train to start the mission in FS or OS mode.
- 5.4.11.10 To guarantee an unambiguous train position when the SoM is performed close to switches, additional wayside engineering methods should be necessary.
- 5.4.11.11 If the SoM is performed by a slave engine which becomes a leading engine after a change of train orientation, RBC shall be able to shift the MA location reference.
- 5.4.11.12 Where RBC can determine that the train is the first to enter the route section, RBC shall authorize the train to start immediately in FS mode.
- 5.4.11.13 The correct engineering of routes and TVP sections, as well as the use of train data or other information coming from CBI and TMS, should allow RBC to determine that the presence of another train is sufficiently improbable.
- 5.4.11.14 Where RBC is not able to ascertain that there is no other train between the train front and the route entry point, this first portion of MA shall be granted in OS mode.
- 5.4.11.15 No MA shall be granted if the route is not set or route conditions for MA are not fulfilled or the train position is unknown or invalid and cannot be validated by RBC.
- 5.4.11.16 Where available, information from RBC, TMS and CBI should be used by RBC as condition to trigger the SR authorization, mitigating any misunderstandings in verbal communication between driver and dispatcher.



- 5.4.11.17 On HSR tracks where SoM in SR is likely to occur due to the train awakening without a valid position, a relocation balise group shall be placed sufficiently in rear of the route entry point to enable the train to obtain a valid position and receive the MA from RBC before passing the ETCS marker board.
- 5.4.11.18 In the previous scenarios ATAF (Automatic TAF) may be required to switch from OS/SR to FS mode.
- 5.4.11.19 In case ATAF is proposed to mitigate the risk of a driver incorrectly acknowledging a Track Ahead Free request, it is recommended to follow the basic principles defined in EUG Engineering Guideline #69 - Automatic Track Ahead Free (ATAF) B3 (refer to 2.6), adapted to the requirements of the new ETCS Baseline 4 and related system versions, where necessary.
- 5.4.11.20 Safe procedures and adequate trackside configuration shall mitigate the risk of moving in SR mode through a different track/path/direction than the expected one, as well as prevent ETCS trains from passing critical locations in SR mode or entering routes with ETCS Level 0 erroneously selected and stored on board.
- 5.4.11.21 In general, any hazardous scenarios related to the SoM shall be clearly identified by risk analysis.

5.4.12 ETCS level transitions

- 5.4.12.1 The ETCS shall allow dynamic level transitions L2<-->L0 at the specified project locations, such as the project borders.
- 5.4.12.2 The engineering of balises in the level transition area shall allow ETCS trains to perform the level transition at the precise location defined in the LT announcement.
- 5.4.12.3 The LT announcements shall be designed to allow the ETCS trains to pass the transition point at the maximum speed permitted by the infrastructure for the nominal situation.
- 5.4.12.4 The maximum speed applied in the transition point shall also consider the possible speed limitations imposed by the adjacent network system and by the temporary restrictions overlapping the LT area.
- 5.4.12.5 The transition point shall be fitted with both a light signal and an LT ETCS board which shall inform the train driver about the transition between the national signalling system and the RBC area.
- 5.4.12.6 The delay time to establish the safe communication between RBC and the trains entering ETCS L2 shall not reduce the performance set out in requirement 5.4.12.3.
- 5.4.12.7 Note: according to UNISIG standard SS-037-2 (Euroradio FIS), normally the safe connection establishment delay is less than 40s. This time span is commonly used in ETCS applications over GSM-R to set the position of "session BGs" in rear of the transition announcement; it must be confirmed that 40s is a delay able to fit the Wireless Communication Systems applications]
- 5.4.12.8 The transition to ETCS L2 should only be announced to the trains routed to the ETCS border. If this announcement cannot be avoided, for example because there is a diverging route after the announcement location, then it must be cancelled before performing the transition.
- 5.4.12.9 Note: using LEUs and switchable balises (not recommended solution), or announcing the level transition via RBC, could avoid unnecessary radio connections and several dedicated balise groups for cancellation and disconnection
- 5.4.12.10 The engineering of level transition area shall at least ensure that no trains are routed to ETCS L2 border unless connected to RBC, to prevent trains not equipped with ETCS and/or the Wireless Communication System from entering HSR.
- 5.4.12.11 The trackside configuration supporting level transitions L0<-->L2 should follow the basic principles defined in EUG Engineering Guideline #77 – Level Transition from LNTC to L2 (refer to 2.6), adapted to the requirements of the new ETCS Baseline 4 and related system versions, where necessary.

5.4.13 Handover RBC/RBC

- 5.4.13.1 The transition between RBCs shall fulfil the handover requirements set out in the relevant UNISIG standards SS-026, SS-034 and SS-098.
- 5.4.13.2 The ETCS shall manage the handover RBC/RBC at each specified project location of HSR.



- 5.4.13.3 The handover areas shall be designed to allow ETCS trains to pass the border at the maximum speed permitted by the infrastructure for the nominal situation, taking into account the connection establishment delay with the Accepting RBC (refer to 5.4.12.6) and the registration delay on GSM-R network when required (refer to UNISIG standard SS-093).
- 5.4.13.4 The Handing Over RBC shall be able to grant authorizations beyond the transition point after receiving from the Accepting RBC the following route related information, when available:
- Movement authorities ;
 - Linking ;
 - International static speed profiles ;
 - Axle Load Speed profiles ;
 - Gradients ;
 - Temporary speed restrictions ;
 - Mode profiles ;
 - Temporary speed restriction revocations ;
 - Track Conditions ;
 - Level Transition orders ;
 - Route Suitability Data ;
 - National Values ;
 - Adhesion Factor.
- 5.4.13.5 The trackside engineering of handover areas should follow the basic principles defined in EUG Engineering Guideline #74 - RBC-RBC Handover (refer to 2.6), adapted to the features of the new ETCS Baseline 4 and related system versions, where necessary.
- 5.4.14 Emergency messages**
- 5.4.14.1 Emergency stop messages shall be used to provide hazard mitigations and increase the overall safety level of train operations in case of emergency situations.
- 5.4.14.2 Conditional Emergency Stop (CES) and Unconditional Emergency Stop (UES) messages shall fulfil the requirements set out in UNISIG standard SS-026.
- 5.4.14.3 It shall be possible to send CES/UES messages spontaneously by RBC to provide a quick response to an emergency, or manually by the traffic operator via the TMS HMI.
- 5.4.14.4 CES messages shall be used to allow ETCS-OB to accept the stop message when the train has not yet passed, with its minimum safe front end, the stop location.
- 5.4.14.5 Note: if the stop location is not beyond the current EOA/LOA, the CES message is handled by ETCS-OB similarly to a shortening of MA, as the new stop location shall be supervised as EOA/SvL
- 5.4.14.6 The emergency stop locations shall be clearly identified during the design phase of TSCC Contractor as part of the risk mitigation analysis, and these may include:
- 5.4.14.7 Any safety-related location (switch, hot box detection, falling road vehicle detection, etc.) where the train should be stopped when the relevant safety conditions in the current MA are no longer supervised (see also requirement 5.4.5.14).
- 5.4.14.8 Limit of TVP sections to ensure the track occupancy supervision based on the position of the train in the MA.
- 5.4.14.9 The engineering of CES messages (message identity, stop location, etc.) when used shall be consistent with the balise engineering, to take into consideration the odometer errors which may lead ETCS-OB to accept the CES improperly.



5.4.14.10 CES/UES messages, once accepted by the train, shall be revoked via TMS HMI before resuming train operations.

5.4.15 Text messages

5.4.15.1 It shall be possible to transmit information from RBC to ETCS-OB to be displayed on the onboard DMI (Driver Machine Interface) in the form of text messages.

5.4.15.2 According to UNISIG standard SS-026, each transmitted text information shall individually contain:

- The class of message: auxiliary or important information.
- The conditions for Start/End of Indication: location, mode, level, time.
- If driver acknowledgement is requested or not.
- For Plain Text Messages, a customized text string element to be displayed in the required language.
- For Fixed Text Messages, a number selecting the fixed message stored on-board.

5.4.15.3 Note: fixed text messages are stored on-board in all languages that can be selected by the driver, for example 1-“Acknowledgement”

5.4.15.4 Plain and fixed text messages shall be coherent with the relevant operational scenarios of HSR, to inform the driver on the conditions which may require the activation of a specific ETCS mode, or an emergency stop, or a temporary speed restriction, or to provide other specific and general information.

5.4.15.5 Plain text messages should include, but not be limited to, the following text strings:

- “Route not protected”.
- “Road vehicle intrusion location not protected”.
- “Strong wind detected”.
- “Earthquake detected”
- “Flooding detected”
- “Station platform partially occupied”.
- “Working area on the adjacent track”.
- “Acknowledgement”.

5.4.16 Shunting operations and related mode

5.4.16.1 Shunting operations in HSR local facilities shall be performed in Shunting (SH) mode according to the operational requirements 5.3.34 and 5.3.35.

5.4.16.2 SH authorization by RBC shall require the shunting movement to be performed in a safe envelope set by CBI as a shunting area.

5.4.16.3 SH authorization by RBC shall be granted for movement from shunting signals when movement is protected by interlocking.

5.4.16.4 If it is not possible for RBC to grant SH mode because RBC cannot validate the train position in the shunting area, it shall be possible for the traffic operator to grant authorization via TMS HMI.

5.4.16.5 The “start of shunting” and “end of shunting” locations shall be marked with specific trackside boards.

5.4.16.6 End of shunting balises shall be placed at the “end of shunting” locations to prevent shunting trains in SH mode from passing such locations. A level transition order, from L0 to L2, may also be required together with the “danger for shunting” information to trip the trains in case of wrong level selection by the driver.

5.4.16.7 SH mode shall also be possible to allow maintenance vehicles (yellow fleet) equipped with ETCS onboard to move in a temporary working area.



5.4.16.8 [Note: according to UNISIG standard SS-026-4, SH mode does not manage level transitions, however immediate orders shall be accepted and stored for later evaluation]

5.4.17 Diagnostic, maintenance and recording functions

5.4.17.1 ETCS trackside shall be equipped with diagnostic and maintenance supporting functions capable of monitoring the health of the system and its interfaces.

5.4.17.2 The Diagnostic and Maintenance module of ETCS shall collect data, incidents, malfunctions, failures, and alarms relating to the system components.

5.4.17.3 Diagnostic information, failures, alarms, and other data shall be recorded for maintenance purpose (corrective and preventive maintenance) and incident investigations.

5.4.17.4 The Maintainer shall interact with the System and its components, both hardware and software, through dedicated D&M consoles.

5.4.17.5 The supporting functions shall allow operators to perform preventive and corrective maintenance, consisting of:

- Showing the status of trackside components and interfaces;
- Real-time monitoring and interrogation functions;
- Acknowledgement of alarms ;
- Recording and archiving of data on non-volatile media for statistics, playback, and post-analysis.

5.4.17.6 The recorded data for maintenance purposes shall be available for a minimum period of 12 months.

5.4.17.7 The ETCS system shall support data recording for regulatory purpose (incident investigation).

5.4.17.8 The recorded data shall be available in a separate standalone JRU (Juridical Recording Unit) for a minimum of 90 days, or a longer period if required by national laws/regulations.

5.4.17.9 All recorded information shall be accessible in a readable format and shall be provided with a user manual for the correct understanding of the retrieved information.

5.4.17.10 The ETCS supporting functions shall fulfil the general cyber security requirements defined in 5.7.

5.5 Performance Requirements

5.5.1 The ETCS design, and more generally the TCS design, should optimize capacity of the line and reduce the journey time.

5.5.2 ETCS equipment shall ensure that the line can be operated without service interruption on 24 hours and 7 days a week all year round (with required traffic stops for maintenance work).

5.5.3 ETCS equipment shall fulfil safety requirements defined in UNISIG standard SS-091 (Safety Requirements for Technical Interoperability of ETCS in Levels 1 & 2).

5.5.4 ETCS trackside shall fulfil the requirements defined in UNISIG standard SS-088 part 3 THR Apportionment (ETCS Application Levels 1 & 2 - Safety Analysis).

5.5.5 The TSCC Contractor shall implement adequate mitigations for the ETCS hazards identified in UNISIG standard SS-113 ETCS Hazard Log.

5.5.6 ETCS shall comply with the safety requirements defined in the TCS Safety Analysis Report which is a mandatory document.

5.5.7 ETCS shall comply with the RAM requirements defined in the TCS RAM Analysis Report.



- 5.5.8 The ETCS project shall consider the technical performance requirements of ERTMS equipment which are relevant for interoperability defined in UNISIG standard SS-041 in terms of:
- Response times ;
 - Accuracy ;
 - Clock.
- 5.5.9 Time-related performance: RBC generates and grants movement authorities to trains based on route information sent by CBI; the maximum time for data processing and data transmission through the communication chain CBI > RBC > Wireless Communication System > OBU (EVC/DMI) shall not exceed 5s (five seconds), from the moment the information is transmitted from CBI to RBC until ETCS On-Board Unit (OBU) processes the radio message and displays the MA on the DMI.
- 5.5.10 Diagnostic, maintenance and recording performance shall fulfil requirements set out in 5.4.17.

5.6 Requirements for Eurobalises

- 5.6.1 The Eurobalise Transmission System shall comply with RAMS requirements defined in UNISIG standard SS-036.
- 5.6.2 Eurobalises shall fulfil installation criteria defined in 11.2.
- 5.6.3 Accessibility: installation locations of balise groups on open line sections (between stations) shall respect the possibility of direct access from already designed maintenance roads.
- 5.6.4 Relocation balise groups shall be provided close to the signals at station tracks and in open line, to minimize the odometer error of the trains approaching the end of the movement authority.
- 5.6.5 Number and location of BGs should be optimized considering balise size, telegram lengths and user bit availability, to define when a same BG can fulfil multiple purposes.

5.6.6 Requirements for Radio Block Centre

- 5.6.6.1 RBC shall be upgradable for future track layout modifications and/or extensions.
- 5.6.6.2 RBC shall be designed to allow modifications without significant disruption on the traffic operations.
- 5.6.6.3 One RBC shall be able to manage at least 100 connected trains simultaneously and process up to 1.200 trackside element information (TVP, switch, etc.).
- 5.6.6.4 One RBC shall be able to interface with more than one CBI.
- 5.6.6.5 In case of start-up of RBC, or restart following a shutdown of the operating system, the initialization of RBC shall take no longer than 3 minutes and shall not require any intervention by the operator.
- 5.6.6.6 At each start-up RBC must restore operations in the safest conditions, ensure synchronization with the interfaced systems, such as CBI, TMS, including TSRs, and present the restored data on the HMI.
- 5.6.6.7 Any previous communications or radio connections that were active before the restart of RBC must be deleted.

5.6.7 Key Management System (KMS)

- 5.6.7.1 The cryptographic key management shall be based on an Offline KMS and shall involve in the key-distribution all RBCs and OBUs of HSR railway line.
- 5.6.7.2 The KMC shall be required to support offline key management configurations.
- 5.6.7.3 Off-line KMC shall comply with the relevant UNISIG standards SS-038, for the interface with other off-line KMC, and SS-114, for the interface with ETCS entities.
- 5.6.7.4 KMC setups and inter-KMC arrangements should comply with the solutions recommended by KMC Expert Group in EUG 23E064-1A KMS Guideline (refer to 2.6).



- 5.6.7.5 The TCS design should also fulfil the Cyber Security guidelines created by OCORA and RCA, and EULYNX regarding the security risk assessment for System Design process based on IEC 62443 and CLC/TS 50701 (refer to Section 2.4 of this specification for the EULYNX standard).

5.7 Cybersecurity Requirements

- 5.7.1 ETCS System shall comply with the general HSR cybersecurity policies specified in the related Technical Specification for Cybersecurity.
- 5.7.2 The ETCS shall be protected against cyber threats which can compromise its availability and integrity requirements.
- 5.7.3 Adequate defences shall be also provided for the communication interfaces as any safety-related equipment connected through open communication networks can be subjected to many different IT security threats (EN50159 – refer to 2.4).
- 5.7.4 Any threats which are not to be assumed shall be agreed with the safety authority and/or railway authority and shall be put into the safety-related application conditions.
- 5.7.5 The following communications subsystems and functions of ETCS System shall require to be protected/secured against cybersecurity threats:
- Balise - On-Board Unit (OBU);
 - Programming of balises ;
 - RBC - OBU via the Wireless Communication System (Euroradio protocol) ;
 - RBC/TMS Operator interface;
 - RBC - RBC (UNISIG standard SS-098);
 - RBC - CBI (EULYNX cybersecurity requirements);
 - RBC - TMS (for critical functions);
 - RBC - Master Clock System (for internal RBC clock synchronisation);
 - KMC Operator interfaces (set-up keys and access authorization);
 - KMC Key transmission to OBU and RBC.
- 5.7.6 Cyber threat defences in the ETCS design shall include measure for the balises to verify the authenticity of data.
- 5.7.7 Cyber threat defences in the ETCS design shall include measure to minimise the effect of reduced availability on the communication between OBU and RBC.
- 5.7.8 Cyber threat defences in the ETCS design shall include measure for integrity and authenticity of the communication, especially from/to RBC.
- 5.7.9 Cyber threat defences in the ETCS design shall include measure event logging and analysis.
- 5.7.10 Cyber threat defences in the ETCS design shall include access control measures, such as “Administrative accounts” and “Authentication and identification” security measures.
- 5.7.11 Cyber threat defences in the ETCS design shall include an update/patching policy for key components (Wireless Communication System, RBC, etc.).
- 5.7.12 Cyber threat defences in the ETCS design shall implement network controls measures (network segregation, no direct internet connection, no remote access by administrators, ensuring unnecessary services, interfaces, protocols, and port numbers are not activated, etc.).
- 5.7.13 Cyber threat defences in the ETCS design shall include up-to-date key and certification management and distribution.
- 5.7.14 Cyber threat defences in the ETCS design shall include scalable KMS.



6 INTERFACES

6.1 General Requirements

- 6.1.1 Interfaces are classified as below:
- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR TSCC Contractors);
 - External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors);
 - Internal interfaces between systems within the TSCC scope.
- 6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.
- 6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.

6.2 Third Parties Interfaces

6.3 External interfaces - Trainsets Contractor

- 6.3.1 The ETCS, and more generally the whole TCS Subsystem, shall interface with the Trainset Subsystem of HSR Railway in accordance with Commission Regulation (EU) 321/2013 concerning the technical specification for interoperability relating to the subsystem Trainset - freight wagons of the rail system in the European Union (LOC&PAS TSI - WAG TSI).
- 6.3.2 The interface with Trainset Subsystem shall mainly refer to the following general aspects in relation to the passenger and freight train operation on HSR Railway:
- Compatibility with trackside train detection systems including EMC: Trainset characteristics (CBI scope);
 - Train braking performance and characteristics;
 - Position of on-board antennas;
 - Isolation of ETCS-OB functionality;
 - Visibility of trackside marker boards;
 - Interface with onboard Data Recording for regulatory purposes;
 - Interface with Train Interface Unit: forwarding information/orders and receiving status information from Trainset;
 - Construction of TCS onboard equipment: material requirements;
 - Emergency and service braking commands.
- 6.3.3 [Note: most aspects refer to the interface between ETCS onboard and Trainset Subsystem which does not fall within the scope of work of TSCC Contractor, and they are reported within this technical specification only for completeness of the technical topics]
- 6.3.4 The visibility of trackside marker boards shall refer to the compatibility between dimensions, optical properties, and position of the marker board on the infrastructure, and the driver's external field of view.
- 6.3.5 The optical properties (colours and retroreflection coefficients) of any trackside board shall fulfil EN12899-1 (refer to 2.4) and shall be adapted to the optical features of train head lamps manufactured in accordance with EN15153-1. The driver shall be able to easily read the information in any condition and at any time.



- 6.3.6 The relevant information/orders that ETCS-OB receives from ETCS-TS shall be forwarded to the train interface unit. This train interface shall comply with the ETCS onboard requirements defined in UNISIG standard SS-034 (Train Interface FIS) and UNISIG standard SS-119 (Train Interface FFFIS).

6.4 External Interfaces – facilities contractor

- 6.4.1 The TSCC Contractor shall install ETCS equipment in the OCC and facilities being provided by the facilities contractor.
- 6.4.2 The TSCC Contractor shall provide to the facilities contractor:
- Equipment dimensions
 - Equipment clearances requirements
 - Equipment mounting and fixings requirements
 - Cable routes/containment requirements
 - Equipment loadings
 - Installation and maintenance requirements
 - Equipment heating loads
 - Equipment cooling loads
 - Equipment hydraulic requirements
- 6.4.3 To be provided by facilities contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:
- Room dimensions and layouts
 - Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
 - Room raised floor system
 - Delivery access routes.
 - Maintenance access routes

6.5 Internal Interfaces

6.5.1 Track interfaces

- 6.5.1.1 The ETCS shall interface with the Track Subsystem of HSR Railway in accordance with Commission Regulation (EU) 1299/2014 on the technical specifications for interoperability relating to the 'infrastructure' subsystem of the rail system in the European Union (INF TSI).
- 6.5.1.2 The interface between ETCS and INFRA Subsystem shall mainly refer to the following components of ETCS in relation to the structure gauge parameters of HSR Railway:
- Eurobalise communication system: space for installation;
 - Trackside Control-Command and Signalling objects: trackside marker boards;
 - Eurobalises and trackside marker boards shall be located on HSR according to the installation requirements defined in 11.2.
- 6.5.1.3 The interface shall also relate to the track gradient, track objects and speed profiles determined by track (and Operation) and the corresponding track model implemented in the RBC. TSCC Contractor shall implement a SIL 4 process for the treatment of data.

6.5.2 Computer Based Interlocking (CBI)

- 6.5.2.1 RBC and CBI shall operate in the same TCS domain as depicted in the HSR operational context (refer to 4.3).
- 6.5.2.2 RBC shall have a redundant interface with CBI via the transmission network (DCN).
- 6.5.2.3 RBC-CBI-(TMS) interworking shall ensure that the expected functions set out in 5.4 are achieved.
- 6.5.2.4 The interface between RBC and CBI shall be based on the Standard Common Interface SCI-RBC of EULYNX Baseline Set 4 Release 4, which provides a common set of Messages and Commands (Orders)



- 6.5.2.5 RBC shall be able to receive from CBI the following set of Messages based on the EULYNX standard interface:
- Signal status;
 - Switch status;
 - TVP section status (axle counter system);
 - I/O generic element status: alarms, any other possible alarm received from the detection devices;
 - Emergency Stop Area (ESA) status;
 - Local Shunting Area (LSA) status;
 - Working Area (WA) status;
 - Route status.
- 6.5.2.6 [Note: in an ERTMS/ETCS L2 domain it may be the status of the “virtual signal” associated to an ETCS marker board]
- 6.5.2.7 RBC shall be able to send to CBI the following set of Messages based on the EULYNX standard interface:
- Train data;
 - Flank Protection status;
 - Signal cancelling reply;
 - Signal occupation;
 - Route cancelling reply;
 - Route occupation.
- 6.5.2.8 RBC shall be able to receive from CBI the following Commands based on the EULYNX standard interface:
- Signal cancelling;
 - Route cancelling.
- 6.5.2.9 RBC shall be able to send to CBI the following Commands based on the EULYNX standard interface:
- I/O generic element control;
 - Signal control;
 - Signal overlap control;
 - Route control.
- 6.5.2.10 Any additional message or command that for operational needs must integrate the previous list shall be exchanged via the EULYNX interface, if feasible, otherwise through a different safe communication interface.
- 6.5.2.11 The full set of messages/commands exchanged between RBC and CBI shall be defined during the design phase of TSCC Contractor.
- 6.5.3 Traffic Management System (TMS)**
- 6.5.3.1 RBC and TMS shall operate in the same TCS domain as depicted in the HSR operational context (refer to 4.3).
- 6.5.3.2 RBC shall have a redundant interface with TMS via the Digital Communication Network (DCN).
- 6.5.3.3 RBC-TMS-(CBI) interworking shall ensure that the expected functions set out in 5.4 are achieved.
- 6.5.3.4 The SCI-CC interface specification of EULYNX is currently used to interface TMS with CBI; it may also be used to interface RBC to TMS for some specific functions.



- 6.5.3.5 The user interface (TMS HMI) shall show to the Traffic Operator the status of the line, and of the trains, under its jurisdiction.
- 6.5.3.6 RBC shall be interfaced with the TMS to exchange a general set of information/orders (messages/commands) related to:
- Movement Authorities;
 - ETCS modes;
 - Traction Power conditions;
 - Trackside Conditions: non-stopping area, etc;
 - Emergency stop areas, shunting areas, and working areas, via CBI;
 - Train information: train running number, train position, train speed, status of radio connection;
 - ETCS equipment: integrity status, alarms, and events;
 - Temporary speed restrictions;
 - Emergency messages;
 - Text messages;
 - Any other information or order to fulfil HSR operational/safety needs.
- 6.5.3.7 The full set of messages/commands exchanged between RBC and TMS shall be defined during the design phase of TSCC Contractor.
- 6.5.3.8 The user interface shall be provided with - but not limited to - the following general commands:
- Temporary speed restriction: activation/deactivation.
 - Non-stopping area: activation/deactivation.
 - Shunting area/train authorized in shunting mode association.
 - Emergency stop message: activation/revocation.
- 6.5.3.9 The traffic operator shall manage TSRs using the following specific commands:
- Plan a TSR.
 - Activate a TSR.
 - Deactivate a TSR.
 - Remove a TSR.
- 6.5.3.10 To make the TSR implementation a safe process, the TSR module shall include authority rights as regard to planning, activation, deactivation, and removal. The TSCC Contractor should adopt protocols and techniques coming from the best practice for possession management in safety-related railway systems (for example, planning a TSR in 2 steps executed by different operators, 1 for preparation and 1 for validation; double commands to avoid unexpected deactivation or removal).
- 6.5.3.11 The traffic operator shall be informed about the presence of issues in the actions performed through dedicated alarms (e.g., TSR planning rejection, TSR activation rejection, TSR removal rejection, CES rejection, etc.).
- 6.5.4 Wireless Communication System**
- 6.5.4.1 Wireless Communication System used as radio bearer service for ETCS shall be as specified in Schedule 5(r) - WCS Specification].
- 6.5.4.2 RBC shall have a redundant interface with the Wireless Communication System via the Digital Communication Network (DCN).
- 6.5.5 Hazard Detection and Early Warning System**
- 6.5.5.1 Hazard Detection and Early Warning detectors shall be deployed on HSR Railway to ensure:



- Monitoring of trackside assets;
- Monitoring of meteorological events.

6.5.5.2 RBC shall interface the alarms raised by the Hazard Detection and Early Warning detectors via direct interface, or TMS or CBI, depending on the outcome of the Hazard Analysis that shall be performed to define the level of mitigation required (e.g. immediate emergency stop order, confirmation or not by the controller before the mitigation is put in place, Maker board set to danger, application of TSR...)

6.5.5.3 The ETCS design shall include any other mitigation that may be further required by the hazard analysis.

6.5.6 Enterprise Asset Management System (AMS)

6.5.6.1 The maintenance of ETCS trackside shall be integrated with the maintenance of the other Systems of TCS Subsystem.

6.5.6.2 The ERTMS/ETCS system shall be interfaced with the Enterprise Asset Management System (EAMS).

6.5.6.3 RBC shall have a redundant interface with EAMS.

6.5.6.4 ETCS shall provide EAMS with the following types of information:

- Incidents and alarms related to the system;
- Subsystem and component failures;
- Data records to prepare the Preventive Maintenance.

6.5.6.5 The full set of information to be transmitted to EAMS, and the format in which this should be presented by ETCS, shall both be defined during the design phase of TSCC Contractor.

6.5.7 Network Timing System (NTS)

6.5.7.1 The ETCS trackside shall interface with the NTS for time distribution to RBC and precise synchronisation with the other interfaced systems of TCS subsystem, including ETCS onboard.

6.5.7.2 [Note: out of the TSCC Contractor scope of work, individual GPS-based clock receivers shall be provided on the trains for the time synchronisation]

6.5.7.3 ETCS-NTS shall be a redundant interface.

6.5.7.4 Features and performance required for NTS are set out in the relevant NTS Technical Specification for TSCC.

6.5.7.5 Whatever time protocol is to be supported (PTP, NTP, SNTP, etc.), it must be considered that ETCS requires accurate time synchronisation and rigorous timestamping of Euroradio messages and data records.

6.5.8 Digital Communication Network (DCN)

6.5.8.1 RBC system shall use the Digital Communication Network to centrally interface with CBI, TMS, the Wireless Communication System, AMS/SCADA and MCS, as well as with neighbouring RBCs.

6.5.8.2 All previous communications shall be redundant.

6.5.8.3 Features and performance required for the core network are set out in the relevant DCS System Technical Specification for TSCC.

6.5.9 Low Voltage Power Supply (LVPS)

6.5.9.1 The ETCS trackside equipment shall have a redundant interface with the LVPS system.

6.5.9.2 The ETCS equipment shall be considered by LVPS as an “emergency load” requiring uninterrupted power.

6.5.9.3 Features and performance required for LVPS system are set out in the relevant MV+LV Power Supply System Technical Specification for TSCC.



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

- 7.1.1 According to the European Construction Products Regulation (CPR) 305/2011/EU, the ETCS trackside components shall be provided with a CE mark accompanied by information on the level or class of performance of the Essential Characteristics. There shall be a clear marking that identifies the Balise Class of the Eurobalise as required by UNISIG SS-026, while the labelling of trackside boards shall comply with the EN12899-1 standard.
- 7.1.2 The Eurobalise shall also be equipped with a supplementary tag containing the specific ETCS project information, such:
- Type/main function of the balise or balise group;
 - “Country or Region Identifier” (NID_C) and “BG Identifier” (NID_BG);
 - Progressive number of the balise within the BG;
 - Direction of validity of the message it contains.



8 TOLERANCES

- 8.1.1 The design, dimensions, optical properties, mechanical performances, and maintenance requirements of trackside boards shall fulfil the European Standards EN12899-1 and EN16494 (refer to 2.4).
- 8.1.2 The tolerance for each dimension referred in EN16494 shall be $\pm 1\%$ with a minimum of $\pm 2\text{mm}$.
- 8.1.3 Tolerances for balise installation (height, lateral, angular, etc.) shall fulfil UNISIG standard SS-036.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 General requirements related are described in Technical Contract Requirements.

9.2 Specific Requirements

9.2.1 The ETCS scope of supply and delivery shall include (not limited to):

- Central ETCS servers;
- TMS/RBC Operator Workstations/HMIs;
- Maintenance Workstations;
- Workstation and servers for tests on-site and laboratory compliance tests;
- ETCS On Board Subsystem for laboratory tests;
- Eurobalises, brackets and cover plates adapted to track configuration;
- Trackside boards, including masts and brackets;
- Cabling and connectors;
- Racks;
- Tools and simulators for on-site and laboratory compliance tests, and for CHSR Authority training purposes;
- Software architecture including full definition of protocols used;
- Management System;
- SW licenses.

9.2.2 Specific configuration shall be delivered enabling the testing at operational speed of 350 km/h + 10 %, keeping ETCS supervision active on-board the train (with SIL 4).



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.

11.2 Specific Requirements

11.2.1 The installation of TSCC objects shall fulfil the basic TSI parameters in terms of interoperability, visibility, and compatibility with the railway infrastructure.

11.2.2 The installation of TSCC objects shall meet the clearance gauge requirements of HSR Railway.

11.3 Installation requirements for balises

11.3.1 The installation of balises shall ensure that the expected operational, functional and performance requirements defined in this technical specification are achieved.

11.3.2 Balise installation shall fulfil clearance gauge requirements relating to the lower envelope.

11.3.3 The TSCC Contractor shall propose the fixing methods of the balises and provide information relating to the specific support used: whatever solution is proposed, this shall not require drilling of sleepers or rails.

11.3.4 The general installation rules for balises shall comply with UNISIG standard SS-036 for the following main aspects:

- Crosstalk protection.
- Location reference accuracy.
- Time and distance requirements for constraints on distances between Balise Groups.
- Height Tolerances for Balise Mounting.
- Distance from Top of Rail to Balise Reference Mark.
- Lateral and Angular Tolerances for Balise Installation.
- Distance between Balises.
- Number of Balises in a Balise Group.
- Balise Installation in Narrow Curves.
- Metallic Masses and Cables in proximity.
- Environmental Conditions.

11.3.5 The installation of balises shall fulfil UNISIG standard SS-040 (Dimensioning and Engineering rules) for the following main aspects:

- Maximum distance between balises within a group.
- Minimum distance in rear of EOA/LOA of a balise group giving an immediate level transition order or giving a "Stop if in SR".
- Balise installation relative to track conditions.
- Balise installation relative to mission profile (UNISIG SS-091).
- The minimum distance between two adjacent balises of the same balise groups shall be:
- Main running tracks: 5m from centre to centre to meet maximum speed requirements for dynamic tests (300km/h + 10%) with active ETCS L2 supervision.
- For other tracks: 3m from centre to centre.

11.3.6 Balises shall be installed with an accuracy location of the balise group non greater than $\pm 5\text{m}$.



- 11.3.7 According to the safety requirements for technical interoperability set out in UNISIG standard SS-091, the maximum distance between two consecutive balise groups shall never exceed 2500m.
- 11.3.8 In general, the installation of balises should be avoided in proximity of cables, metal masses, and other interfering conductive materials, unless it is possible to respect the metal free area around the balise required by UNISIG standard SS-036. This restriction may apply to:
- Turnout area.
 - Steel sleeper.
 - Derailment plinth with metallic reinforcement.
 - Metal plane.
 - Guard rails.
- 11.3.9 Specific locations of HSR where the installation of balises should be avoided are:
- Railway bridges where guard rails may be used to provide protection against derailments, as in the case of Neris bridge (approximately 1.500 meters long).
- 11.3.10 If balises cannot be avoided in proximity of guard rails for any operational, or safety, or interoperability need of ETCS application, such balises shall be positioned on the track under the conditions defined in UNISIG standard SS-036.
- 11.3.11 [Note: typical solutions which make balises able to operate in presence of guard rails are the longitudinal mounting or a gap/cut in the guard rails]

11.4 Installation requirements for trackside marker boards

- 11.4.1 The installation of marker boards shall ensure that the expected operational, functional and performance requirements defined in this technical specification are achieved.
- 11.4.2 The installation of trackside marker boards shall be compatible with both sighting requirements (driver's field of view) and infrastructure requirements (curves, tunnels, bridges, etc.), taking also into account the adverse climatic conditions which may affect the visibility of marker boards (e.g., the high snow level).
- 11.4.3 Marker board installation shall fulfil gauge requirements relating to lateral and upper envelope.
- 11.4.4 Since EN16494 provides five sizes for ERTMS trackside boards (500m, 600m, 700m, 800m, 900m), in case a size smaller than 500m must be used, the height/width ratio of the dimensions shall be same of standard size.
- 11.4.5 ETCS Stop and Location markers shall not be placed in areas where stopping the train may lead to dangerous situations. Bridges, tunnels, ecoducts, and similar areas, should be avoided.
- 11.4.6 ETCS Stop and Location markers shall be installed on the left side, on the right side or on the top side of the track, in such a way that they clearly indicate the track to which they belong.
- 11.4.7 ETCS Stop and Location markers in double-track sections should be aligned to the same miles point.
- 11.4.8 Trackside boards shall be mounted on a dedicated mast or, when possible (mainly in open line), on existing structure (e.g., the catenary pole).
- 11.4.9 Poles of marker boards shall be made of elements of polyester reinforced with glass fibers, or galvanized steel.
- 11.4.10 Marker boards and their supporting poles shall be resistant to static and dynamic loads, including snow, rain, wind and overpressures due to aerodynamic effects generated by passing trains. During the design phase TSCC Contractor shall provide type and dimensions of the mast foundation blocks, taking into consideration the geognostic properties of the soil.



11.5 Mounting requirements for indoor equipment

- 11.5.1 RBC, TSR, and D&M servers shall be mounted in 19" rack cabinets whose dimensions shall comply with EN 60297-3 (refer to 2.4).



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.

12.2 Specific Requirements

12.2.1 The ERTMS/ETCS tests shall verify the compatibility with other TCS subsystems and related interfaces.

12.2.2 The ERTMS/ETCS tests shall verify:

- The safe integration of all internal components and interfaces that form the architecture of the ETCS subsystem.
- The safe integration of all external interfaces of the ETCS subsystem, within its direct physical, functional, environmental, operational and maintenance context.
- The safe integration between ETCS trackside and ETCS onboard.



13 SUBMITTALS

13.1 General Requirements

13.1.1 submittals required for the Interlocking system are defined in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Contract and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the CHSR Authority reserves the right to request from the TSCC Contractor and related Suppliers, information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence ETCS system reliability, availability and maintainability characteristics.



16 LOGISTICS

16.1.1 General logistics requirements are defined in the Agreement.



Schedule 5(f)

Fire Protection System (FPS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0010 – Fire Protection System (FPS)

Rev. 0.0

Authorized:

A handwritten signature in black ink, appearing to read "Harshal Jadhav".

Harshal Jadhav, Telecom System Lead

12/22/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Thomas Newey".

Thomas Newey, Telecom Lead

12/22/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Bruno Comperat".

Bruno Comperat, Deputy Director of Rail Engineering

12/23/2025

Date

Approved:

A handwritten signature in blue ink, appearing to read "Ryan Scott".

Ryan Scott, Director of Rail Engineering

12/23/2025

Date

Released:

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Amit Joshi, Configuration Manager

12/23/2025

Date



Document Revision History – FPS Specifications**Second Edition****December 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition
1.0	December 2025	Second Edition for Addendum 2 release



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION.....	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.1	GENERAL	6
2.2	DESIGN GUIDELINES.....	6
2.3	TSI	6
2.4	STANDARDS	6
2.5	OTHER DOCUMENTS	7
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	9
3.1	TERMS, DEFINITIONS AND ABBREVIATIONS	9
4	SYSTEM DESCRIPTION	10
4.1	PURPOSE OF THE FPS	10
4.2	FPS SYSTEM DEFINITION	10
4.3	FPS SYSTEM OPERATIONAL CONTEXT	10
4.4	DESIGN LIFE	10
5	SYSTEM REQUIREMENTS.....	11
5.1	GENERAL REQUIREMENTS.....	11
5.2	ENVIRONMENTAL CONDITIONS REQUIREMENTS.....	12
5.3	FUNCTIONAL REQUIREMENTS FOR FPS.....	12
5.4	PERFORMANCE REQUIREMENTS FOR FPS.....	13
5.5	CYBERSECURITY AND SECURITY REQUIREMENTS.....	14
6	INTERFACES REQUIREMENTS.....	15
6.1	GENERAL REQUIREMENTS.....	15
6.2	THIRD PARTY INTERFACE	15
6.3	EXTERNAL INTERFACE – FACILITIES CONTRACTOR.....	15
6.4	INTERNAL INTERFACE.....	15
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS.....	17
7.1	GENERAL REQUIREMENTS.....	17
7.2	SOFTWARE AND HARDWARE REQUIREMENTS	17
7.3	EMC REQUIREMENTS.....	17
8	TOLERANCES	18
9	SCOPE OF SUPPLY AND DELIVERY.....	19
9.1	GENERAL REQUIREMENTS.....	19
9.2	SPECIFIC REQUIREMENTS	19
10	MANUFACTURING.....	20
10.1	GENERAL REQUIREMENTS.....	20
11	INSTALLATION AND INTEGRATION.....	21
11.1	GENERAL REQUIREMENTS.....	21



12	TESTING & ACCEPTANCE	22
12.1	GENERAL REQUIREMENTS.....	22
12.2	SPECIFIC REQUIREMENTS	22
13	SUBMITTALS.....	23
13.1	GENERAL REQUIREMENTS.....	23
14	QUALITY MANAGEMENT.....	24
14.1	GENERAL REQUIREMENTS.....	24
15	ADDITIONAL INFORMATION REQUESTED	25
15.1	GENERAL REQUIREMENTS.....	25
16	LOGISTICS	26
16.1	GENERAL REQUIREMENTS.....	26



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Fire Protection System, hereinafter: FPS. Specific requirements relating to TSCC systems are listed in this document. Stations and facilities FPS are under shall stations contractor scope and facilities contractor scope.
- 1.1.2 The requirements are formulated using the following words and their meanings:
- **"Shall"**: Indicates mandatory requirement that must be strictly implemented; a waiver from a mandatory requirement is permissible only with approval of a design variance.
 - **"Should"**: Indicates a preferred course of action; a design variance is not required if it is not exercised.
 - **"Must"**: Indicates an obligation or a mandatory requirement.
 - **"May"**: Indicates a permissible course of action within the limits of the standards; a design variance is not required if it is not exercised.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the standards, guidelines, and specifications provided in this chapter for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, and training.

2.2 Design Guidelines

- 2.2.1 The latest version of the following Design Guidelines shall be applied:

ID	Code	Title
[R1]	Design Criteria Manual	Chapter 5 – Safety and Security
[R2]	Design Criteria Manual	Chapter 20 – Fire Protection and Alarm
[R2]	AREMA standards	Chapter 17 – High-Speed Rail Systems

TABLE 18 DESIGN GUIDELINES

2.3 TSI

- 2.3.1 There are no applicable TSIs for the FPS.

2.4 Standards

- 2.4.1 The TSCC Contractor shall fully consider and apply the following standards.

ID	Standard	Title
[R3]	EN 54	Fire detection and fire alarm systems
[R4]	EN 620-2:2012 +A1:2017	Fire safety – Safety signs
[R5]	ISO 3864	Safety colours and safety signs
[R6]	ISO 8421	Fire protection – Vocabulary
[R7]	ISO 13943	Fire safety – Vocabulary
[R8]	EN 15004	Fixed firefighting systems – Gas extinguishing systems
[R9]	EN 50121	Railway applications - Electromagnetic Compatibility
[R10]	EN 50122-1	Railway applications - Fixed installations - Electrical safety, earthing and the return circuit - Part 1: Protective provisions against electric shock
[R11]	EN 50124	Railway Applications - Insulation Coordination
[R12]	EN 50125	Railway Applications - Environmental Conditions for Equipment
[R13]	EN 50130-4	Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems
[R14]	EN 50173	Information technology - Generic cabling systems
[R15]	EN 50174	Information technology - Cabling installation



ID	Standard	Title
[R16]	EN 50346	Information technology -Cabling installation -Testing of installed cabling
[R17]	EN 61034	Measurement of smoke density of cables burning under defined conditions
[R18]	EN 62305	Protection against lightning
[R19]	IEC 61000	Electromagnetic compatibility (EMC)
[R20]	IEC 60331	Tests for electric cables under fire conditions
[R21]	IEC 60332	Tests on electric and optical fibre cables under fire conditions
[R22]	IEC 60529	Degrees of protection provided by enclosures (IP Code)
[R23]	IEC 60754	Test on gases evolved during combustion of materials from cables
[R24]	IEC 61643	Components for low-voltage surge protection
[R25]	ETSI EN 300 386	Telecommunication network equipment; Harmonized standard for ElectroMagnetic Compatibility (EMC) requirements
[R26]	ETSI EN 301 462	Human Factors (HF); Symbols to identify telecommunications facilities for deaf and hard of hearing people
[R27]	ISO 11064	Ergonomic design of control centers
[R28]	ISO 9001	Quality management systems — Requirements
[R29]	NFPA 72	National Fire Alarm and Signaling Code
[R30]	NFPA75	Standard for the fire protection of information technology equipment
[R31]	NFPA76	Standard for the fire protection of telecommunications facilities
[R32]	NFPA 130	Standard for Fixed Guideway Transit and Passenger Rail Systems
[R33]	NFPA 780	Standard for the Installation of Lightning Protection Systems
[R34]	NFPA 2001	Standard on clean agent fire extinguish systems
[R35]	2010 ADA	2010 ADA Standards for Accessible Design
[R36]	2025 California fire code	2025 California fire code
[R37]	UL2900 series	Cybersecurity for Network-Connectable Products
[R38]	TSA SD 1580/82-2022	Cybersecurity Requirements for High-Risk Rail Operators
[R39]	ANSI/ISA-18.2	Management of Alarms Systems for the Process Industries
[R40]	ANSI/UL 217	Standard for Safety Smoke Alarms
[R41]	ANSI/UL 2034	Standard for Single and Multiple station Carbon Monoxide Alarms

TABLE 19 LIST OF APPLICABLE STANDARDS

2.5 Other Documents

2.5.1 The following documents shall be referred:



ID	Document	Title
[R39]	Schedule 16	Scope of Work
[R40]	Schedule 5(a) SPEC-0005	Technical Specification Cybersecurity
[R41]	Schedule 3	Safety, Security and RAM Requirements

TABLE 20 OTHER DOCUMENTS

3 TERMS, DEFINITIONS, AND ABBREVIATIONS

3.1 Terms, Definitions and Abbreviations

- 3.1.1 All the terms, definitions and abbreviations are provided in Schedule 5(t) SPEC-0024 – Glossary of Terms, Abbreviations, and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of the FPS

- 4.1.1 The purpose of the FPS is to perform fire detection and notification of fire to the OCC operators and extinguish the fire within the California High Speed Rail infrastructure.
- 4.1.2 The FPS shall protect life, safeguard railroad assets, support operational continuity, mitigate fire risks, and ensure compliance with applicable fire safety regulations and standards.

4.2 FPS System Definition

- 4.2.1 FPS shall be an integrated system meant for reliable protection against fire hazards.
- 4.2.2 FPS shall be a state-of-the-art, software-controlled automatic system with necessary programming functions, annunciation, self-test and controls.
- 4.2.3 The control and monitoring of the FPS in station and facilities shall be performed by station management system and facilities management system, as designed by station and facilities contractors.
- 4.2.4 FPS in equipment housings and buildings shall be capable of being monitored and controlled from fire alarm display at OCC.

4.3 FPS System Operational Context

- 4.3.1 The mission of the FPS is to perform the following main functions: Fire Detection and Alarm and Fire Extinguishing.
- 4.3.2 The end users of the FPS are Authority personnel.
- 4.3.3 The FPS shall be operated according to the Authority's procedures.

4.4 Design Life

- 4.4.1 The Design Life requirements of the FPS shall be 30 years.
- 4.4.2 The TSCC Contractor shall provide an equipment lifecycle plan demonstrating how all FPS components will be maintained to meet the specified design life.
- 4.4.3 The TSCC Contractor shall ensure FPS components with shorter design lifespans shall be managed by scheduled technology refresh strategies and spares management plans.
- 4.4.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce, supply and support FPS components, or provide replacements with equal or compatible technical specifications, for the entire lifetime required.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

- 5.1.1 The FPS shall be designed in accordance with the requirements described in this specification, other relevant documents listed in Section 2 of this specification, other CHSR technical specifications and the Contract technical Requirements. In the event of any conflict between these documents, the requirements of this specification shall take precedence.
- 5.1.2 The FPS System shall be deployed in shelters and substations.
- 5.1.3 The TSCC Contractor shall perform the design, manufacturing, delivery, installation, inspection, test, commissioning, supply of necessary documentation, spare parts, special tools, and training for the FPS and its components in accordance with the relevant standards and regulations as it is stated in section 2.
- 5.1.4 Monitoring and control of the FPS in stations and facilities shall be performed by station building management systems and facilities building management systems, designed by the stations and facilities contractors.
- 5.1.5 The FPS for TSCC equipment shall be monitored and controlled through integration with ICSS at the OCC.
- 5.1.6 The FPS system shall be capable of triggering the CCTV system to display relevant CCTV views on the video wall or ICSS HMI in OCC.
- 5.1.7 The TSCC Contractor shall ensure compatibility and integration of the FPS, ICSS and the CCTV Systems for the monitoring and control.
- 5.1.8 The FPS protected areas (including raised floors and false ceilings, if applicable) shall be equipped with fire detection sensors.
- 5.1.9 Fire detection sensors shall be of addressable type and connected to the local control panel.
- 5.1.10 Fire detection sensor types shall be selected based on the characteristics of various occurrences and the area of application.
- 5.1.11 Each fire detection sensor shall have 2 levels of triggers, one to warn of a potential risk of fire and one to warn in case of a fire.
- 5.1.12 The fire detection sensors shall be selected based on the goal of earliest and safest detection possible, when choosing a fire detection sensor, the following criteria shall be considered.
 - What is to be detected (smoke / heat / flame).
 - Type of fire / fire development.
 - Environment / Surroundings.
 - Location.
 - Coverage area.
 - Acceptable degree of nuisance alarms.
- 5.1.13 The objective is to select the correct sensor for the appropriate application, to provide the earliest warning of fire without the risk of false alarm.
- 5.1.14 Positioning and selection of fire detection sensors shall be in strict compliance with applicable standards, legislations of the countries and manufacturer's instructions.
- 5.1.15 If required by Authority and applicable regulation, the Fire extinguishing system in TSCC equipment rooms and shelters shall be based on NOVEC™ 1230 extinguishing agent. NOVEC™ 1230 agent, which contains no chlorine or bromine, has an ozone depletion potential of zero.
- 5.1.16 Regardless of regulatory requirements, shelters and medium + low voltage power supply equipment rooms shall be equipped with a fire alarm system as a minimum requirement.



- 5.1.17 FPS cables shall be different color than other systems cables and separated from power cables.
- 5.1.18 The FPS components shall be arranged to be accessible and to facilitate the inspection, testing, loading and maintenance operations and to minimize interruption of protection.
- 5.1.19 The FPS equipment layout shall be standardized as much as practical.

5.2 Environmental Conditions Requirements

- 5.2.1 The TSCC Contractor's FPS system design shall be appropriate for, and resilient to, the local environmental and climatic conditions at each installation site. The equipment in shelters/building shall be compliant to the climatic class T2 defined in EN50125-3 according to environmental classification provided by EN 60721-2-1, concerning Temperature and Humidity.
- 5.2.2 All equipment shall be protected from damage or degradation in performance due to shock or vibration as experienced in the railway environment.
- 5.2.3 The IP rating of the outdoor equipment shall be at least IP65.
- 5.2.4 All outdoor equipment that is directly exposed to the sun shall be UV-protected.
- 5.2.5 All FPS equipment shall be suitable for their target environment and location to operate satisfactorily under all variations that may be met in normal usage.
- 5.2.6 All FPS equipment shall comply with WEEE and RoHS directives for electronic waste and hazardous substances, and a component take-back or recycling plan shall be provided.

5.3 Functional Requirements for FPS

- 5.3.1 Fire alarm activation shall be provided through fire detection sensors, manual call points and / or interface modules.
- 5.3.2 The alarms signal shall immediately be transmitted to the fire alarm display at OCC.
- 5.3.3 In the event of a fire incident, the FPS shall trigger the CCTV system to display the relevant CCTV view on the video wall or ICSS HMI in OCC.
- 5.3.4 Any alarm, trouble or supervisory indication shall not be reset until it has been acknowledged.
- 5.3.5 Alarms shall have priority over trouble signals. "Trouble" means a signal indicating a fault or impairment of the fire alarm system or a monitored circuit/component (e.g., device/loop fault, ground fault, power/battery failure, communications failure) per NFPA 72; Trouble shall not inhibit, delay, or mask any Alarm annunciation or action.
- 5.3.6 The local control panel shall receive all the signals from automatic fire detection sensors, audible/visual alarms, manual fire alarms (glass breaking type) and from fire suppression equipment.
- 5.3.7 All alarm handling and FPS features shall be controlled and monitored from the local control panel.
- 5.3.8 The local control panel shall monitor and control all the FPS equipment and shall forward the alarms and failure conditions (including loss of primary or secondary power) to the fire alarm display at the OCC.
- 5.3.9 The FPS shall also provide a rapid visual indication of the location of a fire incident and shall trigger the CCTV system to display the relevant CCTV view on the video wall or the ICSS HMI in the OCC.
- 5.3.10 The local control panels shall have trouble signal and alarm silencing switches and shall be equipped with a silence before reset feature to prevent accidental FPS reset during an alarm condition.
- 5.3.11 The OCC operator shall be capable of acknowledging the alarm, once it has been verified that the alarms and fire incident have been resolved.
- 5.3.12 The audible alarm shall be able to generate an appropriate sound level according to the applicable standards and legislation.
- 5.3.13 Measures to prevent false activation shall be developed by the TSCC Contractor.



- 5.3.14 The time delay between the pre-discharge alarm and the discharge shall allow personnel evacuation prior to discharge and shall not exceed the maximum disposure time for the agent.
- 5.3.15 In case of a failure of fire detection, the fire extinguishing container shall have the ability of manual operation.
- 5.3.16 The container shall be provided with necessary indicators of the agent quantity, any failure shall be reported to the local control panel and further to the fire alarm display at OCC and triggering the CCTV system to display relevant CCTV view.
- 5.3.17 Fire Protection System (FPS) shall be capable of integration with a Public Address and Customer information system (PACIS) to enable live or pre-recorded audio announcements during a fire incident. This integration allows the Operations Control Center (OCC) operator to issue instructions, provide information on the incident, and guide occupants to safety, facilitating faster and more organized evacuations.

5.4 Performance Requirements for FPS

5.4.1 Safety Requirements

- 5.4.1.1 FPS shall comply with the safety requirements defined in the System Safety Plan.
- 5.4.1.2 During the extinguishing process, all doors leading to the extinguishing area shall be closed (equipped with a puller) and with the possibility to open from the inside manually even when locked from the outside.
- 5.4.1.3 The doors shall be provided with signage in English and Spanish, which informs about the existence of an extinguishing system in the room and gives instructions to the personnel on how to act.
- 5.4.1.4 The safety precautions shall be ensured by the TSCC Contractor according to the applicable standards and legislation.

5.4.2 RAM Requirements

- 5.4.2.1 The TSCC Contractor shall be responsible for performing all the activities as specified in the Schedule 1.
- 5.4.2.2 FPS shall be operational 24/7 during operational service.
- 5.4.2.3 The FPS shall maintain an operational availability of 99.9% or greater over a 12-month period.
- 5.4.2.4 FPS shall maintain reliability of signal that provides a certainty of 99.99% that the received message is identical to the transmitted message.
- 5.4.2.5 The mean time to repair (MTTR) shall be less than 4 hours for critical components.

5.4.3 Secondary Power Operation

- 5.4.3.1 Operation on secondary power shall not affect the system and supervising signals including alarm, supervisory, and trouble signals and indications.

5.4.4 Detection Sensitivity

- 5.4.4.1 Each smoke detector shall comply with applicable standards such as ANSI/UL 217.
- 5.4.4.2 Each carbon monoxide alarm and detector shall meet the sensitivity testing and alarm thresholds of ANSI/UL 2034.

5.4.5 Alarm and Signal Detection

- 5.4.5.1 FPS shall transmit fire detection and alarm signal to the OCC within 5 seconds (95th percentile) and withing 8 seconds (99th percentile).
- 5.4.5.2 FPS shall transmit other alarm signals such as supervisory, trouble signal and indication to the OCC within 10 seconds (95th percentile).



- 5.4.5.3 FPS shall provide alarm information with priority coding such as fire alarm or faults to enable OCC operators to triage events effectively.
- 5.4.5.4 Alarm information shall include site ID, shelter location, type of alarm and timestamp.
- 5.4.6 **Alarm manageability and event logging**
 - 5.4.6.1 To avoid alarm flooding, the system alarm design shall follow guidelines in ANSI/ISA-18.2 standard.
 - 5.4.6.2 FPS shall be designed to minimize false alarms. Only actionable alarms are announced to operators; routine status/telemetry is logged but not announced.
 - 5.4.6.3 FPS shall log all fire events, faults, resets, and maintenance activities with timestamp accuracy of ± 1 second, synchronized to the NTS.
- 5.4.7 **Environmental**
 - 5.4.7.1 The FPS shall meet all performance requirements while operating under the conditions of the local environment.

5.5 Cybersecurity and Security Requirements

- 5.5.1 The FPS design, configuration, and operation shall be fully compliant with the CHSR Cybersecurity Technical Specification. All generic security controls, roles, logging, patching cadence, incident-response procedures, and assurance measures are established within the Authority's Cybersecurity Technical Specification.
- 5.5.2 The FPS shall have a System Owner who shall be accountable for cybersecurity risk ownership and mitigation.
- 5.5.3 The System Owner shall be responsible for ensuring that appropriate resources attend cybersecurity threat modelling and risk assessment activities.
- 5.5.4 Digital, IP-based communications shall be authenticated and protected from injection and tampering.
- 5.5.5 Interfaces between FPS systems and other systems, including EACS, HMIs, CCTV systems, ISCC, and others shall be co-engineered with the cybersecurity team in accordance with the CHSR Cybersecurity Technical Specification.
- 5.5.6 The FPS software and associated hardware shall support the protocols and technologies outlined in the Cybersecurity Specification; these capabilities shall be evaluation criteria and requirements in the procurement process.
- 5.5.7 The FPS software shall be securely configured by default by disabling all features and changing all default credentials prior to enabling required functionality during configuration.
- 5.5.8 Vendor hardening guidelines or other industry standards or benchmarks shall be implemented for software and hardware components procured for the FPS.
- 5.5.9 The FPS COTS software vendor shall be assessed to ensure that they take appropriate steps to mitigate supply chain vulnerabilities, will provide regular security patches for the duration of the products intended service life, has a vulnerability disclosure program, and follows secure software development practices in addition to other requirements outlined in the CHSR Cybersecurity Technical Specification.



6 INTERFACES REQUIREMENTS

6.1 General Requirements

- 6.1.1 Interfaces are classified as below:
- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR contractors).
 - External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors).
 - Internal interfaces between systems within the TSCC scope.
- 6.1.2 The TSCC Contractor shall develop the FPS design considering the identified external interfaces and internal interfaces to ensure the required functionalities and performance described in this specification for FPS.
- 6.1.3 The TSCC Contractor shall assess the identified interfaces and, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification for FPS.
- 6.1.4 The TSCC Contractor shall ensure the integration of the FPS with all identified third party, external and internal interfaces.

6.2 Third party Interface

- 6.2.1 The TSCC Contractor shall co-ordinate with the local fire authorities to include but not limited to planning approval.

6.3 External Interface – facilities contractor

- 6.3.1 The TSCC Contractor shall install the TSCC FPS equipment, as required and stipulated in this specification. The TSCC Contractor shall coordinate with the facility contractor to ensure integration with ICSS at the OCC, if required. The Facility Contractor, responsible for the construction of the OCC, shall install the FPS equipment that provides protection for the OCC facilities, and this work shall remain under the Facility Contractor's scope.

6.4 Internal Interface

- 6.4.1 **Interface with Network Timing System (NTS)**
- 6.4.1.1 FPS shall have a redundant interface to the Network Timing System (NTS) to retrieve a time reference.
- 6.4.2 **Interface with Digital Communications Network (DCN)**
- 6.4.2.1 FPS shall have a redundant interface to the DCN to allow monitoring and control of the FPS from the fire alarm display at OCC and triggering the CCTV system to display relevant CCTV view on the video wall or ICSS HMI in OCC.
- 6.4.3 **Interface with Electronic Access Control System (EACS)**
- 6.4.3.1 FPS shall have a redundant interface to the Electronic Access Control (EAC) system to release the lock of the doors on the emergency exit ways controlled by the local EACS control unit.
- 6.4.4 **Interface with Low Voltage Power System (LVPS)**
- 6.4.4.1 FPS shall have a redundant interface with the LVPS to ensure an uninterruptible power supply.
- 6.4.5 **Interface with Closed Circuit Television (CCTV), Integrated Control and Supervisory System (ICSS) and Passenger Announcement and Customer Information System (PACIS)**
- 6.4.5.1 FPS shall be interconnected with the CCTV System at the central level. In case of fire alarm, video related to the area where such the alarm is generated shall be highlighted to the operators in the OCC.



- 6.4.5.2 FPS shall have a redundant interface to the fire alarm display at OCC and trigger the CCTV system for the following functionality:
- 6.4.5.3 Equipment technical statuses (in service, in failure...) shall be transmitted to the fire alarm display at OCC and trigger the CCTV system to display the relevant CCTV view on the video wall or ICSS HMI in OCC.
- 6.4.5.4 Operation statuses (in maintenance, inhibited, operational, out of service, etc...) shall be transmitted to the fire alarm display at OCC and trigger the CCTV system to display the relevant CCTV view on the video wall or ICSS HMI in OCC.
- 6.4.5.5 Notifications, warnings and alarms shall be transmitted to the fire alarm display at OCC and trigger the CCTV system to display the relevant CCTV view on the video wall or ICSS HMI in OCC.
- 6.4.5.6 OCC operators shall be able to visualize and acknowledge FPS alarms. Acknowledge functions shall only be permitted once the incident has been verified and resolved.
- 6.4.5.7 The FPS shall interface with the Public Address and Customer Information (PACIS) system to enable integration with the Public Announcement system by OCC operator during a fire incident.
- 6.4.5.8 The TSCC Contractor shall:
- Support and provide any related equipment for the FPS alarm display in the OCC.
 - Coordinate with the ICSS for equipment arrangement at OCC, if applicable.
 - Provide support for ergonomic studies in the OCC control room, if applicable.
- 6.4.5.9 Events archiving and reports yielding shall be provided by the fire alarm display at OCC.
- 6.4.5.10 Authority personnel shall be able to visualize the equipment room/building layouts including location of the fire detection sensors.
- 6.4.5.11 The fire alarm display at OCC and triggering the CCTV system to display relevant CCTV view on videowall or ICSS HMI in OCC shall have a redundant interface for supervision of the Fire Protection System of the equipment room or building.
- 6.4.5.12 FPS shall provide an interface to the related cable containment to ensure proper pathway for the FPS cables.
- 6.4.6 **Interface with Enterprise Asset Management System (EAMS)**
- 6.4.6.1 The FPS shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied by the TSCC Contractor shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards. Refer to 2.4.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the design life requirements.
- 7.1.3 The FPS shall be complete with all equipment, supporting structures hardware, licenses, software, cabling and ancillary services which are useful for efficient operation of the FPS components. Such accessories and materials shall be deemed to be within the scope of this specification whether specifically mentioned or not.
- 7.1.4 All special tools and test equipment intended for configuration of the FPS shall be deemed to be within the scope of this specification whether specifically mentioned or not.

7.2 Software and Hardware Requirements

- 7.2.1 The FPS design shall be based on COTS (Commercial Off-The-Shelf), open architecture, and modular system architecture, with standard non-proprietary interfaces.
- 7.2.2 All cabling for FPS shall be designed, supplied, installed, and commissioned by the TSCC Contractor.
- 7.2.3 The FPS controllers shall have a redundant power supply.
- 7.2.4 The FPS devices shall be connected to the power supply of the facility where they are located (OCC, station, etc.).
- 7.2.5 The electrical cables, control and communication cables for FPS shall be fire-rated and comply with the relevant EN standards or other applicable recognized standards. Refer to 2.4.
- 7.2.6 The FPS controllers at each shelter (if applicable) shall be connected to the Digital Communication Network (DCN) to allow monitoring and control by the OCC operator. The interface connections and protocols shall be compatible with the relevant EN/IEEE standards or other applicable standards, as coordinated and agreed with the TSCC Contractor.
- 7.2.7 In cases where a network switch is required by the FPS to establish a connection through the DCN, a minimum of a Level 2 managed network switch shall be provided, fully compliant with the relevant EN/IEEE standards.
- 7.2.8 To avoid conflicts in network configuration with the DCN provided by the TSCC Contractor, the FPS IP configuration scheme shall be fully coordinated with, and formally approved by, the TSCC Contractor.

7.3 EMC Requirements

- 7.3.1 The FPS shall be fully immune and protected from any Electromagnetic Interference (EMI) with traction power, multi-tubular cabling, and Radio Frequency Interference (RFI). The EMI emissions shall be mitigated in accordance with applicable standards (EN 50122 or equivalent)



8 TOLERANCES

Not applicable to FPS.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 The TSCC Contractor shall supply and deliver all components related to this specification.

9.2 Specific Requirements

9.2.1 The FPS scope of supply and delivery shall include (but is not limited to):

- Local control panels.
- Mimic panels.
- Fire detection sensors.
- Manual call points.
- Sounders with flashers.
- I/O modules.
- Agent storage containers.
- Actuators.
- Discharge piping.
- Discharge nozzles.
- Valves, gaskets, O-rings, sealants and other valve components.
- Software architecture, including a full definition of protocols used.
- Network switching.
- Management System.
- Fire alarm workstation in OCC, if applicable.
- All HW/SW licenses required.
- Auxiliary elements, supporting structures, specials tools and test equipment
- Spare parts.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Schedule 16 Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.

12.2 Specific Requirements

12.2.1 The TSCC Contractor shall ensure the integrity of FPS functionality through the OCC operator in the event of a fire alarm. This shall include:

- Display of the fire alarm condition on the fire alarm display monitor.
- Automatic triggering of CCTV views of the related CCTV view on the video wall or ICSS HMI in OCC.
- Integrate with the Passenger Announcement and Customer information system (PACIS) and allow the PACIS system to issue public announcements, either pre-recorded or live announcements by the OCC operator, during fire incidents.



13 SUBMITTALS

13.1 General Requirements

13.1.1 General submittal requirements are defined in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence FPS subsystem reliability, availability, and maintainability characteristics.



16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.



Schedule 5(g)

Hazard Detection and Early Warning System (HDEWS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0011 – Hazard Detection and Early Warning System (HDEWS)

Rev. 0.0

Authored:

A handwritten signature in blue ink, appearing to read 'O. Meriot'.

Olivier Meriot, System Engineer

15 October 2025

Date

Checked:

A handwritten signature in black ink, appearing to read 'T. Newey'.

Thomas Newey, Telecoms Lead

10/15/2025

Date

Checked:

A handwritten signature in black ink, appearing to read 'Bruno Comperat'.

Bruno Comperat, Deputy Director of Rail Engineering

10/16/2025

Date

Approved:

A handwritten signature in blue ink, appearing to read 'Ryan Scott'.

Ryan Scott, Director of Rail Engineering

10/16/2025

Date

Released:

A handwritten signature in blue ink, appearing to read 'Amit Joshi'.

Amit Joshi, Configuration Manager

10/16/2025

Date



Document Revision History – HDEWS Specifications

First Edition

September 2025

Revision	Date	Revision Description
0.0	September 2025	First Edition



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION.....	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.1	GENERAL	6
2.2	TSI	6
2.3	STANDARDS	6
2.4	UIC RECOMMENDATIONS	7
3	TERMS, DEFINITIONS AND ABBREVIATIONS	8
3.1	GENERAL	8
4	SYSTEM DESCRIPTION	9
4.1	PURPOSE OF THE HDEWS	9
4.2	HDEWS DEFINITION	9
4.3	HDEWS OPERATIONAL CONTEXT	9
4.4	DESIGN LIFE	10
5	SYSTEM REQUIREMENTS.....	11
5.1	GENERAL REQUIREMENTS.....	11
5.2	ENVIRONNEMENTAL CONDITIONS REQUIREMENTS	14
5.3	OPERATIONAL REQUIREMENTS.....	14
5.4	FUNCTIONAL REQUIREMENTS.....	14
5.5	PERFORMANCE REQUIREMENTS.....	20
5.6	SECURITY AND CYBERSECURITY REQUIREMENTS.....	21
6	INTERFACES REQUIREMENTS.....	22
6.1	GENERAL REQUIREMENTS.....	22
6.2	THIRD PARTY INTERFACES	22
6.3	EXTERNAL INTERFACES – FACILITIES CONTRACTOR	22
6.4	INTERNAL INTERFACES FOR THE HDEWS.....	23
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS.....	25
7.1	GENERAL REQUIREMENTS.....	25
7.2	SW AND HW REQUIREMENTS	25
7.3	EMC REQUIREMENTS.....	25
8	TOLERANCES	26
9	SCOPE OF SUPPLY AND DELIVERY.....	27
9.1	GENERAL REQUIREMENTS.....	27
9.2	SPECIFIC REQUIREMENTS	27
10	MANUFACTURING.....	28
10.1	GENERAL REQUIREMENTS.....	28
11	INSTALLATION AND INTEGRATION.....	29
11.1	GENERAL REQUIREMENTS.....	29



12	TESTING & ACCEPTANCE	30
12.1	GENERAL REQUIREMENTS.....	30
13	SUBMITTALS.....	31
13.1	GENERAL REQUIREMENTS.....	31
14	QUALITY MANAGEMENT.....	32
14.1	GENERAL REQUIREMENTS.....	32
15	ADDITIONAL INFORMATION REQUESTED	33
16	LOGISTICS	34
16.1	GENERAL REQUIREMENTS.....	34
17	SPEED LIMITATION BASED ON METEOROLOGICAL CHANGE EXAMPLE	35
17.1	GENERAL DESCRIPTION.....	35
17.2	VALUES (IN METRIC SYSTEM) PROVIDED AS AN EXAMPLE	39



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's requirements for the Hazard Detection and Early Warning System, hereinafter: HDEWS.
- 1.1.2 The functional architecture of the HDEWS is presented in Appendix A.
- 1.1.3 The requirements are formulated using the following words and their meanings:
- **“Shall”**: Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure).
 - **“Should”**: Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents.
 - **“Must”**: Indicates an obligation or a mandatory requirement.
 - **“May”**: Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines and specifications provided in this technical specification for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, training, operations and maintenance.
- 2.1.2 All generic standards to be used are provided in: Schedule 16.

2.2 TSI

- 2.2.1 The applicable TSIs are listed below:

ID	TSI	Title
[R1]	SRT TSI	Commission Regulation (EU) No 1303/2014 of 18 November 2014 - concerning the technical specification for interoperability relating to 'safety in railway tunnels' of the rail system of the European Union including commission regulation (EU) 2016/912 of 9 June 2016 L 153 28 10.6.2016 and commission implementing regulation (EU) 2019/776 of 16 May 2019
[R2]	OPE TSI	The Commission has published the latest version of the TSI OPE under the Implementing Regulation 2023/1693 (TSI OPE 2023). This amends the Implementing Regulation 2019/773 (TSI OPE 2019). TSI OPE 2019 is in force since 16 June 2021 except for: 4.2.2.1.3.2 on Train visibility – rear end – freight trains (Tail Plates), Appendix A on ERTMS operational principles and rules (Appendix A) and Appendix C on communication (Appendix C). TSI OPE 2023 is published as an amendment to 2019 version and it enters into force 20 days after its publication (28 September 2023). Railway undertakings and infrastructure managers shall adapt their SMSs to the changes introduced by the TSI OPE 2023 within 9 months after TSI's publication (28 June 2024)
[R3]	TSI INF	Commission Regulation (EU) No 1299/2014 of 18 November 2014 on the technical specifications for interoperability relating to the 'infrastructure' subsystem of the rail system in the European Union, amended on 16/05/2019, including commission implementing regulation (EU) 2019/776 of 16 May 2019 and commission implementing regulation (EU) 2023/1694 of 10 August 2023
[R4]	ENE TSI	Commission Regulation (EU) No 1301/2014 of 18 November 2014 on the technical specifications for interoperability relating to the 'energy' subsystem of the rail system in the Union Text with EEA relevance including commission implementing regulation (EU) 2018/868 of 13 June 2018 and commission implementing regulation (EU) 2019/776 of 16 May 2019 and commission implementing regulation (EU) 2023/1694 of 10 August 2023

TABLE 1 LIST OF TSI AND REGULATIONS

2.3 Standards

- 2.3.1 The relevant European standards to be used for HDEWS are listed below.
- 2.3.2 The TSCC Contractor shall fully consider and apply the following standards in the provision of the Services, the in-force standards shall be applied.



ID	Standard	Title
[R5]	EN ISO 11205	Acoustics Noise emitted by machinery and equipment Engineering method for the determination of emission sound pressure levels in situ at the workstation and at other specified positions using sound intensity
[R6]	EN 13460	Maintenance – Documentation for maintenance
[R7]	EN 13775-1	Railway applications – Measuring of new and modified freight wagons – Part 1: Measuring principles
[R8]	EN 17230	Information technology – RFID in rail
[R9]	EN 15273-1	Railway applications – Gauges – Part 1: General – Common rules for Rolling Stock and Infrastructure
[R10]	EN 15273-2	Railway applications – Gauges – Part 2: Rolling stock gauge
[R11]	EN 15273-3	Railway applications – Gauges – Part 3: Structure gauges
[R12]	EN 14067-6	Railway applications — Aerodynamics — Part 6: Requirements and test procedures for cross wind assessment
[R13]	EN 15437-1	Railway applications - Axle box condition monitoring - Interface and design requirements Part 1: track side equipment and rolling stock axle box
[R14]	EN 15437-2	Railway applications - Axle box condition monitoring - Interface and design requirements Part 2: performance and design requirements of on-board systems for temperature monitoring
[R15]	EN 16729-3	Railway applications – Infrastructure – Non-destructive testing on rails in track – Part 3: requirements for identifying internal and surface rail defects
[R16]	EN 50119	: Railway application – Fixed installations – Overhead contact lines for electric traction, Principle drawing 21404/304730 – Obstacle and electrical insulation template

TABLE 2 LIST OF APPLICABLE STANDARDS

2.4 UIC Recommendations

2.4.1 The relevant UIC recommendations to be followed are listed below listed below.

UIC	Title
UIC 505-1	Railway transport stock - Rolling stock construction gauge
UIC 515	Cars – Running gear
UIC 608	Pantograph/Overhead line Interaction
UIC 660	Measures to ensure the technical compatibility of high-speed trains
UIC 779	Safety in railway tunnels

TABLE 3 - LIST OF UIC RECOMMENDATIONS

3 TERMS, DEFINITIONS, AND ABBREVIATIONS

3.1 General

- 3.1.1 All the terms, definitions, and abbreviations are provided in Schedule 5(t) SPEC-0024 – Glossary of Terms, Abbreviations, and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of the HDEWS

- 4.1.1 The HDEWS is a collection of integrated technologies and sensors designed to oversee and manage various auxiliary components of the trainsets and wayside infrastructure. This system will monitor and control the trainset health, broken rail or falling vehicles detection, among others.
- 4.1.2 The primary objectives of HDEWSs are:
- Reducing maintenance costs.
 - Collecting data for railroad service provision.
 - Preventing damage to the environment.
 - Preventing accidents: Vehicles and infrastructure damage can result in expensive repairs and erode public confidence in the transportation system.
 - Preventing human injuries or fatalities: The transportation system must ensure safety.
 - Minimizing downtime resulting from infrastructure damage and extending the lifespan of assets.
- 4.1.3 The HDEWS shall be based on the methods of automatic identification of the irregularities based on data from several Modular Sensors and initiation of the procedures to reduce the impact on service in general and rather on safety (e.g.: by sending alarms to the OCC). Probabilistic decision-making methods and theories shall be used to analyze the collected data and compare them with the reference systems information to make recommendations about any further actions.

4.2 HDEWS definition

- 4.2.1 The HDEWS is composed of the:
- A set of servers and data collectors for the control and supervision of the HDEWS subsystems
 - Hot-Axle Box Detection System (HABDS)
 - Derailment Detection System (DDS)
 - Broken Rail Detection System (BRDS)
 - Rail Temperature Monitoring System (RTMS)
 - Road Vehicle Detection System (RVDS)
 - Flooding Detection System
 - Earthquake Detection System
 - Meteorological Condition Detection System (MCDS)

4.3 HDEWS operational context

- 4.3.1 The mission of the HDEWS is to prevent accidents, to maintain expected availability of service, to reduce downtime of the railway line and to improve the asset life cycle by implementing systems (as stated in the general requirement) dedicated to the monitoring of the trainset, infrastructure, and other conditions.
- 4.3.2 The personnel involved in the operation of the HDEWS are maintenance and operation managers.
- 4.3.3 The HDEWS shall be operated according to Authority procedures. These procedures should be aligned with the system's operational requirements. Provisions for continuous information sharing and lessons learned shall be integrated into the operational framework.



4.4 Design Life

- 4.4.1 The design life for the HDEWS shall be 30 years in compliance with the General requirements Installation and Integration.
- 4.4.2 The TSCC Contractor shall ensure that the manufacturers will be able to produce HDEWS components, with equal or better technical specifications, throughout the required operational lifetime, recognizing the potential for successive generations and evolving sensor technology.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

5.1.1 Trainset Health Monitoring Equipment

5.1.1.1 Equipment targeting the detection of the correct health of the train are wayside detectors that monitor passing trains for defects. Monitored defects may require immediate action and require corrective maintenance. The wayside detectors will provide information directly to the Operational Control Center, to the train or to dedicated remote systems and to the train control system that permits a safe stop of the faulty train. The HDEWS shall include the following modular sensors dedicated to the monitoring of the trainset:

- Hot-Axle Box Detection System (HABDS),
- Derailment Detection System (DDS),

5.1.2 Infrastructure Monitoring Systems

5.1.2.1 The HDEWS shall include the following modular sensors dedicated to the monitoring of Infrastructure:

- Broken Rail Detection System (BRDS),
- Rail Temperature Monitoring System (RTMS),
- Road Vehicle Detection System (RVDS), which derivative can be used as a landslide/falling rock detection system,

5.1.3 Environmental Monitoring Equipment

5.1.3.1 The HDEWS shall include the modular sensors dedicated to the:

- Meteorological Condition Detection System (MCDS) wind,
- Meteorological Condition Detection System (MCDS) rain,
- Flooding Detection System (MCDS),
- Earthquake Detection System (MCDS),

5.1.4 Data Collectors

5.1.4.1 The locations and compositions of the Modular Sensor provided in different locations shall be selected based on its purpose during the detailed design phase and in conjunction with the Employer

5.1.4.2 The TSCC Contractor shall provide a specific strategy of data collector locations.

5.1.4.3 The program for the implementation of all HDEWSs, what detectors and at what location, shall be justified. The TSCC Contractor shall provide an additional analysis of the detection sensors needed and their geographical distribution.

5.1.4.4 The exact positions of Data Collectors and Modular Sensors shall be defined based on the technologies chosen to meet the requirements according to the Reference Standards and Documents.

5.1.4.5 When defining the exact location for the Data Collector, the TSCC Contractor shall consider the concentration of the equipment in the predefined land plot reservation areas at block section locations, cross-over and station turnout areas – system equipment locations (SEL).

5.1.4.6 All Modular Sensors included in the HDEWS of a location shall be provided as a trackside modular system.

5.1.4.7 All Modular Sensors included in the HDEWS of a location shall be integrated within the Data Collector.



- 5.1.4.8 Each independent detection sensor shall be connected to the Data Collector.
- 5.1.4.9 All monitored, measured, or controlled parameters must communicate using a standardized and open protocol, defined in an EN or ISO standard, an IETF RFC, or an equivalent unencumbered specification, available for industry review before submission.
- 5.1.4.10 Data collectors shall be based on standard architecture to ensure independence from any specific manufacturer, programming language, or operating system.
- 5.1.4.11 No constraints shall be imposed on data ownership or the usage of the protocols.
- 5.1.4.12 The protocol used between the Data Collector and peripheral sensors shall be fully aligned with the Cybersecurity Technical Specification.
- 5.1.4.13 The protocols used shall be fully documented, including documented data schema. The implementation shall be documented in both human and machine-readable formats.
- 5.1.4.14 The protocols used shall include:
- Message namespace,
 - Version control,
 - Sensor node status,
 - Messaging on status changes such as values, events, or threshold breaches.
- 5.1.4.15 The Data Collector shall be equipped to facilitate communication using a set of specified protocols to ensure seamless integration and interoperability. The protocols are divided into two groups: primary protocols, and secondary protocols, that can be used only within subsystems. Other open protocols can be proposed.
- 5.1.4.16 The primary protocols, for system interaction, include, but are not limited to:
- OPC UA,
 - MQTT / MQTT Sparkplug,
 - EULYNX.
- 5.1.4.17 The secondary protocols, used within subsystems only, include, but are not limited to:
- IEC 60870-5,
 - IEC 61850,
 - SNMP V3,
 - BACnet,
 - Profibus,
 - Profinet,
 - Profisafe.
- 5.1.4.18 The data collector ensures interoperability by understanding and converting data from different ancillary systems into a common format. This facilitates seamless communication and sharing of information between disparate systems.
- 5.1.4.19 The data collector is designed to operate within a specific geographical area. It shall be programmed to collect data from ancillary systems located within a defined region, ensuring that the information gathered is relevant to the specific context or location.



- 5.1.4.20 The design of the data collector shall be scalable to accommodate an increasing number of ancillary systems or expanding geographical coverage. This ensures that the system can adapt to changing requirements and growth.
- 5.1.4.21 The Data Collector shall be based on PLC, PC or RTU solution.
- 5.1.4.22 Data shall be transferred into a streaming data pipeline which will correlate and consolidate event information and actions across multiple subsystems to provide a single user interface and to support analytics and other longer-term uses.
- 5.1.4.23 Data collector nodes, located at the edge of network, should be designed to be manageable from the core infrastructures. These nodes should be treated as edge compute devices, enabling centralized monitoring, configuration, and control.
- 5.1.4.24 In case sensors generate substantial volumes of data, the HDEWS shall incorporate a local data analysis capability to handle it.
- 5.1.4.25 The Data Collector shall be modular, scalable, and able to receive information from with each type of Modular Sensors.
- 5.1.4.26 The Data Collector shall be able to transform formats into a limited number of standardized formats, such as the primary and secondary protocols. This transformation ensures that core systems are relieved from managing raw data across different protocols.

5.1.5 Communications

- 5.1.5.1 The HDEWS shall be designed to accommodate an extensive range of network connections, without imposing limitations, including the potential utilization of advanced network protocols like the 5G CHSR FRMCS private network.
- 5.1.5.2 The communication system must adhere to a documented data scheme, rather than relying on standalone applications.
- 5.1.5.3 The system must allow the automation of node discovery.
- 5.1.5.4 The data generated by the ancillary systems, shall be treated as confidential and shall be the sole property of CHSR. It is required that this data be securely stored on CHSR servers and made readily accessible to CHSR Incident Managers for analysis.

5.1.6 Technical solutions

- 5.1.6.1 A Multicriteria Analysis (MCA) must be conducted to assess and select a technical solution that aligns with the specific needs of CHSR. The evaluation criteria for the MCA must be clearly defined and aligned with CHSR requirements before the assessment of technical solutions is initiated. Consideration should be given to factors beyond cost alone, ensuring that the chosen solution is not only cost-effective but also optimally suited to meet the unique requirements of CHSR.
- 5.1.6.2 Data must adhere to the structure specified in the CHSR requirements and be accessible for integration into the Asset Management System.
- 5.1.6.3 The TSCC Contractor may propose the Light Detection and Ranging, also called LiDAR for HDEWSs if the proposed solution meets all the requirements described in this TS.
- 5.1.6.4 The TSCC Contractor's proposal for HDEWSs should include a detailed explanation of how LiDAR technology will be integrated and utilized, including key functionalities, data processing methods and system interactions.



- 5.1.6.5 The TSCC Contractor shall ensure that LiDAR solution is fully compliant with all the protocol's requirements and shall adhere to the mentioned modular principles, allowing for seamless integration and future expansion without needing extensive system modifications.
- 5.1.6.6 The TSCC Contractor should propose solution which allow the concept of the "intelligent gate" (combining all these sensors into a virtual gateway at transition points).

5.2 Environmental Conditions Requirements

- 5.2.1 The HDEWS equipment shall meet the environmental requirements described in the general requirements.
- 5.2.2 The trackside HDEWS equipment shall be immune to solar rays.
- 5.2.3 The HDEWS equipment shall comply with the EMC requirements according to the related standards and considering the typical electrified railway environment.

5.3 Operational Requirements

- 5.3.1 The TSCC Contractor shall ensure compliance with the CHSR operational rules when defining any additional locations required beyond those to the locations specified in 5.1.
- Establishing alarm, warning and notification levels and thresholds.
 - Developing alarm triggering procedures.
 - Implementing alarms, protocols, and procedures.
 - Defining the structure and classification of reports, considering factors such as track blocks and critical assets.

5.4 Functional Requirements

5.4.1 General Requirements

- 5.4.1.1 The HDEWS shall include components for monitoring, control, reporting, archiving, and analyzing several functions.
- 5.4.1.2 The HDEWS shall be capable of exporting data related to the Trainsets to the potential 3rd party Trainsets Asset Management System.
- 5.4.1.3 The HDEWS shall be capable of checking the required parameters and sending alarms, notifications, warnings to the ICSS systems if some noncompliance is detected.
- 5.4.1.4 The alarms, warnings, and status from Modular Sensors shall be provided by the HDEWS to the ICSS and shall be represented at the related HMI.
- 5.4.1.5 Data provided to the ICSS systems shall supply continuous and effective monitoring and control of the concerned assets.
- 5.4.1.6 All alarm indications shall be flashing when requiring immediate attention and steady if less urgent attention is necessary.
- 5.4.1.7 Alarms shall be provided for any conditions affecting normal operation.
- 5.4.1.8 Specific procedures shall be put in place for rail temperature, pantograph, load condition, gauge, road vehicle, broken rail, and wheel flat, and alarms thresholds shall be remotely configurable.
- 5.4.1.9 The HDEWS shall provide data and alarms directly to the AMS and AMS modules (predictive, supply chain, etc.):



- Significant measure deviations of an asset during a single journey (device failure suspicious).
- Indicators such as number of operations, time of use, number of failures, etc.

- 5.4.1.10 The HDEWS shall provide alarms on the abnormal conditions detected by the HABDS, BRDS, RTMS and MCDS to the OCC (Traffic Management System, Interlocking and ETCS).
- 5.4.1.11 The HDEWS shall provide alarms on the abnormal conditions detected from the DDS, RVDS, MCDS (flood) to the train control system.
- 5.4.1.12 The HDEWS shall collect and store the data shared by national weather conditions institutions to define at a minimum parameters such as temperature, humidity, wind, precipitations and forecast of wind, temperature, and precipitations.
- 5.4.1.13 The HDEWS shall be able to provide Asset Information data for maintenance purposes when requested to the EAMS
- 5.4.1.14 Vehicle tracking may also be used as a source for correlating information for other sensors.
- 5.4.1.15 The overall monitoring system shall include a functionality for correlating information from the sensors, enhancing the overall railroad operations and facilitating efficient data correlation.

5.4.2 Hot-Axle Box Detection System (HABDS)

- 5.4.2.1 The HABDS shall check the wheel temperatures and shall determine which axle is outside of the normal parameters.
- 5.4.2.2 The HABDS sensors shall be installed at a regular interval on both side of the main track to stop a faulty train at a pre-determined location on the main track (to be defined by the safety study)
- 5.4.2.3 The HABDS shall also integrate the function of detecting brake binding.
- 5.4.2.4 The HABDS shall be implemented along the line to monitor the train component overheating.
- 5.4.2.5 The HABDS shall be implemented to prevent a train on fire entering a tunnel.
- 5.4.2.6 The HABDS shall be designed according to EN 15437.
- 5.4.2.7 The HABDS shall be designed to monitor various types of axles and possess radiation immunity.
- 5.4.2.8 The HABDS shall be designed to monitor various types of axles and possess radiation immunity.
- 5.4.2.9 It will have the capability to acquire, at minimum, the following trainset parameters:
- Temperature of axle boxes,
 - Temperature of wheels treads/rim/brake disc,
 - Speed of a wheelset.
- 5.4.2.10 The HABDS shall be able to monitor all types of axles.

5.4.3 Derailment Detector System

- 5.4.3.1 The DDS sensors shall be installed at a regular interval on both side of the main track to stop a faulty train before it reaches a sensitive area on the main track (such as a viaduct, switch area... to be defined by the safety study)
- 5.4.3.2 DDS detectors shall be interfaced with the train control System and complex operation (rerouting of following and passing train) shall be applied in case of faulty train detected within a configurable reaction time



- 5.4.3.3 The DDS System shall send alarms to the OCC if one axle derailment is detected.
- 5.4.3.4 Detection of default by the Derailment Detection System shall result in automatic emergency stopping of the faulty trains
- 5.4.3.5 The TSCC Contractor shall develop an adequate general interface document
- 5.4.3.6 The DDS detection system should directly interact with the train control system to stop the faulty train
- 5.4.3.7 The DDS shall be able to monitor trainsets running at 220 mph.
- 5.4.3.8 The number of false alerts shall be minimized to 1 / 1000 maximum
- 5.4.3.9 DDS system shall be at least SIL 2

5.4.4 Broken Rail Detection System (BRDS)

- 5.4.4.1 The BRDS shall be able to identify if an abnormal rail parameter is detected.
- 5.4.4.2 The BRD System shall provide an alarm to the OCC in case BRDS identifies abnormal conditions
- 5.4.4.3 Different alarms shall be trigger at the OCC level for the various parameters of the rail detected
- 5.4.4.4 Detection of default by the BRD system shall result in automatic emergency stopping of all approaching trains in the concerned area
- 5.4.4.5 The TSCC Contractor may propose the fiber optic sensing solution for HDEWSs if the proposed solution meets all the requirements described in this technical specification.
- 5.4.4.6 The TSCC Contractor may propose an acoustic solution for broken rail detection if the proposed solution meets all the requirements described in this technical specification.
- 5.4.4.7 Both systems can be used in combination (optic fiber for open line and acoustic for switch machines area, to be defined by the safety study)
- 5.4.4.8 The area monitored by the BRDS shall be determined in accordance with the TSCC Contractor's design or the country's regulations
- 5.4.4.9 BRDS detectors shall be interfaced with the train control System and complex operation (rerouting of following and passing train) shall be applied in case of rail default detected within a configurable reaction time
- 5.4.4.10 For the generation, update or removal of BRDS-related operation stopped, an alert shall be triggered at the operator level
- 5.4.4.11 The number of false alerts shall be minimized to 1 / 1000 maximum
- 5.4.4.12 BRD system shall be at least SIL 2.

5.4.5 Rail Temperature Monitoring System (RTMS)

- 5.4.5.1 The temperature sensors' range shall be -60°C to +120°C (precision 3%)
- 5.4.5.2 The RTM sensor shall be installed in the immediate vicinity of the train track, eventually inside the rail core itself, with direct exposure to the sun if not embedded in the rail.
- 5.4.5.3 The sensor shall report rail temperature at a configurable frequency that should be chosen in accordance with speed of the variation of the natural phenomena.
- 5.4.5.4 The threshold of the rail temperature triggering a speed restriction will be selected specifically for track exposed to the sun to avoid completely the risk of derailment of the train.



- 5.4.5.5 Several thresholds associated with several speed restrictions shall be determined in accordance with the TSCC Contractor's designs, or the country's regulations to mitigate the risk without being too restrictive for the Authority's operating plan.
- 5.4.5.6 Trackside rail temperature detectors shall be interfaced with the train control System and temporary speed restrictions shall be applied in case of high rail temperature within a configurable reaction time.
- 5.4.5.7 For the generation, update or removal of rail temperature-related speed restriction, an alert shall be triggered at the operator level.
- 5.4.5.8 Trends analysis shall be possible.
- 5.4.6 Road Vehicle Detection System (RVDS) and derivative landslide/falling rock detection system**
 - 5.4.6.1 The RVDS shall provide warning at all overpasses against vehicle impact.
 - 5.4.6.2 The RVDS shall be able to detect any vehicle intrusion from overpasses, onto the CHSR tracks.
 - 5.4.6.3 When used as a landslide/falling rock detection system, The RVDS shall be able to detect any rock intrusion or landslide from overpasses, onto the CHSR tracks.
 - 5.4.6.4 Detection of intrusions shall result in automatic emergency stopping of approaching trains.
 - 5.4.6.5 The RVDS shall be able to transfer alarms and information to the Data Collector.
 - 5.4.6.6 The TSCC Contractor shall define, according to the CHSR operational needs, an alarm triggering, validation and response procedure.
 - 5.4.6.7 The TSCC Contractor shall cooperate with the Authority for the definition of alarms, protocols, and procedures.
 - 5.4.6.8 To prevent false positives, the TSCC Contractor shall establish a redundant detection system.
 - 5.4.6.9 Remote cancellation of alarms shall be possible from the OCC Including the possible involvement of onboard staff should risk analysis identify this need.
 - 5.4.6.10 The RVDS shall be interfaced with the train control System. Detection of intrusions shall result in emergency stopping of approaching trains.
 - 5.4.6.11 For the generation, update or removal of BRDS-related operation stopped, an alert shall be triggered at the operator level.
 - 5.4.6.12 The RVDS detection system should directly interact with the train control system to stop the approaching train
 - 5.4.6.13 The number of false alerts shall be minimized to 1 / 1000 maximum
 - 5.4.6.14 RVDS system should be SIL 4 and shall at least achieve SIL 2.
- 5.4.7 Meteorological Condition Detection System (MCDS): Wind**
 - 5.4.7.1 The TSCC Contractor shall provide Wind Detectors, as part of the MCDS.
 - 5.4.7.2 A study shall be made to identify the need for dedicated wind detection on exposed structures (bridges, viaducts, embankments, etc.) where high crosswinds would result in a threat to the safe operation of trains.
 - 5.4.7.3 The Trackside Wind detectors shall not be installed in the immediate vicinity of the track to avoid train shuffles, and shall not be installed near the ground level to avoid ground effect.



- 5.4.7.4 The sensor shall report wind speed at a configurable frequency that should be chosen in accordance with speed of the variation of the natural phenomena.
- 5.4.7.5 The threshold of the wind speed triggering a speed restriction will be selected specifically for every exposed structure to avoid completely the risk of derailment of the train.
- 5.4.7.6 Thresholds associated with speed restrictions shall be determined in accordance with TSCC Contractor's studies and/or the Federal and State regulations to mitigate the risk without being too restrictive for the Authority's operating plan.
- 5.4.7.7 Based on the study and the proposed solution for wind detection, the TSCC Contractor shall develop an adequate general interface document.
- 5.4.7.8 The Trackside Wind detectors shall be able to handle the measurement of the speed on range from zero to hundred miles an hour (5% precision), and direction from zero to 360° (precision 5°).
- 5.4.7.9 The Trackside Wind detectors shall have an integrity SIL2.
- 5.4.7.10 Trackside Wind detectors shall be interfaced with the train control System and temporary speed restrictions shall be applied in case of high wind within a configurable reaction time.
- 5.4.7.11 For the generation, update or removal of Wind-related speed restriction, an alert shall be triggered at the operator level.
- 5.4.7.12 The number of false alerts shall be minimized to 1 / 1000 maximum.

5.4.8 Meteorological Condition Detection System (MCDS): Rain

- 5.4.8.1 The TSCC Contractor shall provide Rain Detectors, as part of the MCDS.
- 5.4.8.2 A study shall be undertaken to identify the need for dedicated rain detection on exposed structures (bridges, viaducts, embankments, etc.) where heavy rain would result in a threat to the safe operation of trains.
- 5.4.8.3 The sensor shall report rainfall at a configurable frequency that should be chosen in accordance with speed of the variation of the natural phenomena.
- 5.4.8.4 The threshold of the rain quantity triggering a speed restriction will be selected specifically for every exposed structure to avoid completely the risk of derailment of the train.
- 5.4.8.5 Several thresholds associated with several speed restrictions shall be determined in accordance with study and/or the Federal and State regulations to mitigate the risk without being too restrictive for the Authority's operating plan.
- 5.4.8.6 Based on the study and the proposed solution for rain detection, the TSCC Contractor shall develop an adequate general interface document.
- 5.4.8.7 The rain detectors shall be able to handle the measurement of the rain quantity per hour on a range from zero to twenty inches (precision 5%) and rain quantity per day (24 hour) on a range from zero to sixty inches (precision 5%).
- 5.4.8.8 Trackside rain detectors shall be interfaced with the Operating Control Center and temporary speed restrictions shall be applied in case of heavy rain within a configurable reaction time.
- 5.4.8.9 For the generation, update or removal of rain-related speed restriction, an alert shall be triggered at the operator levels
- 5.4.8.10 The number of false alerts shall be minimized to 1 / 100 maximums

5.4.9 Meteorological Condition Detection System (MCDS) Flood



- 5.4.9.1 The TSCC Contractor shall provide Water flood Detectors, as part of the MCDS.
- 5.4.9.2 A study shall be made to identify the need for dedicated water flood detection on exposed structures (tunnel, platform, embankments, etc.) where water flood would result in a threat to the safe operation of trains.
- 5.4.9.3 The water flood detectors shall be installed in the immediate vicinity of the train track to prevent flood reaching the platform underlay or reaching the base of the rails or to cause any other damage.
- 5.4.9.4 The threshold of the water flood triggering a speed restriction will be selected specifically for every exposed structure to avoid completely the risk of derailment of the train.
- 5.4.9.5 Two thresholds associated with two speed restrictions shall be determined in accordance with study and/or the Federal and State regulations to mitigate the risk without being too restrictive for the Authority's operating plan.
- 5.4.9.6 Based on the study and the proposed solution for water flood, the TSCC Contractor shall develop an adequate general interface document.
- 5.4.9.7 The MCDS Flood detection system should directly interact with the train control system to stop approaching trains.
- 5.4.9.8 The water flood detectors shall have an integrity SIL2 whether they have or do not have moving parts.
- 5.4.9.9 Water flood detectors shall be interfaced with the train control system and temporary speed restrictions shall be applied in case of high wind within a configurable reaction time.
- 5.4.9.10 For the generation, update or removal of flood-related speed restriction, an alert shall be triggered at the operator level.
- 5.4.9.11 The number of false alerts shall be minimized to 1 / 1000 maximum.
- 5.4.9.12 The flood detection system should directly interact with the train control system to stop the train.

5.4.10 Meteorological Condition Detection System (MCDS): earthquake

- 5.4.10.1 The TSCC Contractor shall provide earthquake Detectors, as part of the MCDS.
- 5.4.10.2 A study shall be undertaken by the TSCC Contractor to identify the areas where earthquake detection is requested.
- 5.4.10.3 The Earthquake detectors shall not be installed in the immediate vicinity of the track to avoid train movement disturbing the measurements, and shall not be installed near any other source of vibration such as road, factory etc.
- 5.4.10.4 The detection of an earthquake shall trigger a speed restriction to avoid completely the risk of derailment of the train.
- 5.4.10.5 Based on the study and the proposed solution for earthquake detection, the TSCC Contractor shall develop an adequate general interface document.
- 5.4.10.6 The earthquake detectors shall be able to handle the measurement of the ground movement on range from zero to hundred gal (5% precision).
- 5.4.10.7 The earthquake detectors shall have an integrity of SIL2.
- 5.4.10.8 Earthquake detectors shall be interfaced with the Operating Control Center and temporary speed restrictions shall be applied in case of detection of an earthquake.



5.4.10.9 For the generation, update or removal of earthquake-related speed restriction or operation stopped, an alert shall be triggered at the operator level.

5.4.10.10 The number of false alerts shall be minimized to 1 / 1000 maximum.

5.5 Performance Requirements

5.5.1 Safety Requirements

5.5.1.1 The TSCC Contractor shall conduct safety studies in order:

- To monitor train health, meteorological events, and infrastructure conditions, the Authority must conduct a safety study to determine the types of sensors to be installed,
- To monitor train health, meteorological events, and infrastructure conditions, the Authority must conduct a safety study to determine the place of each type of sensors to be installed,
- The Authority needs to perform a safety analysis to establish the threshold that initiates actions on train circulation for each type of event, including monitoring train health, meteorological conditions, and infrastructure status,
- The Authority is required to carry out a safety assessment to identify the appropriate actions, such as imposing speed limits or halting the train, for each type of event, while monitoring train health, weather conditions, and infrastructure status.

5.5.1.2 Part C – Supplementary Technical Requirements – Technical Specifications (including this document). Terms, abbreviations, and definitions are specified in the Parts A, B, and C of the Contract. The HDEWS shall comply with the safety requirements defined in the safety studies organized by the Authority.

5.5.1.3 The Trainset Health Monitoring Equipment shall be designed, installed, and tested to ensure their correct functioning.

5.5.1.4 The infrastructure monitoring systems shall be designed, installed, and tested to ensure they function correctly.

5.5.1.5 The meteorological systems shall be designed, installed, and tested to ensure they function correctly.

5.5.2 RAM Requirements

5.5.2.1 The HDEWS shall comply with the RAM requirements defined in the Schedule 1.

5.5.2.2 The HDEWS shall ensure uninterrupted operation.

5.5.2.3 The HDEWS shall be designed and implemented to ensure geographical and hardware redundancy.

5.5.2.4 The HDEWS shall have field-proven reliability and intrinsic fault tolerance aligning with CHSR RAM objectives.

5.5.2.5 The whole HDEWS shall be designed to have optimum maintainability (quick replacement of faulty parts, equipment swap-out only) in each operating section of the main line.

5.5.2.6 The HDEWS shall be designed and implemented to ensure sufficient accessibility and maneuverability space for installation, testing, operation, inspection, maintenance, and repair.

5.5.2.7 Standard labelling and marking shall be applied for all HDEWS equipment according to GS1 Application Standard for the rail sector in a manner to be agreed with CHSR, which will be uniform across all systems.

5.5.2.8 The TSCC Contractor shall supply an obsolescence management plan to be communicated to the AMS system.



5.6 Security and Cybersecurity Requirements

- 5.6.1 The HDEWS design shall be in full compliance with cybersecurity controls specified in the CHSR Cybersecurity Technical Specification.
- 5.6.2 The HDEWS shall have a System Owner who is accountable for cybersecurity risk ownership and mitigation.
- 5.6.3 The HDEWS System Owner shall be responsible for ensuring that resources with appropriate expertise attend cybersecurity threat modelling and risk assessment activities to facilitate risk identification and mitigation strategies.
- 5.6.4 IP-based/digital based communications between HDEWS components, such as PLCs, RTUs, and sensors shall use cryptographic means of protection and authentication as outlined in the CHSR Cybersecurity Technical Specification to verify the integrity and authenticity of messages.
- 5.6.5 Information deemed confidential shall be stored in compliance with the information security requirements outlined in the CHSR Cybersecurity Technical Specification.
- 5.6.6 Interfaces identified between HDEWS and other internal or external systems must be co-engineered with the Cybersecurity Lead to ensure they comply with the cybersecurity objectives.



6 INTERFACES REQUIREMENTS

6.1 General Requirements

6.1.1 Interfaces are classified as below:

- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR contractors).
- External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors).
- Internal interfaces between systems within the TSCC scope.

6.1.2 The TSCC Contractor shall develop the FPS design considering the identified external interfaces and internal interfaces to ensure the required functionalities and performance described in this specification for FPS.

6.1.3 The TSCC Contractor shall assess the identified interfaces and, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.

6.1.4 The TSCC Contractor shall ensure the integration with all identified third party, external and internal interfaces.

6.2 Third Party Interfaces

6.2.1 The HDEWS system shall collect data from third-party systems such as:

- Weather services
- USGS (United States Geological Survey) ShakeAlert System

6.3 External Interfaces – facilities contractor

6.3.1 The TSCC Contractor shall install HDEWS equipment in the OCC and facilities being provided by the facilities contractor.

6.3.2 The TSCC Contractor shall provide to the facilities contractor:

- Equipment dimensions
- Equipment clearances requirements
- Equipment mounting and fixings requirements
- Cable routes/containment requirements
- Equipment loadings
- Installation and maintenance requirements
- Equipment heating loads
- Equipment cooling loads
- Equipment hydraulic requirements

6.3.3 To be provided by facilities contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:

- Room dimensions and layouts
- Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
- Room raised floor system
- Delivery access routes.
- Maintenance access routes

6.3.4 With regard the level 0 interface, the TSCC Contractor shall follow the process defined in the Authority Interface Management Plan and shall support the Authority in developing the requirements and a scope



split with related stakeholders. The TSCC Contractor shall execute the level 0 interfaces based on defined requirements and scope split.

6.4 Internal Interfaces for the HDEWS

6.4.1 Interface with Low Voltage Power System (LVPS)

- 6.4.1.1 The HDEWS shall have a redundant interface with the LVPS for the power supply of the related HDEWS equipment.

6.4.2 Interface with Digital Communications Network (DCN)

- 6.4.2.1 The HDEWS shall have a redundant interface with the DCN to ensure the related data transmission from the Data Collector to the OCC / BOCC. Data concerning alarms and status shall be prioritized over raw data transmitted to OCC HDEWS server.

6.4.3 Interface with Network Time System (NTS)

- 6.4.3.1 The HDEWS shall have redundant interface with the NTS for accurate current time synchronization.

6.4.4 Interface with Integrated Control and Supervision System

- 6.4.4.1 The HDEWS shall have a redundant interface with the ICSS system:
- 6.4.4.2 A graphical interface of the HDEWS shall be provided within the ICSS system.
- 6.4.4.3 The dedicated ICSS graphical interface shall enable monitoring and status provision of the HDEWS equipment.
- 6.4.4.4 The HDEWS shall at least provide the data to allow the ICSS to calculate and show the following information of each connected sensor:
- Status,
 - Failure codes.

6.4.5 Interface with Enterprise Asset Management System (EAMS)

- 6.4.5.1 The HDEWS System shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.

6.4.6 Interface with Interlocking

- 6.4.6.1 The HDEWS shall have a redundant interface with the IXL to have a safety response from the train control system in case of hot axle detection, high wind detection, and Road Vehicle intrusion detection. This interface needs to be specified and shall be with the Safety Integrity level SIL 2 (safety relay or safety communication network, to be defined).

6.4.7 Interface with Traffic Management System (TMS)

- 6.4.7.1 The HDEWS shall have a redundant interface with the TMS to send alarms from at least:
- HABDS,
 - DDS,
 - BRDS,
 - RTMS,
 - RVDS,
 - MCDS.



- 6.4.7.2 The HDEWS shall have an interface with the TMS to identify the train ID that is concerned by an alarm. For this specific purpose the TSCC Contractor may propose a different solution.
- 6.4.7.3 The HDEWS shall have a functional interface with the Point Heating System to receive data related to temperature, snow level, wind level, humidity.
- 6.4.7.4 The HDEWS shall interface with cybersecurity systems according to the Cybersecurity Technical Specifications.
- 6.4.8 **Interface with ETCS**
 - 6.4.8.1 RBC shall interface the alarms raised by the HDEWS detectors via direct interface, or TMS or CBI, depending on the outcome of the Hazard Analysis that shall be performed to define the level of mitigation required (e.g. immediate emergency stop order, confirmation or not by the controller before the mitigation is put in place, Maker board set to danger, application of TSR...)



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied shall conform to the requirements and test methods of the relevant standards and regulations as described in Reference Standards and Documents.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the designed life requirements.
- 7.1.3 The HDEWS equipment shall be complete with all parts and accessories or material which are useful for efficient operation of the HDEWS components. Such accessories and materials shall be deemed to be within the scope of this specification whether specifically mentioned or not.
- 7.1.4 The supply shall include all supporting structures, load bearing structures, fittings, embedded parts, auxiliary equipment, mechanical linkages, auxiliary circuits wiring necessary for their efficient operation. All such parts and accessories shall be deemed to be within the scope of this specification whether specifically mentioned or not.
- 7.1.5 The TSCC Contractor shall provide necessary fittings, supporting and load bearing structures for the installation of the related Modular Sensors.
- 7.1.6 The design of the supporting and load bearing structures shall comply with the relevant Eurocode (EN 1990, EN 1992, EN 1993 etc.).
- 7.1.7 The foundations shall be maintenance free all its lifetime.
- 7.1.8 The foundation design shall be subjected to ground investigation and structure load assessment; all foundation positions shall be confirmed after undertaking site surveys.
- 7.1.9 The foundations shall be sited to avoid underground utilities such as power cables, piping systems, IT and telecommunication systems and railway-related installations (e.g., sealing in the track embankment) where reasonably practicable or demanded by a railway restriction.
- 7.1.10 The structures, supports and other components made of steel shall be provided with corrosion protection. Corrosion protection shall be carried out in accordance with standards. The preferred solution for steel parts shall be hot-dip galvanization.

7.2 SW and HW Requirements

- 7.2.1 The HDEWS design shall be based on COTS, open architecture, and modular system architecture, with standard non-proprietary interfaces.
- 7.2.2 The TSCC Contractor's design for all central servers shall be on-premises, either physical, virtualized or cloud-base to ease systems evolution complying the requirement of Security and Cybersecurity Requirements.
- 7.2.3 All cabling for HDEWS shall be designed, supplied, installed, tested, and commissioned by the TSCC Contractor.
- 7.2.4 The HDEWS servers/controllers shall have redundant power supply.
- 7.2.5 All cable requirements must be classified according to the Construction Products Regulation (CPR) codification. Low toxicity, low smoke emission, low flammability, zero halogen fire retardant cable shall be used.

7.3 EMC Requirements

- 7.3.1 The EMC requirements are described in the Technical Specification – EMC and Grounding/Bonding.



8 TOLERANCES

Not applicable to the HDEWS



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 General requirements related to the TSCC Contractor Scope of Work are defined in Schedule 16.

9.2 Specific Requirements

9.2.1 The HDEWS scope of supply and delivery shall include (not limited to):

- All monitoring sensors with central and local servers.
- Workstations/HMIs.
- Controllers.
- Amplifiers (if needed).
- Cabling and connectors.
- Racks.
- Software architecture including full definition of protocols used.
- Management System.
- SW licenses.
- Supporting and load bearing structures, fittings, etc.
- Spare parts.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.



13 SUBMITTALS

13.1 General Requirements

13.1.1 The submittals required for the Interlocking system are defined in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the Contractor and related Suppliers, information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence HDEWS reliability, availability, and maintainability characteristics.



16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.



17 SPEED LIMITATION BASED ON METEOROLOGICAL CHANGE EXAMPLE

17.1 General description

The values provided in section 17.2 come from the Korean National High-Speed Network that makes use (among others) of 46 High Speed Train (18 cars, 300Kph) of French manufacturer Alstom model named KTX. The Korea HSL network initially makes use of French regulation with regards of detectors. Values provided here were used at least from 2004 to 2007 (and more) and come in this document as an example since it is the responsibility of the TSCC Contractor in agreement with the Authority to establish values for the CHSR network

17.2 Values (in metric system) provided as an example



Rail Temp.		Snow		Earthquake		Rain & Flood		Wind (coefficient applied)	
Over 45	After work, below 100 km/h, Until stabilization period, below 170 km/h	Rail surface is not seen	Below 30 km/h	Earthquake Yellow alarm (40 gal-65gal)	First Train Below 90 km/h	The rainfall for 24hours is over 140mm. Rainfall per hour is over 30mm.	Below 170 km/h	Wind Speed Below 30 m/sec	Systematic speed reduction based on wind speed
Over 50	Person in charge of installation should continuously monitor temperature detector. If needed, he or she should notify the person concerned.	Over 21 centimeter inside track	Below 130 km/h	Earthquake Red alarm (over 65gal)	Operation shall be Stopped	The rainfall for 24hours is over 150mm. Rainfall per hour is below 35mm.	Below 90 km/h	Wind Speed Over 30m/sec and Below 40m/sec	Below 170km/h
Over 55	Below 230 km/h	Over 14cm and under 21cm Inside track	Below 170 km/h			The rainfall for a day is over 150mm. Rainfall per hour is over 60mm.	Operation shall be stopped (The rainfall per hour in the overhead and bridge sections is over 70 mm).	Wind Speed Over 40m/sec and Below 45m/sec	Below 90km/h
Over 60	Below 70 km/h	Over 7cm and below 14cm	Below 230km/h			Gravel is scattered or the head of rail sank.	Operation shall be stopped.	Over 45m/sec	Operation is held or stopped.
Over 64	Operation shall be stopped.	The sound which snowball or ice splatters	Below 230 km/h			Gravel is not scattered// Water level is below the head of rail and over the rail tile pad.	Below 40 km/h		
		Reoccurrence	Below 170 km/h						



Schedule 5(h)

Integrated Control and Supervision System Specifications (ICSS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specification

SPEC-0012 – Integrated Control and Supervision System Specifications (ICSS)

Rev. 0.0

Authored:

A handwritten signature in black ink, appearing to read 'Harshal'.

Harshal Jadhav, Telecom System Lead

10/15/2025

Date

Checked:

A handwritten signature in black ink, appearing to read 'Thomas'.

Thomas Newey, Telecoms & SCADA Lead

10/15/2025

Date

Checked:

A handwritten signature in black ink, appearing to read 'Bruno'.

Bruno Comperat, Deputy Director of Rail Engineering

10/16/2025

Date

Approved:

A handwritten signature in blue ink, appearing to read 'Ryan Scott'.

Ryan Scott, Director of Rail Engineering

10/16/2025

Date

Released:

A handwritten signature in blue ink, appearing to read 'Amit Joshi'.

Amit Joshi, Configuration Manager

10/16/2025

Date



Document Revision History – ICSS Specifications**First Edition****September 2025**

Revision	Date	Revision Description
0.0	September 2025	First Edition



TABLE OF CONTENT

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION.....	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.1	GENERAL	6
2.2	DESIGN GUIDELINES.....	6
2.3	TSI	6
2.4	STANDARDS	6
2.5	OTHER DOCUMENTS	8
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	10
3.1	TERMS, DEFINITIONS AND ABBREVIATIONS	10
4	SYSTEM DESCRIPTION	11
4.1	PURPOSE OF THE ICSS	11
4.2	ICSS DEFINITION	11
4.3	ICSS OPERATIONAL CONTEXT	12
4.4	DESIGN LIFE	13
5	SYSTEM REQUIREMENTS.....	14
5.1	GENERAL REQUIREMENTS.....	14
5.2	ENVIRONMENTAL CONDITIONS REQUIREMENTS.....	14
5.3	OPERATIONAL REQUIREMENTS FOR ICSS	15
5.4	FUNCTIONAL REQUIREMENTS FOR ICSS	16
5.5	PERFORMANCE REQUIREMENTS FOR ICSS	31
5.6	CYBERSECURITY AND SECURITY REQUIREMENTS.....	32
6	INTERFACE REQUIREMENTS	35
6.1	GENERAL REQUIREMENTS.....	35
6.2	EXTERNAL INTERFACES – STATION CONTRACTOR.....	35
6.3	EXTERNAL INTERFACES - FACILITIES CONTRACTOR.....	36
6.4	INTERNAL INTERFACES	36
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS	38
7.1	GENERAL REQUIREMENTS.....	38
7.2	SOFTWARE AND HARDWARE REQUIREMENTS	38
7.3	EMC REQUIREMENTS.....	40
8	TOLERANCES	41
9	SCOPE OF SUPPLY AND DELIVERY	41
9.1	GENERAL REQUIREMENTS.....	41
9.2	SPECIFIC REQUIREMENTS FOR ICSS.....	41
10	MANUFACTURING.....	42
10.1	GENERAL REQUIREMENTS.....	42



11	INSTALLATION AND INTEGRATION.....	42
11.1	GENERAL REQUIREMENTS.....	42
12	TESTING & ACCEPTANCE	42
12.1	GENERAL REQUIREMENTS.....	42
12.2	SPECIFIC REQUIREMENTS FOR ICSS.....	42
13	SUBMITTALS.....	43
13.1	GENERAL REQUIREMENTS.....	43
13.2	SPECIFIC REQUIREMENTS FOR ICSS.....	43
14	QUALITY MANAGEMENT.....	43
14.1	GENERAL REQUIREMENTS.....	43
15	ADDITIONAL INFORMATION REQUESTED	43
15.1	GENERAL REQUIREMENTS.....	43
16	LOGISTICS	43
16.1	GENERAL REQUIREMENTS.....	43



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Integrated Control and Supervision System (ICSS).
- 1.1.2 The functional architecture of the ICSS is presented in Appendix A.
- 1.1.3 The requirements are formulated using the following words and their meanings:
- **"Shall"**: Indicates a mandatory requirement that must be strictly implemented; a waiver from a mandatory requirement is permissible only with approval of a design variance.
 - **"Should"**: Indicates a preferred course of action; a design variance is not required if it is not exercised.
 - **"Must"**: Indicates an obligation or a mandatory requirement.
 - **"May"**: Indicates a permissible course of action within the limits of the standards; a design variance is not required if it is not exercised.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines and specifications provided in this technical specification for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, training, operations and maintenance.

2.1.2 All generic standards to be used are provided in: Schedule 16.

2.2 Design Guidelines

2.2.1 The latest version of the following Design Guidelines shall be applied:

ID	Code	Title
[R1]	Design Criteria Manual	Chapter 5 – Safety and Security
[R2]	Design Criteria Manual	Chapter 12 – Communication Systems and Train Control
[R3]	AREMA Standards	Chapter 17 – High-Speed Rail Systems

TABLE 21 DESIGN GUIDELINES

2.3 TSI

2.3.1 There are no applicable TSIs for the Integrated Control and Supervision System (ICSS).

2.4 Standards

2.4.1 The TSCC Contractor shall fully consider and apply the following standards.

ID	Standard	Title
[R4]	EN 11205	Acoustics -- Noise emitted by machinery and equipment -- Engineering method for the determination of emission sound pressure levels in situ at the work station and at other specified positions using sound intensity
[R5]	EN 50121 series	Railway Applications – Electromagnetic Compatibility
[R6]	EN 50122 series	Railway applications - Fixed installations - Electrical safety, earthing and the return circuit
[R7]	EN 50124	Railway applications - Insulation coordination
[R8]	EN 50125	Railway applications - Environmental conditions for equipment
[R9]	EN 50126	Railway applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS)
[R10]	EN 50128	Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems
[R11]	EN 50129	Railway applications — Communication, signaling and processing systems — Safety related electronic systems for signaling
[R12]	EN 50159	Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems



ID	Standard	Title
[R13]	EN 50289-1-6	Communication cables - Specifications for test methods - Part 1-6: electrical test methods - Electromagnetic performance
[R14]	EN 61000-6 series	Electromagnetic compatibility (EMC) - generic standards
[R15]	EN 60947-4 et 2 series	Low-voltage switchgear and control gear
[R16]	EN 60269-2	Low-voltage fuses - Part 2: Supplementary requirements for fuses for use by authorized persons
[R17]	EN 62305	Protection against lightning
[R18]	EN 50164	Lightning Protection Components
[R19]	EN 50173 series	Information technology - Generic cabling systems
[R20]	EN 50174	Information technology - Cabling installation
[R21]	EN 50310	Application of equipotential bonding and earthing in buildings with information technology equipment
[R22]	EN 55024	Information technology equipment. Immunity characteristics. Limits and methods of measurement.
[R23]	EN 60297-3	Mechanical structures for electronic equipment - Dimensions of mechanical structures of the 482,6 mm (19 in) series - Part 3-100: basic dimensions of front panels, subracks, chassis, racks and cabinets
[R24]	EN 61034 series	Measurement of smoke density of cables burning under defined conditions
[R25]	EN 61508 series	Functional safety of electrical/electronic/programmable electronic safety-related systems
[R26]	EN/IEC 62682	Management of alarms systems for the process industries
[R27]	IEEE 1220	IEEE Standard for Application and Management of the Systems Engineering Process
[R28]	ISO/CEI 15288	Systems engineering - Systems life cycle processes
[R29]	EN 45011	General requirements for bodies operating product certification systems.
[R30]	EN 60038	CENELEC standard voltages
[R31]	ISO 9001	Quality management systems - Requirements
[R32]	ISO 9000	Quality management systems - Fundamentals and vocabulary
[R33]	ISO 9241	Ergonomics of Human-Computer Interaction
[R34]	ISO 11064 series	Ergonomic design of control centres
[R35]	IEC 60331	Tests for electric cables under fire conditions
[R36]	IEC 60364 series	Low-voltage electrical installations
[R37]	IEC 60068 series	Environmental testing
[R38]	IEC 62395	(Parts 1 & 2) Electrical resistance trace



ID	Standard	Title
[R39]	IEC 60870 -5	heating systems for industrial and commercial
[R40]	NFPA 130	applications
[R41]	IEC 62443	Industrial Control System security
[R42]	IEEE 802.1Q	Networking standard that supports virtual local area networking (VLANs) on an IEEE 802.3 Ethernet network
[R43]	IEEE 802.3	Standard for Ethernet networks
[R44]	IEEE 802.1P	The 802.1p method is a Quality of Service (QoS) process defined within the IEEE 802.1Q standard.
[R45]	ISA 112	SCADA standards
[R46]	IEC 61131	PLC standards
[R47]	EN 50125-3	Railway applications – Environmental conditions for equipment – Part 3: Equipment for signaling and telecommunications
[R48]	EN 12464-1	Light and lighting – Lighting of workplaces – Part 1: Indoor workplaces

TABLE 22 LIST OF APPLICABLE STANDARDS

2.5 Other Documents

2.5.1 The following documents shall be referred to:

ID	Document	Title
[R49]	Schedule 16	Scope of Work
[R50]	Schedule 3	Safety, Security and RAM Requirements
[R51]	Schedule 5	Wireless Communication Systems Technical Specification
[R52]	Schedule 5	Cybersecurity Technical Specification
[R53]	Schedule 5	Hazard Detection and Early Warning System Technical Specification
[R54]	Schedule 5	Fire Protection System Technical Specification
[R55]	Schedule 5	Enterprise Asset Management System Technical Specification
[R56]	Schedule 5	Non-Traction Power Supply Technical Specification
[R57]	Schedule 5	Operation Center Arrangement Display drawings
[R58]	Schedule 5	Telephony System Technical Specification
[R59]	Schedule 5	Public Address and Customer Information System Technical Specification
[R60]	Schedule 5	Network Timing Systems Technical Specification
[R61]	Schedule 5	CCTV System Technical Specification
[R62]	Schedule 5	Electronic Access Control Systems Technical Specification
[R63]	Schedule 5	Digital Communication Network Technical Specification



[R64]	Schedule 5	Fiber Optical Cable Technical Specification

TABLE 23 OTHER DOCUMENTS

3 TERMS, DEFINITIONS, AND ABBREVIATIONS

3.1 Terms, Definitions and Abbreviations

3.1.1 All the terms, definitions, and abbreviations are provided in Schedule 5(t) SPEC-0024 – Glossary of Terms, Abbreviations and Definitions.

3.1.2 Below are a few ICSS-specific definitions used in this specification.

- ICSS HMI: The ICSS HMI refers to the graphical interface through which operators interact with the ICSS. It provides real-time visualization of system status, alarms, events, and control functions in a user-friendly and intuitive format, enabling effective monitoring and control of all integrated subsystems.
- ICSS Workstation: The ICSS Workstation is a computer terminal equipped with all necessary peripherals required to deliver the functionality of sub-systems integrated into the ICSS via ICSS HMI.
- LOTO: Lockout-Tagout is a control-inhibit applied to equipment to disable control during unsafe conditions or maintenance works. Removal of a LOTO requires authorization.
- Control: An operator command to initiate a change of state of in controlled equipment or a change of behavior in a controlled system.



4 SYSTEM DESCRIPTION

4.1 Purpose of the ICSS

- 4.1.1 The purpose of the Integrated Control and Supervision System (ICSS) is to monitor and control the California High-Speed Rail System. It is designed to assist operational personnel in closely overseeing critical railroad systems and promptly responding to any disruptions, ensuring that transportation services remain uninterrupted.

4.2 ICSS Definition

- 4.2.1 The ICSS shall provide integrated monitoring and control functions to facilitate the real-time overall control and supervision of the operation and maintenance of the parts of the CHSR System.

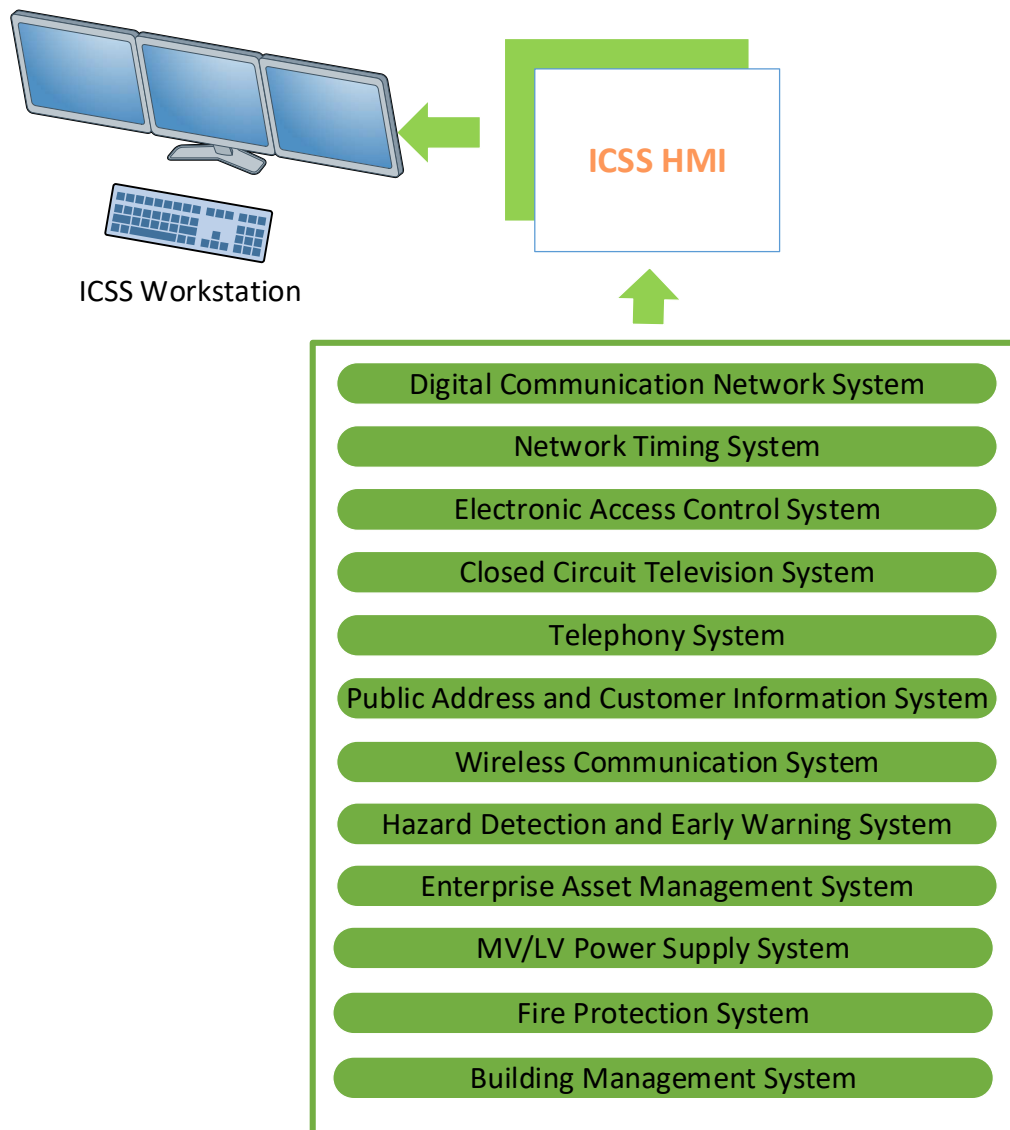


FIGURE 4. ICSS HMI ARCHITECTURE EXAMPLE**4.3 ICSS Operational Context**

- 4.3.1 The mission of the ICSS is to facilitate full and seamless control and/or monitoring of sub-systems, plant and equipment throughout the California High-Speed Rail System.
- 4.3.2 The ICSS shall be used operationally by various user groups, from various locations, to support high-speed rail operations.
- 4.3.3 The ICSS shall support a diverse set of operational use groups including, but not limited to:
- Train Controllers / Dispatchers
 - OCC Supervisors / Duty Managers / Operations Managers
 - Station Controllers / Station Masters
 - Incident Controllers / Emergency Response Coordinators
 - Maintenance Controllers
 - Train Control & Telecoms Technicians
 - Civil / Building Maintenance Personnel
 - Network / IT Administrators
 - Fire Protection System Operator
 - Security / CCTV Operators
 - Asset Managers
 - Training Supervisors
- 4.3.4 The ICSS HMI (Human Machine Interface) shall be the primary method of operator control for the systems where operational control is required.
- 4.3.5 The ICSS HMI shall, as a minimum, provide all normal operator functions that are available within each of the controlled systems.
- 4.3.6 The ICSS HMI shall provide all necessary operator functionalities to enable full operation of the interfaced sub-systems such that, during business-as-usual rail service operations, the operator shall not be required to use the interfaced sub-systems' equipment directly.
- 4.3.7 The ICSS system shall interface to the following systems as a minimum, to provide required alarm and status monitoring and/or operational control functionality.

No.	System	Alarm and Status Information	Operational Control
1	Digital Communication Network	Yes	No
2	Network Timing System	Yes	No
3	Electronic Access Control System	Yes	Yes
4	Closed Circuit Television System	Yes	Yes
5	Telephony System	Yes	Yes
6	Public Address and Customer Information System	Yes	Yes
7	Wireless Communication System	Yes	No
8	Hazard Detection and Early Warning System	Yes	No
9	Enterprise Asset Management System	Yes	No
10	MV/LV Power Supply System	Yes	Yes
11	Fire Protection System	Yes	No



12	Building Management System (Stations, Facilities, Substations, and Shelters)	Yes	Yes

TABLE 24 ICSS INTEGRATED SUB-SYSTEMS.

- 4.3.8 Communication interfaces shall be provided to all systems and equipment via the Digital Communication Network (DCN) for the transfer of event and alarm data, and allow the ICSS to have monitoring and control functionalities over the connected system.
- 4.3.9 In addition to the control and monitoring of assets, the ICSS platform shall integrate the HMI functionality required for the day-to-day operation of each interfaced system, including but not limited to functions defined in Section 5.4 of this document.
- 4.3.10 All sub-system statuses and alarms having the potential to impact on a sub-system's functionality, operation, and availability shall be provided to the ICSS.
- 4.3.11 The ICSS shall perform alarm triage, including normalization, deduplication, correlation, and suppression, and shall compute a service-impact-based priority so that the operator is alerted to the highest-priority incident.
- 4.3.12 All information required to fulfil a subsystem's operational tasks shall be available on the ICSS HMI.
- 4.3.13 The ICSS shall disburse sub-system statuses and alarms for all interfaced sub-systems to the Enterprise Asset Management System for data collection, maintenance programming, and record.

4.4 Design Life

- 4.4.1 The TSCC Contractor shall design and implement the ICSS for a design life of 30 years.
- 4.4.2 The design life requirements of the ICSS shall allow for the pertinent evolution and technological change of the ICSS throughout its life to ensure it remains fit for purpose.
- 4.4.3 The TSCC Contractor shall ensure that ICSS components with shorter design lifespans and software shall be managed by scheduled technology refresh strategies and spares management plans.
- 4.4.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce ICSS components (with equal or compatible technical specifications) for the entire design life required.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

- 5.1.1 The ICSS shall be designed in accordance with the requirements described in this specification.
- 5.1.2 The TSCC Contractor shall determine and supply all necessary ICSS equipment required to support the system functionality and interfaces at the following locations:
- Operation Control Center.
 - Stations.
 - Depots.
 - Train Care Facilities.
 - Workshops and Maintenance Facilities.
 - Substations.
 - Wayside locations and Shelters.
 - any other locations necessary to support the operations and maintenance of the CHSR System.
- 5.1.3 The ICSS shall be supplied with redundant core equipment and with necessary hardware and software at the OCC to meet the functional and performance requirements defined in this specification.
- 5.1.4 Each ICSS workstation shall be a multi-screen, audio-enabled configuration for operators to control and monitor various connected systems utilizing a common display format.
- 5.1.5 The ICSS workstations shall be located at all control positions as specified in 5.1.2 of this document.
- 5.1.6 The TSCC Contractor shall provide printing facilities at all locations necessary to support the operations and maintenance of the CHSR System, subject to the Authority's approval.
- 5.1.7 The TSCC Contractor shall provide printing facilities in all control rooms, printer rooms, maintenance rooms, and other rooms equipped with ICSS workstations supplied by the TSCC Contractor throughout the CHSR System.
- 5.1.8 The printers shall print both black and white and color information in A4 and A3 formats.
- 5.1.9 The printers for control rooms and printer rooms shall be multi-functional laser devices.

5.2 Environmental Conditions Requirements

- 5.2.1 The TSCC Contractor's ICSS design shall be appropriate for, and resilient to, the local environmental and climatic conditions at each installation site.
- 5.2.2 The ICSS equipment shall be designed for operation in an indoor office-like environment with HVAC, clean power supply, and dust control.



- 5.2.3 The ICSS equipment shall operate within the following environmental conditions:
- Temperature (operational): +5 °C to +40 °C
 - Temperature (storage/transport): –10 °C to +55 °C
 - Relative Humidity: 5% to 85% non-condensing
 - Air Pressure: 86 kPa to 106 kPa (up to 1000 m altitude)
 - Pollution Level: IEC 60664-1 Pollution Degree 2 (office environment)
- 5.2.4 The ICSS equipment shall not be subject to excessive vibration or shock, except for normal levels associated with office furniture and equipment movement.
- 5.2.5 The ICSS equipment shall be designed to operate without degradation of performance under normal office acoustic and lighting conditions.
- 5.2.6 The ICSS equipment shall comply with the climatic and environmental classification for indoor stationary equipment as defined in EN 50125-3.
- 5.2.7 The ICSS workstation areas shall be provided with suitable lighting levels (minimum 300–500 lux at desk level, glare-free) to ensure clear visibility of displays, operator controls, and alarm indicators, in compliance with EN 12464-1.
- 5.2.8 ICSS displays and operator interfaces shall remain legible under both normal and emergency lighting conditions, ensuring continued operational usability during power outages or degraded lighting scenarios.

5.3 Operational Requirements for ICSS

- 5.3.1 The TSCC Contractor's ICSS design shall ensure compliance with the California HSR planned operations and shall allow the operation and maintenance of the main line and related local facilities as per the Concept of Operations.
- 5.3.2 The ICSS shall monitor and control all interfaced system equipment necessary to allow effective management of the CHSR System.
- 5.3.3 ICSS shall serve as the platform for OCC operators to perform real-time monitoring and operational control of system equipment. All maintenance activities and detailed diagnostic functions shall remain the responsibility of the dedicated management systems provided with each respective subsystem.
- 5.3.4 The ICSS application shall, as a minimum, provide all operator functions available within each of the interfaced systems listed in Section 5.4 and elsewhere within the specification required to achieve day-to-day operation.
- 5.3.5 The ICSS shall perform controls over other systems determined and defined as part of a systems integration process, and as agreed with the Authority.
- 5.3.6 The ICSS HMI shall undergo an ergonomic design approach in line with ISO 11064.
- 5.3.7 The ICSS HMI shall present system status through graphical displays, alarms, trends, and reports in an intuitive and user-friendly format.
- 5.3.8 The ICSS shall allow multi-level access based on operator roles and responsibilities.



5.4 Functional Requirements for ICSS

5.4.1 General Overview of Function

- 5.4.1.1 All ICSS system equipment and software shall be proven in use in a similar railroad environment and be able to provide a demonstrably stable and reliable platform.
- 5.4.1.2 The TSCC Contractor shall provide ICSS RTUs/PLCs (Remote Terminal Units/Programmable Logic Controllers) at all locations containing interfacing systems or equipment that do not have a DCN connection for monitoring and/or control by the ICSS.
- 5.4.1.3 The TSCC Contractor shall liaise with all station and facilities contractors to ensure that all interfaces and data requirements are captured and managed to ensure successful integration of the ICSS.
- 5.4.1.4 The ICSS HMI shall, as a minimum, provide all operator functions available within each of the interfaced systems required to achieve day-to-day operation.
- 5.4.1.5 Any subsystem functionality required by the operator shall be incorporated in the ICSS such that the presentation of the functions and features is consistent across the ICSS HMI.
- 5.4.1.6 The TSCC Contractor shall ensure liaison with all station and facility contractors and the Authority to determine control functionality detail across all connected systems.
- 5.4.1.7 The ICSS shall be designed to ensure that the total failure of the ICSS at any single location, including full loss of the ICSS within the OCC, shall not affect the ability to perform ICSS control and monitoring over the rest of the systems or CHSR System.
- 5.4.1.8 The ICSS shall be configured such that no single point of failure can cause failure of the monitoring and control functions of the System at its workstations.

5.4.2 HMI Functionality

- 5.4.2.1 The ICSS workstations shall be provided with several monitors that work as one desktop area.
- 5.4.2.2 The desktop area shall be able to be subdivided into split screens in order to simultaneously display multiple graphical displays as required by the operator. Split screens shall be resizable by the operator for optimal use of the desktop area.
- 5.4.2.3 The ICSS HMI design for visual displays and operator interaction, including video feed interaction and audio interface functionality, shall be in accordance with the ergonomic and human factors.
- 5.4.2.4 All ICSS functionality and level of control and authority available at any given workstation shall be determined and/or limited by the operator's login profile utilizing Role Based Access Controls.
- 5.4.2.5 The level of control and authority of individual ICSS operator profiles shall be pre-defined by the system administrator and correspond to the control levels as per the CHSR Concept of Operations.
- 5.4.2.6 The system administrator shall have the authority required to manage and configure all operator profiles.



- 5.4.2.7 The HMI functionality for the ICSS shall allow full control over and access to all ICSS functionality and data. This shall include, but not be limited to:
- Controls.
 - Event and alarm management and functionality.
 - Automation/scheduling functionality.
 - Printing.
 - Database and Views configuration and management.
 - Access authority management.
 - Backup and archiving management.
 - Control inhibition.
 - Lockout/Tagout (LOTO).
 - Alarm inhibition.
 - Object state forcing.
 - Software functions available within each of the sub-systems (as required to achieve day-to-day operation).
- 5.4.2.8 The HMI shall allow the operator to apply a LOTO procedure to any controlled equipment.
- 5.4.2.9 The HMI shall display an indication of the applied LOTO on the corresponding equipment symbol.
- 5.4.2.10 The removal of LOTO shall be performed through an additional confirmation procedure to be approved by the Authority during detailed design.
- 5.4.2.11 All tagged, LOTO, and inhibited equipment shall be listed in an operator navigable view, with filtering capabilities.
- 5.4.2.12 A test facility shall be provided to enable control outputs to be exercised for a dummy circuit breaker at any selected RTU/PLC.
- 5.4.2.13 The TSCC Contractor shall undertake all necessary software development in order to integrate the ICSS and sub-system functionality, as required by the Authority, into the ICSS Platform. These shall include, but not be limited to:
- Drivers.
 - SDK (Software Development Kit).
 - API (Application Programming Interface).
 - Database integration.
 - GUI (Graphical User Interface) integration.
 - Peripheral integration.
- 5.4.3 Graphical Display**
- 5.4.3.1 The ICSS HMI Graphical User Interface shall provide a readily navigable series of display pages to enable efficient operator usage of the ICSS connected systems, to enable efficient control and monitoring of the CHSR System.
- 5.4.3.2 These display pages shall include, but not be limited to:
- Geographical location dynamic displays showing the site layout or train layout, in plan view and elevation, onto which the location of each item of monitored equipment is to be



superimposed, along with the associated equipment description and identification numbers. The geographical coordinates shall be included in this view, if applicable.

- Coordinated plan views representing all systems in a respective location.
- Sub-system views.
- Event/status/health and alarm lists.
- Dynamic graphical displays.
- Dynamic symbols.
- Equipment tags.
- Executive summary of the CHSR System status for a quick display of key data.
- Synoptic and schematic views of all controlled and monitored systems.
- Help pages.

- 5.4.3.3 It shall be possible to filter coordinated plan views for symbols pertaining to selected systems and equipment types.
- 5.4.3.4 Display pages and symbol libraries shall be submitted to the Authority for review and approval.
- 5.4.3.5 Access to all functions shall be quick, and “hot spots” shall be used as gateways between functions and/or views.
- 5.4.3.6 Monitored points shall be dynamically presented through appropriate symbols and analogue displays.
- 5.4.3.7 The ICSS workstation display icons, graphic displays, and pictorial representations shall be harmonized across all sub-systems integrated into the ICSS.
- 5.4.3.8 The state of a displayed symbol shall always reflect the real-time field status and shall highlight, by means of a change in color and an alarm, if the equipment has “lost communication” with the ICSS.
- 5.4.3.9 The sound file and volume for audio alerts shall be configurable by the operator.
- 5.4.3.10 The user interface shall feature simple point and click actions that minimize the use of the keyboard.
- 5.4.3.11 The user interface shall be designed and developed so as to provide a consistent look and feel to the operator for all functionality within the ICSS, as defined in ISO 11064-5.

5.4.4 DCN Monitoring Functionalities

- 5.4.4.1 The functionality integrated into ICSS HMI shall allow monitoring of the DCN system, refer to STS Digital Communication Network.
- 5.4.4.2 The ICSS shall be able to gather information from the DCN system for equipment diagnostics in the CHSR System.
- 5.4.4.3 The ICSS HMI shall display:
- The DCN equipment description, identification, and equipment label in each location.
 - Operational state of the DCN equipment in each location.
- 5.4.4.4 The ICSS HMI shall provide:
- Hierarchical view of the network map.



- Network topology and logical connections between the various levels of the hierarchy.
- Function for equipment identification.
- Indication of faulty DCN equipment or system faults.

5.4.5 NTS Monitoring Functionalities

- 5.4.5.1 The functionality integrated into ICSS HMI shall allow monitoring of the NTS system, refer to STS Network Timing System.
- 5.4.5.2 The ICSS shall be able to gather information from the NTS for equipment diagnostics in the CHSR System.
- 5.4.5.3 The ICSS HMI shall display:
- The NTS equipment description, identification, and equipment label in each location.
 - Operational state of the NTS equipment in each location.
- 5.4.5.4 The ICSS HMI shall provide:
- Function for equipment identification.
 - Indication of faulty NTS equipment or system faults.

5.4.6 EACS Operation and Monitoring Functionalities

- 5.4.6.1 The functionality integrated into ICSS HMI shall allow control and monitoring of the EACS system, refer to STS Electronic Access Control System.
- 5.4.6.2 The ICSS shall be able to gather information from the EACS for equipment diagnostics in the CHSR System.
- 5.4.6.3 The ICSS HMI shall display:
- The EACS equipment description, identification, and equipment label in each location.
 - Operational state of the EACS equipment in each location.
- 5.4.6.4 The ICSS HMI shall provide:
- Function for equipment identification.
 - Indication of faulty EACS equipment or system faults.
- 5.4.6.5 The ICSS shall be able to exchange information with EACS equipment for:
- Intrusion alarm notifications on the ICSS HMI.
 - Door management (opening/closing/automatic camera switching) on the ICSS HMI.
- 5.4.6.6 On the occurrence of an Intruder Detection or Access Control security alarm, the ICSS Workstation operator at the relevant Control Room shall be alerted to the location of the alarm, and the nearest CCTV shall be triggered to display the real-time image.

5.4.7 CCTV Operation and Monitoring Functionalities

- 5.4.7.1 The functionality integrated into ICSS HMI shall allow control and monitoring of the CCTV system, refer to Schedule 5(k) Closed Circuit Television System.
- 5.4.7.2 The ICSS shall be able to gather information from the CCTV system for equipment diagnostics in the CHSR System.



- 5.4.7.3 The ICSS HMI shall display:
- The CCTV equipment description, identification, and equipment label in each location.
 - Operational state of the CCTV equipment in each location.
- 5.4.7.4 It shall be possible to view live video streams and pre-recorded video across the CHSR System, regardless of geographical location, from any ICSS workstation.
- 5.4.7.5 The number of tiles (each displaying an individual camera feed) per display screen at each ICSS HMI shall be quantified during the detailed design for the Authority's approval.
- 5.4.7.6 The ICSS HMI shall work in conjunction with a keyboard and pointing devices for selecting the camera and system icons so as to provide the interaction between the operator and the CCTV system for picture selection, camera control, and fault information.
- 5.4.7.7 The ICSS HMI shall also work in conjunction with an integrated joystick for the control of PTZ cameras.
- 5.4.7.8 The ICSS HMI shall, as a minimum, provide the following fully programmable functions listed below. Available functionality shall be dependent on the operator profile:
- Equipment identification.
 - Indication of faulty CCTV equipment or system faults.
 - Pan, tilt, and zoom control, where appropriate.
 - Selection of each camera to be displayed.
 - Automatic panning on a group or individual basis.
 - Reprogramming and auto-sequence of camera images.
 - Manual control of Network Video Recorder functions, such as playback of recordings.
 - Manual selection by the Operator for any single video image or a combination of video images for display simultaneously.
 - Automatic selection in accordance with a pre-set configuration in the event of an alarmed condition, such as the CCTV images in the event of an intrusion detection alarm.
 - Manual selection by the Operator of any sequence of camera images with each image displayed in time sequence with a variable dwell time pre-set by the Operator.
 - Monitoring and annunciation of CCTV system alarms.
 - Operator to create/manage layout or tiles.
- 5.4.7.9 The ICSS shall conform to ONVIF (Open Network Video Interface Forum) to ensure compatibility with future updates in camera firmware and the addition of new cameras conforming to ONVIF.
- 5.4.7.10 The ICSS HMI shall automatically project onto a designated tile the real-time image associated with an alarm trigger and initiate alarm-triggered recording, for the following scenarios as a minimum:
- Fire detection.
 - Intrusion detection (using CCTV video analytics).
 - Intrusion detection (using EACS).
 - Passenger Help Point call.
 - Any other condition requiring immediate operator attention.

5.4.8 Telephony Operation and Monitoring Functionalities

- 5.4.8.1 The ICSS shall allow industry-standard telephony operator functionalities via the ICSS HMI.



- 5.4.8.2 The functionality integrated into ICSS HMI shall allow control and monitoring of the Telephony system to allow full compliance with the Telephony system requirements, refer to STS Telephony System. This shall include, but not be limited to:
- Monitoring and annunciation of Telephones and system alarms.
 - Full control of the Telephony system to enable all normal and emergency call handling functionalities.
- 5.4.8.3 Call handling shall include, as a minimum, the following features with visual and audible prompts provided to the operator at the Control Room ICSS HMI, as appropriate to the call function to be processed:
- Call queuing in order of call arrival.
 - Call prioritization for emergency services and user-defined requirements.
 - Intrusion, standard, private, night service, and manager/secretary call facilities.
 - Incoming call answering, outgoing call, conference call.
 - Call Hold and Call Park.
 - Call Terminations.
 - Call back and call forward.
 - Call Transfer to the recipient via the external systems accessible to the Telephony system, including the PSTN, the Administrative Telephone Network.
 - Display of each user's telephone status (availability).
 - Display of Call Line Identity.
 - Display and scrolling through the telephone directory.
- 5.4.8.4 It shall be possible to make and receive outgoing and incoming calls, route calls based on the selection of a destination by entering an extension number.
- 5.4.8.5 It shall be possible to handle various forms of number dialing, including short-code and preconfigured single-button dialing.
- 5.4.8.6 The ICSS shall be able to gather information from the Telephony system for equipment diagnostics in the CHSR System.
- 5.4.8.7 The ICSS HMI shall display:
- The Telephony equipment description, identification, and equipment label in each location.
 - Operational state of the Telephony equipment in each location.
- 5.4.8.8 The ICSS shall allow Operators to switch between waiting calls by holding an ongoing call and taking another call.
- 5.4.8.9 The ICSS shall provide the function for telephony equipment identification on the ICSS HMI.
- 5.4.8.10 The ICSS HMI shall notify the Operators that a call is being made from a specific location, including manual-dial telephones, PHPs (Passenger Help Points), and auto-dial telephones.
- 5.4.8.11 The ICSS shall be able to send commands to the PHPs, thereby allowing discrete ambient listening at the station.
- 5.4.8.12 When the caller presses the call button at the PHPs or lifts up the auto-dial telephone, a notification /ring tone shall be sent to a hunting group, and the associated CCTV camera stream (from the nearby camera) is automatically displayed on ICSS HMI.



5.4.9 PACIS Operation and Monitoring Functionalities

- 5.4.9.1 The functionality integrated into ICSS HMI shall allow control and monitoring of the PACIS, refer to STS Public Address and Customer Information System.
- 5.4.9.2 The ICSS shall be able to gather information from the PACIS for equipment diagnostics in the CHSR System.
- 5.4.9.3 The ICSS HMI shall display:
- The PACIS equipment description, identification, and equipment label in each location.
 - Operational state of the PACIS equipment in each location.
- 5.4.9.4 The ICSS HMI shall, as a minimum, provide the following functions listed below for the Public Address System. Available functionality shall be dependent on the operator profile:
- Equipment identification.
 - Indication of faulty PA equipment or system faults.
 - Operator to make direct live announcements to one or several zones/stations (group selection).
 - Operator to initiate automatic digitally pre-recorded announcements at once to one or several zones/stations (group selection).
 - Creation, modification, and deletion of pre-recorded messages.
 - Selection and broadcast of priority pre-recorded messages.
 - Broadcast pre-recorded announcements automatically repeated in a cyclical sequence.
 - Capability to enable or disable broadcast functionality in order to activate/deactivate PA broadcast for the selected zone.
 - Manage one zone and/or multiple zones based on Operator selection.
- 5.4.9.5 The ICSS HMI shall, as a minimum, provide the following functions listed below for the Customer Information System. Available functionality shall be dependent on the operator profile:
- Equipment identification.
 - Indication of faulty CIS equipment or system faults.
 - Operator to send live or pre-defined visual messages on displays.
 - Selection of an individual, a group, or all the PIDs in one location or in all the locations.
 - Operator to type instant messages.

5.4.10 WCS Monitoring Functionalities

- 5.4.10.1 The functionality integrated into ICSS HMI shall allow monitoring of the WCS, refer to Schedule 5(r) Wireless Communication System.
- 5.4.10.2 The ICSS shall be able to gather information from the WCS for equipment diagnostics in the CHSR System.
- 5.4.10.3 The ICSS HMI shall display:
- The WCS equipment description, identification, and equipment label in each location.
 - Operational state of the WCS equipment in each location.
- 5.4.10.4 The ICSS HMI shall provide:
- Function for equipment identification.
 - Indication of faulty WCS equipment or system faults.



5.4.11 HDEWS Monitoring Functionalities

- 5.4.11.1 The functionality integrated into ICSS HMI shall allow monitoring of the HDEWS, refer to Schedule (g) Hazard Detection and Early Warning System.
- 5.4.11.2 The ICSS shall be able to gather information from the HDEWS for equipment diagnostics in the CHSR System.
- 5.4.11.3 The ICSS HMI shall display:
 - The HDEWS equipment description, identification, and equipment label in each location.
 - Operational state of the HDEWS equipment in each location.
- 5.4.11.4 The ICSS HMI shall provide:
 - Function for equipment identification.
 - Indication of faulty HDEWS equipment or system faults.

5.4.12 EAMS Monitoring Functionalities

- 5.4.12.1 The functionality integrated into ICSS HMI shall allow monitoring of the EAMS, refer to Schedule 5(d) Enterprise Asset Management System.
- 5.4.12.2 The ICSS shall be able to gather information from the EAMS for equipment diagnostics in the CHSR System.
- 5.4.12.3 The ICSS HMI shall display:
 - The EAMS equipment description, identification, and equipment label in each location.
 - Operational state of the EAMS equipment in each location.
- 5.4.12.4 The ICSS HMI shall provide:
 - Function for equipment identification.
 - Indication of faulty EAMS equipment or system faults.
- 5.4.12.5 The ICSS shall send alarms, events, and status data having a maintenance implication to the EAMS for all interfaced systems. The alarm and status information shall be transmitted by the ICSS to the EAMS upon a change of state.
- 5.4.12.6 Associated events or fault alarms intended to automatically trigger an action within the EAMS (e.g., generation of a notification) shall be identified on the I/O Lists provided to EAMS, specifying the action required. These shall be coordinated with the station and facility contractors and proposed for the Authority's review and approval during the design stage.
- 5.4.12.7 For alarms and events sent to the EAMS, the asset numbering and alarm tag identification shall also be consistent with the numbering implemented in the EAMS database.
- 5.4.12.8 The addition, modification, and removal of assets and alarms to be sent to the EAMS shall be carried out by the ICSS administrator by means of a user-friendly Graphical User Interface in the ICSS, and verifiable on the EAMS Graphical User Interface. All configuration changes shall be logged in both systems.

5.4.13 Medium/Low-Voltage Power Supply Operation and Monitoring Functionalities



- 5.4.13.1 The functionality integrated into ICSS HMI shall allow control and monitoring of the MV+ LV PS, refer to Schedule 5(j) Medium Voltage and Low Voltage Power Supply Systems.
- 5.4.13.2 The ICSS shall be able to gather information from the MV+LV PS for equipment diagnostics in the CHSR System.
- 5.4.13.3 The ICSS HMI shall display:
- The MV+ LV PS equipment description, identification, and equipment label in each location
 - Operational state of the MV+ LV PS equipment in each location.
- 5.4.13.4 The ICSS shall, at least, monitor the following MV+LV PS equipment:
- MV switchgear (if available)
 - LV switchgear.
 - Transformers.
 - UPS.
 - Battery.
 - Generator.
 - Local renewable energy source (if available)
 - Inverter.
 - Rectifier.
 - Metering device.
- 5.4.13.5 The ICSS HMI shall, as a minimum, provide the following functions listed below for the MV+LV PS. Available functionality shall be dependent on the operator profile:
- Equipment identification.
 - Indication of faulty MV+LV PS equipment or system faults.
 - Real-time monitoring of equipment operational status (ON/OFF, available, standby, unknown).
 - Display of electrical parameters (voltage, current, frequency, load, power factor, etc.).
 - Alarm annunciation and categorization (critical, major, minor).
 - Event logging and time-stamped fault records.
 - Control commands where authorized (start/stop, reset, changeover, etc.).
 - Indication of supply source status (normal mains, UPS, generator, battery backup).
 - Trend monitoring of key parameters for performance and predictive maintenance.
 - System interlocks and protection status display.
 - Remote acknowledgement and clearance of alarms (based on operator profile).
 - Graphical single-line diagram view of power system topology and switching status.
 - Redundancy and failover status of MV+LV PS/UPS systems.
 - Reporting function (historical data, alarms, energy consumption).
- 5.4.13.6 The ICSS shall, at least, provide switching commands for the following MV+ LV PS equipment:
- MV switchgear (if available)
 - LV switchgear
- 5.4.13.7 The ICSS shall, at least, provide testing commands for the following MV+ LV PS equipment:
- UPS
 - Battery
 - Energy generation equipment



- 5.4.13.8 The ICSS shall retrieve timestamped measurement data from the MV+ LV PS system at least for:
- Commercial metering (Distributed System Operator interface)
 - Metering MV+ LV PS systems parameters at MV and LV levels
 - Metering of future equipment
- 5.4.13.9 The ICSS shall ensure that at any one time only one operator may select and control one control output circuit or a group of output circuits.
- 5.4.13.10 The ICSS to MV+ LV PS communications protocol shall be capable of supporting secure select and execute type commands, time synchronization from the host, and time-tagged event-based reporting. The protocol shall comply with the requirements of IEC 60870-5-104.
- 5.4.13.11 The MV+ LV PS digital inputs shall be time tagged at source (i.e., within the MV+ LV PS IED/RTU/PLC) to a resolution of 1ms. This time tag will be transmitted with the event to the ICSS.
- 5.4.14 BMS Operation and Monitoring Functionalities**
- 5.4.14.1 The functionality integrated into ICSS HMI shall allow control and monitoring of Building Management Systems.
- 5.4.14.2 The ICSS scope for control and monitoring of BMS includes the Mechanical and Electrical (M&E) equipment provided by station contractors, facility contractors, and the Contractor.
- 5.4.14.3 The ICSS shall be interfaced with the external BMS systems (i.e., BMS provided by station and facility contractor) at the OCC through a connection to the DCN.
- 5.4.14.4 The TSCC Contractor shall be interfaced with the internal BMS system (i.e., BMS provided by TSCC Contractor) at the OCC through a connection to the DCN. Alternatively, if needed, the TSCC Contractor shall provide a Remote Terminal Unit (RTU) or Programmable Logic Controller (PLC) to connect with the BMS equipment located at the Shelters and Substations.
- 5.4.14.5 The ICSS shall be able to gather information from the BMS for equipment diagnostics in the CHSR System.
- 5.4.14.6 The ICSS HMI shall display:
- The BMS equipment description, identification, and equipment label in each location.
 - Operational state of the BMS equipment in each location.
- 5.4.14.7 The ICSS shall, at least, control and/ or monitor the following BMS equipment provided:
- Fire Protection System
 - Elevators
 - Escalators
 - Lighting
 - HVAC
 - Hydraulic
 - Low Voltage Power Supply



5.4.14.8 The ICSS HMI shall, as a minimum, provide the following functions listed below for the BMS. Available functionality shall be dependent on the operator profile:

- **Fire Protection System**
 - Equipment identification (panels, detectors, suppression devices).
 - Indication of faulty fire system equipment or active alarms.
 - Display of fire zones and alarm locations on graphical floor plans.
 - Event logging and time-stamping of fire alarms, resets, and faults.
 - Indication of system interlocks (e.g., HVAC shutdown, elevator recall).
- **Elevators**
 - Equipment identification (car number, shaft, control panel).
 - Real-time status (in service, out of service, fault, floor position).
 - Alarm indication for faults or entrapments.
 - Event logging of operational states and faults.
 - Remote commands where permitted (e.g., shutdown, fire service mode).
- **Escalators**
 - Equipment identification (escalator ID, location).
 - Status monitoring (running, stopped, fault, direction).
 - Alarm indication for faults or emergency stops.
 - Event logging of faults and operational changes.
 - Control functionality where authorized (start/stop/reset).
- **Lighting System**
 - Equipment identification (zones, panels, circuits).
 - Indication of faulty lighting circuits or failures.
 - Status monitoring (ON/OFF, auto/manual, emergency lighting).
 - Energy consumption monitoring where applicable.
 - Remote control where permitted (switching on/off, dimming).
- **HVAC System**
 - Equipment identification (AHUs, chillers, pumps, VAVs, thermostats)
 - Monitoring of operating parameters (temperature, humidity, pressure, airflow).
 - Fault alarms (filter clogged, compressor trip, high temperature, etc.).
 - Trend monitoring of key parameters for performance optimization.
 - Control commands where authorized (start/stop/reset, mode change).
- **Hydraulic Systems**
 - Equipment identification (pumps, pressurization units, tanks).
 - Monitoring of operational status (running, standby, fault).
 - Indication of alarms (low pressure, leakage, pump trip).
 - Event logging of changes and faults.
 - Remote control where authorized (start/stop/reset).
- **Low Voltage Power Supply**
 - Equipment identification (switchgear, transformers, UPS).
 - Real-time monitoring of supply status (energized, fault, standby).
 - Display of electrical parameters (voltage, current, load, frequency).
 - Alarm annunciation (faults, overloads, trip conditions).
 - Graphical single-line diagram representation.



- Trend monitoring of load and energy consumption
- Remote commands where applicable

5.4.14.9 The TSCC Contractor shall coordinate with station and facility contractors for interfacing requirements (i.e., specifications, protocols, connections, etc.).

5.4.15 Alarms

5.4.15.1 Alarms and indications for each interfaced system shall be provided to the ICSS.

5.4.15.2 Alarms and events shall be displayed and timestamped.

5.4.15.3 The TSCC Contractor shall design ICSS alarms in accordance with EN/IEC 62682 standard.

5.4.15.4 All alarm indications shall be flashing when requiring immediate attention and steady if less urgent attention is necessary.

5.4.15.5 Alarms shall be provided for any conditions affecting normal operation of the ICSS and its interfaces.

5.4.15.6 The alarm indications shall display at a minimum:

- the type: operation, safety and security, maintenance.
- the severity: emergency, alert, critical, error, warning, notice, info, debug.
- the origin subsystem(s): PACIS, CCTV...
- the recipient: OCC Supervisor, ICSS Operator... They are the responsible users intended to react/respond to the alarm occurrence.

5.4.15.7 The TSCC Contractor shall submit an alarm management plan and design to the Authority for approval.

5.4.16 Alarm Type

5.4.16.1 The following alarm types shall be at least managed by the ICSS:

- Operational alarms: corresponding to a failure of a piece of equipment that can disturb the operation of the line.
- Safety and Security alarms: corresponding to an abnormal situation occurring that has the potential to affect safety or security (i.e., distress alarms sent by the passengers, vandalism to equipment...).
- Maintenance alarms: corresponding to maintenance activities.

5.4.16.2 The qualification of alarms into above mentioned types shall be done by the TSCC Contractor and submitted to the Authority for approval.

5.4.17 Alarm Severity

5.4.17.1 The alarm severity levels shall be at a minimum:

- Level 1 severity - None: associated with events (i.e., no alarm is raised by the ICSS, e.g., notice, info, debug).
- Level 2 severity - Minor: related to events that the ICSS operator needs to know but does not request a quick reaction (i.e., warning).
- Level 3 severity - Major: alarms related to events requesting quick reaction for service affecting reasons (Impact on Traffic) (i.e., error).



- Level 4 severity - Critical: alarms related to events requesting immediate actions for safety and service (impact on traffic and safety), such as fire detection (i.e., emergency, alert, critical).

5.4.17.2 Alarms' severity shall be easily configurable by dedicated maintenance operators without third-party involvement.

5.4.17.3 The definition of severity shall be done by the TSCC Contractor and submitted to the Authority for approval.

5.4.18 Alarm Management

5.4.18.1 The TSCC Contractor shall provide an alarm management function, including alarm routing for the subsystems interfaced with the ICSS.

5.4.18.2 Alarm management shall be designed in such a way that the ICSS operator's workload is never exceeded.

5.4.18.3 The TSCC Contractor shall design the ICSS to manage alarm avalanches without any alarm loss. Alarm avalanche is a situation where a single or minor event triggers a massive cascade of alarms, which may overwhelm operators with a flood of notifications, making it difficult to identify the root cause and react appropriately.

5.4.18.4 The TSCC Contractor shall manage the alarm avalanches based on alarm families, i.e., all subsequent alarms to the occurrence of a particular alarm must be hidden to avoid any inconsistency of treatment by operators.

5.4.18.5 The TSCC Contractor shall also manage the alarm avalanches based on scenarios, i.e., the consequences of an alarm occurrence on other equipment must be considered to present comprehensive alarms to the operators.

5.4.18.6 The TSCC Contractor shall provide an alarm avalanche management plan (hierarchization, scenarios) to the Authority for approval.

5.4.18.7 Alarms' history shall be available on all operators' workstations and shall be displayed with filter functions allowing sorted lists.

5.4.19 Archiving, Reporting and Printing

5.4.19.1 Every ICSS system's faults, alarms, and events shall be recorded and archived.

5.4.19.2 Online data storage of at least one month shall be provided through an archiving function, enabling users to access and browse the previous 30-day records at any time.

5.4.19.3 The archiving function (using a commonly used format such as syslog so that standard off-the-shelf tools can be used for managing data, analytics) shall also store records in a suitable manner to allow transfers of each month's records to external processors or to suitable media for archival storage.

5.4.19.4 The archiving function shall at least provide the following features:

- Separate physical media units required for each month's records.
- A simple means of retrieval and display of the archival information is required.
- Enough media for at least 12 months of records shall be provided.



- 5.4.19.5 The archiving system shall use a storage array encryption algorithm to ensure data security.
- 5.4.19.6 Security assessments shall be guaranteed through authentication with very restricted access to repositories and password policies.
- 5.4.19.7 All devices shall be protected by Uninterruptible Power Supply (UPS) systems with autonomy to perform an ordered switch off to reduce data loss.
- 5.4.19.8 The ICSS shall provide a reporting function allowing the ICSS operator to edit/modify, create, enable, disable, and delete reports and report templates.
- 5.4.19.9 The ICSS shall include a database facility that shall maintain and update records of alarms, events, controls, and the status of all the selected equipment. This database shall be updated as a real-time activity and shall be accessible from any ICSS workstation.
- 5.4.19.10 Historical data storage (using a commonly used format such as syslog so that standard off-the-shelf tools can be used for managing data, analytics) and software backup systems shall be provided, designed to ensure that stored data is retained in an efficient manner and allows rapid search against selectable criteria. The storage facilities shall also ensure that historical records can be rebuilt in a readable data form.
- 5.4.19.11 The printing function shall be available on all ICSS operator workstations.
- 5.4.19.12 All generated reports shall be printable for all operators.
- 5.4.19.13 All equipment failures description shall be printable.

5.4.20 **Playback**

- 5.4.20.1 The ICSS shall provide a Playback function based on recorded events and pictures for later viewing, post-inquiring, or training.
- 5.4.20.2 The Playback function shall allow ICSS operators to select starting points, playback speed (typically 0.1, 0.5, x1, x2, x10, x100), pause, and reverse.
- 5.4.20.3 Outputs shall be available as screen displays and playback. It shall be possible to filter outputs by time span, activity type, and event priority.

5.4.21 **Training Simulator**

- 5.4.21.1 The ICSS shall provide a dynamic training function/simulator of the CHSR System operations for the training of the ICSS operators.
- 5.4.21.2 The ICSS simulator shall provide a real-time simulation of all ICSS interfaces.
- 5.4.21.3 Within the ICSS simulator, the operator position shall be the same as the one in the OCC control room.
- 5.4.21.4 The ICSS simulator shall, at a minimum, allow the trainer to:
 - Write, edit, and play scenarios.
 - Switch on/off equipment.
 - Run the replay mode of a real situation or a training session.
 - Manage several trainees at the same time.
- 5.4.21.5 The ICSS shall, at least, allow the trainee to:



- React and operate as if he was in real operation.
- Run a replay of his training session.

5.4.21.6 The ICSS simulator shall consist, at a minimum, of:

- server with the same database as the active system.
- RTU representing the same type of I/O's.
- trainee workstations.
- teacher workstation.
- Printer.

5.4.22 Maintenance Management

5.4.22.1 The ICSS shall include all necessary tools and licenses to allow configuration and modification of the database and the workstation views.

5.4.22.2 Configuration of any distributed ICSS equipment shall be possible from the OCC.

5.4.22.3 ICSS Maintenance workstations shall be provided with:

- Capability to perform configuration and modification of the ICSS HMI and database configuration.
- Capability to perform maintenance and diagnostic activities for all ICSS equipment.
- A Network Management System (NMS) to facilitate ICSS internal network monitoring, management, maintenance functions, network bandwidth allocation, routing setup, traffic monitoring, VLAN settings, IP address allocation, and other functions.

5.4.22.4 All configuration and management functions shall be subject to sufficient login privileges.

5.4.22.5 Maintenance laptop computers shall be provided with diagnostic, testing, and maintenance software for the RTU/PLC/IED.

5.4.22.6 The maintenance laptops shall also be provided with diagnostic and testing software for interfaced system protocols.

5.4.23 Video wall in OCC for CCTV

5.4.23.1 The TSCC Contractor shall provide a video wall in the OCC for displaying CCTV video images.

5.4.23.2 The video wall shall enable OCC operators to monitor live CCTV feeds from stations, depots, trains, and other wayside facilities.

5.4.23.3 The video wall shall support both continuous surveillance and event-based display.

5.4.23.4 The video wall shall be capable of displaying CCTV video images either upon command from the ICSS workstation or automatically upon activation of a coordinated event (e.g., a CCTV image triggered by a passenger help point activation, fire alarm, etc.).

5.4.23.5 The system shall allow operators to configure layouts dynamically (e.g., single large view, multi-camera grid, picture-in-picture).

5.4.23.6 The video wall shall support 24x7 operation with high availability and reliability.

5.4.23.7 The operators shall be able to select and display any CCTV camera feed on the video wall from the ICSS workstation.



- 5.4.23.8 The operators shall be able to define and recall preset display layouts.
- 5.4.23.9 The video wall shall allow zooming, panning, and rearranging of feeds in real-time.
- 5.4.23.10 The video wall shall be based on the latest technology in Direct View LED.
- 5.4.23.11 The video wall shall be modular and scalable to allow future expansion of display area or resolution.
- 5.4.23.12 The system shall support the addition of new CCTV sources without major hardware/software replacement.
- 5.4.23.13 The video wall shall support display of CCTV video at a minimum resolution of 4K, higher resolutions (e.g., 8K) shall be supported where commercially available.
- 5.4.23.14 The displayed video shall be free from distortion, jitter, or synchronization issues.
- 5.4.23.15 Brightness, contrast, and color reproduction shall be uniform across the entire video wall.
- 5.4.23.16 The size and configuration of the video wall shall be determined based on ergonomic studies and shall be submitted to the Authority for review and approval prior to implementation.

5.5 Performance Requirements for ICSS

5.5.1 System Performance and Capacity

- 5.5.1.1 When a new graphic picture is called up for display on a Workstation, the response time from the finish of the entry of the command requesting the display until the conclusion of the drawing of the display, including all data items, shall not exceed 4 seconds.
- 5.5.1.2 Where several pictures are called simultaneously, then the maximum response shall not be greater than 8 seconds for all the Workstation's displays. These displays may be either identical or different in content.
- 5.5.1.3 Where text Information is called, the screen shall start writing within 2 seconds from the entry of the command and be completed with a screen containing 1000 characters, including blanks, in not more than 4 seconds. Multiple screen requests are possible, and this shall be in such a way that all screens complete writing within 8 seconds.
- 5.5.1.4 The maximum propagation and response times specified shall be achieved under worst-case system loading conditions.
- 5.5.1.5 Under normal or degraded modes, the CPU loading of any core equipment shall be less than 35% on average when measured over a period of 5 minutes.
- 5.5.1.6 Under emergency conditions, the CPU loading of any core equipment shall be less than 70% on average when measured over a period of 5 minutes.
- 5.5.1.7 Buffering shall be controlled so that a full buffering condition will not cause the system to become unavailable.

5.5.2 Response Times

- 5.5.2.1 The initialization of the ICSS application on the workstations shall last less than 1 minute.



- 5.5.2.2 The initialization time of the ICSS application on the real-time data servers (Hot & Stand-by) shall be less than 2 minutes.
- 5.5.2.3 The ICSS initialization after hardware reset shall not exceed 10 minutes.
- 5.5.2.4 The elapsed time between the change of an attribute of remote equipment and its display on the HMI (OCC workstations and Local Workstations) shall not exceed 1.5s.
- 5.5.2.5 The elapsed time between the validation of an order from the ICSS HMI and the control's arrival at the input level of remote equipment shall not exceed 1.5s.
- 5.5.2.6 Switching time between real-time redundant servers shall not exceed 5s.
- 5.5.2.7 The Acknowledgement of an alarm (Elapsed time between its request from the ICSS HMI and the update of the list of alarms on all workstations) shall not exceed 0.5s.
- 5.5.2.8 The feedback to ICSS operator action (Elapsed time between an operator request from the ICSS HMI and the display on the workstation reporting that it has been considered) shall not exceed 1.5s.

5.5.3 **Expandability and Scalability**

- 5.5.3.1 The ICSS shall be a fully flexible and scalable system, which shall be upgradable with only configuration data and modular software modification to incorporate future integration of any functionality, equipment, and as required by Section 5.4 of this document.
- 5.5.3.2 The ICSS shall be able to be upgraded and/or modified to incorporate any other changes which may be required during the lifetime of the system.
- 5.5.3.3 The ICSS shall be open and modular in nature to provide maximum adaptability and flexibility during the life of the system.
- 5.5.3.4 The TSCC Contractor shall provide details of any future proposed updates to the core equipment foreseen within the lifetime of the system.
- 5.5.3.5 The TSCC Contractor shall provide documentary evidence as to how changes to the core operating equipment, including all hardware and software, post commissioning, are to be managed during the lifetime of the system, determining effective strategies to combat the system obsolescence.

5.5.4 **Safety Requirements**

- 5.5.4.1 ICSS shall comply with the safety requirements defined in the Schedule 1 and the Authority's System Safety Plan.

5.5.5 **RAM Requirements**

- 5.5.5.1 The TSCC Contractor shall be responsible for performing all the activities as specified in the Schedule 1 – Safety, Security and RAM Requirements.

5.6 **Cybersecurity and Security Requirements**

5.6.1 **Security and Confidentiality**



- 5.6.1.1 The ICSS design, procurement activities, configuration, and operation shall be fully compliant with the California HSR Cybersecurity Technical Specification. All technical security controls, access controls, logging requirements, patching cadence and procedures, incident-response procedures, cryptographic requirements, backup and restoration strategies, and assurance measures shall be co-engineered with the TSCC Contractor's Cybersecurity Lead.
- 5.6.1.2 All ICSS components, including servers, RTUs/PLCs shall be treated as networked endpoints and subject to the Authority's cybersecurity compliance reviews, threat modeling, and supply chain risk assessments.
- 5.6.1.3 The ICSS must have an accountable System Owner who shall be the risk owner of all cybersecurity risk associated with the ICSS.
- 5.6.1.4 The system shall be protected against threat-based cybersecurity risks identified during threat modelling exercises and risk assessment activities facilitated by the TSCC Contractor's Cybersecurity Lead as outlined in the California HSR Cybersecurity Technical Specification. The System Owner shall be responsible for ensuring that appropriate technical SMEs and system design experts attend threat modelling exercises and inform risk assessment activities. Threat modelling exercises shall consider the threats described in the California HSR Technical Specification and information gathered by the Cybersecurity Lead from threat sources.
- 5.6.1.5 All interfaces with other systems shall be secured in compliance with the cybersecurity technical specification, with detailed documentation that demonstrates how the security objectives are achieved, where systems are in different cybersecurity zones, connectivity shall be facilitated by appropriately design security conduits that are reviewed by the Cybersecurity Lead.
- 5.6.1.6 The ICSS System Owner shall maintain a risk register containing cybersecurity risks and mitigating actions, risk updates shall be provided to the Cybersecurity Lead periodically.
- 5.6.2 **Access Authority**
 - 5.6.2.1 For system security, the ICSS shall be equipped with a configurable user access authentication system that shall restrict the actions that can be performed by different operators on the different devices in the system, according to operator profiles. The user access authentication system shall be integrated with the centralized authentication and directory services to enable centralized identity and access management as outlined in the California HSR cybersecurity specification.
 - 5.6.2.2 The ICSS shall enforce a strong password policy and multi-factor authentication, as described in the California HSR Technical Specification.
 - 5.6.2.3 The system shall implement Role-Based Access Control to enforce the minimum set of permissions for different operator profiles; each operator shall only have the required access to perform their duties. Further detail on access control is provided in the cybersecurity specification.
 - 5.6.2.4 The ICSS System Owner shall design roles that enable the implementation of Role-Based Access Control such that:



- Control roles (e.g., OCC Operators) shall be granted full supervisory control of assigned sub-systems.
- Monitor-only roles (e.g., Maintenance staff, Emergency Services) shall be restricted to alarm and alert viewing only.
- Managerial roles (e.g., Operations and Maintenance Managers) shall be restricted to data analytics, trend monitoring, and reporting functions only.

5.6.2.5 Role-Based Access Control privileges shall be enforced in accordance with the principle of least privilege, with segregation of duties applied between operational, maintenance, and administrative functions. The user access management system shall have the following typical functions:

- Definition of user profiles.
- Definition of users.
- Profiles management:
 - Add/remove profiles.
 - Defining profile permissions.
 - Mapping profiles to directory service profiles/groups/roles
- Users' management:
 - Add/remove users.
 - Centralized authentication service integration.
 - Centralized directory service integration

5.6.2.6 The system administrator shall work with the centralized access management team to ensure that roles are mapped between the ICSS and Directory Services to enable on-boarding and off-boarding of users to the user access management system. The access authority system shall ensure that only one “logged in” operator has authority over a defined area of control and alarm acknowledgement, at any one time.

5.6.2.7 The access authority design shall include liaison with the Authority, and the Access and Authority Strategy shall be submitted for review and approval by the Authority.

5.6.3 Remote Access Security

5.6.3.1 The diagnostic and maintenance access, and any other remote access, shall be on-boarded to a centrally managed remote access solution as defined in the California HSR Cybersecurity Technical Specification, the System Owner shall work with the Cybersecurity and network teams to facilitate and configure this connectivity.

5.6.3.2 Remote access sessions shall be managed and activities performed during remote access shall be monitored and automatically recorded in the event log, these logs shall be available for audit purposes as required.



6 INTERFACE REQUIREMENTS

6.1 General Requirements

6.1.1 The interfaces are classified as the following:

- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Parties (excluding CHSR contractors)
- External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, stations contractors, facilities contractors, Solar PV and BESS contractors)
- Internal Interfaces: Interfaces between systems within the TSCC scope

6.1.2 The preferred communication interfaces to other systems and equipment shall be through a communication protocol via the DCN, direct to Core Equipment, Controllers, RTU, PLC, or IED provided as part of the interfaced systems and equipment.

6.1.3 For interfaced systems or equipment that do not possess a DCN connection, but that require a connection to the ICSS, the TSCC Contractor shall allow for this requirement by hardwiring the interface to the ICSS RTU/PLC.

6.1.4 All communications links and interfaces between the ICSS and interfaced systems shall use IP-based communications via the DCN.

6.1.5 All communications links and interfaces shall operate with open and standard protocols.

6.1.6 Where the use of proprietary protocols is unavoidable, the TSCC Contractor shall make the protocol details freely available to the Authority and to be shared with the interfacing contractors.

6.1.7 ICSS RTU/PLC with I/O Cards and serial interfaces (Modbus and/or other protocols) shall be provided with converter devices, where necessary to interface to other systems and equipment, where communication via IP protocols is not possible.

6.1.8 ICSS RTU/PLC shall communicate with core ICSS equipment over open protocols.

6.1.9 It shall be the responsibility of the TSCC Contractor to implement a logical and structured IP addressing policy that they agree with the Authority during the detailed design stage, without conflicting with existing equipment.

6.1.10 The TSCC Contractor shall provide necessary design information and coordinate with each interfacing party, recording the agreed interface design parameters, including IP addresses, subnets, VLANs, protocols, I/O Lists, and other requirements to achieve interface resolution.

6.1.11 The ICSS shall be fed via the UPS and not be directly exposed to network energy so that it is not affected by energy fluctuations or blackouts.

6.1.12 Power distribution within rooms, wayside enclosures, and the TSCC Contractor's specific equipment cabinets shall be the responsibility of the TSCC Contractor.

6.2 External Interfaces – station contractor

6.2.1 The ICSS shall interface with station BMS Mechanical and Electrical (M&E) equipment provided by station contractor. The interface shall fulfill functionality as described in Section 5.4.14.

6.2.2 The TSCC Contractor shall coordinate with the station contractors regarding the space provisioning and mounting arrangement for ICSS equipment.



- 6.2.3 The TSCC Contractor shall coordinate with the station contractors for the provisioning of cable containment.
- 6.2.4 The TSCC Contractor shall arrange interface meetings/strategy to define the interfaces and HMI functions.

6.3 External interfaces - facilities contractor

- 6.3.1 The ICSS shall interface with facility BMS Mechanical and Electrical (M&E) equipment provided by facility contractors. The interface shall fulfill functionality as described in Section 5.4.14.
- 6.3.2 The TSCC Contractor shall install all ICSS equipment in the OCC and facilities being provided by the facilities contractor.
- 6.3.3 The TSCC Contractor shall provide to the facilities contractor:
- Equipment dimensions
 - Equipment clearances requirements
 - Equipment mounting and fixings requirements
 - Cable routes/containment requirements
 - Equipment loadings
 - Installation and maintenance requirements
 - Equipment heating loads
 - Equipment cooling loads
 - Equipment hydraulic requirements
- 6.3.4 To be provided by facilities contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:
- Room dimensions and layouts
 - Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
 - Room raised floor system
 - Delivery access routes.
 - Maintenance access routes

6.4 Internal Interfaces

6.4.1 Digital Communication Network (DCN)

- 6.4.1.1 The ICSS interface with DCN shall fulfill functionality as described in Section 5.4.4.
- 6.4.1.2 The ICSS shall utilize the DCN for communication with all subsystems.

6.4.2 Network Timing System (NTS)

- 6.4.2.1 The ICSS interface with NTS shall fulfill functionality as described in Section 5.4.5.
- 6.4.2.2 The ICSS interface with NTS for time synchronization of ICSS servers, HMI, and controllers.

6.4.3 Electronic Access Control System (EACS)

- 6.4.3.1 The ICSS interface with EACS shall fulfill functionality as described in Section 5.4.6.

6.4.4 Closed Circuit Television System (CCTV)

- 6.4.4.1 The ICSS interface with the CCTV system shall fulfill functionality as described in Section 5.4.7.

6.4.5 Telephony System



- 6.4.5.1 The ICSS interface with the Telephony system shall fulfill functionality as described in Section 5.4.8.
- 6.4.6 **Public Address and Customer Information System (PACIS)**
 - 6.4.6.1 The ICSS interface with PACIS shall fulfill functionality as described in Section 5.4.9.
- 6.4.7 **Wireless Communication System (WCS)**
 - 6.4.7.1 The ICSS interface with WCS shall fulfill functionality as described in Section 5.4.10.
- 6.4.8 **Hazard Detection and Early Warning System (HDEWS)**
 - 6.4.8.1 The ICSS interface with HDEWS shall fulfill functionality as described in Section 5.4.11.
- 6.4.9 **Enterprise Asset Management System (EAMS)**
 - 6.4.9.1 The ICSS interface with EAMS shall fulfill functionality as described in Section 5.4.12.
 - 6.4.9.2 The ISCC shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.
- 6.4.10 **Medium/Low Voltage Power Supply (MV+LV PS)**
 - 6.4.10.1 The ICSS interface with MV+LV PS shall fulfill functionality as described in Section 5.4.13.
 - 6.4.10.2 The ICSS equipment shall receive LV power from UPS.
- 6.4.11 **BMS and electromechanical equipment system at Substations**
 - 6.4.11.1 The ICSS interface with BMS equipment provided at substations shall fulfill functionality as described in Section 5.4.14.



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied by the TSCC Contractor shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards. Refer to section 2.4.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the design life requirements.
- 7.1.3 Any failure of a single element within the ICSS shall be isolated to prevent propagation and shall not affect the operation of other elements.
- 7.1.4 The redundancy of the ICSS shall guarantee:
 - no interruption of display.
 - no interruption of the communication with connected systems.
 - no interruption to full functionality.
- 7.1.5 The redundancy solution shall allow uninterrupted operation, that is, in case of shutdown of one system, the operation continues without interruption with the intervention of the ICSS back-up.
- 7.1.6 The ICSS shall be able to transfer data to and from any point in the ICSS network.
- 7.1.7 Failure of any equipment element or node within the ICSS network shall not affect the operation of any selected equipment.
- 7.1.8 The operating system shall be the currently supported version of existing commercial operating systems.
- 7.1.9 In the event of a communications failure between a station and the equipment located in the OCC, the ICSS equipment and the connected selected equipment shall continue to run as normal in a standalone mode.
- 7.1.10 Security access to ICSS archives shall be guaranteed through authentication at the centralized security management database level, with very restricted access to repositories and password policies.

7.2 Software and Hardware Requirements

7.2.1 ICSS Servers

- 7.2.1.1 The ICSS servers shall have redundant architecture, including hardware, software, network, power supply, cabling, cooling, data backup, and disaster recovery planning and physical security, so that the ICSS survives during any one failure of hardware, power supply, cabling, and software.

7.2.2 ICSS RTU

- 7.2.2.1 Dual redundant RTU CPU, power supply, and COM modules shall be able to be connected directly via modular analogue I/O modules to the equipment and indirectly via digital communication interface modules to the network.
- 7.2.2.2 Both monitor and control shall be performed through the RTUs interface to the plant via digital and analogue inputs/outputs. This data shall be transferred to the central ICSS simultaneously.
- 7.2.2.3 The RTUs shall also be provided with analogue and digital control outputs to switch equipment such as circuit breakers.
- 7.2.2.4 The RTU shall be assembled from modular units, e.g. power supply module, CPU and communications module, communication interface modules and modules for input/output purposes.



- 7.2.2.5 I/O and serial cards shall be able to be arranged in the RTU rack in any order.
- 7.2.2.6 The remote terminal units shall at least respect the whole set of the following features:
- The average load of each CPU per slice of one minute shall be smaller than 60%.
 - Connection to redundant LAN shall be achieved through dual-attachment network interface cards.
 - Connection to external systems shall be carried out through physical interface such as I/O expandable cards, serial link modules, and Ethernet modules.
 - RTU shall support standard lower-level transport/network protocols (e.g., TCP/IP)
 - RTU shall support standard application protocols (e.g., OPC).
 - In case RTU needs a separate rack, it shall have a structure of 19 inches wide, mounted in an industrial cabinet.
 - For maintenance purposes, electronics status and troubleshooting LED codes shall be displayed on the RTU's front & rear panels.
 - RTU's power supply shall conform to electrical values such as: voltage range from 100V up to 240V and frequency range from 50Hz up to 60Hz.
- 7.2.2.7 Data from PLCs and Remote Terminal Units (RTUs) shall be relayed to the ICSS, and commands shall be entered into the HMI to adjust the processes they control.

7.2.3 ICSS Software

- 7.2.3.1 The ICSS software shall be designed to work on several platforms (cross-platform software).
- 7.2.3.2 Open and industry-standard protocols shall be implemented for all interfaces between systems.
- 7.2.3.3 All software and protocols shall be fully specified such that a 3rd party is able to implement the protocol for replacement/modified systems.
- 7.2.3.4 The supply of the ICSS shall include all necessary software perpetual licenses.
- 7.2.3.5 All licenses shall be fully transferred to the Authority on completion of the works.
- 7.2.3.6 All intellectual property rights for bespoke software designs and development, including all design documentation, source codes, development environment, and simulators, shall be transferred to the Authority on completion of the works.
- 7.2.3.7 The TSCC Contractor shall include provision for the evolution, upgrade path, and support of software and systems for the period specified in the contract.
- 7.2.3.8 All commercial "off the shelf" third-party software, except for operating systems, shall be the latest version available.
- 7.2.3.9 All software required to allow the ICSS to interface with other subsystems shall be defined and/or developed during the detailed design phase.
- 7.2.3.10 All interface software shall be written to allow full control of the respective sub-system.
- 7.2.3.11 The TSCC Contractor shall manage design coordination between all interfaced systems to ensure that all interfaces are fully developed, tested, and commissioned.
- 7.2.3.12 The TSCC Contractor shall, as part of the design phase, develop a Functional Architecture detailing how each sub-system functionality shall be implemented in the ICSS.
- 7.2.3.13 The design of the ICSS shall allow for fallback operation of the system database.
- 7.2.3.14 A Database Management Plan shall be prepared by the TSCC Contractor to address how the database is to be managed such that it does not become excessively large and complex.
- 7.2.3.15 The Database Management Plan shall also detail how the database can be updated and modified.



- 7.2.3.16 An alarm shall be raised in the ICSS upon its database and/or storage capacity exceeding a pre-set threshold.

7.2.4 Protocols

- 7.2.4.1 The ICSS shall be at least able to manage the following protocols:

- OPC UA
- BACnet
- IEC 60870-5
- IEC 61850
- SNMP V3
- MQTT
- Profisafe
- Modbus
- Profibus
- Profinet
- Or other open protocols can be proposed.

- 7.2.4.2 Open standard shall not be a proprietary or undocumented protocol.

- 7.2.4.3 Any protocol suggested shall be based on an Open public specification defined in an EN or ISO standard or an IETF RFC or similar, or another published and unencumbered specification that is available in full for industry review prior to any submission.

7.2.5 Human Factors requirements

- 7.2.5.1 The TSCC Contractor shall provide a Human Factors study prior to detailed design and submit it for approval to the Authority for the ICSS (present at the OCC and in Local within its scope).
- 7.2.5.2 The Human Factors design approach shall be based on best practices of industrial automation developed by the Abnormal Situation Management consortium and according to ISO 11064.
- 7.2.5.3 The ICSS HMI shall provide dynamic layout or diagrams of the monitored/controlled systems and shall allow the use of pan and zoom features to seamlessly navigate in the selected layout or diagrams.
- 7.2.5.4 The ICSS shall provide sufficient displays to allow operators at the OCC and in stations to supervise their area of responsibility.
- 7.2.5.5 The Human Factors (HF) methodology shall use a holistic approach bringing together all relevant stakeholders to ensure that the system will be defined correctly, and the design will meet all identified needs.

7.3 EMC Requirements

- 7.3.1 ICSS and associated electrical and electronic devices shall be designed to the requirements defined in the EN 50121-4 standard (Rail Applications - Electromagnetic Compatibility - Part 4: Emission and Immunity of Signaling and Telecommunications apparatus).
- 7.3.2 All equipment shall be provided with its own electromagnetic interference-free enclosure where necessary to ensure correct operation and avoid permanent degradation



8 TOLERANCES

Not applicable to the ICSS.

9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

- 9.1.1 The TSCC Contractor shall supply and deliver all components related to the ICSS Scope of Work.
- 9.1.2 Virtualized, cloud (on-premises) solutions may be proposed by the TSCC Contractor.
- 9.1.3 All central servers may be on-premises or virtualized machines to ease systems' evolution, complying with the Cybersecurity requirements.

9.2 Specific Requirements for ICSS

- 9.2.1 The ICSS scope of supply and delivery shall include (but is not limited to):
 - Servers.
 - Workstations/Displays /HMI/printers.
 - RTUs.
 - Cabling and connectors.
 - Racks.
 - Software architecture, including a full definition of protocols used.
 - HW/SW licenses.
 - Maintenance tools.
 - Any necessary supporting structures for ICSS.
 - Any auxiliary elements needed for ICSS.
 - Spare parts.
 - Maintenance laptops.
 - Video wall and controller.
- 9.2.2 The cables used in the ICSS shall be low-smoke, flame-retardant, halogen-free type.
- 9.2.3 The TSCC Contractor shall provide the ICSS cable schedule and layout.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.

11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.

12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.

12.2 Specific Requirements for ICSS

12.2.1 The TSCC Contractor shall develop a simulated environment to conduct all tests that can be performed using the simulated environment for the equipment and interfaces, before the on-site testing phase. The main goals are as follows:

- Prove the ICSS functionalities.
- Integrate ICSS with other systems.
- Test all interfaces.
- Test operational scenarios.
- Redundancy and robustness test.

12.2.2 The ICSS simulation environment(s) shall confirm that the CHSR operational principles are fully implemented on the prototypes, and this implementation complies with the expected behavior.

12.2.3 The TSCC Contractor shall propose and fulfil a set of functional and operational tests that comply with all the functionality of CHSR operational principles. These test scenarios shall be accepted by the Authority.



13 SUBMITTALS

13.1 General Requirements

13.1.1 General submittal requirements are defined in the Scope of Work.

13.2 Specific Requirements for ICSS

13.2.1 The design and supply of the ICSS shall include, as a minimum, the following plans/strategies:

- Alarm Management Strategy.
- Database Management Plan.
- Integration Plan.
- Access Authority Strategy.
- HMI specification.
- Functional Architecture.
- Future Expansion Strategy.

14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.

15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor and Supplier information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence ICSS system reliability, availability, and maintainability characteristics.

16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.



Schedule 5(i)

Interlocking System (IXL)

California High-Speed Rail Authority



Standard Specifications

TSCC Specification

SPEC-0013 – Interlocking System (IXL)

Rev. 0.0

Authorized:

A handwritten signature in blue ink, appearing to read "T. Stary".

Tomas Stary / Vincent Decanter, TCS Engineer

10/15/2025

Date

Checked:

A handwritten signature in blue ink, appearing to read "A. Clapham".

Andrew Clapham, Train Control Lead

10/15/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Bruno Comperat".

Bruno Comperat, Deputy Director of Rail Engineering

10/16/2025

Date

Approved:

A handwritten signature in blue ink, appearing to read "Ryan Scott".

Ryan Scott, Director of Rail Engineering

10/16/2025

Date

Released:

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Amit Joshi, Configuration Manager

10/16/2025

Date



Document Revision History – Interlocking System Specifications**First Edition****September 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF TECHNICAL SPECIFICATION	5
2	REFERENCE STANDARDS, NORMS AND DOCUMENTS	5
2.1	GENERAL	5
2.2	ENGINEERING RULES GUIDELINES	5
2.3	STANDARDS	5
3	TERMS, DEFINITION AND ABBREVIATION	7
4	SYSTEM DESCRIPTION	7
4.1	PURPOSE OF THE INTERLOCKING SYSTEM	7
4.2	INTERLOCKING SYSTEM DEFINITION	7
4.3	INTERLOCKING SYSTEM OPERATIONAL CONTEXT	7
5	SYSTEM REQUIREMENTS.....	9
5.1	GENERAL REQUIREMENTS.....	9
5.2	ENVIRONMENTAL CONDITION REQUIREMENTS	9
5.3	OPERATION REQUIREMENTS.....	10
5.4	FUNCTIONAL REQUIREMENTS.....	12
5.5	PERFORMANCE REQUIREMENTS.....	17
5.6	SECURITY AND CYBERSECURITY REQUIREMENTS.....	18
5.7	WAYSIDE OBJECT REQUIREMENTS.....	18
6	INTERFACES.....	22
6.1	GENERAL REQUIREMENTS.....	22
6.2	EXTERNAL INTERFACES – TRAINSETS	23
6.3	EXTERNAL INTERFACES – FACILITIES CONTRACTOR	23
6.4	INTERNAL INTERFACES	23
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS	26
7.1	GENERAL REQUIREMENTS.....	26
7.2	SW&HW REQUIREMENTS.....	26
7.3	ASSOCIATED COMPUTER TOOLS	27
7.4	OBSOLESCENCE	28
7.5	INTERLOCKING CABLE REQUIREMENTS	28
7.6	CABLEWAY REQUIREMENTS FOR INTERLOCKING CABLES.....	28
8	TOLERANCES	29
9	SCOPE OF SUPPLY AND DELIVERY	30
9.1	GENERAL REQUIREMENTS.....	30
9.2	SPECIFIC REQUIREMENTS	30
10	MANUFACTURING.....	31
10.1	GENERAL REQUIREMENTS.....	31
11	INSTALLATION AND INTEGRATION.....	32



11.1	GENERAL REQUIREMENTS.....	32
12	TESTING & ACCEPTANCE	33
12.1	GENERAL REQUIREMENTS.....	33
12.2	SPECIFIC REQUIREMENTS	33
13	SUBMITTALS.....	34
13.1	GENERAL REQUIREMENTS.....	34
14	QUALITY MANAGEMENT	35
14.1	GENERAL REQUIREMENTS.....	35
15	ADDITIONAL INFORMATION REQUESTED	36
15.1	GENERAL REQUIREMENTS.....	36
16	LOGISTICS	37
16.1	GENERAL REQUIREMENTS.....	37



1 INTRODUCTION

1.1 Scope of Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Interlocking System, hereinafter: IXL.
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of the IXL alongside other Train Control Systems is presented in Appendix A.
- 1.1.4 The requirements are formulated using the following words and their meanings:
- "Shall": Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure).
 - "Should": Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents.
 - "Must": Indicates an obligation or a mandatory requirement.
 - "May": Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.

2 REFERENCE STANDARDS, NORMS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines and specifications provided in this technical specification for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, training, operations and maintenance.
- 2.1.2 All generic standards to be used are provided in: Schedule 16.

2.2 Engineering Rules Guidelines

- 2.2.1 Engineering Rules shall be considered as a guideline that has been used for reference design purpose and can be adjusted by the TSCC Contractor if necessary.
- 2.2.2 The latest version of the following Engineering Rules shall be applied:

ID	Code	Title
[R36]	19_STS	Signaling Engineering Rules
[R37]	DCM_01	Design Criteria Manual Chapter 1: Overview
[R38]	DCM_12	Design Criteria Manual Chapter 12: Communication Systems and Train Control
[R39]	AREMA_17	AREMA Standards Chapter 17 – High-Speed Rail Systems

TABLE 25 - ENGINEERING RULES

2.3 Standards

- 2.3.1 The TSCC Contractor shall fully apply the following specific IXL standards in the provision of the works, the in-force standards shall be applied.



TABLE 2 – LIST OF APPLICABLE STANDARDS

ID	Code	Title
[R40]	EULYNX Baseline Set 4 Release 4	EULYNX Baseline Set 4 Release 4
[R41]	EN 50125	Railway applications - Environmental conditions for equipment - Part 3: Equipment for signaling and telecommunications
[R42]	EN 50124-1	Railway applications - Insulation coordination - Part 1: Basic requirements - Clearances and creepage distances for all electrical and electronic equipment
[R43]	EN 50121	Railway applications - Electromagnetic compatibility - Part 1: General
[R44]	EN 50129	Railway applications - Communication, signaling and processing systems - Safety related electronic systems for signaling
[R45]	TSI	Technical Specifications for Interoperability
[R46]	TSI LOC&PAS	Rolling Stock - Locomotives and Passengers TSI
[R47]	ISO 27001	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[R48]	NIST 800-53	Security and Privacy CFR 236y Controls for Information Systems and Organizations
[R49]	MIL-STD-810G	U.S. Department of Defense Test Method Standard, Environmental Engineering Considerations and Laboratory Tests
[R50]	EN 50159-1	Railway applications - Communication, signaling and processing systems - Part 1: Safety-related communication in closed transmission systems
[R51]	EN ISO/IEC 17020	Conformity assessment — Requirements for the operation of various types of bodies performing inspection
[R52]	EN 50126	Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
[R53]	EN 50716	Railway Applications - Requirements for software development
[R54]	49 CFR 236 – Subparts C and H	RULES, STANDARDS, AND INSTRUCTIONS GOVERNING THE INSTALLATION, INSPECTION, MAINTENANCE, AND REPAIR OF SIGNAL AND TRAIN CONTROL SYSTEMS, DEVICES, AND APPLIANCES: Subpart C – Interlocking and Subpart H “Standards for Processor-Based Signal and train control Systems”



3 TERMS, DEFINITION AND ABBREVIATION

- 3.1.1 All the terms, definitions, and abbreviations are provided in Schedule 5(t) SPEC-0024 – Glossary of Terms, Abbreviations and Definitions.

4 SYSTEM DESCRIPTION

4.1 Purpose of the Interlocking System

- 4.1.1 The purpose of the Interlocking system is to ensure protection against the following hazardous situations:

- collision of trains;
- train derailment;
- operation mishandling by the Dispatcher.

- 4.1.2 The Interlocking system shall operate switch machines and shunting signals to set a safe route for each train's movement, and to ensure that any other route conflicting with the already set route is prohibited.

4.2 Interlocking System Definition

- 4.2.1 The Interlocking system is composed of:

- Computer Based Interlocking (CBI): Safety equipment that contains the interlocking logic which processes the route setting activity based on the TMS commands, and the control of the wayside objects. The CBI is usually composed of several racks centrally located in the OCC buildings;
- Object Controllers (OC): Electronic units that monitor and control wayside objects (e.g., switch machines, axle counter sensors). They are in technical buildings (technical rooms) or Train control equipment housings on the open line;
- Wayside Objects: All wayside objects shall be connected with CBI by means of OCs;
- Interlocking Maintenance and Diagnostic Terminal (MDT) to collect diagnostic, status, alarms and maintenance data related to the Interlocking system.

- 4.2.2 The CBI interface with OC shall implement EULYNX specifications [R1].

4.3 Interlocking System Operational Context

- 4.3.1 The Interlocking system shall enable:

- 24h service all year around;
- Management of train movements along the line with the given headway;
- Bidirectional operation on each track with same performance in both directions;
- Management of interfaces with other subsystems of railway system;
- Recording diagnostic information and alarms for maintenance purposes;

- 4.3.2 The Interlocking system shall comply with the operational rules applicable on the CHSR line and shall allow safe movement of all train configurations defined for CHSR line at maximum design speed.

- 4.3.3 The Interlocking system shall be deployed over the entire railway network on the CHSR line, managing all types of railway infrastructure, e.g., main line and Facilities.

Note to reader: Definition of Facilities is provided in Chapter 4.3.

- 4.3.4 The Interlocking system shall ensure:

- Main route, shunting route and call-on routes management on the CHSR main line under operation from Main line TMS located in Fresno OCC;



- Route management between CHSR main line and transfer tracks of Facilities (and vice versa) under operation of main line TMS or the Facilities workstations, when authorized;
- Route management in Facilities operated from Facilities workstations, including on transfer tracks.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

- 5.1.1 The Interlocking system shall be designed in accordance with the requirements described in this specification, others relevant technical specifications and the rest of CHSR documentation.
- 5.1.2 The interlocking logic associated with the main line operations (e.g., operations controlled by the TMS system located in the OCC) shall be implemented in a centralized interlocking core, that shall be a CBI type.
- 5.1.3 The Interlocking system shall be able to accommodate a high centralization capacity in such a way that one CBI location shall be sufficient to control all the train control system infrastructure of the CHSR line.
- 5.1.4 The CBI shall be in an equipment room at the OCC in Fresno.
- 5.1.5 The object controllers shall be installed in one of the following configurations:
 - Gathered in technical buildings/rooms connected to wayside objects using long tail cables, or long field cables and short tail cables (interfaced with a junction box);
 - Near wayside objects, in dedicated object controller housings (train control equipment housings) dispatched along the track and connected to wayside objects using short tail cables.
- 5.1.6 The position of equipment and Train control equipment housings, and geographical boundaries controlled by each housing are to be designed and defined by the TSCC Contractor and shall be submitted to the Authority for approval.
- 5.1.7 The link between OCs and wayside objects shall consist of a direct link through copper cable, fiber optic cable or equivalent. This link shall be designed and supplied by the TSCC Contractor.

5.2 Environmental Condition Requirements

- 5.2.1 Refer to Technical Contract Requirements for general environmental requirements.
- 5.2.2 The additional following environment requirements apply to the Interlocking system:
 - The CBI shall be installed in OCC equipment room with climatic control (air-conditioning);
 - OCs shall be installed either in train control equipment housings along the track or in technical buildings/rooms (with climatic control).
- 5.2.3 For each implementation, equipment housing shall be proposed by the TSCC Contractor according to environment and approved by the Authority. The values for climatic conditions to be considered for all the OCs are those applicable to train control equipment housings.
- 5.2.4 Train Control equipment shall be placed in locations where they do not infringe people's passage.
- 5.2.5 Train Control wayside equipment shall be designed to ensure adequate protection from rodent actions.
- 5.2.6 The Interlocking system equipment (CBI, OC...) shall meet requirements for operation in cubicles, Train control equipment housings, and buildings as defined in standard EN 50125 Part 3.
- 5.2.7 The Interlocking system shall be compatible with the operation of the 2×25 kV AC Overhead Contact System (OCS). OCS and high voltage traction equipment shall not interfere with the operation of interlocking system equipment, requirements from standard EN 50124-1 shall be respected.
- 5.2.8 The Interlocking system, when installed along the track, shall not be disturbed by the operation of the 2×25kV AC OCS.



- 5.2.9 In addition, the interlocking system shall not be disturbed by High Voltage Power Lines parallel to CHSR line.
- 5.2.10 The Interlocking system shall fulfil requirements from standard EN 50121 series and standards related to EMC, emissions, and immunity.
- 5.2.11 The Interlocking system shall be compliant with EN 50124-1 for insulation coordination of wayside equipment.
- 5.2.12 The Interlocking system equipment shall be capable of resisting an overvoltage from lightning to a maximum of 2kV.
- 5.2.13 To limit the touch voltage to a safe level, all the accessible metallic parts that eventually can reach dangerous voltage, shall be connected to the return circuit by means of local grounding systems.
- 5.2.14 Ventilation
- 5.2.14.1 Natural ventilation shall be preferred to forced ventilation.
- 5.2.14.2 If forced ventilation is necessary:
- A breakdown in the ventilation system shall be reported to the maintenance team;
 - The ventilated equipment must be fully functional at least three days after a ventilation breakdown.

5.3 Operation Requirements

- 5.3.1 A unique and dedicated interlocking shall manage mainline, passengers' stations MOWS (Corcoran), TCF and sidings. This interlocking shall be in the equipment room in Fresno OCC. This interlocking is called Mainline interlocking in this document.
- 5.3.2 Dedicated IXL(s) (i.e. physically segregated from the mainline IXL) shall manage Light and Heavy Maintenance Facilities (LMF&HMF) as well as Maintenance of Way Facilities (MOWF). Depending on the configuration and location of these Facilities, the same interlocking could manage multiples facilities (for example Fresno's MOWF and HMF could be managed by a single IXL). But each Facility (except TCF) will have its own TMS workstations and local operator to manage the area under its responsibility.
- 5.3.3 When a train is requested to enter the main line from Fresno's facilities (except TCF), the Local Control shall request authorization from OCC.
- 5.3.4 The list of area types, type of operation and associated interlocking logic is summed up in the table below.

Area	Type of Supervised Operation	Interlocking Logic
Maintenance Of Way Facility (MOWF) in Fresno	Operated by a dedicated MOWF operator and from dedicated TMS workstation	Dedicated interlocking for Facilities, it could be mutualized with LMF/HMF interlocking
Train Certification Facility (TCF) in Fresno	Operated from Main line TMS workstation in OCC	Main line interlocking
Maintenance Of Way Facility Siding (MOWS) in Corcoran	Operated from Main line TMS workstation in OCC	Main line interlocking
Light Maintenance facility (LMF)	Operated by a dedicated LMF operator and from dedicated TMS workstation	Dedicated interlocking for Facilities, it could be



Area	Type of Supervised Operation	Interlocking Logic
		mutualized with MOWF/HMF interlocking
Heavy Maintenance Facility (HMF)	Operated by a dedicated HMF operator and from dedicated TMS workstations	Dedicated interlocking for Facilities, it could be mutualized with MOWF/LMF interlocking
Transfer tracks (Transfer tracks are used to route trains in or out of some Facilities or private sidings)	Operated from Main line TMS workstation in OCC or, when authorized, by Facilities workstation.	Boundary between Main line interlocking and Dedicated interlocking for Facilities
Main tracks and passing loops for stations are part of the main line and shall not be considered as a Facilities. (Tracks not used for permanent shunting purposes, except for coupling/decoupling or reversing towards dead end track).	Operated from Main line TMS workstation in OCC	Main line interlocking

TABLE 2: AREA AND OPERATION TYPES

- 5.3.5 Shunting operations shall be managed with shunting signals supporting train movement in ETCS SH mode.
- 5.3.6 The TSCC Contractor shall propose a train control solution without shunting signals when technically possible.
- 5.3.7 For Facilities operated without RBC supervision (such as MOWF, LMF, HMF), the CBI in Facilities shall be designed to ease a potential evolution to RBC supervised operations in the future. When interfacing a future RBC to this CBI, impact on the CBI shall be minimized.
- 5.3.8 TCF will be equipped with mainline ETCS (ETCS Marker Boards, balise, RBC coverage) to test the trains.
- 5.3.9 Depending on the proposed interlocking solution from the TSCC Contractor, on the track configuration and on the operational needs, the transfer tracks shall either be managed by the main line interlocking or by the dedicated interlocking of the Facilities.

Note to reader: Dedicated tracks separating the main line from Facilities shall enable any train movement from the main line to the Facilities and from the Facilities to the main line. Those tracks are called “transfer tracks”.

- 5.3.10 Any train movement between the main line and transfer tracks of a Facilities shall be supervised and controlled with the same level of safety as any train movement on the main line. This level of safety shall be SIL4.
- 5.3.11 The Facilities CBI shall, at least, interface with:
- Facilities TMS / workstations
 - Main line CBI



- Object Controllers for:
 - Axle counters,
 - Shunting signals when relevant,
 - Switch machines and derailleurs,
 - HDEWS when relevant,
 - Other equipment if required.

5.4 Functional Requirements

5.4.1 The Interlocking system shall perform, at least, the following functions:

- Check and evaluate the command received from the TMS;
- Compile status information and report fault indication of wayside equipment;
- Exchange information with adjacent interlocking (between mainline IXL and Facilities IXL's);
- Ensure route interlocking and route protection (Route setting, locking, detecting and release ...);
- Ensure time of operation locking
- Ensure out of correspondence alarms/controls for switch detection
- Ensure flank protection and control
- Ensure approach locking, track deadlocking, switch deadlocking, fouling controls for transfer tracks at facilities
- Exchange the information with ETCS wayside subsystem (bi-directional) and transmit route status to the ETCS wayside subsystem (as per EULYNX SCI-RBC specification);
- Manage and perform emergency commands (such as emergency route release, signal blocking, signal group replacement);
- Manage track possession activation;
- Manage normal route, shunting route, Call-on route;
- Manage fleeting operations;
- Ensure Interlocking functions as per CFR 236 [R15]
- Ensure normal and degraded modes controls and operation
- Manage Interlocking diagnostic information and alarms.
- Auto-normalization controls for switch machines, when relevant
- ...

5.4.2 The Interlocking system shall set, lock, monitor and release route for train movements.

5.4.3 The Interlocking system shall allow sectional route locking and sectional route release of the routes, section by section, to allow compatible train movements as soon as possible.

Note to reader: A signaling section corresponds to a portion of track between 2 neighboring axle counters.

5.4.4 The Interlocking system shall manage route cancellation features. The safety conditions to cancel the route shall be defined by the TSCC Contractor.

5.4.5 The RBC and CBI shall cooperate to manage approach locking and route cancellation/release (cooperative shortening of MA).



5.4.6 The route supervision function shall ensure continuous supervision of all routes, including the status of train detection sections, the position of the different turnouts, derailleurs and their locking states, maintenance work protection, and, when required, ancillary system alarms detection.

5.4.7 The Interlocking system shall be capable of controlling and monitoring at least the following wayside objects and monitoring their status:

- Switch Machines;
- Derailleurs;
- Signals;
- Axle counters;
- Staff Protection System;
- Other devices, if required, such as HDEWS.

5.4.8 Computer Based Interlocking (CBI)

5.4.8.1 A railway signalling CBI is a functional safety programmable controller with a safety integrity level capability of SIL 4 (as defined in EN 50129).

5.4.8.2 Main line CBI shall be SIL 4.

5.4.8.3 Facilities CBI may be SIL 4 or lower.

5.4.8.4 Lower SIL level to save costs may be used to Facilities CBI only after positive evaluation in the risk assessment from the TSCC Contractor.

5.4.8.5 The TSCC Contractor shall conduct a safety study to determine the appropriate safety level for each facility CBI.

5.4.8.6 The CBI equipment shall provide the following features:

- Application logic;
- Programming, debugging, and testing tools for the application logic both in creation of an installation and during maintenance of the installation;
- Evaluation of the application logic;
- Interfaces to equipment;
- Secure safe response according to the status of the supervised objects;
- Defined on-line support tool functionality.

5.4.9 Start-up

5.4.9.1 At start-up, the Interlocking system shall set all outputs to their restrictive states.

5.4.9.2 All protection shall be set during the start-up, and any active protection set prior to the start-up of the interlocking system shall be restored after the start-up. If the status of the protection prior to the start-up cannot be determined with the appropriate safety integrity level (SIL4), the protection shall be active by default.

5.4.9.3 The start-up of the Interlocking system shall take no longer than 3 minutes and shall not require any operator intervention to initialize the Interlocking system.

5.4.9.4 The Interlocking system shall not process any command from the TMS during start-up.

5.4.9.5 The operator shall be informed when the start-up phase is on-going and when the timer has elapsed.



5.4.10 ETCS Overlap and Interlocking

- 5.4.10.1 On the CHSR Main line, the nominal overlap shall be 70 meters (refer to ETCS Technical Specification). The Interlocking system may implement detection points to manage different overlap values at specific locations. The specific locations shall be detailed at specific application requirements level.

Note to reader: In accordance with ETCS Technical Specification, the ETCS design will detail the need to use different overlaps (including longer overlaps).

5.4.11 Shunting Movements in Station

- 5.4.11.1 Shunting is an activity where trains are prepared, moved, split, or combined in preparation for service.
- 5.4.11.2 The shunting movements in a station could be performed by means of ETCS Shunting (SH) mode. In this case several shunting areas can be defined for each station to allow shunting operation only inside a selected shunting area. The dispatcher shall set up a pre-defined Temporary Local Shunting Area to authorize shunting movement in the area. The interlocking system will process the TMS request and will inform the ETCS to authorize the shunting mode inside the selected shunting area.

5.4.12 Call-on route

- 5.4.12.1 Certain locations are permitted to allow more than one train into a single section, e.g. to join trains or enable 2 trains to use one platform. The movement of the second train into an occupied section is authorized by setting a "call-on" route.
- 5.4.12.2 The Interlocking shall manage call-on routes for the trains in ETCS On-Sight mode allowing these trains to entry in occupied sections.

5.4.13 Individual turnouts local control

- 5.4.13.1 Long turnouts that are operated by multiple switch machines (if used) require local control to electrically move the multiple switch machines using a local control panel. The local control panel shall be located at the side of the track and contain electrical switch(s). The trained field operator with the correct security access level can use such a local control panel.
- 5.4.13.2 The field operator shall request and obtain permission from the TMS for the local operation in the time slot of relevant possession.
- 5.4.13.3 After TMS authorization and when the safety and operational conditions are met, the interlocking shall allow the individual turnout to be set in local mode so field operator can control the turnout locally.
- 5.4.13.4 When the field operator activates the local turnout control, the interlocking shall inform the TMS of the respective status of the turnout and shall protect the turnout area from incoming train and discard any command from the TMS involving the individual turnout.
- 5.4.13.5 The Interlocking shall not authorize the setting of any route that includes a turnout which is in local mode.

5.4.14 Staff Protection

- 5.4.14.1 The Staff Protection function shall allow protection of maintenance staff or protection of equipment in case of unavailability of a piece of track (for works reasons, hazard on the section, environmental circumstances...).
- 5.4.14.2 The Staff Protection function shall be a SIL 4 function.



5.4.14.3 The following means shall be used to ensure the Staff Protection:

- Elementary protection sections:
 - The CHSR railway network shall be divided into elementary protection sections consisting of one or few track clearance detection sections (subject of review and approval by the Authority);
 - The activation of the elementary protection section shall exclude this section from the train traffic.
- Engineering Possession Management:
 - a. A list of preconfigured and predefined engineering possessions shall be available to the TMS dispatcher;
 - b. The TMS dispatcher shall be able to select Engineering Possessions from this list and activate it. Maintenance work protections shall be set automatically by activating the corresponding elementary protection sections.
- Staff Protection wayside device:
 - c. Staff protection wayside device shall allow the maintenance staff to set up their own protection in addition to the engineering possession;
 - d. Staff protection wayside device shall allow the maintenance staff located along the track to confirm the protected status (activation) of the elementary protection section.

5.4.14.4 The TSCC Contractor shall develop the Staff Protection wayside device to be used in conjunction with the Possession Management by the TMS, to mitigate operators' error of setting up an incorrect engineering possession.

5.4.14.5 The activation/deactivation of an elementary protection section shall be done under a commonly agreed operational procedure between operator and wayside maintenance chief engineer.

5.4.14.6 Clear indication of the track layout divided into elementary protection sections as well as the status of each elementary protection section shall be provided.

5.4.14.7 The Staff protection wayside device shall be designed to prevent unintentional setting or un-setting of the protection.

5.4.14.8 The activation of an elementary protection section shall be considered by the CBI as an occupation of the detection area covered by the elementary protection section.

5.4.14.9 A section of track shall be considered protected if the corresponding elementary protection section is activated from the Staff protection wayside device or if a request from TMS has been made and confirmed.

5.4.14.10 Elementary Protection sections shall correspond to:

- Every block section limit (Marker Board) in the open line;
- At dedicated access point for maintenance purpose in station areas.

5.4.14.11 Drawings indicating without ambiguity elementary protection sections shall be supplied by the TSCC Contractor.

5.4.15 Data Recording

5.4.15.1 The Interlocking system shall record any necessary information for maintenance purposes and for incident investigation. The information shall be directly accessible to CHSR staff in a readable format and shall be provided with a user manual that allows the understanding of the downloaded information.

5.4.15.2 The Interlocking system shall record at least the following information:



- All changes for each input and output of the Interlocking system. Each record shall be time and date stamped;
- The complete status of all information at start-up and regular intervals;
- The event in the record file when the event recorder starts recording, time or date is adjusted and when event recorder stops recording with a date and time stamp;
- All interlocking system equipment alarms or warning messages with a date and time stamp.

5.4.15.3 Separate record files for manageable geographic regions of the interlocking system installation shall be stored. Every record file shall include a reference to the site-specific data name.

5.4.15.4 A minimum of 90 days of recorded information shall be available.

5.4.15.5 Records shall be stored in non-volatile media. The non-volatile media shall be able to restore the complete information without damage for a minimum duration of 6 years.

5.4.15.6 The first line maintainer shall have facilities to select, view and export recorded events to either a removable medium or another system. The use of these facilities shall not interrupt or delay the recording and timestamping of events. The implementation of this facility shall consider the cybersecurity constraints.

5.4.15.7 If the event recorders' power is lost, then all events shall remain recorded except for events occurring in the preceding 1 minute which may be lost.

5.4.15.8 The event recorder shall automatically restart and begin recording after the mains power is applied to the event recorder.

5.4.15.9 The start-up delay for the event recorder shall be less than or equal to the start-up delay for the equipment that it is recording information for.

5.4.16 Replay

5.4.16.1 The Interlocking system shall provide a replay feature which uses the information recorded by the event recorder.

5.4.16.2 The replay facility shall allow the commencement of replay at any 10 min time interval.

5.4.16.3 Replay controls shall be modelled on the controls for playing a video. For example, play, fast forward, slow forward, fast reverse, slow reverse, pause and stop. Fast speeds shall range from 2 to 30 times the normal speed. Slow speeds shall range from 0.5 to 0.1 times the normal speed. At least two intermediate speed options shall be provided in each range.

5.4.16.4 The replay display will be used by people that normally view signalling equipment status on a TMS display. The replay display states, and layout shall be designed so that it is unlikely that these people misinterpret the information when it is viewed on an intermittent basis (less than once every six months).

5.4.17 Maintenance Support

5.4.17.1 The interlocking Maintenance and Diagnostic Terminal (MDT) shall collect incidents, alarms and any maintenance information related to CBI, Object Controllers, wayside objects (including switch machines) and related interface.

5.4.17.2 Object controllers and CBI shall interface the MDT using SDI and SMI Eulynx Baseline 4 Release 4 (or higher) specifications.

5.4.17.3 The MDT shall enable equipment malfunctions and failures to be identified at a line replaceable unit (LRU) level.



- 5.4.17.4 Any interlocking system alarms indicating a failure that causes or are likely to cause an operational delay shall be configurable to be sent to the dispatcher HMI interface to advise of the failure.
- 5.4.17.5 The different interlocking system components shall provide active indications of correct operation without the use of additional equipment.
- 5.4.17.6 The interlocking Maintenance and Diagnostic Terminal (MDT) shall provide the following maintenance functionality to support the maintainer performing corrective maintenance, preventive maintenance, and investigation of incidents:
- Maintenance display that shows the status of the Interlocking system and interfaced objects and related associated telecommunications links.
 - Management of the display, acknowledgement and archiving of alarms and warnings for the CBI equipment, related equipment, and associated telecommunications links.
 - Operation of all control, monitoring and interrogation functions provided as part of the interlocking system equipment for use by the maintainer.
 - Facilities required by first line maintenance personnel to configure the Interlocking system and interfaced objects for the specific site and usage as part of corrective maintenance.
- 5.4.17.7 The interlocking Maintenance and Diagnostic Terminal (MDT) shall provide remote facilities for uploading OC configurations.
- 5.4.17.8 MDT connections shall fulfil the cyber security requirements defined in the Cybersecurity technical specification.
- 5.4.18 Track Vacancy Detection
- 5.4.18.1 From a signaling point of view, the CHSR line will consist of block sections separated by marker boards and axle counters.
- 5.4.18.2 The CHSR line shall use fixed block working operation without lineside signals.
- 5.4.18.3 Block sections shall be designed for the required headways and operation performance.
- 5.4.18.4 Block sections shall be designed for bidirectional running on all tracks. Both directions of traffic shall reach the same level of performance.
- 5.4.18.5 Additional informative guidance (engineering rules) for axle counter placement is described in the document "Signaling Engineering Rules".

5.5 Performance Requirements

5.5.1 Capacity

- 5.5.1.1 A CBI shall be able to control at minimum all OC necessary for all wayside objects of the whole EOS line.
- 5.5.1.2 A provision of 50% shall be provided (in terms of wayside objects management and space in technical buildings / Train Control Equipment Housing) for potential future network extension.

5.5.2 Safety Requirements

- 5.5.2.1 The Interlocking system shall comply with the safety requirements defined in the TSCC Safety documentation.

5.5.3 RAM Requirements



- 5.5.3.1 The Interlocking system shall comply with the RAM requirements defined in Schedule 1 – Safety, Security and RAM Requirements.

5.6 Security and Cybersecurity Requirements

- 5.6.1 The Interlocking system shall be in full compliance with CHSR cybersecurity controls defined in Cybersecurity Technical Specification.
- 5.6.2 One or more System Owners (as defined in the Cybersecurity Technical Specification) shall be nominated as the accountable entity that shall be the risk owner of all cybersecurity risks associated with interlocking, or individual components of interlocking.
- 5.6.3 Safety critical interlocking traffic shall be protected from spoofing or tampering, all messages between interlocking systems shall be authenticated.
- 5.6.4 The System Owners that are nominated to own cybersecurity risks associated with interlocking systems shall ensure that appropriate resources are available and attend threat modelling workshops and risk assessment activities.
- 5.6.5 The System Owners that are nominated shall ensure that security requirements are embedded into the procurement process for all interlocking components.
- 5.6.6 System Owners shall demonstrate how cybersecurity requirements are being met by the interlocking systems and co-engineer solutions with the Cybersecurity Lead where specific controls cannot be implemented.
- 5.6.7 EULYNX communication protocols shall be evaluated to ensure that the most secure option that achieves the functional and safety requirements is selected and implemented in compliance with the CHSR Cybersecurity Technical Specification.

5.7 Wayside Object Requirements

5.7.1 Axle Counters

- 5.7.1.1 The mainline train detection system shall be based on axle counter technology.
- 5.7.1.2 Axle counters shall have a safety integrity level capability of SIL 4 (as defined in EN 50129).
- 5.7.1.3 The train detection system shall be compatible with the following characteristics:
- Electrical 2x25 kV trainset traction;
 - Operation speeds up to 354 km/h (220 mph) (note: During testing phase, axle counters shall support a speed up to 390 km/h (242 mph) (speed+10%));
 - Wheel characteristics, geometry and Axle distance as defined in “LOC&PAS / Interface between control-command signaling wayside and other subsystems TSI” document;
 - All rail profiles used on CHSR network;
 - Rail temperatures specified for CHSR line.
- 5.7.1.4 The Track Vacancy Proving equipment shall allow operation of 205m EMUs and 410m double EMUs.
- 5.7.1.5 The length of the trainset will be no more than 205 m (672.6 feet). The overall length of the double-traction train for operational purposes will be no more than 410 meters (1,345.2 feet).
- 5.7.1.6 As per Eulynx Specification SCI-TDS, the train detection system shall report to the CBI at least the following TVP occupancy status: Vacant, Occupied, Disturbed.



- 5.7.1.7 As per Eulynx Specification SCI-RBC, the CBI shall then report to the RBC the following TVP section status: Section occupied, Section vacant, Section failed.
- 5.7.1.8 The train detection system, in addition, shall be able to indicate at least the following conditions:
- Proper operation;
 - Fail Safe State;
 - Temporary interruptions;
 - Isolated, e.g., intentionally not used.
- 5.7.1.9 The axle counter shall define a track section as occupied as soon as the first axle of the train passes the axle counter border.
- 5.7.1.10 The equipment shall be able to handle train movements in both directions.
- 5.7.1.11 The train detection system shall operate correctly and detect any type of trainsets (passengers, freight, maintenance etc.) permitted to operate on the CHSR network and to circulate on the line whatever the speed of movement is.
- 5.7.1.12 For each axle counter installation, the environmental conditions under which axle counter is required to operate shall be considered.
- 5.7.1.13 The train detection system shall not be disrupted by electromagnetic interferences from external sources and shall be compliant with the EMC requirements either indoor or outdoor equipment installation.
- 5.7.1.14 Wheel sensors cables shall be laid separately from electric power lines, motors lines etc., where the immunization of the field equipment and cabling requires this, because of EMC.
- 5.7.1.15 The train detection system shall be compatible with the ballast and slab type of track.
- 5.7.1.16 The axle counters shall be mounted on rail without drilling.
- 5.7.1.17 The axle counters deployed shall be compatible with different IXL platforms and SIL 4 IXL protocols in the market and shall support EULYNX.
- 5.7.1.18 The Axle counter solution designed and proposed by the TSCC Contractor shall be compliant with general CHSR cybersecurity policies and in accordance with, at least, ISO 27001 and NIST 800-53 security standards.
- 5.7.1.19 The Axle counter sub-system shall include software within the Interlocking system or a specific one, for the management of the equipment.
- 5.7.1.20 Changing the Axle counter counting sensor should not require digging up cable between Axle counter sensor and junction box.
- 5.7.1.21 The axle counter tail cabling should not be buried.
- 5.7.1.22 It shall be possible to update the Axle counter software remotely.
- 5.7.1.23 It shall be possible to initiate an axle counter Reset/Restore from the TMS (in case of miscounting for example). The Interlocking system shall process the TMS request and evaluate the safety conditions to restore the section.
- 5.7.1.24 Feature/process for reset of axle counters shall ensure safety of train operation by acquiring evidence of the non-occupation of the corresponding track section prior to allowing restoration of nominal operation.



- 5.7.1.25 Interface between axle counter evaluator (i.e. Axle counter Object controller) and the CBI shall be based on SCI-TDS Eulynx Baseline 4 Release 4 (or higher) specification.
- 5.7.1.26 Interface between axle counter evaluator and the MDT shall be based on SDI-TDS and SMI-TDS Eulynx Baseline 4 Release 4 (or higher) specification.
- 5.7.1.27 In case a default appears on an axle counter sensor, a feature or procedure shall be developed to restore nominal train operation, without requiring maintenance staff in the field.
- 5.7.1.28 Intelligent fault tolerance measures shall be applied to improve Reliability and Availability of the axle counter system.

5.7.2 Staff Protection wayside device

- 5.7.2.1 This chapter specifies the technological requirements for the Staff Protection wayside device used in "Staff protection function" described in section 4.4.14.
- 5.7.2.2 The staff protection wayside device may be based on ruggedized portable tablets with communication supported by FRMCS.

5.7.3 Switch Machine

- 5.7.3.1 There shall be several types of turnouts for the following 3 different diverging track speeds:
 - Main line crossovers: 80 mph;
 - Stations: 60 mph;
 - Sidetracks: 50 mph.
- 5.7.3.2 The TSCC Contractor shall be responsible for choosing the correct switch machines for the traversal speed.
- 5.7.3.3 There shall be provision of support system facilities for the switch machines at turnout and crossover locations for TCS and OCS sub-sectioning support (Controller, LV feeding, telecom link...)
- 5.7.3.4 Only components with proven service records for application on track with at least the same or higher speed and axle load, and a minimum of 5 years' service on such conditions, shall be considered.
- 5.7.3.5 Switch machines shall comply with a design life of at least 30 years.
- 5.7.3.6 Switches, swing nose crossing (if used) shall be equipped with:
 - Locking devices;
 - Devices enabling to detect whether movable components lay in correct required position and are;
 - correctly locked.
- 5.7.3.7 Switch position detection shall be failsafe and be designed to meet availability requirements.
- 5.7.3.8 Switch machines shall be compatible with the use of magnetic braking systems for emergency braking.
- 5.7.3.9 Switch machines shall be equipped with devices for local switching.
- 5.7.3.10 Protection class shall be IP54, IP55, or IP67 based on environment (higher IP rating preferred).
- 5.7.3.11 Maximum operating time shall be lower than 5 seconds (faster operation preferred for high-speed lines).
- 5.7.3.12 Condition monitoring shall be used to offer predictive rather than corrective maintenance.



5.7.3.13 High speed switch machines shall be non-trailable.

5.7.3.14 Switch machines in Facilities may be trailable, depending on operational requirements.

5.7.4 Shunting Signals

5.7.4.1 On tracks located in permanent shunting areas in Facilities and in temporary shunting areas in mainline stations, dwarf shunting signals shall be provided by the TSCC Contractor.

5.7.4.2 The shunting signals shall be dwarf signals with appropriate aspects. The TSCC Contractor shall develop and approve the design of the shunting signal with the Authority.

5.7.4.3 The TSCC Contractor shall develop and approve the color scheme of the shunting signal with the Authority.

5.7.4.4 The light source used for signal aspects shall use LED technology.

5.7.4.5 The light source used for signal aspects shall appear to the observer to be circular in shape.

5.7.4.6 Signals shall be positioned to give drivers an approach view for a minimum sighting distance and a minimum reading time that shall be evaluated by the TSCC Contractor. Sighting distance shall be considered with respect to the view of the whole signal. Where a signal can be approached from more than one line, the minimum reading time shall be achieved on all approaches.

5.7.4.7 There shall be no interruption of the driver's view of a signal during the required reading time which implies an unacceptable risk of the driver disregarding or misreading the signal.

5.7.4.8 When the LED unit is broken, the signal failure message shall be sent to interlocking. A failure indication of a signal shall state which signal unit contains a broken LED unit. If a signal becomes "dark" due to a breakage of the LED unit, this shall send a signal dark indication.

5.7.4.9 The failures in signal lamp circuits shall cause a failure message. These failures include a short circuit between the wires of the signal circuits, an earth leakage and an external voltage caused by e.g., a short circuit between the wires.

5.7.4.10 The lamp circuits included in the aspects that allow proceeding shall be furnished with 2-pole disconnection. Also, short circuits in an LED unit circuit shall be indicated as a failure. When the lamp of "proceed" aspect is broken, the signal shall be set to "stop" aspect.

5.7.4.11 The LED unit must be US-approved.

5.7.4.12 There must be a marking to indicate the type, version, and serial number of the LED unit.

5.7.4.13 There must be a marking to indicate the LED unit manufacturer and the date of manufacturing.

5.7.4.14 There must be a warning text if it is forbidden to look directly at the LED unit's light beam.

5.7.4.15 All mandatory classifications that are marked on the LED unit must be easily detectable and clearly visible.

5.7.4.16 LED units' classification for casing (including inlet sleeve, grommet, and shield case) must be at least IP54.

5.7.4.17 There must not be any light emitted from the back of the signal with LED units, when LED unit is activated.

5.7.4.18 LED units shall not vibrate mechanically in a way that is observable to a driver of a passing train.



- 5.7.4.19 The elements of the LED unit should be arranged so that a fault in one element or in a group of elements does not have a significant effect on the distribution or the light intensity of the illuminated area.
- 5.7.4.20 The LED unit must not display a wrong aspect, because of reflection from other light sources or background lighting.
- 5.7.4.21 The LED unit is 'failed' if its luminous intensity is less than 50% of the original intensity.
- 5.7.4.22 The luminous intensity of the LED unit must not decrease more than 50% after 100 000 hours in use.
- 5.7.4.23 LED units shall be equipped with overvoltage protection. It must be possible to check visually if the overvoltage protector is damaged.
- 5.7.4.24 A commercially available overvoltage protector component must be used for overvoltage protection. The overvoltage protector must function before the overvoltage does any harm to any other components.
- 5.7.4.25 Maintenance operations shall be facilitated and from a safe area. LED replacement shall be performed from the back of the signal.
- 5.7.4.26 Interface between shunting signals object controller and the CBI shall be based on SCI-LS Eulynx Baseline 4 Release 4 (or higher) specification.
- 5.7.4.27 Interface between shunting signals object controller and the MDT shall be based on SDI-LS and SMI-LS Eulynx Baseline 4 Release 4 (or higher) specification.

Derailers

- 5.7.5 The TSCC Contractor shall analyze the track layout and location of the dead-end tracks/trap points and perform a risk assessment to evaluate the need for additional derailleurs. In such case, the TSCC Contractor shall define, provide and install derailleurs.
- 5.7.6 Derailleurs or dead-end tracks are used to protect main railway lines from unauthorized vehicles moving onto them from sidings or branch lines. Either of these track arrangements may lead the vehicles into a sand drag or safety siding, to safely stop them after they have left the main tracks.
- 5.7.7 An unauthorized movement may be due to a runaway wagon or may be a train passing a Marker Board (MB) at danger. When a MB controlling passage onto a main line is set to "danger", the derailleurs are set to derail any vehicle passing that MB. Interlocking shall make sure that the MB cannot allow passage onto the main line until the trap points or derailleurs have been aligned to ensure this movement can take place.

6 INTERFACES

6.1 General Requirements

- 6.1.1 Interfaces are classified as below:
 - Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR contractors);
 - External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors);
 - Internal interfaces between systems within the TSCC scope.
- 6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.
- 6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.



- 6.1.4 The TSCC Contractor shall achieve Interoperability by systematically identifying the interfaces between operations and maintenance, railway systems, trainsets, infrastructure, stations, and track.
- 6.1.5 The TSCC Contractor shall achieve interoperability by also proactively managing the interfaces between the various System and Sub-System elements.

6.2 External Interfaces – trainsets

- 6.2.1 The TSCC Contractor shall ensure compatibility of trainsets detection systems as per [R46] Rolling Stock - Locomotives and Passengers TSI.

6.3 External Interfaces – facilities contractor

- 6.3.1 The TSCC Contractor shall install all CBI equipment in the OCC and facilities being provided by the facilities contractor.
- 6.3.2 The TSCC Contractor shall provide to the facilities contractor:
- Equipment dimensions
 - Equipment clearances requirements
 - Equipment mounting and fixings requirements
 - Cable routes/containment requirements
 - Equipment loadings
 - Installation and maintenance requirements
 - Equipment heating loads
 - Equipment cooling loads
 - Equipment hydraulic requirements
- 6.3.3 To be provided by facilities contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:
- Room dimensions and layouts
 - Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
 - Room raised floor system
 - Delivery access routes.
 - Maintenance access routes

6.4 Internal Interfaces

6.4.1 Interface with Tracks system

6.4.2 Interface with TMS

- 6.4.2.1 These interfaces shall be redundant and shall comply with the EULYNX set of specifications (RaSTA protocol, SCI-CC and SCI-RBC).
- 6.4.2.2 The Interlocking system shall be able to communicate with the main line TMS and, when relevant, to a local TMS for Facilities.
- 6.4.2.3 Functional data that is transferred through the link between a TMS shall be configured through the data configuration process by the data configuration tool.

6.4.3 Interface with interlocking (CBI)

- 6.4.3.1 RBC and CBI shall operate in the same TCS domain as depicted in the HSR operational context.
- 6.4.3.2 RBC shall have a redundant interface with CBI via the transmission network (DCN).



- 6.4.3.3 The interface between RBC and CBI shall be based on the Standard Common Interface SCI-RBC of EULYNX Baseline Set 4 Release 4, which provides a common set of Messages and Commands (Orders)
- 6.4.3.4 RBC shall be able to receive from CBI the following set of Messages based on the EULYNX standard interface:
- Signal status;
 - Switch status;
 - TVP section status (axle counter system);
 - I/O generic element status: alarms, any other possible alarm received from the detection devices;
 - Emergency Stop Area (ESA) status;
 - Local Shunting Area (LSA) status;
 - Working Area (WA) status;
 - Route status.
- 6.4.3.5 [Note: in an ERTMS/ETCS L2 domain it may be the status of the “virtual signal” associated to an ETCS marker board]
- 6.4.3.6 RBC shall be able to send to CBI the following set of Messages based on the EULYNX standard interface:
- Train data;
 - Flank Protection status;
 - Signal cancelling reply;
 - Signal occupation;
 - Route cancelling reply;
 - Route occupation.
- 6.4.3.7 RBC shall be able to receive from CBI the following Commands based on the EULYNX standard interface:
- Signal cancelling;
 - Route cancelling.
- 6.4.3.8 RBC shall be able to send to CBI the following Commands based on the EULYNX standard interface:
- I/O generic element control;
 - Signal control;
 - Signal overlap control;
 - Route control.
- 6.4.3.9 Any additional message or command that for operational needs must integrate the previous list shall be exchanged via the EULYNX interface, if feasible, otherwise through a different safe communication interface.
- 6.4.3.10 The full set of messages/commands exchanged between RBC and CBI shall be defined during the design phase of TSCC Contractor.



6.4.4 Interface with Hazard Detection and Early Warning System (HDEWS)

- 6.4.4.1 The interlocking system may have an interface with HDEWS to trigger a safety response in the event of an external hazard (such as unexpected obstacle on the track, flood, ...).
- 6.4.4.2 Architecture of the interface between the interlocking system and HDEWS shall be determined by the TSCC Contractor to meet the safety and availability targets.
- 6.4.4.3 CBI shall interface the alarms raised by the Hazard Detection and Early Warning detectors via direct interface, or TMS depending on the outcome of the Hazard Analysis that shall be performed to define the level of mitigation required.
- 6.4.4.4 The complete list of safety hazards and HDEWS to be interfaced with the interlocking shall be defined by the TSCC Contractor during detailed design and safety analysis.

6.4.5 Interface with Digital Communications Network (DCN)

- 6.4.5.1 The Interlocking systems shall have redundant interface with the DCN to ensure secure and reliable transport of Interlocking data and to provide resilient interconnection between all CBI and Object Controllers
- 6.4.5.2 Eulynx protocol (i.e. RaSTA protocol as described in Eulynx set of specification shall be implemented between CBI and OCs, between CBI and adjacent CHSR CBIs, between CBI and RBC and between CBI and TMS (i.e. apply for each SCI type interface).

6.4.6 Interface with Wireless Communication Systems (WCS)

- 6.4.6.1 The WCS shall provide wireless communication between Trackside Worker Protection Devices, that are in a handheld ruggedized tablet form factor, and the Interlocking System. The FRMCS shall provide high priority for mission-critical (safety-critical) communications.

6.4.7 Interface with Network Time System (NTS)

- 6.4.7.1 The Interlocking system shall have redundant interface with the NTS for accurate current time synchronization.

6.4.8 Interface with Enterprise Asset Management System (EAMS)

- 6.4.8.1 The Interlocking System shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.

6.4.9 Interface with Low Voltage Power System

- 6.4.9.1 The interlocking equipment shall interface with the Low Voltage Power Distribution.
- 6.4.9.2 Power supply parameters of object controllers and wayside objects shall be derived from the proposed interlocking architecture and confirmed by design. Limitations of power supply parameters shall be introduced to minimize the risk of electrocution as per safety analysis of subsystems.
- 6.4.9.3 It shall be ensured that access by personnel to exposed live wires from the power supply of the Interlocking system is eliminated.
- 6.4.9.4 The power supply of CBI, OCs and wayside objects shall be galvanically isolated from each other to avoid interference.
- 6.4.9.5 The TSCC Contractor shall ensure compatibility with the power supply required to power all actuators and auxiliary sub-systems of turnouts.
- 6.4.9.6 The TSCC Contractor shall ensure compatibility with all subsystems with the Uninterrupted Power Supply system.



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied by the TSCC Contractor shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards.
- 7.1.2 All materials supplied shall be new and have sufficient grade and quality to meet the designed life requirements.

7.2 SW&HW Requirements

- 7.2.1 The CBI equipment is primarily railway specific equipment. The use of general commercial off-the-shelf (COTS) equipment as components, line replaceable units (LRUs) and modules to form CBI equipment or its support tools is accepted.
- 7.2.2 Design shall use standard materials and equipment, unless otherwise approved.
- 7.2.3 Equipment and materials shall meet industry standards, be available off the shelf unless otherwise approved, and supplied by established manufacturers.
- 7.2.4 Selection of equipment and materials shall consider:
 - Long-term costs;
 - Ease of construction;
 - Maintenance;
 - Readily available technical support.
- 7.2.5 The use of COTS equipment shall not prevent the CBI equipment or installations from meeting the overall requirements defined in this requirement document when it is applied as part of an integrated railway interlocking.
- 7.2.6 The Interlocking system shall be based on an existing approved product and must hold an approval certificate from one of the EU countries. Exceptions may apply to the EULYNX interfaces and are subject to Authority approval.
- 7.2.7 The certification of the CBI equipment used for the interlocking system shall include the following:
 - Declaration of conformity for regulatory compliance by the manufacturer;
 - Quality management system approval certificate covering design, manufacturing, and maintenance of the equipment;
 - Evidence of conformity to the nominated standards produced by the manufacturer;
 - Confirmation of the equipment being suitable for the purpose is supported by an ISA;
 - CFR 236 requirements;
 - A CHSR type approval for the application interlocking.
- 7.2.8 Conformity Assessment shall be compliant with standard EN ISO/IEC 17020.
- 7.2.9 The Interlocking system shall be structured into 3 layers in accordance with EN 50126/50716 and 50129 Standards:
 - Generic product: Safety automated and associated tools that can support the generic application.
 - Generic application: based on the CHSR operating and maintenance principles, the generic application corresponds to the functionalities of the system applicable to the entire railway line.



- Specific application: The configuration data for specific equipment and locations

7.2.10 The CBI shall manage the different main line stations as separate entities in such a way that:

- When data evolution is necessary for a station, the data of the other stations does not need to be modified or verified.
- The upload of the configuration of a specific station only requires the disabling of that station

7.2.11 Facilities shall be considered as separate entities in such a way that:

- When a track layout is modified within Facilities, the interlocking configuration data and logic related to the other Facilities does not need to be modified or verified, ensuring that the safety case of the other LFs is not affected.
- The upload of the configuration of specific Facilities only requires the disabling of those Facilities.

7.2.12 The architecture of the interlocking system shall allow the functioning of the system independently of the distance between CBI and OC, and between each OC.

7.2.13 The replacement of a failed OC or OC component shall not require shutting down the CBI while replacing the failed OC or OC component.

7.2.14 The replacement of a failed CBI, OC, or wayside asset shall not necessitate any software or hardware modifications of the equipment it is connected to.

7.2.15 Telecommunication parameters such as IP addresses shall be modified through a specific process which is separated from the data configuration process.

7.2.16 The OC shall be compatible with any future upgrade of wayside equipment requiring only minor software adaptation.

7.3 Associated Computer Tools

7.3.1 A set of test and commissioning tools shall be supplied. Among their functionalities, the following shall be implemented:

- The monitoring of the OC from any access point on the network: track movable elements (switch machines, derailleurs), displaying individual signal aspects, reinitializing axle counters once the authorization is granted by TMS.
- The simulation of any interface of the CBI such as OC, TMS and adjacent CBI.
- The testing of the CBI application logic

7.3.2 All tools provided by the TSCC Contractor shall operate on standard COTS computers using a standard Operating System (OS) to be validated by the Authority.

7.3.3 During the maintenance contract period, all IT tools provided to the Authority shall be supported by a commonly used OS, if the OS becomes unsupported. In case of a future OS update, the IT tools shall be updated accordingly to remain fully functional and shall not require any CBI interruption.

7.3.4 A set of tools allowing the delivery of control tables and the configuration of the data, its verification and validation shall be supplied.

7.3.5 The configuration data tools shall have a graphical interface reproducing the track layout.



7.4 Obsolescence

- 7.4.1 The TSCC Contractor shall guarantee the supply of any component (or an Authority approved alternative replacement component) of the CBI and Object controller, including the associated tools for a duration of 30 years from putting the system in operation.
- 7.4.2 The system conception shall be designed in such a way that the hardware obsolescence shall be managed without any impact on either the generic application or the specific application.

7.5 Interlocking Cable Requirements

- 7.5.1 CBI and OC cables shall be electromagnetic compatible considering the other cables and environment conditions.
- 7.5.2 All wires within a cable shall each have a unique visible identifier. The terminal each wire is connected to shall have corresponding visible identifiers.
- 7.5.3 The buried cables shall be protected against attacks by rodents and other animals.
- 7.5.4 All cables shall have protection for water immersion.

7.6 Cableway Requirements for Interlocking Cables

- 7.6.1 The TSCC Contractor shall assess if available capacity of cableways, manholes, ducts, and cable channels is sufficient for interlocking cables. In case if the capacity is not sufficient, the TSCC Contractor shall implement complementary cableways.



8 TOLERANCES

Not applicable to Interlocking System.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 General requirements related to the TSCC Contractor Scope of Work are defined in Scope of Work.

9.2 Specific Requirements

9.2.1 The interlocking system scope of supply and delivery shall include (not limited to):

- CBIs;
- Object Controllers and axle counter evaluators;
- Maintenance and Diagnostic Terminal (MDT);
- Wayside assets (signals, switch machines, axle counters, staff protection system, derailleurs, etc.);
- Displays /HMI's;
- Cabling and connectors;
- Racks;
- Software architecture including full definition of protocols used;
- SW licenses;
- Maintenance and testing tools;
- Auxiliary elements and gear (cases, bird repellent spikes, attachments, bindings, testing equipment, etc.);
- Spare parts.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in the scope of Work and Schedule 3.

12.2 Specific Requirements

12.2.1 The TSCC Contractor shall be responsible for the V&V of the interlocking system requirements and associated interfaces requirements described in this technical specification.

12.2.2 V&V activities include (not limited to):

- Generic Product V&V;
- Generic Application V&V;
- Specific Application V&V;
- Tools V&V.

12.2.3 The TSCC Contractor shall develop a simulation environment to conduct as much testing on the equipment as possible before the on-site testing phase. The main goals are as follows:

- Test CHSR Signaling Principles within the CBI;
- Integrate CBI with TMS, adjacent CBI, OC, RBC;
- Test of the EULYNX interfaces;
- Test operational scenarios.

12.2.4 The CBI simulation environment(s) shall confirm that the CHSR Signaling Principles are fully implemented on the prototypes, and this implementation complies with the expected behavior.

12.2.5 The TSCC Contractor shall propose and fulfil a set of functional and operational tests that comply with all the functionality of CHSR signaling principles. These tests scenario shall be accepted by the Authority.

12.2.6 The CBI simulation environment shall be used to conduct specific application data testing.



13 SUBMITTALS

13.1 General Requirements

13.1.1 The submittals required for the Interlocking system are defined in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor and related Suppliers, information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence Interlocking system reliability, availability and maintainability characteristics.



16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.



Schedule 5(j)

Medium Voltage Power System (MVPS) and Low Voltage Power System (LVPS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0014 – Medium Voltage Power System (MVPS) and Low Voltage Power System (LVPS)

Rev. 1.0

Authored:		12/22/2025
	Marc Benazech, Power Supply Lead	Date
Checked:		12/22/2025
	Intakhab (Indy) Modak, HV & Traction Power Lead (SME)	Date
Checked:		12/23/2025
	Bruno Comperat, Deputy Director of Rail Engineering	Date
Approved:		12/23/2025
	Ryan Scott, Director of Rail Engineering	Date
Released:		12/23/2025
	Amit Joshi, Configuration Manager	Date



Document Revision History – MVPS and LVPS Specifications**Second Edition****December 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition
1.0	December 2025	Second Edition for Addendum 2



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.1	GENERAL	6
2.2	TSI	6
2.3	STANDARDS	6
2.4	NATIONAL LAWS AND REGULATIONS	9
2.5	UIC RECOMMENDATIONS	9
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	10
4	SYSTEM DESCRIPTION	11
4.1	PURPOSE OF MVPS AND LVPS	11
4.2	DEFINITION OF MVPS AND LVPS.....	11
4.3	OPERATIONAL CONTEXT OF MVPS AND LVPS	11
4.4	DESIGN LIFE	13
5	SYSTEM REQUIREMENTS.....	14
5.1	GENERAL REQUIREMENTS.....	14
5.2	ENVIRONMENTAL REQUIREMENTS.....	14
5.3	FUNCTIONAL REQUIREMENTS.....	15
5.4	PERFORMANCE REQUIREMENTS.....	15
5.5	SECURITY AND CYBERSECURITY REQUIREMENTS.....	17
6	INTERFACES REQUIREMENTS.....	18
6.1	GENERAL REQUIREMENTS.....	18
6.2	THIRD PARTIES INTERFACES.....	18
6.3	EXTERNAL INTERFACES – STATIONS CONTRACTORS	18
6.4	EXTERNAL INTERFACES – FACILITIES CONTRACTORS	19
6.5	INTERNAL INTERFACES	19
7	MATERIALS, PRODUCT, AND COMPONENTS REQUIREMENTS	21
7.1	GENERAL REQUIREMENTS.....	21
7.2	LV DISTRIBUTION	21
7.3	LV CABLES.....	22
7.4	UNINTERRUPTABLE POWER SUPPLY SYSTEM	24
7.5	BACK-UP GENERATOR.....	25
7.6	OCC POWER SUPPLY	25
7.7	34.5kV MV SYSTEM - PRODUCTION AND DISTRIBUTION	26
7.8	34.5kV MV SYSTEM – FIELD STRUCTURE AND CABLE LINKS.....	26
7.9	34.5kV/LV DISTRIBUTION TRANSFORMERS.....	28
7.10	LV PRODUCTION ON REMOTE SITES.....	28
8	TOLERANCES	29
9	SCOPE OF SUPPLY AND DELIVERY	30
9.1	GENERAL REQUIREMENTS.....	30



9.2	SPECIFIC REQUIREMENTS	30
10	MANUFACTURING.....	31
10.1	GENERAL REQUIREMENTS.....	31
11	INSTALLATION AND INTEGRATION.....	32
11.1	GENERAL REQUIREMENTS.....	32
11.2	SPECIFIC REQUIREMENTS	32
12	TESTING & ACCEPTANCE	33
12.1	GENERAL REQUIREMENTS.....	33
13	SUBMITTALS.....	34
13.1	GENERAL REQUIREMENTS.....	34
14	QUALITY MANAGEMENT.....	35
14.1	GENERAL REQUIREMENTS.....	35
15	ADDITIONAL INFORMATION REQUESTED	36
15.1	GENERAL REQUIREMENTS.....	36
16	LOGISTICS	37
16.1	GENERAL REQUIREMENTS.....	37



1 INTRODUCTION

1.1 Scope of the technical specification

- 1.1.1 The scope of this Technical Specification is to define the Authority Requirements for the Medium Voltage Power System and Low Voltage Power System, hereinafter: MVPS and LVPS.
- 1.1.2 The functional architecture of MVPS and LVPS is presented in Appendix A.
- 1.1.3 The requirements are formulated using the following words and their meanings:
 - **“Shall”**: Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure).
 - **“Should”**: Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents.
 - **“Must”**: Indicates an obligation or a mandatory requirement.
 - **“May”**: Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines and specifications provided in this chapter for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning and training.

2.1.2 All generic standards to be used are provided in: Schedule 16.

2.2 TSI

2.2.1 The applicable TSIs are listed below:

ID	Standard	Title
[R1]	ENE TSI	COMMISSION REGULATION (EU) No 1301/2014 of 18 November 2014 on the technical specifications for interoperability relating to the 'energy' subsystem of the rail system in the Union including the Commission Implementing Regulation (EU) 2018/868 of 13 June 2018, Commission Implementing Regulation (EU) 2019/776 of 16 May 2019 and Commission Implementing Regulation (EU) 2023/1694 of 10 August 2023
[R2]	SRT TSI	Commission Regulation (EU) No 1303/2014 of 18 November 2014 - concerning the technical specification for interoperability relating to 'safety in railway tunnels' of the rail system of the European Union including commission regulation (EU) 2016/912 of 9 June 2016 L 153 28 10.6.2016 and commission implementing regulation (EU) 2019/776 of 16 May 2019

TABLE 27 LIST OF TSI AND REGULATIONS

2.3 Standards

2.3.1 The relevant standards to be used for MVPS and LVPS are listed below:

ID	Standard	Title
[R3]	IEC 17000	Conformity assessment — Vocabulary and general principles
[R4]	ISO 50001	Energy management systems - Requirements with guidance for use
[R5]	EN 13501-6	Fire classification of construction products and building elements – Classification using data from reaction to fire tests on power, control and communication cables
[R6]	EN 50110-1	Operation of electrical installations - Part 1: General requirements
[R7]	EN 50160	Voltage characteristics of electricity supplied by public distribution systems
[R8]	EN 50178	Electronic equipment for use in power installations
[R9]	EN 50200	Method of test for resistance to fire of unprotected small cables for use in emergency circuits.



ID	Standard	Title
[R10]	EN 50266	Common test methods for cables under fire conditions - test for vertical flame spread of vertically mounted bunched wires or cables part 2-4: procedures.
[R11]	EN 50267	Common test methods for cables under fire conditions - tests on gases evolved during combustion of materials from cables - part 2-3: procedures - determination of degree of acidity of gases for cables by determination of the weighted average of ph and conductivity.
[R12]	EN 50268	Common test methods for cables under fire conditions. Measurement of smoke density of cables burning under defined conditions. Procedure.
[R13]	EN 50362	Method of test for resistance to fire of larger unprotected power and control cables for use in emergency circuits
[R14]	EN 50399	Common test methods for cables under fire conditions - Heat release and smoke production measurement on cables during flame spread test - Test apparatus, procedures, results
[R15]	EN 50575	Cable Compliance Standards
[R16]	EN 600068-3-3	Environmental testing-Part 3: guidance, Seismic test methods for equipment
[R17]	IEC 60050	International Electrotechnical Vocabulary
[R18]	IEC 60085	Electrical insulation - Thermal evaluation and designation
[R19]	IEC 60255	Electrical Relays
[R20]	IEC 60228	Conductors of insulated cables
[R21]	IEC 60332-1	Tests on electric and optical fiber cables under fire conditions - Part 1-2: Test for vertical flame propagation for a single insulated wire or cable - Procedure for 1 kW pre-mixed flame.
[R22]	IEC 60322-3/C	Tests on electric and optical fiber cables under fire conditions - Part 3-24: Test for vertical flame spread of vertically mounted bunched wires or cables.
[R23]	IEC 60364 series	Low-voltage electrical installations
[R24]	IEC 60479-1	Effects of current on human beings and livestock, Part 1: General aspects.
[R25]	IEC 60529	Degrees of protection provided by enclosures (IP Code)
[R26]	IEC 60670	Boxes and enclosures for electrical accessories for household and similar fixed electrical installations



ID	Standard	Title
[R27]	IEC 60754-1	Test on gases evolved during combustion of materials from cables - Part 1: Determination of the halogen acid gas content
[R28]	IEC 60754-2	Test on gases evolved during combustion of materials from cables - Part 2: Determination of acidity (by pH measurement) and conductivity.
[R29]	IEC 60811	Electric and optical fiber cables - Test methods for non-metallic materials
[R30]	IEC 60947	Low-voltage switchgear and controlgear
[R31]	IEC 60950--1	Information technology equipment – Safety.
[R32]	IEC 61000-3-11	Electromagnetic compatibility (EMC) - Part 3-11: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems - Equipment with rated current ≤ 75 A and subject to conditional connection
[R33]	IEC 61000-3-12	Electromagnetic compatibility (EMC) - Part 3-12: Limits - Limits for harmonic currents produced by equipment connected to public low-voltage systems with input current > 16 A and ≤ 75 A per phase
[R34]	EN 61000-6	Electromagnetic compatibility (EMC) - Part 6: Generic Standards
[R35]	IEC 61034	Measurement of smoke density of cables burning under defined conditions
[R36]	IEC 61439	Low-voltage switchgear and controlgear assemblies
[R37]	IEC EN 62040-1	Uninterruptible power systems (UPS) - Part 1: General and safety requirements for UPS.
[R38]	IEC 62208	Empty enclosures for low-voltage switchgear and controlgear assemblies
[R39]	IEC 62262	Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)
[R40]	IEC 62282 Series	Fuel cell technologies
[R41]	FCC CFR47 Part 15	Radio Frequency Devices, Subpart A, B.
[R42]	ETSI EN 300 019: 2-1 (Class 1.2), 2-2 (Class 2.2) & 2-3 (Class 3.2) Equipment	Equipment Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment.
[R43]	EN 300 396 V.1.6.1	Equipment Engineering (EE); Telecommunication network equipment; Electromagnetic Compatibility (EMC) requirements.

TABLE 28 LIST OF APPLICABLE STANDARDS

2.4 National Laws and Regulations

2.4.1 The version of the following indicative national laws and regulations shall be applied. The TSCC Contractor is responsible for the compliance to Federal and State legislation and the correct application of all regulations.

No	Standard	Description
[R44]	California Electrical Code (CEC)	Based on the National Electrical Code (NEC), it regulates the installation and grounding of electrical systems.
[R45]	Title 24, Part 3, California Code of Regulations	Contains specific standards for electrical installations.
[R46]	California Building Standards Code	Regulates the use of cables in construction, including safety and performance requirements.
[R47]	National Electrical Code (NEC)	Although a national code, it is adopted by California to regulate electrical cables.
[R48]	California Fire Code	Establishes standards for fire prevention, including alarm and suppression systems.
[R49]	Title 19, California Code of Regulations	Fire safety in buildings and public facilities.
[R50]	California Public Utilities Commission (CPUC) Regulations	Oversees telecommunications services and their infrastructure.
[R51]	California Building Standards Code	Includes standards for telecommunications installations in buildings.
[R52]	California Public Utilities Code	Regulates railway and public transportation systems.
[R53]	Federal Railroad Administration (FRA) Regulations	Although federal, these regulations also apply in California for railway systems.
[R54]	California Independent System Operator (CAISO) Tariff	Regulates grid management and interoperability with energy providers.

TABLE 3 LIST OF APPLICABLE CALIFORNIAN REGULATIONS

2.5 UIC Recommendations

Not applicable to the MVPS and LVPS.



3 TERMS, DEFINITIONS, AND ABBREVIATIONS

- 3.1.1 All the terms, definitions, and abbreviations are provided in the Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of MVPS and LVPS

4.1.1 The MVPS and LVPS shall provide a safe, high-quality and reliable power supply for the TSCC systems and subsystems and other consumers as defined in Chapter 4.3.

All references to 34.5 kV in this Specification are indicative only. In the event that upstream clean energy sources are deferred, the TSCC Contractor shall verify and confirm the actual service voltage(s) in coordination with the serving utility during design development. The TSCC Contractor shall ensure that all system architecture, equipment ratings, insulation levels, protection settings, and interface requirements are adapted as necessary. This shall maintain reliable and safe operation of the traction and non-traction power systems, including MVPS and LVPS.

4.1.2 The MVPS and LVPS shall be deployed along the alignment of CHSR, to include:

- System Equipment Locations along the main line
- Facilities (TCF, LMF, HMF, MOWFs)
- Passenger Stations (Merced, Madera, Kings Tulare, Bakersfield)
- Traction Power SubStations (TPSS)
- Operation Control Center (OCC)
- Other locations identified as part of the TSCC Contractor's scope

4.2 Definition of MVPS and LVPS

4.2.1 The MVPS consists of the following components and systems.

- 34.5 kV cable links connected to the Point of Common Coupling;
- 34.5kV cable rings;
- Ring Main Units (RMUs);
- Three-phase step-down transformers

4.2.2 The LVPS consists of the following components and systems.

- LV production;
- LV switchboards;
- Uninterruptible Power Supply Systems;
- Associated secondary feeders to technical buildings and auxiliary systems.

4.3 Operational context of MVPS and LVPS

4.3.1 MVPS Supply Sources

4.3.1.1 The MVPS, shall be supplied at the MV level of the power structure by two independent medium voltage feeder links originating from the 34,5kV busbar(s) located in the TPSS.

4.3.1.2 The 34.5 kV switchgear at the TPSS shall serve as the primary Point of Common Coupling (PCC) between the traction and non-traction power systems.

4.3.2 Wayside Equipment Location

4.3.2.1 At wayside equipment location, the LVPS system is provided with:

- One or two RMUs connected to the MV rings of the MVPS and MV / LV transformers.



- or alternatively for remote areas featuring a power consumption under 10kVA, one connection to the OCS and a UPS system with an extended autonomy can be proposed to the authority.

4.3.3 Passenger stations

- 4.3.3.1 At stations, the TSCC Contractor shall provide two Ring Main Units connected to the MVPS.
- 4.3.3.2 Stations LV Power system is connected to the RMUs, the MV / LV Transformers are in the stations contractor scope.
- 4.3.3.3 TSCC LVPS to feed TSCC equipment is connected to the stations LV main switchboards provided by the stations contractor.

4.3.4 Facilities

- 4.3.4.1 At facilities, the TSCC Contractor shall provide two Rings Main Units connected to the MVPS.
- 4.3.4.2 Facilities LV Power system is connected to the RMU, the MV / LV Transformers are in the facilities contractor scope.
- 4.3.4.3 TSCC LVPS to feed TSCC equipment in facilities is connected to the facilities LV main switchboards provided by the facilities contractor.

4.3.5 Traction substations, switching stations and paralleling switchyards

- 4.3.5.1 At Traction substations, switching stations and paralleling switchyards, the LVPS system is provided with RMU(s) (two in substations and switching stations, one in paralleling switchyards) connected to the MV rings of the MVPS and MV / LV transformers.

4.3.6 Power Consumers

- 4.3.6.1 During the design phase, the TSCC Contractor shall perform the power balance for each MVPS and LVPS location of CHSR.
- 4.3.6.2 Based on the power balance, the TSCC Contractor shall perform an analysis of the issued connection technical conditions for MVPS and LVPS sites, and shall state:
 - a confirmation of connection technical conditions implementation;
 - or a justification for the connection technical conditions amendment;
 - or a justification for the new connection technical conditions request;
 - or a justification for the case when a connection point is not necessary.
- 4.3.6.3 The TSCC shall retain responsibility for overall integrated design, modelling, and studies of the electrical system downstream of the PCC, as defined in the traction power specification.
- 4.3.6.4 The TSCC Contractor shall provide all necessary load profiles, connected equipment data, and electrical parameters of the non-traction systems to be connected to the 34.5 kV network, in order for the detailed system modelling, calculations, studies, and integrated power supply design of the overall electrical network to be performed by TSCC as defined in the traction specification.

4.3.7 Class of the loads supplied by the MVPS and LVPS

- 4.3.7.1 The TSCC Contractor shall design the MVPS and LVPS to supply the systems equipment in compliance with the consumer load class and consumer power supply requirement.
- 4.3.7.2 The LVPS shall provide power supply to all TSCC subsystems in all locations.
- 4.3.7.3 The following classification of loads is defined as below:



- Emergency Loads shall be connected to two separate and redundant power supplies and UPS (with minimum 12 hour battery backup) unless they are located in a remote site and feature a power consumption under 10kVA: then a single power supply and a UPS with an extended autonomy can be proposed instead to the Authority.
- Essential Loads shall be connected to two separate and redundant power supplies, unless they are located in a remote site and feature a power consumption under 10kVA: then a single power supply and a UPS with an extended autonomy can be proposed instead to the Authority.
- Non-essential loads shall be connected to one power supply source.

4.3.7.4 The following systems shall be considered as Emergency Loads:

- ETCS
- Interlocking
- Traffic Management System (TMS)
- Hazard Detection and Early Warning System (HDEWS)
- Wireless Communication System (except the Passenger Wi-Fi System)
- Digital Communication Network (DCN)
- Network Timing System (NTS)
- Enterprise Asset Management System (EAMS)
- CCTV
- Electronic Access Control System (EACS)
- Telephony System
- Cybersecurity
- Public Address and Customer Information System (PACIS)
- Integrated Control and Supervision System (ICSS)
- Fire Protection System (FPS)
- Power SCADA
- All auxiliaries supplying control and monitoring equipment at traction substations, switching stations, and paralleling switchyards shall be considered as emergency loads.
- All TSCC equipment located at the OCC Control Room and OCC Equipment Rooms.
- Intrusion Detection

4.3.7.5 The following systems shall be considered as Emergency Loads:

- Switch motors
- Substations, shelters, switching stations, and paralleling switchyards utilities (lighting, HVAC, household sockets)

4.3.7.6 The loads which do not belong to the TSCC systems shall not be provided with power supply from the LVPS UPS system.

4.4 Design life

4.4.1 The design life of the MVPS and LVPS equipment shall be 30 years in compliance with the requirements of the CHSR Design Criteria Manual, Chapter 2 Basis of Design, section 2.2.2.2.2, Table 2-1.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

- 5.1.1 The MVPS and LVPS systems shall be future proof, based on the most up-to-date and proven technology.
- 5.1.2 Proven technology means that the MVPS and LVPS shall be based on components that have been proven in similar service for at least five years and configured in an arrangement that has been demonstrated in a report to provide the required performance.
- 5.1.3 Low voltage levels of the LV distribution system shall follow IEC 60038.
- 5.1.4 The voltage level of the LV distribution system shall be selected considering the distance and the power required by the consumer.
- 5.1.5 The voltage drop shall comply with the requirements of applicable standards and regulations.
- 5.1.6 Neutral conductors shall be of the same size of the phase conductors to avoid overheating due to intrinsic residual harmonic content and unbalances in the system.
- 5.1.7 The MVPS and LVPS Power Supply system shall be designed such that it is possible to upgrade it in the future, by installation of the additional equipment only and without necessity of the replacement of initially supplied equipment; therefore, in addition to the spare circuit breakers, a 30% space for circuit breaker future installation shall be foreseen within a LV switchboard.
- 5.1.8 Adequate space shall be provided at TSCC locations for the future provision of MVPS and LVPS equipment.
- 5.1.9 As a minimum, the following calculations shall be performed, in compliance to the relevant standards and regulations, and submitted to the Authority for review:
 - Detailed load analysis for each circuit, with accurate consideration of the power factor, load factor and simultaneity factor;
 - Cable sizing calculation;
 - UPS power balance;
 - Back-up generator set and fuel storage calculation including autonomy time;
 - Battery sizing calculation, accompanied by evidence of discharge/recharge times;
 - Power system harmonic impacts/assessments;
 - Step and touch voltage analyses;
 - Electrical equipment heat dissipation estimation.

5.2 Environmental Requirements

- 5.2.1 MVPS and LVPS systems shall meet the environmental requirements described in the applicable regulations.
- 5.2.2 MVPS and LVPS equipment shall be designed to operate satisfactorily under all variations of load, pressure, UV light, ozone, and temperature that may occur under normal and abnormal conditions.
- 5.2.3 IP rating (according to EN 60529) shall be at least IP31 for indoor MVPS and LVPS equipment and at least IP54 for outdoor MVPS and LVPS equipment.
- 5.2.4 The MVPS and LVPS equipment shall be protected against pests and local fauna.



5.3 Functional Requirements

- 5.3.1 The TSCC Contractor shall implement energy efficiency optimization solutions with the support of intelligent metering function and plant automation.
- 5.3.2 Every switchboard shall be equipped with data acquisition devices to allow the remote monitoring of the health parameters of the system, like phase to phase and phase to ground voltages, phase currents, power factor, energy consumptions, UPS parameters, other relevant parameters.
- 5.3.3 Remotely controlled switching devices shall be able to be operated from:
- From OCC by dedicated workstation of the Power SCADA (for MVPS) and of the ICSS (for LVPS)
 - Locally from the local HMI and manual operation directly from the equipment.
- 5.3.4 Under normal operating conditions, the MVPS and LVPS system shall be monitored and operated from a dedicated workstation of the Power SCADA and ICSS system in the OCC.
- 5.3.5 The TSCC Contractor shall implement the programmable logic controller / remote terminal unit / gateways needed for the local control and further data exchange with the TSCC Power SCADA and ICSS.
- 5.3.6 The TSCC Contractor shall ensure provision of the monitoring data (operating states, alarms, malfunctions, power failures, etc.) and control function of the LV distribution components including switching and metering devices to the ICSS system.
- 5.3.7 The TSCC Contractor shall ensure provision of the monitoring data and control function of the Uninterruptable Power Supply system components including batteries and chargers to the ICSS system.
- 5.3.8 Data to be considered for the supervision system are, but not limited to: operation mode, internal UPS temperature, bypass state, battery charging level, battery voltage and impedance, battery room temperature, alarms, malfunctions, power failures, etc.
- 5.3.9 The TSCC Contractor shall ensure provision of the monitoring data (operating states, alarms, malfunctions, power failures, etc.) and control function of the back-up generators to the ICSS system.
- 5.3.10 Under abnormal operating conditions, it shall be possible to operate the MVPS and LVPS system locally.
- 5.3.11 Local HMIs or interface ports shall be available at each location to provide MVPS and LVPS operators with a local control device.
- 5.3.12 The TSCC Contractor shall provide proper protection coordination, to ensure a high level of vertical and horizontal selectivity and to prevent healthy circuits and loads from being affected by a single fault in a faulty circuit or load.
- 5.3.13 Cables, busbar, electrical equipment and devices shall be protected against fault and overload effect in compliance with IEC 60364 and other relevant standards.
- 5.3.14 Energy metering functionality shall be implemented, based on the intelligent metering devices to be provided in each switchboard.
- 5.3.15 The MVPS and LVPS shall provide timestamped measurement data to the ICSS and Power SCADA covering the metering: energy, power, currents and voltages, power factor, etc.

5.4 Performance Requirements

5.4.1 General

- 5.4.1.1 The TSCC Contractor shall ensure the redundancy of the MVPS and LVPS system for the essential and emergency loads.



- 5.4.1.2 The MVPS and LVPS system design shall ensure that redundant cables and equipment are adequately separated or protected so that a single failure of any element of the power supply system does affect the operation or result in the failure of any other MVPS and LVPS element, thus resulting in the total loss of power.
- 5.4.1.3 The MVPS and LVPS design shall ensure that redundant cables and equipment are adequately separated or protected so that the probability of an incident external to the MVPS and LVPS affecting the operation of the MVPS and LVPS or resulting in a total loss of power distribution to any part of the network, is minimized.
- 5.4.1.4 The power supply and distribution system and its elements shall be designed to revert to safe modes under failure conditions. The TSCC Contractor shall employ high quality components, proven systems, redundancy, interlocking, checking devices and other techniques to achieve this goal.
- 5.4.1.5 The power quality of the MVPS and LVPS shall comply with EN 50160.
- 5.4.1.6 The averaged power factor measured at the Point of Common Coupling shall comply with the local legislation, as referred in Section 2.
- 5.4.1.7 The TSCC Contractor, if necessary, shall supply power factor correction equipment required to prevent incurred financial penalties under operation.
- 5.4.1.8 The TSCC Contractor shall develop the MVPS and LVPS architecture ensuring compliance to the MVPS and LVPS RAMS requirements.
- 5.4.1.9 The TSCC Contractor shall develop the MVPS and LVPS architecture ensuring there are no obstacles for future connection to Solar PV and Battery Energy Storage System (BESS) equipment.

5.4.2 Safety Requirements

- 5.4.2.1 The MVPS and LVPS shall comply with the safety requirements defined in Authority safety documentation.
- 5.4.2.2 The TSCC Contractor shall consider the MVPS and LVPS safety as an integral part of the system design. The MVPS and LVPS safety shall be emphasized at the start of design so that potential problems can be identified, assessed and resolved with minimal impact.
- 5.4.2.3 The MVPS and LVPS design and operational procedures shall include incorporation of fail-safe principles where failures would otherwise disable the system or cause human injury, damage to equipment, or inadvertent operation of critical equipment.
- 5.4.2.4 The MVPS and LVPS design shall include locating equipment so that access to the MVPS and LVPS equipment by the required personnel during operation, maintenance, or repair shall not require exposure to hazards, such as entrapment, chemical burns, electric shock, cutting edges, or toxic atmospheres.
- 5.4.2.5 The MVPS and LVPS system design and operational procedures shall include providing suitable warning and caution notes in operation, assembly, maintenance and repair instructions, and distinctive markings on hazardous components, equipment, or facilities for personnel protection.
- 5.4.2.6 Energy equipment shall be placed in locations where it does not affect the movement of people.
- 5.4.2.7 To provide power supply disconnection in case of fire in TSCC technical rooms, proper emergency buttons shall be provided to isolate the TSCC electrical systems.

5.4.3 RAM Requirements

- 5.4.3.1 The MVPS and LVPS shall comply with the RAM requirements in Schedule 1.
- 5.4.3.2 The MVPS and LVPS and related equipment shall be of modular design and of the error-proofing principles.



- 5.4.3.3 The MVPS and LVPS design and implementation shall be able to contend with any single failure at any level of the power structure with no effect on train operation.
- 5.4.3.4 Two independent power supplies shall be provided, to ensure the reliability of power supply of the Essential Loads.
- 5.4.3.5 Two independent power supplies and a UPS system shall be provided to ensure the reliability of power supply of the MVPS and LVPS Emergency Loads, unless they are located in remote areas and feature a power consumption under 10kVA, then a single power supply and a UPS with an extended autonomy can be proposed to the authority.
- 5.4.3.6 In case of failure of one of the two power supplies, the other power source shall take over and provide power supply to all the MVPS and LVPS Essential and Emergency Loads.
- 5.4.3.7 Automatic changeover function shall be implemented for the essential and emergency AC loads. For emergency loads no power supply interruption is allowed during the changeover.
- 5.4.3.8 Dual busbars with anti-backflow diodes, or chargers featuring intrinsically the anti-backflow function, shall be implemented for the essential and emergency DC loads.
- 5.4.3.9 Power lines outgoing from the UPS system should be of IT system (isolated neutral) to guarantee the continuity of the power supply to MVPS and LVPS Emergency Loads. In case a different system is used, the MVPS and LVPS design shall ensure that any single failure does not cause the loss of power for emergency loads.
- 5.4.3.10 The MVPS and LVPS equipment layout shall be standardized as much as practical as per location type.
- 5.4.3.11 Adequate accessibility and maneuverability space for installation, testing, operation, inspection, maintenance, repair and replacement for all MVPS and LVPS equipment shall be provided.
- 5.4.3.12 The standards to be applied for all MVPS and LVPS equipment shall be as per this specification and those specified in Schedule 16.
- 5.4.3.13 Each electrical assembly shall be identified by an appropriately sized label which clearly indicates the functional units and their electrical characteristics.
- 5.4.3.14 The main circuit breaker of a TSCC system or subsystem shall be indicated with a specific label, to support the power supply disconnection procedure in case of emergency or maintenance.
- 5.4.3.15 The TSCC Contractor shall specify each subcircuit on the switchboard single line diagram and allocate supply phases of each single-phase circuit to balance the load across the phases.

5.5 Security and Cybersecurity Requirements

- 5.5.1 The MVPS and LVPS shall be fully compliant with CHSR cybersecurity policies and the requirements specified in the document Technical Specification - Cybersecurity.



6 INTERFACES REQUIREMENTS

6.1 General Requirements

6.1.1 Interfaces are classified as below:

- Third Party interfaces: interfaces between TSCC systems and a system or systems provided by a Third Party (excluding CHSR contractors)
- External interfaces: interface between TSCC systems and a system or systems provided by CHSR contractors (Civils packages, stations contractor, facilities contractor, Solar PV and BESS contractors)
- Interfaces between systems within the TSCC scope

6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.

6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.

6.2 Third Parties Interfaces

No Third-Party interfaces identified at this stage.

6.3 External Interfaces – Stations contractors

6.3.1 The TSCC Contractor shall install MVPS and LVPS equipment in stations.

6.3.2 The TSCC Contractor shall provide to the stations contractor:

- Equipment dimensions
- Equipment clearances requirements
- Equipment mounting and fixings requirements
- Cable routes/containment requirements
- Equipment loadings
- Installation and maintenance requirements
- Equipment heating loads
- Equipment cooling loads
- Equipment hydraulic requirements

6.3.3 To be provided by stations contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:

- Room dimensions and layouts
- Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
- Room raised floor system
- Delivery access routes.
- Maintenance access routes

6.3.4 The TSCC Contractor shall manage the electrical interfaces for the connection of power supply point LV Switchboards provided by TCSS in stations with LV power systems provided by stations contractors.

6.3.5 The TSCC Contractor shall consider that, with the aim of allowing the stations contractors to consider the TSCC load in the sizing of the station power supply system, a preliminary power balance shall be delivered to other contractors as a mean of interface resolution.



- 6.3.6 Based on the TSCC design development, the TSCC Contractor shall perform necessary coordination and collaboration with the stations contractors to ensure on time implementation of the related interfaces.

6.4 External Interfaces – Facilities Contractors

- 6.4.1 The TSCC Contractor shall install MVPS and LVPS equipment in facilities.
- 6.4.2 The TSCC Contractor shall provide to the facilities contractor:
- Equipment dimensions
 - Equipment clearances requirements
 - Equipment mounting and fixings requirements
 - Cable routes/containment requirements
 - Equipment loadings
 - Installation and maintenance requirements
 - Equipment heating loads
 - Equipment cooling loads
 - Equipment hydraulic requirements
- 6.4.3 To be provided by stations contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:
- Room dimensions and layouts
 - Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
 - Room raised floor system
 - Delivery access routes.
 - Maintenance access routes
- 6.4.4 The TSCC Contractor shall manage the electrical interfaces for the connection of power supply point LV Switchboard provided by TCSS in facilities with LV power systems provided by facilities contractors.
- 6.4.5 The TSCC Contractor shall consider that, with the aim of allowing the facilities contractors to consider the TSCC load in the sizing of the facility power supply system, a preliminary power balance shall be delivered to other contractors as a mean of interface resolution.
- 6.4.6 Based on the TSCC design development, the TSCC Contractor shall perform necessary coordination and collaboration with the facilities contractors to ensure on time implementation of the related interfaces.

6.5 Internal Interfaces

6.5.1 LV Power Supply for TSCC Systems

- 6.5.1.1 The TSCC Contractor shall provide a LV Power Supply to the following systems.
- Train Control Systems
 - Interlocking
 - ETCS
 - Traffic Management System
 - Telecommunications Systems
 - Integrated Control and Supervision System
 - Digital Communication Network
 - Wireless Communication Systems



- Telephony
- Network Timing System
- CCTV
- Electronic Access Control System
- Public Address and Customer Information System
- Hazard Detection and Early Warning System
- Equipment building and housings electromechanical equipment, including lighting, HVAC and Fire Protection Systems.

6.5.2 Network Timing System (NTS)

6.5.2.1 The MVPS and LVPS shall interface with the NTS for time distribution and precise synchronization.

6.5.3 Digital Communication Network (DCN)

6.5.4 The MVPS and LVPS shall have a redundant interface with the Digital Communication Network (DCN) for the connectivity of MVPS and LVP system.

6.5.5 Interface with Integrated Control and Supervisory System (ICSS)

6.5.5.1 The LVPS shall integrate with the ICSS to enable end-to-end monitoring, fault management, and performance reporting. This integration shall support standard interfaces and protocols to ensure compatibility with ICSS subsystems and allow for centralized visibility and control within the broader operational management environment.

6.5.6 Interface with Power SCADA

6.5.6.1 The MVPS shall integrate with the Power SCADA to enable end-to-end monitoring, fault management, and performance reporting. This integration shall support standard interfaces and protocols to ensure compatibility with ICSS subsystems and allow for centralized visibility and control within the broader operational management environment.

6.5.7 Interface with Enterprise Asset Management Systems (EAMS)

6.5.7.1 The MVPS and LVPS shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities, including power consumption.

6.5.8 Physical integration in traction substations, switching stations and paralleling switchyards and wayside

6.5.8.1 The MVPS and LVPS shall interface with the TSCC equipment housings and buildings to ensure proper MVPS and LVPS integration.

6.5.8.2 The MVPS and LVPS shall interface with the cable containment system of the TSCC equipment building to ensure proper pathway for the MVPS and LVPS cables.

6.5.9 Traction Power System

6.5.9.1 The MVPS and LVPS shall interface its MV cable links with the switchgear of the Point of Common Connection in the traction substations.

6.5.9.2 The MVPS shall provide for the cable terminations to the switchgear of the Point of Common Connection.



7 MATERIALS, PRODUCT, AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied shall conform to the requirements and test methods of the relevant standards and regulations.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the designed life requirements.
- 7.1.3 Electrical equipment and cables shall be de-rated according to the manufacturer's recommendations, or applicable codes and standards, for the design conditions.
- 7.1.4 The MVPS and LVPS equipment shall be complete with all parts and accessories or material which are useful for efficient operation of the MVPS and LVPS components. Such accessories and materials shall be deemed to be within the scope of this specification whether specifically mentioned or not.
- 7.1.5 The supply shall include all supporting structures, embedded parts, auxiliary equipment, mechanical linkages, auxiliary circuits wiring, interlocking devices necessary for their efficient operation. All such parts and accessories shall be deemed to be within the scope of this specification whether specifically mentioned or not.
- 7.1.6 TSCC power equipment shall be designed ensuring an adequate protection from rodent actions. Additionally, the TSCC Contractor shall implement any measures to provide rodent protection such as expanding foam..

7.2 LV Distribution

- 7.2.1 Low-voltage AC switchboards shall be used for distribution of AC power.
- 7.2.2 Low voltage switchboards shall be compliant with the relevant standard (EN 61439 series).
- 7.2.3 The main LV switchboard shall have a minimum form of segregation 2 to facilitate maintenance activities.
- 7.2.4 The LV switchboard connected to the Local Facility power supply system / TPSS facility power supply system, shall be provided with all the necessary metering equipment, aligned to the Local Facility / TPSS facility requirement, circuit breakers and load-break isolators/switches, including current/voltage transformers, energy meters, cabinets, fusegear and switchgear as required.
- 7.2.5 All LV equipment, directly connected to the Local Facility power supply system / TPSS facility power supply system, shall be suitable for use at the voltage and short-circuit rating at the connection point and not less than the tabulated short circuit rating tabulated in the Local Facility power supply system / TPSS facility power supply system requirements and relevant IEC standard.
- 7.2.6 The LV switchboard connected to Local Facility power supply system / TPSS facility power supply system shall be provided with the required protection system and shall be coordinated with the Local Facility / TPSS facility.
- 7.2.7 Electrical and mechanical interlocks shall be provided between the incomers and the bus coupler to avoid parallel operation of the external dual supply. Automatic and manual operation shall be possible.
- 7.2.8 As a minimum, the incoming switching devices to each LV switchboard, the outgoing switching devices for the UPS, major consumers (like point heating, for instance) and consumers that do not belong to the TSCC systems (cross border digital infra, for instance) shall be remotely controlled as required in chapter 5.3.



- 7.2.9 A Surge Protection Device system shall be provided, as required, to protect against induced voltages in MV (optional scope) and LV distribution networks arising from lightning strikes and grid-related surges (e.g. faults, switching of equipment).
- 7.2.10 Surge Protection Devices shall be located as close as possible to the system/equipment being protected and/or the main earth terminal of the system/equipment protected in accordance with IEC 60364.
- 7.2.11 Cable connection to Surge Protection Devices shall be kept as short as possible to avoid excessive voltage drop under surge conditions in accordance with IEC 60364
- 7.2.12 Insulation monitoring devices shall be provided for IT systems.
- 7.2.13 LV switchboard main busbars shall be thermally dimensioned for an intensity equal to twice the size of the general switches of the respective section, while the secondary distribution busbars shall be thermally dimensioned for an intensity equal to 1.5 times that of the general switches of the respective section.
- 7.2.14 Cables within LV switchboards shall be identified by means of specific identification plates, installed at the ends of each cable for their univocal identification; as well as the terminal blocks to which the individual cables abut, of the modular type on a unified guide, shall be numbered corresponding to the electrical diagrams and suitably separated with insulating diaphragms between the various users.
- 7.2.15 All units of the distribution boards, including supporting frames, shall be made to be rust-proof with at least two coats of primary paint applied on the interior and exterior surface and followed by a finishing coat.
- 7.2.16 The circuit breaker changeover switch shall be arranged neatly and mounted on the panel which shall be of standard design and provided within a hinged cover to facilitate inspection.
- 7.2.17 The indicating lamps of the distribution boards shall be of low power consumption; they shall be interchangeable and replaceable from the front of the panel.
- 7.2.18 All metallic parts of the panel shall be connected to the main earth loop. Suitable earth terminals for this purpose shall be provided.
- 7.2.19 Short circuit protection devices for TSCC power equipment shall be provided according to applicable standards to avoid development of the fire.
- 7.2.20 Design (calculations of cable sizes, equipment loading etc.), installation of the TSCC power cables shall comply with International Standards and the good engineering practices to guarantee their proper functioning.

7.3 LV Cables

- 7.3.1 LV cables shall comply with "Commission Regulation (EU) No. 305 - Construction Products Regulation (CPR)".
- 7.3.2 LV electrical cables, control and communication cables installed, even partially, within equipment buildings or locally managed facilities shall be of Medium Fire Risk type, Dca according to the EN 13501-6.
- 7.3.3 LV electrical cables, control and communication cables travelling, even partially, inside passenger stations and in tunnels shall be of High Fire Risk type, Cca s1 d1 a1 according to the EN 13501-6.
- 7.3.4 LV electrical cables for the power supply of Safety and Security Systems shall be fire resistant, at least 90min - 830°C in accordance with EN 50200.



- 7.3.5 The maximum continuous current-carrying capacity, the maximum permissible conductor temperature and the factors for determining such rating and temperature and physical protection for all cables shall be based on IEC 60364-5-52 standards and on the conditions anticipated on site. These conditions shall include, but not be limited to, the following:
- Ground and duct temperature,
 - Soil thermal resistivity,
 - Ambient air temperature.
- 7.3.6 The ratings applied to the cable shall be determined by the most onerous installation condition in which the cable is travelling.
- 7.3.7 The LV electrical cables shall have two types of working temperature: Maximum operating temperature 90°C; Maximum short circuit temperature 250°C.
- 7.3.8 Electrical cables exposed to external elements shall be protected with the use of additional enclosures (conduits, etc.). Unprotected cables shall be, as minimum, suitable for the typical ambient temperature range and protected against mechanical damage, UV light, ozone and water.
- 7.3.9 The minimum cross section for main LV electrical cables shall be 4 sqmm for power circuit and 2.5 sqmm for lighting circuit in compliance with IEC standards.
- 7.3.10 The minimum cross section for terminal LV electrical cables shall be 2.5 sqmm for power circuit and 1.5 sqmm for lighting circuit in compliance with IEC standards.
- 7.3.11 The LV electrical cables shall be of insulation type 0.6/1 kV.
- 7.3.12 Insulation type 450/750V cables may be used for protection earth cables and switchboard internal cabling.
- 7.3.13 The LV electrical cables shall be of conductor class 5 according to IEC 60228. The adoption of lower conductor classes shall be approved by the Authority.
- 7.3.14 The LV electrical cable joints shall be minimized as practicable.
- 7.3.15 The LV electrical cable joints shall be identified and shall have an electrical and mechanical performance not less than that of the cable.
- 7.3.16 Proposals for joints in cable runs shall be submitted for Authority approval on an individual basis.
- 7.3.17 Any joints and connections shall be located such that they are readily accessible for maintenance purposes.
- 7.3.18 The LV electrical cables shall have copper conductors.
- 7.3.19 The LV electrical cable insulation shall be halogen free EPR (Ethylene Propylene Rubber) or XLPE (Cross-Linked-Polyethylene).
- 7.3.20 A proper grounding of the cable trays and metal conduits shall be provided to avoid touch voltages and maximize shielding in compliance with IEC 61140.
- 7.3.21 Medium Voltage and Low Voltage circuits shall not be installed in common conduit or containment.
- 7.3.22 Power and control and communication cables shall not be installed in common conduit or containment.
- 7.3.23 Circuits energized from different power sources or separately protected circuits energized from the same power source shall not be combined into a single cable.



- 7.3.24 Emergency circuits shall be separated from non-essential and essential circuits and segregated with dividers or in dedicated cable containment.
- 7.3.25 Manholes, handholes, vaults and boxes, pulling chambers shall be sufficiently sized to allow easy cable pulling and jointing, to allow cable expansion and contraction and according to cables minimum bending radius, ensuring cables can be pulled manhole to manhole within tolerable cable bending radii.

7.4 Uninterruptable Power Supply System

- 7.4.1 A UPS system shall be provided for the power supply of MVPS and LVPS emergency loads.
- 7.4.2 The UPS system shall be of a modular type and shall be designed to withstand a single failure and still be able to deliver the required output to the loads for the designed autonomy (minimum 12 hours), within the acceptable voltage range required by the loads.
- 7.4.3 UPS modules shall be hot-swappable.
- 7.4.4 UPS systems shall be equipped with an internal automatic bypass switch designed to transfer the entire uninterruptable load, from the UPS unit output to the main power supply in case of failures of UPS modules.
- 7.4.5 UPS systems shall be equipped with an external manual bypass switch designed to transfer the entire uninterruptable load, from the UPS system output to the main power supply whenever it's required a maintenance, replacement or repair of UPS or battery bank.
- 7.4.6 The UPS shall have a network management card, using a standard protocol compatible with the used TSCC ICSS system, to enable monitoring and controlling of the UPS devices.
- 7.4.7 The UPS systems shall be provided with intrinsic testing functionality.
- 7.4.8 The precise capacity of the UPS system and batteries shall be determined by the TSCC Contractor to ensure total autonomy of the MVPS and LVPS emergency loads for a time required by the CHSR.
- 7.4.9 UPS Battery packs shall be divided into separate banks to provide physical redundancy.
- 7.4.10 UPS batteries shall be equipped with a health remote monitoring system.
- 7.4.11 UPS batteries shall have a flame retardancy greater or equal than UL94 V-0 or equivalent classification.
- 7.4.12 UPS batteries shall be maintenance-free industrial type.
- 7.4.13 UPS batteries shall be in a temperature-controlled room and kept at a temperature range that maximizes battery lifetime.
- 7.4.14 UPS batteries shall be low emission of dangerous gases.
- 7.4.15 An adequate system for air exchange shall be guaranteed in the room where the UPS batteries are located to prevent formation of explosive atmosphere in compliance with the IEC 62485 - EN 50272.
- 7.4.16 UPS batteries shall be ventilated in accordance with IEC 62485-2 to prevent formation of explosive gases.
- 7.4.17 Battery type for TSCC equipment shall be selected according to applicable standards and considering local environmental characteristics to guarantee their proper functioning and prevent injuries during their maintenance.



7.5 Back-up Generator

- 7.5.1 Each back-up generator shall have a rated power of a minimum of 20% greater than the maximum power demand calculated that the generator is intended to support.
- 7.5.2 Back-up generators shall ensure a high level of reliability and shall be designed to provide an autonomy of at least the time necessary for the restoration of the power supply from the main power source at the rated power.
- 7.5.3 Back-up generators shall be of indoor type and shall be suitable for the environment it will be installed in.
- 7.5.4 In situations where indoor installation is necessary a separate room for the generator placement shall be provided.
- 7.5.5 Back-up generator storage tanks shall be installed with all the relative precautions and safety measures.
- 7.5.6 The back-up generator shall start, operate, and turn off autonomously when requested.
- 7.5.7 Back-up generator remote control, monitoring and interface to the TSCC ICSS system shall be ensured.

7.6 OCC Power Supply

- 7.6.1 The OCC Power Supply System main purpose is to supply, 24/7/365, continuous voltage to TSCC system components of the OCC and alternative voltage to the control and monitoring servers and workstations of the OCC.
- 7.6.2 The design of the OCC Power Supply System shall be of a modular type.
- 7.6.3 The rated power of the OCC Power Supply System can be adapted to the need by increasing the number of converter/rectifier units.
- 7.6.4 "N+1" hot redundancy of each component type of the OCC Power Supply System shall ensure the availability of the adequate output even in the event of the failure of one unit.
- 7.6.5 Each component of the OCC Power Supply System shall be designed so that it can be tested, plugged-in, or unplugged when the OCC Power Supply is operating, without creating disturbance to the output supply.
- 7.6.6 Dual source (AC & DC) converter units of the OCC Power Supply System shall produce the 230Vac output.
- 7.6.7 Each converter unit in the OCC Power Supply System shall feature its own static source changeover switch.
- 7.6.8 AC source of the OCC Power Supply System shall be selected under normal operation conditions (when both supply source active) to lower the chargers load and to improve the efficiency of the conversion,
- 7.6.9 Upon voltage loss or recovery, AC to DC and DC to AC source switchover time of the OCC Power Supply System shall be 0ms. There shall be no voltage dip at the output.
- 7.6.10 As required by the OCC designer, DC/DC converters can be set downstream of the batteries, to regulate the DC voltage output, as the battery output voltage varies depending on the charging status, temperature, and age.
- 7.6.11 The OCC Power Supply System shall be monitored from the ICSS. The monitoring functions shall comprise at least:
 - alarms and faults



- display of main electrical values such as but not limited to:
 - voltage and current of batteries
 - voltage and current of converters
 - voltage and current of rectifiers
 - Input voltages
 - Output voltages
 - Battery temperature
 - Battery charge status
 - Estimated time before end of autonomy on power input loss
 - event recorder with local and remote readout.

7.6.12 The TSCC Contractor shall deploy (design, manufacture, deliver, install, inspect, test, commission, supply necessary documentation, spare parts, special tools, and training) the OCC Power Supply system as a part of the TSCC systems dedicated for the power supply of the TSCC systems and subsystems and other consumers as defined in the Chapter 4.3

7.6.13 The TSCC Contractor shall deploy the OCC Power Supply system according to the power supply requirement of each OCC Power Supply consumer, applicable standards and documents for California High Speed Rail (CHSR).

7.7 34.5kV MV System - Production and Distribution

All references to 34.5 kV in this section, section 7.8, 7.9 & 7.10 are indicative. The TSCC Contractor shall comply with Clause 4.1.1 regarding verification and confirmation of actual service voltage with the serving utility.

7.7.1 The MV System shall be tasked with delivering power to the RMUs inserted on the MV rings.

7.7.2 The MV rings outlets shall be in the traction power substations.

7.7.3 Auxiliary systems of the RMUs shall comprise the logic cabinet required for their operation. The logic cabinet will feature the PLC or RTU required to monitor and control the RMU, the gateway/switch to the power SCADA network, a DC charger and its battery rack. It will monitor the MV/LV transformer as well.

7.7.4 A MV ring shall be connected at its endings either to the switchgear of the Point of Common Connection of two different traction substations, either to two different sections of the busbar serving as the point of common connection in the same traction substation.

7.7.5 A single MV ring outlet at the traction substation shall be able to take over the full load of the ring which it supplies.

7.8 34.5kV MV system – Field structure and Cable links

7.8.1 The MV system power structure shall be made of open rings routing along the line.

7.8.2 The TSCC Contractor shall lay the 34.5kV cables in duct banks running along the right-of-way.

7.8.3 A RMU shall allow to enable ring continuity, or to sever the MV ring of which it is connected, and to supply power to its site according to the power demand.

7.8.4 Each RMU shall be fitted with a fault detection device allowing for a swift re-mapping of the ring in the event of a fault.



- 7.8.5 Each RMU shall be motor operated to allow a remote configuration of the rings from the power SCADA.
- 7.8.6 The design of the RMU control and monitoring subsystem shall meet the IEC 61850 requirements.
- 7.8.7 Rated voltage of auxiliary control circuits of RMUs shall be supplied from a battery-charger system located on each site.
- 7.8.8 RMUs shall be gas or vacuum insulated. Switchgear cubicles shall be industrial standard products. They shall be free standing and suitable for indoor service.
- 7.8.9 The RMU communication abilities shall meet the IEC 61850 requirements.
- 7.8.10 For maintenance purposes, all RMUs:
- shall be provided by the same manufacturer, in the same factory range,
 - shall have the same short-circuit withstand abilities and the same main busbar ampacity,
 - shall accommodate various sizes and types of 34.5kV cables.
- 7.8.11 The Medium Voltage network cable links shall be made primarily of dry insulated, three-core radial-field 26/35(42) kV cables, or dry insulated 26/35(42) kV single cable trefoils, and their connector plugs.
- 7.8.12 The Medium Voltage network cables shall feature aluminum or copper conducting core(s), semi-conductor over the conducting core, cross-linked polyethylene type (XLPE) insulating sheathing, semi-conducting over the insulating sheathing, screen, insulation and protective sheathing.
- 7.8.13 The cross-section value of each type of cable shall be the sole liability of the TSCC Contractor, as part of their design works.
- 7.8.14 The sizing of the 34.5kV cable cross section shall be calculated to ensure that one cable link is able to feed the entire ring which it belongs to.
- 7.8.15 The MV cables (and their screens) shall withstand the short-circuit current under a given fault elimination time without exceeding the maximum acceptable temperature specified for the insulation material.
- 7.8.16 The MV cables shall withstand the RMS current without exceeding the normal operating temperature specified for the insulation material.
- 7.8.17 The standard rated short duration power-frequency withstand voltage and the BIL/LIWL features of the MV cables shall be carefully assessed as part of the insulation coordination design of the 34.5kV network.
- 7.8.18 Connecting junctions/plugs shall reconstitute perfectly all elements of the MV cables. They will present at least the same ampacity, voltage, standard rated short duration power-frequency withstand voltage and the BIL/LIWL as the cable ones.
- 7.8.19 If required, the TSCC Contractor shall provide the surge arresters required for cables and cable screens protection and perform intermediate grounding of the screen in cable links if required.
- 7.8.20 The TSCC Contractor shall design the 34.5 kV cable routing to avoid crossing from one track side to the other track side, as much as it is practically and economically achievable.
- 7.8.21 In all locations, connecting civil works shall be designed and installed with respect to the acceptable bending radius of the cables and to the cable arrangement design. The required depth of technical basements and/or raised floors in technical rooms housing the RMUs shall be determined with due consideration of these requirements.
- 7.8.22 At system equipment locations, facilities, traction sites, the 34.5kV cables shall be laid in cable containment.



- 7.8.23 For burying cables in the ground, the TSCC Contractor shall provide concrete mechanical protective cover and install warning tape 50 cm above.

7.9 34.5kV/LV Distribution Transformers

- 7.9.1 Distribution Transformers shall step down voltage level from 34.5kV AC to LV AC.
- 7.9.2 Distribution Transformers shall be three-limbs-wound dry insulated type ones and fitted with off load tap changers ($\pm 10\%$ primary voltage, 2,5% steps, same rated power on each tap)
- 7.9.3 Distribution Transformers shall be Air Natural cooled.
- 7.9.4 Each distribution transformer shall have a spare power capacity of around 30 % of their nominal AN power rating.
- 7.9.5 Distribution Transformers shall be fitted with temperature sensors and their monitoring relay. The relay shall be mounted on the transformer enclosure or the fence of the transformer housing or the logic cabinet front panel, as per the TSCC Contractor's submitted layout.
- 7.9.6 The insulation level of the transformers primary windings shall be consistent with the 34.5 kV switchgear insulation level.

7.10 LV production on remote sites

- 7.10.1 On remote sites where the TSCC Contractor deems that the installation of a RMU and a 34.5kV/LV transformer will not be cost-effective, the site shall draw the power from the OCS.
- 7.10.2 Sites where power is drawn from the OCS shall include a fused load-break switch connected to the OCS, and an Oil Natural Air Natural single phase 25kV/LV transformer, mounted on a catenary post or a dedicated post located in the immediate vicinity of the OCS.
- 7.10.3 Downstream of the single-phase transformer, the TSCC Contractor shall install an AC/AC converter to uphold a consistent LV voltage albeit the voltage variations of the OCS.
- 7.10.4 Auxiliary systems of the fused load-break switches shall comprise the logic cabinet required for their operation. The logic cabinet will feature the PLC or RTU required to monitor and control the switch, the gateway/switch to the power SCADA network, a DC charger and its battery rack. It will monitor the MV/LV transformer and the AC/AC converter as well.
- 7.10.5 Voltage level, BIL/LIWL of the fused load-break switches and of the 25kV/LV transformer shall be consistent with the voltage level of the OCS.
- 7.10.6 As per required, the single-phase transformer primary bushings shall be fitted with arcing horns and/or connected to surge arresters.
- 7.10.7 On any given traction section, the power drawn from the OCS by the MVPS and LVPS system shall not exceed 500kW.



8 TOLERANCES

Not applicable to MVPS and LVPS.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 General requirements related to the TSCC Contractor Scope of Work are described in Schedule 16

9.2 Specific Requirements

9.2.1 The TSCC Contractor shall supply, deliver, install, test, and commission all components necessary for a fully functional MVPS and LVPS, as specified in this Technical Specification.

9.2.2 The TSCC Contractor shall be responsible for the design, manufacture, factory acceptance testing (FAT), delivery, site installation, integration, site acceptance testing (SAT), and commissioning of the MVPS and LVPS solution to facilitate CHSR in-revenue service.

9.2.3 The scope of supply shall include, but not be limited to

- Cable terminations and connections to the MV switchgear of the Point of Common Connection located in the traction substations.
- MV rings
- RMUs
- Fused load-break switches connected to the OCS
- MV/LV transformers
- Low voltage production
- Low voltage distribution;
- Control and monitoring, and its connection to the power SCADA
- Uninterruptible power supply system;
- Back-up generator at the OCC.
- Hardware and software licences.

9.2.4 The TSCC Contractor shall ensure that all equipment and materials delivered are compliant with relevant standards and project-specific environmental and safety requirements.

9.2.5 The TSCC Contractor shall coordinate all delivery and logistics activities in accordance with the Project Delivery Program and in consultation with the Authority, including any site access restrictions and staging requirements.

9.2.6 The TSCC Contractor shall label and package all equipment and components clearly and securely to facilitate identification, handling, and inventory upon delivery to site.

9.2.7 The TSCC Contractor shall provide a detailed Delivery and Installation Schedule, identifying all major equipment deliveries, installation milestones, and dependencies.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.

11.2 Specific Requirements

11.2.1 The TSCC Contractor shall provide temporary power supplies, if necessary for TSCC Contractor works (construction, installation, test and commissioning, etc.).

11.2.2 Fossil-based power sources should be avoided for temporary power supplies and may be considered only under approval of the Authority.

11.2.3 The TSCC Contractor shall perform the design, manufacturing, delivery, installation, inspection, test, commissioning, supply of necessary documentation, spare parts, special tools, and training for the MVPS and LVPS and its components in accordance with the relevant standards and regulations as it is stated in Section 2.



12 TESTING & ACCEPTANCE

12.1 General Requirements

General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.



13 SUBMITTALS

13.1 General Requirements

13.1.1 The submittals required for the Interlocking system are defined in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor and related Suppliers information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence reliability availability maintainability characteristics.



16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.

APPENDIX A TO EXHIBIT 5(J) MEDIUM VOLTAGE POWER SYSTEM (MVPS) AND LOW VOLTAGE POWER SYSTEMS (LVPS)

Schematic plan	Area	System	Kilometer/Mile	Package Stationing	Type	ID	Comment	ID	CP1 Min	DTD	BMU	DCS FEEDER	Power demand on HV system per load	# HV Power supply point	Power demand on per HV supply points (kVA)	Power demand on OCS per load	# OCS supply point	Power demand per OCS supply points (kVA)
CP1	Intercom	Radio	Kilometer	293.23	Shelter	TCCH-CP1.1 (293.23)			1	0.80	267.325	2	20					
CP1	Radio	Radio	Kilometer		Shelter	FMHCS-HV Radio Site			1	0.80		0	4	1	35			
CP1	road vehicle fall	180	267.7	293.7	30/0/30	LEFT/RIGHT	Avenue 20		0	3.33		0	4					
CP1	road vehicle fall	130	275.6	296.6	30/0/30	LEFT/RIGHT	Avenue 17		1	3.33		1	4					
CP1	Radio	Radio	Kilometer	296.6	Shelter	FMHCS-HV Radio Site			1	4.29		1	4	2	4	1	1	1
CP1	Truck	Truck	Kilometer	296.6	Truck site	35-BAY	RIGHT SIDE DUE TO BNIF		2	6.48		2	110	3	111			
CP1	road vehicle fall	173	275.4	301.4	30/0/30	LEFT/RIGHT	Avenue 15.1/2		3	6.89		0	1			1	2	2
CP1	road vehicle fall	173	275.4	301.4	30/0/30	LEFT/RIGHT	Avenue 15		4	8.96		0	0					
CP1	Radio	Radio	Kilometer	301.4	Shelter	FMHCS-HV Radio Site			1	6.76		0	4	4	84			
Maters	CP1	Signaling	Kilometer	302.189	Shelter	TCCH-CP1.2 (302.189)			2	8.78	276.204	2	80					
Maters	CP1	Signaling	Kilometer	302.120	Shelter	TCCH-CP1.3 (302.120)	Maters Station		2	12.86	280.327	2	1000	5	1172			
Maters	CP1	Signaling	Kilometer	304.445	Shelter	FMHCS-HV Radio Site			4	13.67	280.54	0	12					
CP1	Truck	Truck	Kilometer	304.445	Truck site	PS-12	Maters Station		1	10.12	280.54	0	70					
CP1	road vehicle fall	177	281.9	307.9	30/0/30	LEFT/RIGHT	Maters 5th		5	14.53		0	1	6	72			
CP1	road vehicle fall	177	281.9	307.9	30/0/30	LEFT/RIGHT	Avenue 12		6	14.53		0	1					
Maters	CP1	Signaling	Kilometer	305.544	Shelter	TCCH-CP1.4 (305.544)	Points, back to single track after Maters Station		5	13.54	283.139	2	130		130	1	3	1
CP1	Radio	Radio	Kilometer	305.5	Shelter	FMHCS-HV Radio Site			7	16.14		1	4	7				
CP1	road vehicle fall	179	285.1	311.1	30/0/30	LEFT/RIGHT	Avenue 10		8	17.76		1	1			4	1	1
CP1	road vehicle fall	180	286.7	312.7	30/0/30	LEFT/RIGHT	Avenue 9		9	19.36		1	1					
CP1	road vehicle fall	180	286.7	312.7	30/0/30	LEFT/RIGHT			10	19.36		0						
CP1	road vehicle fall	180	286.7	312.7	30/0/30	LEFT/RIGHT			11	19.36		0						
CP1	road vehicle fall	180	286.7	312.7	30/0/30	LEFT/RIGHT			12	19.36		0						
CP1	road vehicle fall	180	286.7	312.7	30/0/30	LEFT/RIGHT			13	19.36		0						
CP1	road vehicle fall	180	286.7	312.7	30/0/30	LEFT/RIGHT			14	19.36		0						
CP1	road vehicle fall	184	288.3	314.3	30/0/30	LEFT/RIGHT	Avenue 8		15	20.97		0	1	8	5	2		
CP1	Radio	Radio	Kilometer	314.3	Shelter	FMHCS-HV Radio Site			1	20.97		1	4					
CP1	Truck	Truck	Kilometer	314.3	Truck site	PS-830			1	20.97		1	70					
CP1	road vehicle fall	182	289.9	315.9	30/0/30	LEFT/RIGHT	Avenue 7		16	22.57		0	1	9	71			
CP1	road vehicle fall	185	294.7	320.7	30/0/30	LEFT/RIGHT	valencia road		17	25.36		1	4	10				
CP1	Truck	Truck	Kilometer	320.7	Truck site	305-407			17	27.46		1	70					
CP1	Radio	Radio	Kilometer	320.7	Shelter	FMHCS-HV Radio Site			1	27.46		0	12	11	82			
CP1	road vehicle fall	187	297.9	323.9	30/0/30	LEFT/RIGHT	shawn avenue		18	28.62		0	1					
CP1	road vehicle fall	187	297.9	323.9	30/0/30	LEFT/RIGHT	ROAD SIDE DUE TO LPHS		19	28.62		0	1					
CP1	road vehicle fall	188	299.6	325.6	30/0/30	LEFT/RIGHT	valencia avenue		20	32.23		0	1					
CP1	Intercom	Intercom	Kilometer	326.899882	Shelter	TCCH-CP1.5 (326.899882)			6	33.50	318.639	2	30		12	34		
CP1	Radio	Radio	Kilometer	326.8	Shelter	FMHCS-HV Radio Site			21	33.50		0	1					
CP1	road vehicle fall	190	302.9	328.9	30/0/30	LEFT/RIGHT	valencia avenue		22	35.45		1	1					
CP1	road vehicle fall	190	302.9	328.9	30/0/30	LEFT/RIGHT	valencia avenue		23	35.45		1	1					
CP1	road vehicle fall	194	304.4	330.4	30/0/30	LEFT/RIGHT	valencia avenue		24	37.06		1	70		71			
Fresno	CP1	Signaling	Kilometer	331.12	Shelter	TCCH-CP1.7 (331.12)	Points, dual track around Fresno Station		7	37.49	305.225	2	80		14	84		
CP1	Radio	Radio	Kilometer	331.12	Shelter	FMHCS-HV Radio Site			25	37.49		0	4					
CP1	road vehicle fall	192	306.0	332.0	30/0/30	LEFT/RIGHT	valencia avenue		26	38.67		1						
CP1	road vehicle fall	192	306.0	332.0	30/0/30	LEFT/RIGHT	valencia avenue		27	38.67		0	1					
CP1	road vehicle fall	192	306.0	332.0	30/0/30	LEFT/RIGHT	valencia avenue		28	38.67		0	1					
CP1	road vehicle fall	192	306.0	332.0	30/0/30	LEFT/RIGHT	valencia avenue		29	38.67		0	1					
Fresno	CP1	Signaling	Kilometer	335.084	Shelter	TCCH-CP1.8 (335.084)			8	41.43	309.179	2	80		15	86		
Fresno	CP1	Signaling	Kilometer	335.435	Shelter	TCCH-CP1.9 (335.435)	Fresno Station		9	41.73	309.511	0	80					
CP1	road vehicle fall	194	309.2	335.2	30/0/30	LEFT/RIGHT	Fresno 10th		10	41.89		0	1					
CP1	road vehicle fall	194	309.2	335.2	30/0/30	LEFT/RIGHT	valencia avenue		11	41.89		0	1					
CP1	Radio	Radio	Kilometer	335.2	Shelter	FMHCS-HV Radio Site			12	41.89		0	12					
CP1	Truck	Truck	Kilometer	335.2	Truck site	305-407			13	41.89		0	12					
Fresno	CP1	Signaling	Kilometer	336.735	Shelter	TCCH-CP1.10 (336.735)	Points, back to single track after Fresno Station		10	43.02	310.812	2	80		17	88		
CP1	road vehicle fall	196	310.8	336.8	30/0/30	LEFT/RIGHT	valencia avenue		11	43.02		1						
CP1	road vehicle fall	196	310.8	336.8	30/0/30	LEFT/RIGHT	valencia avenue		12	43.02		0						
CP1	road vehicle fall	196	310.8	336.8	30/0/30	LEFT/RIGHT	valencia avenue		13	43.02		0						
CP1	Truck	Truck	Kilometer	336.8	Truck site	PS-206			14	43.02		1	70		76			
CP1	road vehicle fall	196	312.4	338.4	30/0/30	LEFT/RIGHT	valencia avenue		15	45.11		1	1					
CP1	Radio	Radio	Kilometer	338.4	Shelter	FMHCS-HV Radio Site			16	45.11		1	4					
CP1	road vehicle fall	198	317.3	343.3	30/0/30	LEFT/RIGHT	valencia avenue		17	46.23		1	4					
Fresno HOWE	CP1	Signaling	Kilometer	344.153	Shelter	TCCH-CP1.11 (344.153)	Points, for Fresno HOWE		11	50.28	318.248	2	110		20	184		
CP1	Truck	Truck	Kilometer	344.153	Truck site	PS-406			12	50.28		0	70					
CP1	Radio	Radio	Kilometer	344.153	Shelter	FMHCS-HV Radio Site			13	50.28		0	4					
CP1	road vehicle fall	200	318.9	348.9	30/0/30	LEFT/RIGHT	valencia avenue		14	51.34		0	1					
CP1	road vehicle fall	200	318.9	348.9	30/0/30	LEFT/RIGHT	valencia avenue		15	51.34		0	1					
Fresno HOWE	CP1	Signaling	Kilometer	351.40	Shelter	TCCH-CP1.12 (351.40)	Points, back to single track after Fresno HOWE		1	52.68	320.575	2	80		22	86		
CP1	road vehicle fall	201	320.5	351.5	30/0/30	LEFT/RIGHT	valencia avenue		17	53.15		1						
CP1	road vehicle fall	201	320.5	351.5	30/0/30	LEFT/RIGHT	valencia avenue		18	53.15		0						
CP1	road vehicle fall	201	320.5	351.5	30/0/30	LEFT/RIGHT	valencia avenue		19	53.15		0						
CP1	road vehicle fall	201	320.5	351.5	30/0/30	LEFT/RIGHT	valencia avenue		20	53.15		0						
CP1	road vehicle fall	202	322.1	353.1	30/0/30	LEFT/RIGHT	valencia avenue		21	54.76		0	1					
CP1	Radio	Radio	Kilometer	353.1	Shelter	FMHCS-HV Radio Site			22	54.76		1	23		5			
CP1	Truck	Truck	Kilometer	353.1	Truck site	PS-206			23	54.76		1	4					
CP1	road vehicle fall	203	323.7	353.7	30/0/30	LEFT/RIGHT	valencia avenue		24	56.27		2	1					
CP1	Truck	Truck	Kilometer	353.7	Truck site	PS-206			25	56.27		2	110	24	122			
CP1	road vehicle fall	205	326.5	356.5	30/0/30	LEFT/RIGHT	valencia avenue		26	58.39		0	1					
CP1	road vehicle fall	206	328.1	358.1	30/0/30	LEFT/RIGHT	valencia avenue		27	60.41		0	1					
CP1	road vehicle fall	207	330.1	360.1	30/0/30	LEFT/RIGHT	valencia avenue		28	62.53		0	1					
CP1	road vehicle fall	212	338.2	368.2	30/0/30	LEFT/RIGHT	valencia avenue		29	70.66		0	1					
CP1	Radio	Radio	Kilometer	368.2	Shelter	FMHCS-HV Radio Site			30	70.66		0	1					
CP1	Truck	Truck	Kilometer	368.2	Truck site	PS-206			31	70.66		0	1					
CP1	road vehicle fall	209	331.3	371.3	30/0/30	LEFT/RIGHT	ROAD SIDE DUE TO BNIF		32	72.88		1	4					
CP1	Truck	Truck	Kilometer	371.3	Truck site	PS-360			33	72.88		1	70		74			
CP1	Radio	Radio	Kilometer	371.3	Shelter	FMHCS-HV Radio Site			34	72.88		0	4					
CP1	Truck	Truck	Kilometer	371.3	Truck site	TCCH-CP1.13 (371.3)			35	72.88		0	27		36			
CP1	road vehicle fall	212	338.2	368.2	30/0/30	LEFT/RIGHT	valencia avenue		36	74.99		0	1					
CP1	road vehicle fall	212	338.2	368.2	30/0/30	LEFT/RIGHT	valencia avenue		37	74.99		0	1					
CP1	Radio	Radio	Kilometer	368.2	Shelter	FMHCS-HV Radio Site			38	74.99		0	1					
CP1	Truck	Truck	Kilometer	368.2	Truck site	PS-206			39	74.99		0	1					
CP1	road vehicle fall	212																



[illegible]

	CHS	Northridge		455.0	476.6	330	Right		90	107.68			1						
	CHS	East Ventura Hill	281	455.7	482.3	267030	Left Right	interior access	90	105.34		0		1		67	1001	1	34
	CHS	Palmdale				120101010		South access		100.08		2		1000					
	CHS	Palmdale		Kilometer	484.058		Station	TCHS CHS 3.1484.058	3	390.49	457.814	2		30		68	74		
	CHS	Radio				FMCS 98H Radio Site				390.49		0		4					



Schedule 5(k)

Closed-Circuit Television (CCTV)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0015 – Closed-Circuit Television (CCTV)

Rev. 1.0

Authorized:

A handwritten signature in black ink, appearing to read "Harshal".

Harshal Jadhav, Telecom System Lead

22 December 2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Thomas".

Thomas Newey, Telecoms Lead

22 December 2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Bruno".

Bruno Comperat, Deputy Director of Rail Engineering

23 December 2025

Date

Approved:

A handwritten signature in blue ink, appearing to read "Ryan Scott".

Ryan Scott, Director of Rail Engineering

23 December 2025

Date

Released:

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Amit Joshi, Configuration Manager

23 December 2025

Date



Document Revision History – CCTV Specifications**Second Edition****December 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition
1.0	December 2025	Second edition for Addendum 2



TABLE OF CONTENTS

1	INTRODUCTION	6
1.1	SCOPE OF THE TECHNICAL SPECIFICATION.....	6
2	REFERENCE STANDARDS AND DOCUMENTS	7
2.1	GENERAL	7
2.2	DESIGN GUIDELINES	7
2.3	TSI	7
2.4	STANDARDS	7
2.5	OTHER DOCUMENTS	9
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	10
4	SYSTEM DESCRIPTION	11
4.1	PURPOSE OF THE CCTV SYSTEM.....	11
4.2	CCTV SYSTEM DEFINITION	11
4.3	CCTV SYSTEM OPERATIONAL CONTEXT.....	11
4.4	DESIGN LIFE	11
5	SYSTEM REQUIREMENTS.....	12
5.1	GENERAL REQUIREMENTS.....	12
5.2	ENVIRONMENTAL CONDITIONS REQUIREMENTS	14
5.3	OPERATIONAL REQUIREMENTS FOR CCTV	15
5.4	FUNCTIONAL REQUIREMENTS FOR CCTV	16
5.5	PERFORMANCE REQUIREMENTS FOR CCTV	19
5.6	RAM REQUIREMENTS.....	20
5.7	CYBERSECURITY AND SECURITY REQUIREMENTS.....	20
6	INTERFACES REQUIREMENTS	22
6.1	GENERAL REQUIREMENTS.....	22
6.2	EXTERNAL INTERFACE FOR CCTV.....	22
6.3	EXTERNAL INTERFACES – FACILITIES CONTRACTOR.....	22
6.4	EXTERNAL INTERFACES – STATIONS CONTRACTOR	23
6.5	INTERNAL INTERFACES.....	23
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS.....	25
7.1	GENERAL REQUIREMENTS.....	25
7.2	SOFTWARE AND HARDWARE REQUIREMENTS	25
7.3	EMC REQUIREMENTS.....	25
8	TOLERANCES.....	26
9	SCOPE OF SUPPLY AND DELIVERY	27
9.1	GENERAL REQUIREMENTS.....	27
9.2	SPECIFIC REQUIREMENTS	27
10	MANUFACTURING	28



10.1	GENERAL REQUIREMENTS.....	28
11	INSTALLATION AND INTEGRATION	29
11.1	GENERAL REQUIREMENTS.....	29
12	TESTING & ACCEPTANCE	30
12.1	GENERAL REQUIREMENTS.....	30
12.2	SPECIFIC REQUIREMENTS	30
13	SUBMITTALS	31
13.1	GENERAL REQUIREMENTS.....	31
14	QUALITY MANAGEMENT	32
14.1	GENERAL REQUIREMENTS.....	32
15	ADDITIONAL INFORMATION REQUESTED	33
15.1	GENERAL REQUIREMENTS.....	33
16	LOGISTICS	34
16.1	GENERAL REQUIREMENTS.....	34



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Closed-Circuit Television (CCTV) system, hereinafter: CCTV.
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of the CCTV System alongside is presented in Appendix A.
- 1.1.4 The requirements are formulated using the following words and their meanings:
 - **"Shall"**: Indicates a mandatory requirement that must be strictly implemented; a waiver from a mandatory requirement is permissible only with approval of a design variance.
 - **"Should"**: Indicates a preferred course of action; a design variance is not required if it is not exercised.
 - **"Must"**: Indicates an obligation or a mandatory requirement.
 - **"May"**: Indicates a permissible course of action within the limits of the standards; a design variance is not required if it is not exercised.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines, and specifications provided in this chapter for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, and training.

2.2 Design Guidelines

- 2.2.1 The latest version of the following Design Guidelines shall be applied:

ID	Code	Title
[R1]	Design Criteria Manual	Chapter 5 – Safety and Security
[R2]	Design Criteria Manual	Chapter 12 – Communication Systems and Train Control
[R3]	AREMA Standards	Chapter 17 – High-Speed Rail Systems

TABLE 30 DESIGN GUIDELINES

2.3 TSI

- 2.3.1 Not applicable for the CCTV system.

2.4 Standards

- 2.4.1 The TSCC Contractor shall fully consider and apply the following standards, the in-force standards shall be applied.

ID	Code	Title
[R4]	EN 50121	Railway Applications – Electromagnetic Compatibility
[R5]	EN 50122-1	Railway applications - Fixed installations - Electrical safety, earthing and the return circuit - Part 1: Protective provisions against electric shock
[R6]	EN 50124	Railway applications - Insulation coordination
[R7]	EN 50125	Railway applications - Environmental conditions for equipment
[R8]	EN 50126-1	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
[R9]	EN 50126-2	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
[R10]	EN 50128	Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems
[R11]	EN 50159	Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems
[R12]	EN 50164	Lightning Protection Components



ID	Code	Title
[R13]	EN 50173	Information technology - Generic cabling systems
[R14]	EN 50174	Information technology - Cabling installation
[R15]	EN 50289-1-6	Communication cables - Specifications for test methods - Part 1-6: electrical test methods - Electromagnetic performance
[R16]	EN 50310	Application of equipotential bonding and earthing in buildings with information technology equipment
[R17]	EN 55024	Information technology equipment. Immunity characteristics. Limits and methods of measurement
[R18]	EN 60065	Audio, video and similar electronic apparatus - Safety requirements
[R19]	EN 60297-3	Mechanical structures for electronic equipment - Dimensions of mechanical structures of the 482,6 mm (19 in) series - Part 3-100: basic dimensions of front panels, sub racks, chassis, racks and cabinets
[R20]	EN 60664-1	Insulation coordination for equipment within low-voltage systems -- Part 1: Principles, requirements and tests
[R21]	EN 61000-6	Electromagnetic compatibility (EMC) - generic standards
[R22]	EN 61034	Measurement of smoke density of cables burning under defined conditions
[R23]	EN 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
[R24]	EN 62305	Protection against lightning
[R25]	EN 62676	Video surveillance systems for use in security applications
[R26]	IEC 60068	Environmental testing
[R27]	IEC 60331	Tests for electric cables under fire conditions
[R28]	IEC 60364	Low-voltage electrical installations (equivalent to HD 384 series)
[R29]	IEC 60529	Degrees of protection provided by enclosures (IP Code)
[R30]	IEC 61000-3-6	Electromagnetic compatibility (EMC) - Part 3: Limits - Section 6: Assessment of emission limits for distorting loads in MV and HV power systems - Basic EMC publication
[R31]	IEC 61000-3-7	Electromagnetic compatibility (EMC) - Part 3-7: Limits - Assessment of emission limits for the connection of fluctuating installations to MV, HV and EHV power systems
[R32]	IEC 61000-5-2	Electromagnetic compatibility (EMC) - Part 5: Installation and mitigation guidelines - Section 2: Earthing and cabling
[R33]	IEC 61643	Low-voltage surge protective devices
[R34]	IEC 62262	Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)
[R35]	ISO 9001	Quality management systems — Requirements
[R36]	ISO 11064	Ergonomic design of control centers



ID	Code	Title
[R37]	ISO/CEI 15288	Systems engineering - Systems life cycle processes
[R38]	IEEE 1220	IEEE Standard for Application and Management of the Systems Engineering Process
[R39]	IEEE 60068-2-1	Environmental testing - Part 2-1: Tests - Test A: Cold
[R40]	IEEE 60068-2-30	Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)
[R41]	NFPA 780	Standard for the Installation of Lightning Protection Systems
[R42]	APTA IT-CCTV-RP-001-11	Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks, and Trainlines for Use in Transit-Related CCTV Systems

TABLE 31 LIST OF APPLICABLE STANDARDS

2.5 Other Documents

2.5.1 The following documents shall be referred to:

ID	Document	Title
[R43]	Schedule 16	Scope of Work
[R44]	Schedule 5(a) SPEC-0005	Cybersecurity Specification
[R45]	Schedule 1	Safety, Security and RAM Requirements

TABLE 32 OTHER DOCUMENTS

3 TERMS, DEFINITIONS, AND ABBREVIATIONS

- 3.1.1 All the terms, definitions, and abbreviations are provided in: Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of the CCTV System

- 4.1.1 The purpose of the CCTV System is to ensure the achievement of the objectives of security management, including prevention of crime and disorder, protection of passengers and personnel in railroad stations, and protection of the California High-Speed-Rail Assets, including technical equipment installed inside the facilities.
- 4.1.2 Main objectives of CCTV System include, but are not limited to deterrence, prevention, real-time security supervision, supervision of the station and railway operations, investigation of events and violations.

4.2 CCTV System Definition

- 4.2.1 CCTV System is a closed system consisting of CCTV cameras, wired data networks, and Video Management System that enables reliable monitoring of the California High-Speed-Rail railway infrastructure environment from dedicated locations.
- 4.2.2 CCTV System main components include:
- Camera- IP cameras of types such as dome, dome panoramic, bullet, box, and Pan, Tilt, and Zoom (PTZ) cameras.
 - Network Video Recorder (NVR)- server-based NVRs installed at OCC, Depot, and Stations.
 - Video Management System (VMS)- provides centralized management of all devices and servers. It includes management servers installed at OCC.
 - Video Analytics System (VAS)- Seamlessly integrated with the VMS that enhances surveillance by leveraging advanced software and Artificial Intelligence to analyze video feeds in real time or post-event.

4.3 CCTV System Operational Context

- 4.3.1 The mission of the CCTV System is to support the California High-Speed-Rail infrastructure security by providing real-time and historic video coverage, safety and security related alarms for OCC building, stations, depot, maintenance facilities, train care facilities, traction power facilities, strategic locations (tunnels, bridges, etc.) and wayside facilities along the California High-Speed Rail Right-of-Way.

4.4 Design Life

- 4.4.1 The design life of CCTV system shall be 30 years.
- 4.4.2 The design life requirements of the CCTV system shall allow for the pertinent evolution and technological change of the CCTV system throughout its life to ensure it remains fit for purpose.
- 4.4.3 The TSCC Contractor shall ensure that CCTV system components with shorter design lifespans shall be managed by scheduled technology refresh strategies and spares management plans.
- 4.4.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce CCTV system components (with equal or compatible technical specifications) for the entire design life required.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

5.1.1 CCTV System

- 5.1.1.1 The TSCC Contractor shall be responsible for all components, systems, interfaces, and activities necessary to fully design, deliver, integrate, test, and operationalize the CCTV system to the standard required for high-speed rail operations and for CHSR to enter revenue service. This includes, but is not limited to, design, procurement, sourcing, construction, installation, configuration, integration, verification, validation, training, documentation, operations, maintenance, and handover of all CCTV subsystems, in accordance with the requirements of this and other specifications, and subject to acceptance by the Authority.
- 5.1.1.2 The TSCC Contractor shall provide all necessary CCTV equipment, cabling, software, and licenses.
- 5.1.1.3 The CCTV system shall be end-to-end IP (Internet Protocol) based.
- 5.1.1.4 The CCTV system shall provide supervision at OCC building, stations, depot, maintenance facilities, train care facilities, traction power, strategic locations (tunnels, bridges, etc.), and wayside facilities along the California high-speed right-of-way, and they shall be connected through the Digital Communication Network (DCN).
- 5.1.1.5 The CCTV system monitoring and control shall be provided from the ICSS (Integrated Control and Supervision System) workstation. It shall be possible to provide a comprehensive overview of all supervised locations.
- 5.1.1.6 The local CCTV system at stations shall be controllable by the OCC. The TSCC Contractor's CCTV design shall also accommodate future control of the CCTV system from the stations.
- 5.1.1.7 In the event of a major incident, recording media from all camera systems may be required for evidence. It is essential that operators ensure that the recording systems of any CCTV system are protected in this way, and that backup or spare recording media are also provided to allow the systems to continue to be used when major incidents occur. Major incidents need not be limited to terrorist events and may well be linked to environmental or criminal acts. Recording systems shall provide for a minimum of 30 days storage.
- 5.1.1.8 A redundant recording architecture and high availability mechanisms shall be implemented on the CCTV system's recording equipment/resources of the architecture to protect the recording capacity against hardware or software single point of failure.
- 5.1.1.9 The servers of the CCTV system must be provided with the appropriate number of licenses for the number of CCTV cameras designed for across HSR infrastructure.
- 5.1.1.10 Application of different types of CCTV cameras and camera parameters (i.e., optimal CCTV camera location, coverage, orientation, resolution, etc.) shall be precisely defined by the TSCC Contractor when CCTV Equipment Layout and Coverage Study for each location is executed.
- 5.1.1.11 The CCTV cameras shall be installed at locations and according to conditions defined in the CCTV Equipment Layout and Coverage Study for each specific location.
- 5.1.1.12 The TSCC Contractor shall develop a CCTV thermal imaging study to determine the justification for the use of thermal imaging cameras.
- 5.1.1.13 The CCTV cameras on the perimeter shall be installed in such a way that there is no blind spot and the camera is also in the field of view of another camera.



- 5.1.1.14 The CCTV system shall be able to integrate fixed CCTV and PTZ cameras.
- 5.1.1.15 The CCTV system shall allow controlling the Pan, Tilt, and Zoom functions of the PTZ cameras, including user-controlled movement, predefined tour paths, position presets, and event-driven PTZ positioning.
- 5.1.1.16 All CCTV cameras shall receive power through active equipment such as Power over Ethernet (PoE) switches.
- 5.1.1.17 For PTZ cameras requiring a separate power source, the TSCC Contractor shall provide a suitable power source that supplies either 110-120V AC at 60Hz, or alternatively, 12V DC or 24V at 60Hz.
- 5.1.1.18 For CCTV cameras further away from the PoE switches (>90m), PoE extensions shall be used or an optical cable with a CAT6a cable transition.
- 5.1.1.19 The indoor and outdoor CCTV cameras shall be used depending on the installation environment.
- 5.1.1.20 The provision of CCTV coverage within non-public indoor areas shall consider the appropriateness and necessity of surveillance. Camera locations in such areas shall be proposed by the TSCC Contractor and subject to review and approval by the Authority to ensure a balance between security needs and staff privacy.
- 5.1.1.21 The day/night CCTV cameras shall be used for surveillance in poorly lit areas and in areas that require surveillance during the night.
- 5.1.1.22 The CCTV camera must possess the capability to autonomously store video recordings locally in the event of a loss of connection between the CCTV camera and the NVR.
- 5.1.1.23 Upon the restoration of connection with the NVR, the CCTV system is required to initiate an automatic upload of locally stored video footage to the NVR.
- 5.1.1.24 Tamper-evident solution shall be provided for the local storage (memory driver) of the CCTV camera.
- 5.1.1.25 The installation of a communication network in the facilities shall be implemented using halogen-free cable (e.g., S/UTP cat 6.A), and outside the facilities by using (e.g., S/FTP cat 6.A) cables for outdoor installation.
- 5.1.1.26 The CCTV equipment shall be compatible with CHSR branding, visual identity, signage system, and graphical charts, and shall be fully integrated in the overall station designs and shall take architectural constraints into account.
- 5.1.1.27 The CCTV equipment shall respect and adapt to the architectural designs of stations and other facilities to avoid visual impacts on the constructive elements of the different facilities and shall fit and be installed harmoniously.
- 5.1.1.28 The VMS primary and backup central servers shall be installed in OCC.
- 5.1.1.29 The primary and backup central recording of the NVR system shall be installed in OCC.
- 5.1.1.30 Local NVRs in stations shall be installed in the dedicated CCTV distribution cabinet.
- 5.1.1.31 Backup of local recordings shall be provided by the primary/backup central recording in OCC.
- 5.1.1.32 The OCC building and depot outdoor perimeter shall be equipped with dome and PTZ cameras. The technical premises in OCC, where the central equipment of the CHSR system is located, shall also be equipped with dome cameras.
- 5.1.1.33 Types of CCTV cameras to be installed in stations should include, but not be limited to dome, dome panoramic, bullet, box, and PTZ cameras.



- 5.1.1.34 Inside the technical building (or container), cabling shall be done using halogen-free cables that are pulled through halogen-free pipes (in the wall, fixed in a suspended ceiling, raised floor), or laid in cable trays in the suspended ceiling voids/raised floors/cable channels or in a floor distribution system.

5.1.2 CCTV Camaras

- 5.1.2.1 The CCTV camera's resolution shall be at least 4K or the highest commercially available resolution.
- 5.1.2.2 The TSCC Contractor shall carry out a value engineering exercise to investigate the viability of using 4MP (2560 x 1440 pixels) cameras.
- 5.1.2.3 The CCTV cameras' frame rate shall be at least 25 frames per second.
- 5.1.2.4 The CCTV cameras shall have a True Wide Dynamic Range (120dB WDR).
- 5.1.2.5 The CCTV cameras shall have at least a minimum lux rating for color images of 0.0005 lux.
- 5.1.2.6 The CCTV cameras shall have at least a minimum lux rating for black and white images of 0.0001 lux.
- 5.1.2.7 All cameras shall have image stabilization.
- 5.1.2.8 PTZ cameras shall be capable of auto-tracking.
- 5.1.2.9 The PTZ camera shall be capable of panning, tilting and zooming simultaneously.
- 5.1.2.10 The PTZ cameras shall have the capability of setting and recalling pre-set positions.
- 5.1.2.11 PTZ speed shall be configurable.
- 5.1.2.12 The PTZ shall return to home after a configurable period of inactivity.
- 5.1.2.13 The PTZ cameras shall be capable of achieving the inspection or strong identification pixel density for the area they are covering.
- 5.1.2.14 The PTZ camera shall support common protocols for seamless integration and control, such as ONVIF (Open Network Video Interface Forum).
- 5.1.2.15 The pan and tilt range capability of the PTZ cameras shall be sufficient to monitor the location.
- 5.1.2.16 The Automatic Number Plate Recognition (ANPR) cameras shall be provided at Depot and Station Vehicle Entrances and Exits.
- 5.1.2.17 ANPR cameras capture and digitalize images from license plates with very high precision (99% or more).
- 5.1.2.18 ANPR equipment shall work in complex/extreme conditions such as moving targets, very open angles, poor ambient light, fog, dirt, etc.
- 5.1.2.19 The CCTV cameras' images shall be free from interference or distortion.
- 5.1.2.20 The CCTV cameras' images shall be clear and sharp in all lighting conditions.
- 5.1.2.21 The CCTV cameras' images shall have an accurate color representation.

5.2 Environmental Conditions Requirements

- 5.2.1 The TSCC Contractor's CCTV system design shall be appropriate for, and resilient to, the local environmental and climatic conditions at each installation site.
- 5.2.2 All outdoor CCTV cameras shall be installed in weatherproof, CCTV camera housings that ensure the quality of the video image at a lower temperature and/or high humidity.



- 5.2.3 All outdoor CCTV cameras shall be protected against sunlight by sun protection.
- 5.2.4 Camera housing and housing accessories shall comply with APTA IT-CCTV-RP-001 (or later).
- 5.2.5 The CCTV system design shall be compliant (not limited to) to the international standards listed in Chapter 2.4, relevant to Lighting Protection.
- 5.2.6 CCTV cameras shall be protected from vandalism through cages or screens. The TSCC Contractor shall take prior approval from the Authority to ensure the locations of CCTV cameras on which these cages or screens should be installed.
- 5.2.7 Bird repellent spikes shall be used for outdoor CCTV cameras. The TSCC Contractor shall obtain prior approval from the Authority to ensure the locations of CCTV cameras on which these spikes should be installed.
- 5.2.8 All equipment shall be protected from damage or degradation in performance due to shock or vibration as experienced in the railway environment.

5.3 Operational Requirements for CCTV

- 5.3.1 The TSCC Contractor's CCTV System design shall ensure compliance with the California High-Speed-Rail operational rules and operational concept when (at least):
 - Defining the locations required for the placement of the CCTV equipment.
 - Defining messages, alarms, warnings, and notification levels and thresholds.
 - Developing alarm triggering procedures.
 - Implementing alarms, protocols, and procedures for the CCTV System.
- 5.3.2 The CCTV system shall include intelligent event detection and alerting capabilities to assist operators in identifying items of interest. The system shall minimize the need for continuous multi-screen monitoring by automatically highlighting relevant video feeds, such as motion detection, unauthorized access, loitering, or object abandonment, through visual or audible alerts in the ICSS. This shall enable focused operator response and reduce cognitive load.
- 5.3.3 The system shall allow the Operator to specify a date/time range and one or more CHSR System locations for which all associated CCTV recordings shall be retained beyond the standard retention period, until a specified date or until manually cleared, to support investigations or legal proceedings.
- 5.3.4 The system shall allow operators to tag and export video segments related to specific events and associate them with incident IDs or reports, with audit trails maintained for all exports.
- 5.3.5 Authorized personnel must have secure, Role Based Access Control permissions to retrieve video recordings from the CCTV system through a VMS at OCC. The TSCC Contractor shall obtain approval from the Authority for the user access rights and retrieval procedures for recording.
- 5.3.6 Operators shall be able to define and modify geo-fenced zones within the VMS using an intuitive graphical interface, with the ability to set activation time windows and object-type alert filters (e.g. person, vehicle, wildlife).
- 5.3.7 The system shall notify Operators of geo-fence breaches with clearly identifiable alerts, including the camera ID, location, object type detected, and timestamp.
- 5.3.8 The system shall allow Operators to acknowledge, silence, or escalate geo-fence alerts, with actions recorded in an audit log.



- 5.3.9 The VMS shall provide intuitive playback functionality, including timeline navigation, variable playback speeds, and filtering based on metadata such as date/time, camera, event type, or object classification.
- 5.3.10 The CCTV system shall support concurrent access by multiple authorized users, with user actions tracked in an audit log and mechanisms to avoid conflicting control of camera PTZ functions.

5.4 Functional Requirements for CCTV

5.4.1 General requirements

- 5.4.1.1 Normal operation of the CCTV system shall be performed via the Operator ICSS Workstation as part of the ICSS System.
- 5.4.1.2 The CCTV system shall be centrally managed, with the ability to assign different user rights and record event history (time, place, and ID).
- 5.4.1.3 CCTV cameras must be able to transmit, and the storage unit receivers must be able to accept at least two simultaneous, individually configured streams of different resolution and/or diverse types of coding.
- 5.4.1.4 In highly critical areas CCTV cameras shall provide at least two viewpoints to the video surveillance spot.
- 5.4.1.5 The CCTV system shall save all data that can be filtered per the desired parameters in the future.
- 5.4.1.6 The CCTV system shall save recording of events for playback and evidential purposes for a minimum of 30 days. Video recordings shall be allowed to specify start date, time duration, and export by the operator.
- 5.4.1.7 The CCTV system shall support an encryption mechanism during the video exportation process to ensure the integrity of the exported video.
- 5.4.1.8 The CCTV system shall offer a means to verify that no alteration of the exported video record was performed. All images must contain a digital signature to allow for the chain of evidence to be preserved as defined in APTA IT-CCTV-RP-001 (or later).
- 5.4.1.9 The CCTV system shall allow the Operator to save the exported video on external media (network drive, USB drive).
- 5.4.1.10 The CCTV system shall provide surveillance coverage at night and during inclement weather.
- 5.4.1.11 Recognition, Monitoring, Identification, and video analytic application functions shall be applied on all locations according to relevant design guidelines, if any, or shall be determined by the TSCC Contractor, and elaborated during the detailed design stage.
- 5.4.1.12 The CCTV System in the OCC shall be connected to all CCTV components across the CHSR System via the Digital Communication Network (DCN), with connectivity provided in a redundant architecture to ensure continuous operation.
- 5.4.1.13 The VMS shall provide a centralized event, end-user rights, and video recording distribution management.
- 5.4.1.14 The VMS shall be capable of remotely managing and configuring cameras and devices directly associated with the CCTV system from multiple vendors using open source and non-proprietary protocols such as the Open Network Video Interface Forum (ONVIF) Profile S.
- 5.4.1.15 The CCTV system shall be configurable for showing live video from a camera based on an alarm input from another sub-system, such as EACS and Fire Protection System.



5.4.1.16 In case of a safety and security-related incident, an audible alarm shall be triggered, and the image of the best-positioned CCTV camera shall be automatically displayed to a predefined monitor at the OCC. The alarm shall be acknowledged by the Operator to silence the alarm.

5.4.1.17 The safety and security-related incidents shall include, but not be limited to intrusion, unauthorized access, fire detection, direct line telephone calls, falling vehicle detection, falling object detection, wildlife detection, and overcrowding.

5.4.2 CCTV coverage requirements

5.4.2.1 The CCTV Coverage shall be provided at Stations, including but not limited to:

- 95% of the Concourse and Platform areas.
- Access to the Back of the House, including Equipment Rooms.
- All corridors.
- All paid and unpaid areas.
- All cash and ticket offices.
- Ticket gate barrier lines and the approach/run-off areas on each side.
- Cash handling areas and along the cash transfer route.
- All station entrances, Emergency exits, and their associated run-off areas.
- External station pathways to cover the linkway or path towards the Carpark (if any).
- Passenger Intercom points in strategic areas.
- Platform emergency stop plungers.
- Strategic access control points.
- All stairs and escalators, together with associated landing areas.
- Inside the Strong Room.
- The interior of all elevators.
- Other areas, if any, as required by operation and security.

5.4.2.2 The CCTV Coverage shall be provided at facilities, including but not limited to:

- All entrances/exits into the depot area.
- All entrances to and within secure areas such as the Operations Control Center.
- Depot perimeter fences.
- The automatic train wash plant.
- Substations.
- Stabling area, maintenance tracks.
- Workshops.
- Car park area.
- Interior of elevators.
- Fire escape routes.
- All buildings in the depot area.
- Other areas, if any, as required by operation and security.



5.4.3 The CCTV Coverage shall be provided at wayside facilities, including but not limited to:

- Shelter sites.
- Radio sites.
- Equipment cabinet sites.
- Traction Power substations.
- Tunnel & trench portals.
- Transfer Tracks
- Other areas, if any, as required by operation and security.

5.4.4 Surveillance of forecourt, access to the depot building, the station's building, parking, and perimeter around the building shall be enabled by CCTV cameras:

- inner perimeter = standoff distance (up to 15 – 30m from building envelope) shall provide at least recognition level.
- outer perimeter (behind the inner perimeter) – shall provide at least a monitoring level.

5.4.5 Surveillance of entrances and exits to the station building (both staff and passengers) shall be enabled by CCTV cameras with an identification analytic video application function.

5.4.6 Surveillance of key points such as the start and end point of passenger flows shall be enabled by CCTV cameras with recognition and identification analytic video application function.

5.4.7 Surveillance of ticket office, validation gates, if any, and area close to gates, platforms shall be enabled by CCTV cameras with identification analytic video application function.

5.4.8 Surveillance of equipment rooms and access to the Back of the House area shall be enabled by CCTV cameras with an identification analytic video application function.

5.4.9 Surveillance of elevators shall be enabled by CCTV cameras with an identification analytic video application function.

5.4.10 Video Analytics System (VAS)

5.4.10.1 The VAS shall use Machine Learning and Deep Learning algorithms to enable real-time detection, classification, and tracking of objects, people, and events in CCTV footage, enhancing security through automated threat identification and behavior analysis.

5.4.10.2 The VAS shall continually improve its effectiveness and performance using machine learning.

5.4.10.3 The trained video analytics models, developed using Machine Learning and Deep Learning algorithms, shall be immediately functional upon deployment without requiring an on-site learning period.

5.4.10.4 All video analytics models, both server and edge-based, shall be designed to meet the precise detection (above 98%) and classification (above 95%) rates required.

5.4.10.5 The VAS shall also allow for certain adjustments to finetune its performance according to the specific user needs of the Operator.

5.4.10.6 The VAS shall provide a fine adjustment of the alerts it sends to the ICSS.

5.4.10.7 The VAS shall maximize its effectiveness by minimizing false alarms and maintaining a high detection accuracy, with a goal to keep the false alarm rate below 3%.

5.4.10.8 The Operator shall be able to easily dismiss alarms as false alarms and the VAS shall apply learnings to the models.



- 5.4.10.9 The VAS shall seamlessly integrate with the VMS, generating metadata that facilitates alert generation and subsequent incident search.
- 5.4.10.10 The CCTV system shall provide a variety of automatic analytics options for detection of anomalous events in locations as determined by the TSCC Contractor via a risk assessment process in conjunction with Security, Operations, and Maintenance personnel.
- 5.4.10.11 Video analytics available for use shall be at a minimum, as described APTA Video Content Analytics (VCA) Recommended Practice Transit Applications Draft (www.tswg.org); APTA IT-CCTV-RP-001 (or later) as issued at the time of NTP.
- 5.4.10.12 CCTV system shall support and shall implement video analytics applications, including, but not limited to: stop vehicle detection, overcrowding (or crowd density) application, intrusion detection and cross line detection, left objects detection, tailgating, tampering, automatic tracking, loitering, face recognition, person of interest tracking, virtual border crossing detection and automatic emergency detection.
- 5.4.10.13 The alert function or action the system should take when an event is detected shall be applicable with the requirement specified in APTA IT-CCTV-RP-001 (or later).
- 5.4.10.14 The CCTV system shall support the configuration of geo-fenced zones by the Operator using the VMS, allowing virtual perimeters to be defined on a map or video overlay for specific areas within the CHSR System.
- 5.4.10.15 Each geo-fenced zone shall support the assignment of an activation period, including start date/time, end date/time, or a permanent (always-on) status.
- 5.4.10.16 The system shall associate all cameras covering a geo-fenced area with that zone automatically or through Operator assignment, enabling intelligent event detection within the defined perimeter.
- 5.4.10.17 The system shall be capable of detecting and classifying intrusions into geo-fenced zones by persons, vehicles, and wildlife, based on video analytics.
- 5.4.10.18 Upon detection of an intrusion within an active geo-fenced zone, the system shall generate real-time audible and visual alarms to the Operator via the ICSS.
- 5.4.10.19 Geo-fencing alerts shall be retained with associated video clips for post-incident review, searchable by zone name, object type, and time.

5.5 Performance Requirements for CCTV

5.5.1 General Requirements

- 5.5.1.1 The image sensor used in CCTV cameras must match the image resolution used for at least 1:1. CCTV cameras with the actual pixel count of the image sensor lower than that of the image shall not be allowed.
- 5.5.1.2 The compression system of CCTV should be configured to allow at least H.264 or H.265. In the event of any conflict between this specification and referenced standards or guidelines, the TSCC Contractor shall apply the latest proven and widely accepted technology and industry practices that fulfill the intended functional requirements.
- 5.5.1.3 The signal-to-noise ratio of the CCTV cameras shall not be less than 50 db.
- 5.5.1.4 CCTV cameras need to meet the required parameters of a good surveillance CCTV camera by their technical characteristics, i.e., have auto-iris lenses, high light sensitivity, etc.



- 5.5.1.5 The CCTV recordings for each connected camera shall be at 4K, 25fps, and 16:9 aspect ratio resolution.
- 5.5.1.6 The NVRs in the OCC shall enable storage of all footage for a minimum of 30 days, or as otherwise agreed with the Authority.
- 5.5.1.7 Backup central recording of the NVRs in OCC shall enable backup of footage from the local NVRs (depot, stations, or wayside facilities) for at least 30 days.
- 5.5.1.8 The local NVRs in stations, depots, or any wayside facilities shall enable storage of all footage for at least 30 days.
- 5.5.1.9 Local storage of video recordings in the event of a loss of connection between the CCTV camera and the network video recorder shall enable storage of all footage for at least 7 days.
- 5.5.1.10 The NVRs shall provide a spare recording capacity of 20% in each location.
- 5.5.1.11 The incident-based video recordings must be retained for a minimum of 90 days or as otherwise agreed with the Authority to ensure sufficient time for investigation and compliance with regulatory requirements.
- 5.5.1.12 All live and recorded video streams shall contain text identifying camera location, date, time, and be synchronized with the Network Timing System (NTS).
- 5.5.1.13 CCTV cameras shall use either open standard or non-proprietary protocols for communicating with the CCTV and video management systems, such as the Open Network Video Interface Forum (ONVIF) Profile S.

5.5.2 Safety Requirements

- 5.5.2.1 The CCTV system shall comply with the safety requirements defined in the Schedule 1.

5.6 RAM Requirements

- 5.6.1.1 The CCTV system shall comply with the RAM requirements defined in Schedule 1 and the Authorities' RAM management plan.

5.7 Cybersecurity and Security Requirements

- 5.7.1 The TSCC Contractor's design for CCTV shall be in full compliance with the Authority's cybersecurity policies and Cybersecurity Technical Specification.
- 5.7.2 The CCTV system shall implement Role Based Access Control (RBAC), with user roles defined according to their responsibilities and corresponding access permissions.
- 5.7.3 Individual user accounts shall be created for authorized personnel who need access to the CCTV system.
- 5.7.4 Each user shall have a unique username and password for authentication and audit purposes.
- 5.7.5 Strong Password Policies shall be enforced.
- 5.7.6 User Access Control shall be used to control:
 - user access to specific cameras, video streams, or areas within the CCTV system.
 - user access to specific functions within the CCTV system.
 - user access to viewing and exporting recordings.
- 5.7.7 The CCTV system shall provide appropriate access security measures to prevent the connection of unauthorized devices.



- 5.7.8 The CCTV system shall maintain audit logs of user access, configuration changes, video export activities, and system events. These logs shall be secured and retained in accordance with the Authority's data retention policy.
- 5.7.9 The CCTV system shall encrypt data in transit and at rest using industry-standard encryption protocols.
- 5.7.10 The TSCC Contractor shall ensure that all components of the CCTV system receive timely security patches and firmware/software updates.
- 5.7.11 CCTV systems shall have a System Owner who shall be accountable for cybersecurity risk ownership and mitigation.
- 5.7.12 The System Owner shall ensure that cybersecurity risk assessments and threat modelling exercises are appropriately resourced.
- 5.7.13 CCTV Camera procurement shall be informed by the cybersecurity technical specification requirements to ensure that vulnerable devices are not procured.
- 5.7.14 Any connectivity to CCTV cameras shall be strictly controlled and documented, many CCTV cameras have an associated cloud-based application for remote monitoring purposes, where these solutions are used, they must be co-engineered with the Cybersecurity Lead.
- 5.7.15 Power over Ethernet networks and devices used for CCTV cameras must be compliant with the network security requirements outlined in the Cybersecurity Technical Specification.



6 INTERFACES REQUIREMENTS

6.1 General Requirements

6.1.1 Interfaces are classified as below:

- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR contractors);
- External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors);
- Internal interfaces between systems within the TSCC scope.

6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.

6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.

6.1.4 The TSCC Contractor shall achieve interoperability by also proactively managing the interfaces between the various System and Sub-System elements.

6.2 External Interface for CCTV

6.3 External Interfaces – facilities contractor

6.3.1 Visible equipment shall be integrated harmoniously with the architecture of the facilities.

6.3.2 The TSCC Contractor shall design and deploy a suitable CCTV system in every location, in coordination with civil and architectural teams.

6.3.3 The TSCC Contractor shall coordinate with all interfacing parties (Civil, E&M, etc.) to ensure an unobstructed field of view and proper lighting conditions for every camera.

6.3.4 The TSCC Contractor shall interface with the facilities contractor regarding the installation of CCTV inside the elevators.

6.3.5 The TSCC Contractor shall install all Telephony core network equipment in the OCC being provided by the facilities contractor.

6.3.6 The TSCC Contractor shall provide to the facilities contractor:

- Equipment dimensions
- Equipment clearances requirements
- Equipment mounting and fixings requirements
- Cable routes/containment requirements
- Equipment loadings
- Installation and maintenance requirements
- Equipment heating loads
- Equipment cooling loads
- Equipment hydraulic requirements

6.3.7 To be provided by facilities contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:



- Room dimensions and layouts
- Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
- Room raised floor system
- Delivery access routes.
- Maintenance access routes

6.4 External Interfaces – stations contractor

- 6.4.1 Visible equipment shall be integrated harmoniously with the architecture of the stations.
- 6.4.2 The TSCC Contractor shall design and deploy a suitable CCTV system in every location, in coordination with civil and architectural teams.
- 6.4.3 The TSCC Contractor shall coordinate with all interfacing parties (Civil, E&M, etc.) to ensure an unobstructed field of view and proper lighting conditions for every camera.
- 6.4.4 The TSCC Contractor shall interface with the station contractors regarding the installation of CCTV inside the elevators.
- 6.4.5 The TSCC Contractor shall provide to the station contractor:
- Equipment dimensions
 - Equipment clearances requirements
 - Equipment mounting and fixings requirements
 - Cable routes/containment requirements
 - Equipment loadings
 - Installation and maintenance requirements
 - Maintenance access routes

6.5 Internal Interfaces

6.5.1 Interface with Digital Communications Network (DCN)

- 6.5.1.1 The CCTV system shall have an interface with the Digital Communications Network (DCN) for the transport of CCTV data in a secure and reliable way and the interconnection of all CCTV devices along the California High-Speed-Rail Line.

6.5.2 Interface with Network Timing System (NTS)

- 6.5.2.1 The CCTV system shall have an interface with the Network Timing System (NTS) to ensure accurate current timestamping and to provide time synchronization to the CCTV System.

6.5.3 Interface with Telephony System

- 6.5.3.1 The CCTV system shall have an interface with the Telephony System to trigger the transfer of corresponding video sequences to the Operators via the ICSS workstation.

6.5.4 Interface with Electronica Access Control System (EACS)

- 6.5.4.1 The CCTV system shall have an interface with the EACS System to trigger the transfer of corresponding video sequences to the Operators via the ICSS workstation.

6.5.5 Interface with Fire Protection System



6.5.5.1 The CCTV system shall have an interface with the Fire Protection System to trigger the transfer of corresponding video sequences to the Operators via the ICSS workstation.

6.5.6 Interface with Low Voltage Power System

6.5.6.1 The CCTV system shall have a redundant interface with the Low Voltage Power System to ensure an uninterruptible power supply.

6.5.7 Interface with Integrated Control and Supervision System

6.5.7.1 The CCTV system shall have an interface with the ICSS System on standard protocols to allow status monitoring of the CCTV equipment.

6.5.7.2 All detected CCTV system faults and major alarms shall be reported to the ICSS. The faults shall include, but not be limited to, hardware failures, image quality, and recording issues.

6.5.7.3 The CCTV system shall report image quality faults to the ICSS, including but not limited to camera out of focus, camera image distortion, change in camera orientation, and change of field of view.

6.5.7.4 The ICSS shall trigger the CCTV system for the transfer of video sequences corresponding to alarms received by the ICSS from CHSR subsystems.

6.5.8 Interface with Enterprise Asset Management Systems (EAMS)

6.5.8.1 The CCTV System shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards. Refer to 2.4.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the design life requirements.
- 7.1.3 The CCTV System shall be complete with all equipment, supporting structures, hardware, licenses, software, cabling, and ancillary services which are useful for efficient operation of the CCTV System components. Such accessories and materials shall be deemed to be within the scope of this specification, whether specifically mentioned or not.
- 7.1.4 All special tools and test equipment intended for the configuration of the CCTV System shall be deemed to be within the scope of this specification, whether specifically mentioned or not.

7.2 Software and Hardware Requirements

- 7.2.1 Virtualized, cloud (on-premises) solutions may be proposed by the TSCC Contractor.
- 7.2.2 All central servers may be on-premises or virtualized machines to ease systems evolution, complying with the Cybersecurity requirements.
- 7.2.3 The CCTV cameras shall be protected against the electrical and magnetic atmosphere that exists in a typical electrified railway environment.
- 7.2.4 Low toxicity, low smoke emission, low flammability, zero halogen fire retardant cable shall be used for the distribution power and signals to the CCTV cameras.
- 7.2.5 Third parties' cloud solutions, or third-party video data processing shall not be allowed.
- 7.2.6 Hot-swappable elements, such as fans and power supplies, should be swappable without tools.
- 7.2.7 The Operating of all the IT/Network devices shall be provided the latest stable release.
- 7.2.8 All the application software shall be upgraded to the latest stable release and shall support all the requirements specified.
- 7.2.9 For the housing accessories, a minimum housing rating shall be IP66 as defined in section 2.12.1 NEMA environmental rating in APTA IT-CCTV-RP-001 (or later).

7.3 EMC Requirements

The CCTV system shall be fully immune and protected from any Electromagnetic Interference (EMI) with the traction power, multi-tubular cabling, and Radio Frequency Interference (RFI). The EMI emissions shall be mitigated in accordance with applicable standards EN 50122 or APTA IT-CCTV-RP-001 (or later) or equivalent.



8 TOLERANCES

Not applicable to CCTV system.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 The TSCC Contractor shall supply and deliver all components related to the CCTV System as per Schedule 16.

9.2 Specific Requirements

9.2.1 The CCTV System scope of supply and delivery shall include (not limited to):

- Central and local servers.
- Video walls and video wall controller (if needed)
- CCTV cameras.
- Amplifiers/Injectors (if needed).
- Cabling and connectors.
- Racks.
- Software architecture, including full definition of protocols used.
- Video Management System.
- Network Video Recorders.
- Video Analytics System
- HW/SW licenses.
- Auxiliary elements and gear (cases, bird repellent spikes, attachments, bindings, testing equipment, etc.).
- Spare parts.
- Maintenance laptops.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.

12.2 Specific Requirements

12.2.1 Failure event test cases, Interface test cases, video analytic functions test scenarios and the following information (not limited to) shall be recorded and reported during the test procedure:

- In the event of the main central recording or local recording failure, backup shall be taking place as the master one.
- In the event of video management solution main central server failure, backup shall be taking place as the master one.
- All interface tests that trigger the CCTV systems to be automatically recorded and displayed to a predefined monitor, e.g., direct telephone line, EACS, FPS, etc.
- Video analytic alert function test scenario according to the system requirement in APTA IT-CCTV-RP-001 (or later) e.g. Stop vehicle detection, Overcrowding (or crowd density) application, Intrusion detection and cross line detection, left objects detection, Tailgating, Tampering, Automatic tracking, Loitering, Face recognition, Virtual border crossing detection and Automatic emergency detection. A decision should be made regarding what type of activity should trigger an alert and then what form that alert should take.

12.2.2 CCTV camera fields of view shall be tested in the field to demonstrate that the live and recorded images meet the intended function and specification identified by the TSCC Contractor.

12.2.3 CCTV field of view study report shall be submitted for the Authority's approval.



13 SUBMITTALS

13.1 General Requirements

13.1.1 General submittal requirements are specified in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence CCTV subsystem reliability, availability, and maintainability characteristics.

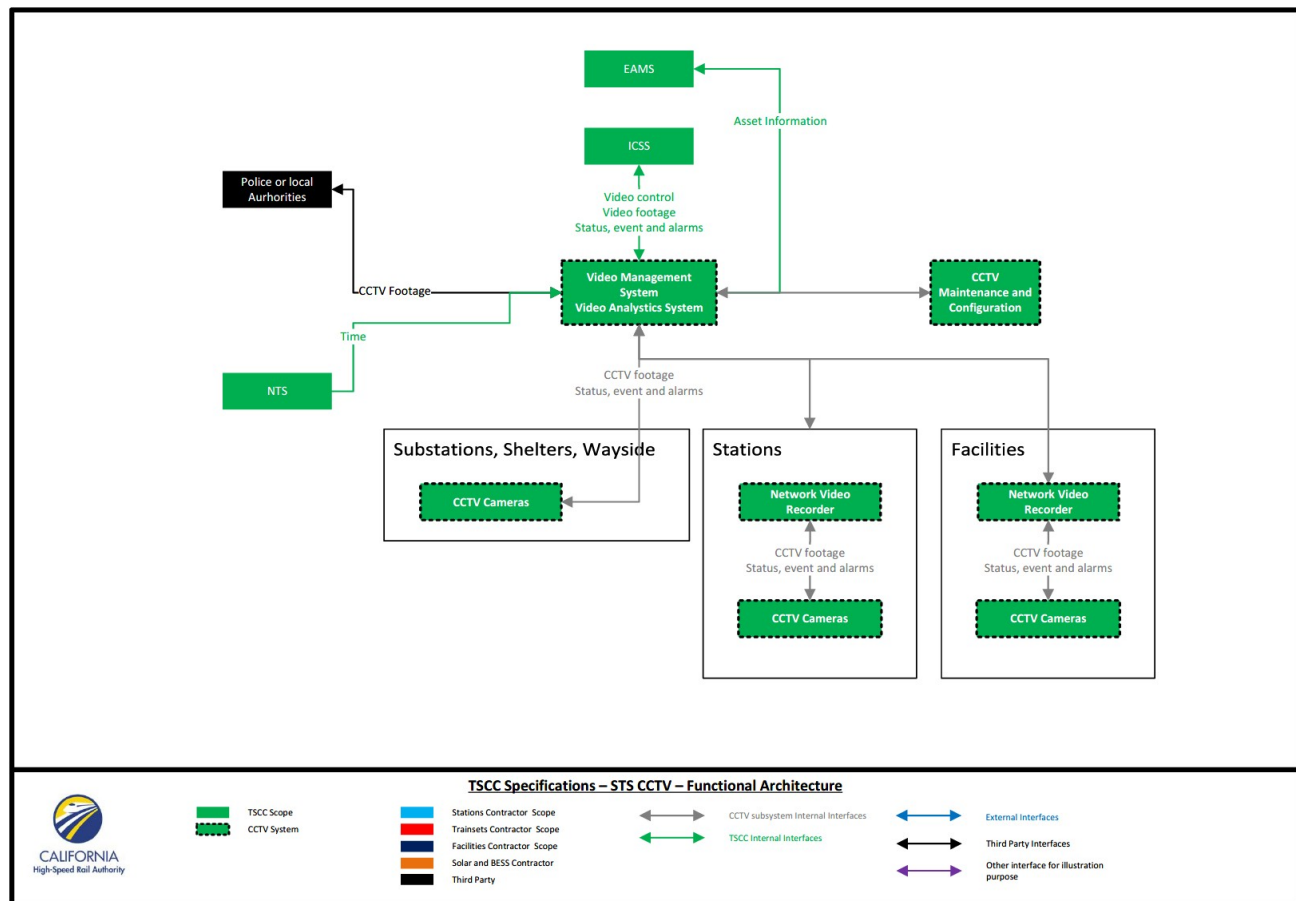


16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.

APPENDIX A TO EXHIBIT 5(K) CLOSED-CIRCUIT TELEVISION (CCTV)



Schedule 5(I)

Network Timing System (NTS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0016 – Network Timing System (NTS)

Rev. 0.0

Authorized:

A handwritten signature in black ink, appearing to read "Harshal".

Harshal Jadhav, Telecom System Lead

15 October 2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Thomas".

Thomas Newey, Telecoms Lead

10/15/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Bruno".

Bruno Comperat, Deputy Director of Rail Engineering

10/16/2025

Date

Approved:

A handwritten signature in black ink, appearing to read "Ryan Scott".

Ryan Scott, Director of Rail Engineering

10/16/2025

Date

Released:

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Amit Joshi, Configuration Manager

10/16/2025

Date



Document Revision History – NTS Specifications**First Edition****September 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION.....	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.1	GENERAL	6
2.2	DESIGN GUIDELINES.....	6
2.3	TSI	6
2.4	STANDARDS	6
2.5	UIC RECOMMENDATIONS	9
2.6	OTHER DOCUMENTS	9
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	10
3.1	GENERAL	10
4	SYSTEM DESCRIPTION	11
4.1	PURPOSE OF THE NTS.....	11
4.2	SYSTEM DEFINITION.....	11
4.3	SYSTEM OPERATIONAL CONTEXT	11
4.4	DESIGN LIFE	11
5	SYSTEM REQUIREMENTS.....	12
5.1	GENERAL REQUIREMENTS.....	12
5.2	ENVIRONMENTAL CONDITIONS REQUIREMENTS.....	13
5.3	OPERATIONAL REQUIREMENTS	13
5.4	FUNCTIONAL REQUIREMENTS.....	13
5.5	PERFORMANCE REQUIREMENTS.....	15
5.6	CYBERSECURITY AND SECURITY REQUIREMENTS.....	18
6	INTERFACES REQUIREMENTS.....	19
6.1	GENERAL REQUIREMENTS.....	19
6.2	EXTERNAL INTERFACES – STATION CONTRACTOR.....	19
6.3	EXTERNAL INTERFACES – FACILITIES CONTRACTOR	19
6.4	INTERNAL INTERFACE FOR NTS.....	20
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS	22
7.1	GENERAL REQUIREMENTS.....	22
7.2	SOFTWARE AND HARDWARE REQUIREMENTS	22
7.3	EMC REQUIREMENTS.....	23
8	TOLERANCES	24
9	SCOPE OF SUPPLY AND DELIVERY	25
9.1	GENERAL REQUIREMENTS.....	25
9.2	SPECIFIC REQUIREMENTS	25
10	MANUFACTURING.....	26
10.1	GENERAL REQUIREMENTS.....	26



11	INSTALLATION AND INTEGRATION.....	27
11.1	GENERAL REQUIREMENTS.....	27
12	TESTING & ACCEPTANCE	28
12.1	GENERAL REQUIREMENTS.....	28
13	SUBMITTALS.....	29
13.1	GENERAL REQUIREMENTS.....	29
14	QUALITY MANAGEMENT	30
14.1	GENERAL REQUIREMENTS.....	30
15	ADDITIONAL INFORMATION REQUESTED	31
15.1	GENERAL REQUIREMENTS.....	31
16	LOGISTICS	32
16.1	GENERAL REQUIREMENTS.....	32



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Network Timing System (NTS), hereinafter: NTS.
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of the NTS is presented in Appendix A.
- 1.1.4 The requirements are formulated using the following words and their meanings:
 - "Shall": Indicates a mandatory requirement that must be strictly implemented; a waiver from a mandatory requirement is permissible only with approval of a design variance.
 - "Should": Indicates a preferred course of action; a design variance is not required if it is not exercised.
 - "Must": Indicates an obligation or a mandatory requirement.
 - "May": Indicates a permissible course of action within the limits of the standards; a design variance is not required if it is not exercised.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines, and specifications provided in this chapter for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, and training.

2.2 Design Guidelines

- 2.2.1 The latest version of the following Design Guidelines shall be applied:

ID	Code	Title
[R1]	Design Criteria Manual	Chapter 12 – Communication Systems and Train Control
[R2]	AREMA Standards	Chapter 17 – High-Speed Rail Systems

TABLE 33 DESIGN GUIDELINES

2.3 TSI

- 2.3.1 There are no applicable TSIs for the NTS.

2.4 Standards

- 2.4.1 The TSCC Contractor shall fully consider and apply the following standards, the in-force standards shall be applied.

ID	Code	Title
[R1]	AES	Advanced Encryption Standard specification for the encryption of electronic data
[R2]	DIN 41091-1	Dials for electric clocks; minute-stroke dials
[R3]	DIN 41091-4	Dials for electric clocks; number dials
[R4]	EN 300 386	Telecommunication network equipment; Electro Magnetic Compatibility (EMC) requirements; Harmonized Standard covering the essential requirements of the Directive 2014/30/EU
[R5]	EN 50112-1	Railway applications - Fixed installations - Electrical safety, earthing and the return circuit -- Part 1: Protective provisions against electric shock
[R6]	EN 50112-2	Railway applications - Fixed installations - Electrical safety, earthing and the return circuit - Part 2: Provisions against the effects of stray currents caused by d.c. traction systems
[R7]	EN 50121	Railway Applications – Electromagnetic Compatibility
[R8]	EN 50121-3-2	Railway applications - Electromagnetic compatibility - Part 3-2: Rolling stock - Apparatus
[R9]	EN 50121-4	Railway applications - Electromagnetic compatibility - Part 4: Emission and immunity of the signaling and telecommunications apparatus
[R10]	EN 50125	Railway applications - Environmental conditions for equipment



ID	Code	Title
[R11]	EN 50126-1	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
[R12]	EN 50126-2	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
[R13]	EN 50128	Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems
[R14]	EN 50159	Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems
[R15]	EN 55024	Information technology equipment. Immunity characteristics. Limits and methods of measurement
[R16]	EN 60065	Audio, video and similar electronic apparatus - Safety requirements
[R17]	EN 60297-3	Mechanical structures for electronic equipment - Dimensions of mechanical structures of the 482,6 mm (19 in) series - Part 3-100: basic dimensions of front panels, sub racks, chassis, racks and cabinets
[R18]	EN 60529	Degrees of protection provided by enclosures (IP Code)
[R19]	EN 60715	Dimensions of low-voltage switchgear and control gear. Standardized mounting on rails for mechanical support of switchgear, control gear and accessories
[R20]	EN 61000-6	Electromagnetic compatibility (EMC) - generic standards
[R21]	EN 61000-6-2	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity standard for industrial environments
[R22]	EN 61000-6-4	Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments
[R23]	EN 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
[R24]	EN 62305	Protection against lightning
[R25]	IEC 60068-2-27	Environmental testing Tests. Test Ea and guidance. Shock
[R26]	IEC 60068-2-6	Environmental testing Tests. Test Fc. Vibration (sinusoidal)
[R27]	IEC 60068-2-75	Environmental testing Tests. Test Eh: Hammer tests
[R28]	IEC 61000-3-6	Electromagnetic compatibility (EMC) - Part 3: Limits - Section 6: Assessment of emission limits for distorting loads in MV and HV power systems - Basic EMC publication
[R29]	IEC 61000-3-7	Electromagnetic compatibility (EMC) - Part 3-7: Limits - Assessment of emission limits for the connection of fluctuating installations to MV, HV and EHV power systems
[R30]	IEC 61000-5-2	Electromagnetic compatibility (EMC) - Part 5: Installation and mitigation guidelines - Section 2: Earthing and cabling
[R31]	IEC 61643	Low-voltage surge protective devices



ID	Code	Title
[R32]	IEC 61850-9-3	Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation
[R33]	IEC 62278	Railway Applications Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
[R34]	IEEE 1220	IEEE Standard for Application and Management of the Systems Engineering Process
[R35]	IEEE 1588v2	IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
[R36]	IEEE 60068-2-1	Environmental testing - Part 2-1: Tests - Test A: Cold
[R37]	IEEE 60068-2-30	Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)
[R38]	IPv4 and IPv6	Dual stack
[R39]	ISO / IEC 18028-2	Network security architecture for providing end-to-end network security Information Security Management System (ISMS).
[R40]	ISO 11064	Ergonomic design of control centers
[R41]	ISO 15408	International standard (Common Criteria) – Standard for computer security certification.
[R42]	ISO 7240-16:2007	Fire detection and alarm systems — Part 16: Sound system control and indicating equipment
[R43]	ISO/CEI 15288	Systems engineering - Systems life cycle processes
[R44]	ITU-T G.811	Timing characteristics of primary reference clocks
[R45]	ITU-T G.8261	Timing and synchronization aspects in packet networks
[R46]	ITU-T G.8262	Timing characteristics of a synchronous equipment slave clock
[R47]	ITU-T G.8264	Distribution of timing information through packet networks
[R48]	ITU-T G.8265.1	Precision time protocol telecom profile for frequency synchronization
[R49]	ITU-T G.8271/Y.1366	Time and phase synchronization aspects of telecommunication networks
[R50]	ITU-T G.8273.2/Y.1368.2	Timing characteristics of telecom boundary clocks and telecom time slave clocks for use with full timing support from the network
[R51]	ITU-T G.8275	Architecture and requirements for packet-based time and phase distribution
[R52]	NFPA 780	Standard for the Installation of Lightning Protection Systems
[R53]	NIST SP 800-125	Guide to Security for Full Virtualization Technologies.
[R54]	NIST SP 800-53	Recommended Security Controls for Federal Information Systems and Organizations.
[R55]	NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security.
[R56]	RFC 1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis,



ID	Code	Title
[R57]	RFC 4330	Simple Network Time Protocol (SNTP)
[R58]	RFC 7384	Security Requirements of Time Protocols in Packet Switched Networks
[R59]	RFC 8633	Network Time Protocol Best Current Practices
[R60]	SNMP	Simple Network Management Protocol
[R61]	SyncE	Synchronous Ethernet
[R62]	TIA / EIA 942-B	Telecommunications Infrastructure Standard for Data Centers

TABLE 34 LIST OF APPLICABLE STANDARDS

2.5 UIC Recommendations

2.5.1 Not applicable to NTS.

2.6 Other Documents

2.6.1 The following documents shall be referred:

ID	Document	Title
[R63]	Schedule 3	Safety, Security and RAM Requirements
[R65]	Schedule 16	Scope of Work
[R66]	Schedule 5(a) SPEC-0005	Cybersecurity specification

TABLE 35 OTHER DOCUMENTS

3 TERMS, DEFINITIONS, AND ABBREVIATIONS

3.1 General

- 3.1.1 All the terms, abbreviations, and definitions are provided in: Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of the NTS

- 4.1.1 The purpose of the Network Timing System (NTS) shall be to distribute a centralized and accurate time reference to all the equipment for the California High-Speed Rail system.

4.2 System Definition

- 4.2.1 An NTS is a synchronized timekeeping infrastructure used to ensure precise and consistent time coordination across distributed devices, systems, or components within a network.

4.3 System Operational Context

- 4.3.1 The mission of the NTS is to provide a centralized and accurate time reference to all the equipment for California High-Speed Rail systems and to broadcast the time-of-day to passengers in compliance with operational needs.

4.4 Design Life

- 4.4.1 The design life shall meet the requirements as specified in the Scope of Work document.
- 4.4.2 The design life requirements of the NTS shall allow for the pertinent evolution and technological change of the NTS throughout its life.
- 4.4.3 The TSCC Contractor shall ensure that the NTS components with shorter design lifespans shall be managed by scheduled technology refresh strategies and spares management plans.
- 4.4.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce NTS components (with equal or compatible technical specifications) for the entire design life required.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

- 5.1.1 The NTS shall be designed in accordance with the requirements described in this specification.
- 5.1.2 A redundant NTS equipped with Global Navigation Satellite System (GNSS) receivers (primarily GPS) shall be designed and installed in the Operational Control Centre (OCC) and shall be used to synchronize all systems requiring time synchronization.
- 5.1.3 The TSCC Contractor's NTS design shall consider Master clocks provided in OCC and Sub-master clocks for each station, OCC, depot, other facilities, etc.
- 5.1.4 The TSCC Contractor's NTS design shall consider slave clocks (analog and digital) for time-of-day information to be installed at each station, OCC, depot, maintenance facilities, train care facilities, traction power, solar sites, and wayside facilities along the California high-speed line.
- 5.1.5 Analog and digital slave clocks in facilities (control and technical rooms, depots, stations, platforms, etc.) shall be provided by the TSCC Contractor and shall be synchronized via the NTS.
- 5.1.6 The TSCC Contractor's NTS design for clocks shall consider external constraints such as resistance to shock, vandalism, waterproofing, dust, reflections, etc.
- 5.1.7 The Network Timing System (NTS) shall transmit, in real time and via the Digital Communications Network (DCN), at a minimum, the following time data elements:
- Year
 - Month
 - Day
 - Hour
 - Minute
 - Second
- 5.1.8 The TSCC Contractor shall ensure that the time displayed in the slave clocks is clearly and easily visible from any point of the public area (platforms, waiting area, etc.); the quantity and location of clocks shall be agreed with the Authority.
- 5.1.9 When an accurate time must be displayed, digital slave clocks shall be designed and installed, for instance, at OCC, Technical Rooms, Station Control Rooms, offices, etc.
- 5.1.10 Upon approval by the Authority and according to architectural and design criteria, some of the digital clocks may be embedded in the Customer Information Displays (CIS).
- 5.1.11 The use of analogue slave clocks makes it possible to increase the consultation distance of the time, and they shall be installed in the station entrance, hall, or concourse of each station, on platforms, in the large halls of the depot areas, or in the storage/shunting area. The offices of each station shall also be equipped with analogue slave clocks.
- 5.1.12 NTS shall be designed considering that the length of passenger platforms for stations is 400m, and in compliance with the station designs.
- 5.1.13 NTS clock design shall be compatible with California HSR branding, visual identity, signage system, and graphical charts, and be fully integrated in the overall station designs and shall take architectural constraints into account.



- 5.1.14 The TSCC Contractor's NTS design shall respect and adapt to the architectural designs of stations and other facilities to avoid impacts on the constructive elements of the different facilities and shall fit and be installed harmoniously.
- 5.1.15 Only technology systems with service-proven records for application on railway infrastructure shall be proposed by the TSCC Contractor.
- 5.1.16 NTS equipment shall be placed in locations where it does not infringe on the passage of people.

5.2 Environmental Conditions Requirements

- 5.2.1 The TSCC Contractor's NTS design shall respect local climatic conditions.
- 5.2.2 All equipment shall be protected from damage or degradation in performance due to shock or vibration as experienced in the railway environment.
- 5.2.3 The TSCC Contractor's design for the NTS shall comply with the following telecom-related environmental requirements (list non-exhaustive):
 - The equipment provided and installation-related material shall be adapted to the special local environmental conditions, e.g., stainless-steel fixations, housings, etc.
 - Based on the different installation sites, different ingress protection (IP) requirements shall be specified.
- 5.2.4 Outdoor NTS elements shall be resistant to high temperatures and de-icing agents.

5.3 Operational Requirements

- 5.3.1 The TSCC Contractor's NTS design shall ensure compliance with the California HSR operational rules and Operational Concept when (at least):
 - Defining the locations required for the placement of the displays for the analog and digital clocks for time of the day information.
- 5.3.2 The TSCC Contractor's NTS design shall allow the operation and maintenance of the main line and related local facilities as per Operational Concept.

5.4 Functional Requirements

- 5.4.1 A Network Time Server natively supporting IEEE 1588v2 Precision Time Protocol - PTP Master clock shall be installed in the technical room of the OCC. It shall be synchronized by a GNSS system (primarily GPS) via antennas ideally installed on the roof of the building (depending on the reception level).
- 5.4.2 All OCC equipment shall be synchronized by the OCC Master clocks.
- 5.4.3 The Master clocks, placed at the OCC, shall be interlinked to achieve full redundancy. Furthermore, in case of failure of the GNSS link of the Master clock, the other Master clock shall provide the time information received from its GNSS to this Master clock through the redundant path.
- 5.4.4 The NTS shall allow to handle leap seconds to ensure accurate and synchronized timekeeping (at least):
- 5.4.5 Leap second insertion and notification: The NTS shall have the capability to insert a leap second when required by international timekeeping authorities (e.g., International Earth Rotation and Reference Systems Service, IERS) and shall be able to receive and process leap second announcements and notifications from authoritative sources like the IERS or relevant national agencies. NTS shall be capable of automatically adjusting the time accordingly when a leap second is announced.



- 5.4.6 Traceability and record-keeping: The NTS shall maintain records of leap second events, including the date and time of insertion and any associated adjustments to the system's timekeeping, and shall ensure that historical data on leap seconds is available for reference and auditing purposes.
- 5.4.7 The NTS receives time-of-day (ToD) source from the GNSS. In the absence of a valid GNSS signal, the Master clock shall operate in free-running mode with the internal clock supplying the time signal. On restoration of the GNSS signal, the receiver shall validate the GNSS signal automatically without any manual intervention. After successful validation, the Master clock shall self-correct, if necessary.
- 5.4.8 In each station or facility, a Sub-Master clock shall be installed. It shall be synchronized with the OCC Master clocks and shall ensure the synchronization of all local equipment.
- 5.4.9 In the absence of a valid Master clock signal, the Sub-Master clocks shall operate in free-running mode with an internal clock supplying the time signals. On restoration of the Master clock signal, the Sub-Master clocks shall validate the signal. After the successful validation, the Sub-Master clocks shall self-correct, if necessary.
- 5.4.10 In the absence of a valid Sub-Master clock signal, the slave clocks for time-of-day information shall synchronize via the Sub-Master clock of an adjacent station or facility or operate in free-running mode with an internal clock supplying the time signals. On restoration of the Sub-Master clock signal, the slave clocks shall validate the signal. After the successful validation, the slave clocks shall self-correct, if necessary.
- 5.4.11 The TSCC Contractor's design for NTS shall be compliant with ITU-T G.811: Timing characteristics of primary reference clocks.
- 5.4.12 The NTS shall be designed to provide synchronized time information within the DCN.
- 5.4.13 The synchronized time information shall be provided to clients as clocks, network devices, servers and end applications using IEEE 1588v2 Precision Time Protocol (PTP) and additional protocols and standards, such as G.8271, G.8275.1&2, G.8273.1&2, SyncE and others, to improve the overall performance of the Network Timing System to achieve the level of accuracy required by the different systems to be synchronized (e.g. FRMCS).
- 5.4.14 The protocols shall incorporate algorithms to compensate for delays in the transmission network, like Best Master Clock Algorithm (BMCA) and/or others.
- 5.4.15 The TSCC Contractor's design for NTS shall include a comprehensive Network Management System (NMS) for the entire network's components and devices. The synchronization and time broadcasting system will be interfaced with the NMS to ensure the reporting, alarms, defects, status, and other relevant information of Master clocks, Sub-Master clocks, and slave clocks, preferably via SNMP v3 (any other standard protocol shall be subject to approval).
- 5.4.16 The TSCC Contractor's NTS design shall support and detail normal and degraded modes of the synchronization system.
- 5.4.17 Switching from the Main Master clock to the Backup Master clock shall be automatic and transparent for synchronized systems.
- 5.4.18 Clocks for time information shall be visible in all lighting conditions and have their own lighting source if necessary.
- 5.4.19 Location of clocks shall consider the installation of other equipment like cameras, information displays, fixed signage, loudspeakers, etc.



- 5.4.20 Clocks installed in public areas shall be sized, designed, and installed such that they can be read from any position easily.
- 5.4.21 For passenger information clocks (digital and analog slave clocks), networked IP-based clocks with PoE-type power supply should be adopted, as soon as transmission distances allow it (typically less than 100m), i.e., in the presence of nearby network switches and according to the consumption of the clocks. For longer distances, other technologies such as Powered Fiber Cable systems may be used to avoid extra power feeding cables and devices.
- 5.4.22 The NTS shall deliver the time and date in a Coordinated Universal Time (UTC) format.
- 5.4.23 Applications which require to timestamp log entries, alarms, events etc., shall use Pacific Standard Time (PST) expressed in the 24-hour format: HH:MM: SS, to an accuracy of one hundredth of a second.
- 5.4.24 Clocks, displaying the common time reference, shall be configurable to display UTC, PST, or Pacific Daylight Time (PDT) in 12- or 24-hour format.
- 5.4.25 Customer facing and operator time displays shall be shown in Pacific Standard and Pacific Daylight time as defined for the United States.
- 5.4.26 The NTS equipment shall be remotely manageable.
- 5.4.27 The NTS shall send alarms to appropriate personnel.
- 5.4.28 Maintenance alarms shall include intermittent and hard failures for delivering the NTS signal.

5.5 Performance Requirements

5.5.1 Master Clock System

- 5.5.1.1 The suggested architecture for the NTS shall be based on a standard hierarchy model (master-slave). The higher the timing equipment is in the hierarchy, the more precise the timing source shall be.
- 5.5.1.2 The Master clock gets the time reference from a GPS satellite signal, which is generated by an atomic clock.
- 5.5.1.3 The Master clock equipment shall have an internal atomic oscillator in the event of a loss of GNSS signals. The oscillator shall be able to provide a holdover value in the range of +/- 1 μ s/day (after 30 days of synchronization).
- 5.5.1.4 At each station, a Sub-Master clock shall be located to provide local timing to local subsystems. The Sub-Master clock shall get its time source from the Master clock. This architecture guarantees a local timing source in the event of a failure of the DCN or the Master clock.
- 5.5.1.5 The Sub-Master clock and slave clocks shall have internal battery backup of at least 12 hours.
- 5.5.1.6 For time servers, every Ethernet and optical port shall be completely independent with its own MAC address, allowing the synchronization of several networks. These ports shall be isolated with no communication and interconnections between them (galvanic separation or any other technique).
- 5.5.1.7 At least the following reference sources shall be selectable to synchronize the system: GPS, PTP/IEEE1588v2, NTP, SyncE.
- 5.5.1.8 A PTP profile is a selection of optional features and attribute values. The purpose of a profile is to set restrictions on the possible PTP attributes to simplify the interoperability between different PTP devices in a certain application. At least the following PTP Profiles shall be supported:
- IEEE 1588v2 (PTPv2)



- IEC 61850-9-3
- ITU-T G.8265.1 Frequency
- ITU-T G.8275.1 Phase/Time
- ITU-T G.8275.2 Phase/Time

5.5.1.9 Time server shall support, at least, 100/1000BaseT/TX/FX Ethernet and optical networks.

5.5.1.10 The TSCC Contractor's NTS design shall support, at least, the following network services: PTP, NTP, SNTP, Syslog, SNMP v3 and MIB, SSL, DHCP, IPv4/IPv6.

5.5.1.11 The GNSS Receiver/Decoder Unit, located adjacent to the antenna, shall continuously collect the external time information for the NTS.

5.5.2 Digital Clock Displays

5.5.2.1 The TSCC Contractor's design of the single-sided digital slave clocks shall be of high quality and blend into the architecture of the area in which they shall be located.

5.5.2.2 All digital slave clocks shall be programmable both for 12 hour and 24-hour display and shall display four digits time in HH:MM format. The default configuration shall present the time information in the 24h format.

5.5.2.3 The TSCC Contractor may propose to display alternative additional strings, such as, for example, date in MM/DD format and temperature, with an adjustable period of display. The digital clock may then be configured in such a way that it shall display Date, Temperature, or Time, alternatively, as per the Authority's requirement.

5.5.2.4 Sufficient digital slave clocks shall be provided to enable a clear view of the time from any location within the facilities (OCC, control and technical rooms, depots, offices, etc.).

5.5.2.5 The character height of the display shall not be less than 5 cm, for a minimum readability distance of 20 meters, and shall allow a viewing angle of at least 120° with perfect visibility, whatever the lighting conditions.

5.5.2.6 Digital Clock Displays' (DCD) front face shall be glare resistant at all ambient lighting conditions.

5.5.2.7 In case of Master Clock loss, the display shall provide a minimum accuracy of 1 second.

5.5.2.8 Accuracy shall be better than ± 0.1 second/24 hour when synchronized and ± 1 second/ 24 hour when in free-run mode (loss of signal).

5.5.2.9 An LED status indicator on the face of the clock may illuminate when the clock is not synchronized.

5.5.3 Analog Clock Displays

5.5.3.1 The TSCC Contractor's design of the analog slave clocks shall be of high quality and blend into the architecture of the area in which they will be located.

5.5.3.2 The shape of the analog clocks shall be round, and the diameter shall be not less than 30 cm.

5.5.3.3 Sufficient analog slave clocks shall be provided to enable that the indicated time is clearly and easily readable from at least 20m from the location of the clock within their respective areas.

5.5.3.4 The face of the clock shall be off-white; the time marks on the face shall be black, visible in all lighting conditions.



- 5.5.3.5 The hour markings shall be in an English numeral format and in an easily read font. Minute / second display shall be provided. The analog clock shall have black hour and minute hands and a red second-hand indicator.
- 5.5.3.6 The analog clocks shall contain a stepper motor drive and state-of-the-art microprocessor and electronics control to rapidly synchronize the hands on the face of the clock to an accurate reference.
- 5.5.3.7 The stepper motor drive and gear system shall be of all metal construction for long, maintenance-free life and high product reliability. The gear and drive train system shall be smooth and quiet in operation to minimize motor noise.
- 5.5.3.8 The analog clocks shall be available with the following options: LED illumination, double-face ceiling or wall mount, stainless steel enclosure.
- 5.5.3.9 A hand positioning sensor should be used to automatically detect and correct the clock's hand positions, thus eliminating manual time adjustments.
- 5.5.3.10 The analog clocks shall be provided with a mandatory feature to configure the turn-on/turn-off of illumination at selected hours.
- 5.5.3.11 The analog clocks shall incorporate a holdover function for the first 24 hours and then stop at the 12 o'clock position to indicate a loss of signal and an unsynchronized state.
- 5.5.3.12 Subject to the architectural constraints for each specific location, the clocks shall either be wall mounted, ceiling mounted, or pole mounted. The TSCC Contractor shall determine the mounting method and shall submit it to the Authority for review before installation.

5.5.4 Network Management System

- 5.5.4.1 The status of the NTS, including GNSS Receiving System, Master clock Units, Clock Distribution System, PTP Servers, Sub-Master clocks and Slave Clocks shall be monitored using SNMP v3 (or better solution) by the proposed dedicated Network Management System (NMS) to be provided at OCC.
- 5.5.4.2 The NMS shall provide full configuration support for Master clock Units, Sub-Master clocks, and slave clocks.
- 5.5.4.3 All server functions and configuration shall be accessible via front panel keypad and by remote management client to support status monitoring, alarm messages (polling or event driven), Built-In-Test functions, configuration, etc.
- 5.5.4.4 Status and diagnostics shall be reported via SNMP v3 (or another standard protocol) to each Management System regarding (not limited to):
- Power supply failure.
 - Loss of GNSS synchronizing time signal.
 - NTS failover.
 - Unauthorized login attempts.
 - Data security: penetration, jamming, spoofing, hacking, or clock manipulation attempts.
- 5.5.4.5 The NTS Server shall retain local logs stored in non-volatile flash memory and be remotely accessible.

5.5.5 Safety Requirements

- 5.5.5.1 NTS shall comply with the safety requirements defined in Schedule 1.



5.5.6 RAM Requirements

- 5.5.6.1 The TSCC Contractor shall be responsible for performing all the activities as specified in Schedule 1 and the Authority's RAM Management Plan.

5.6 Cybersecurity and Security Requirements

- 5.6.1 The TSCC Contractor's NTS design shall be in full compliance with California HSR cybersecurity policies.
- 5.6.2 The TSCC Contractor's NTS design shall be compliant with best practices specified in RFC 8633 for general network security, time protocol-specific security, and PTP and NTP server and client configuration and the security aspects of the security aspects of time distribution protocols in packet networks discussed in RFC 7384 which focuses on the two most common protocols the Network Time Protocol (NTP) and the Precision Time Protocol (IEEE1588/PTP).
- 5.6.3 Hostile cyber operations, such as jamming and spoofing of GNSS signals, are a growing concern. The NTS GNSS server/receiver shall include security mechanisms to prevent GNSS denial and disruption in full compliance with the California HSR cybersecurity policies.



6 INTERFACES REQUIREMENTS

6.1 General Requirements

6.1.1 The interfaces are classified as following:

- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR contractors)
- External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors)
- Internal Interfaces: Interfaces between systems within the TSCC scope

6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.

6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.

6.2 External Interfaces – station contractor

6.2.1 The NTS shall have a redundant interface with the following systems to provide a centralized and accurate time reference and synchronization to all the equipment:

- Heating Ventilation and Air Conditioning
- ETCS system
- Escalators
- Elevators
- Fire Protection Systems
- Station Digital Clocks
- Hydraulic Systems
- Lighting Systems
- LV Power Systems

6.3 External Interfaces – facilities contractor

6.3.1 The NTS shall have a redundant interface with the following systems to provide a centralized and accurate time reference and synchronization to all the equipment:

- Heating Ventilation and Air Conditioning
- ETCS system
- Elevators
- Fire Protection Systems
- Station Digital Clocks
- Hydraulic Systems
- Lighting Systems
- LV Power Systems

6.3.2 The TSCC Contractor shall install all NTS core network equipment in the OCC being provided by the facilities contractor.

6.3.3 The TSCC Contractor shall provide the facilities contractor the following requirements::

- Equipment dimensions



- Equipment clearances requirements
- Equipment mounting and fixings requirements
- Cable routes/containment requirements
- Equipment loadings
- Installation and maintenance requirements
- Equipment heating loads
- Equipment cooling loads
- Equipment hydraulic requirements

6.3.4 To be provided by facilities contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:

- Room dimensions and layouts
- Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
- Room raised floor system
- Delivery access routes.
- Maintenance access routes

6.4 Internal Interface for NTS

6.4.1 Interface with the Digital Communication Network

6.4.1.1 The NTS shall have redundant interfaces with the DCN for the transport of NTS signals and data in a secure and reliable way, and the interconnection of all NTS devices along the project.

6.4.2 Time distribution to TSCC systems

6.4.2.1 The NTS shall have a redundant interface with the following systems to provide a centralized and accurate time reference and synchronization to all the equipment:

- Digital Communications Network
- ETCS system
- Traffic Management System
- Interlocking
- Power SCADA System
- Traction Power Systems
- Wireless Communication Systems
- Integrated Control and Supervision System
- Low Voltage Power System
- Medium Voltage Power System
- CCTV system
- Public Address and Customer Information System
- Telephony system
- Fire Protection System
- Electronic Access Control System
- Asset Protection System.
- Maintenance Management system.
- MEP system.



6.4.3 Interface with Integrated Control and Supervision System

- 6.4.3.1 The TSCC Contractor shall ensure that the NTS NMS is integrated with the Integrated Control and Supervision System (ICSS). The NMS shall expose required interfaces, alarms, status indicators, and performance metrics using standard protocols (e.g., SNMP, RESTful APIs, or as defined by the ICSS integration specifications) to support centralized fault, performance, and configuration monitoring across subsystems.

6.4.4 Interface with Enterprise Asset Management Systems (EAMS)

- 6.4.4.1 The NTS shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.

6.4.5 Interface with Low Voltage Power System

- 6.4.5.1 The NTS shall interface with an Uninterruptible Power Supply (UPS) to get the required power to feed the Telephony System equipment.



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied by the TSCC Contractor shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards. Refer to 2.4.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the design life requirements.

7.2 Software and Hardware Requirements

- 7.2.1 The NTS Servers shall support security hardening and authentication protocols such as RADIUS, TACACS, X.509 Certificate Authority, and LDAP, etc.
- 7.2.2 OCXO or rubidium local oscillator and minimum Coarse/Acquisition (C/A) code 24 channels GNSS receiver.
- 7.2.3 The network equipment carrying synchronization information shall be compliant with (not limited to) IEEE 1588v2 Precision Time Protocol (PTP), G.8271, G.8275.1&2, G.8273.1&2 to provide a time accuracy, expressed in terms of time error with respect to a common reference, in the range of $\sim 1 \mu\text{s}$, taking into special consideration the accuracy requirements of the communications network.
- 7.2.4 Time synchronization shall be distributed via timing protocols such as IEEE 1588v2 PTP, G.8271, G.8275.1&2, G.8273.1&2, and others which define how the time and phase synchronization references are transported over the network. The timing support in the intermediate nodes (e.g., Ethernet switches and/or routers) concerns specific hardware as well as software timing functions.
- 7.2.5 In the case of PTP, these functions may correspond either to the telecom boundary clock (T-BC) or to the telecom transparent clock (T-TC), with hardware timestamping at the related interfaces.
- 7.2.6 The NTS shall be mainly comprised of the following elements (not limited to):
- Redundant centralized Master clock located in the OCC.
 - Sub-Master clock installed at each station.
 - Slave clocks installed throughout selected areas within the Stations, Depot, OCC, wayside facilities.
 - An NMS deployed on server-grade hardware and accessed from dedicated workstations located in the OCC.
- 7.2.7 The NTS shall provide appropriate clock output interfaces, timing, and reference distribution.
- 7.2.8 The type, quantity, and capacity of the Master clocks and Sub-Master clocks outputs shall be determined and dimensioned according to the requirements of the various systems in the project.
- 7.2.9 The NTS shall use GNSS Antennas with mounting hardware, which shall be positioned in an unobstructed area to provide a clear line of sight to no fewer than four of the orbiting satellites at all times and the antenna positions will free from potential obstructions due to future tree growth and surrounding urban development.
- 7.2.10 The GNSS Antennas installation shall include lightning protection.
- 7.2.11 The delivered NTS shall allow synchronization and support future additional expansion of 20% regarding:
- System clients.
- 7.2.12 Systems applications.
- Servers and PCs.
 - Databases.



- Field end-devices.
- Users and/or workstations.

- 7.2.13 Expansion and scalability shall not impose and/or degrade the NTS performance, latency, or response times.
- 7.2.14 The NTS central system shall be designed without a single point of failure.
- 7.2.15 The NTS shall be designed with equipment and circuit redundancy such that a single failure (e.g., electronic card) does not affect the NTS service. In other words, internal redundancy is required for all equipment composing the NTS.
- 7.2.16 The Master clock and backup Master clock components shall be functionally redundant to ensure that Network Synchronization and Time Distribution services remain operational during any single hardware, cabling, or software failure.
- 7.2.17 The NTS Central Servers shall have redundant architecture and connectivity, including hardware, software, network, power supply, cabling, cooling, data backup, disaster recovery planning, and physical security, so that NTS survives during any failure of the aforementioned items.
- 7.2.18 A fault-tolerant design with protection against failure shall be provided to achieve system availability. Protections shall include, but not be limited to, path diversity, redundancy, and duplication of reliability-critical equipment, components, and circuits.
- 7.2.19 Low toxicity, low smoke emission, low flammability, zero halogen fire retardant cable shall be used for the distribution of NTS signals.

7.3 EMC Requirements

- 7.3.1 The NTS shall be fully immune and protected from any Electromagnetic Interference (EMI) with the traction power, multi-tubular cabling, and Radio Frequency Interference (RFI). The EMI emissions shall be mitigated in accordance with applicable standards (EN 50122 or equivalent)



8 TOLERANCES

8.1.1 Not applicable to NTS.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 The TSCC Contractor shall supply and deliver all components related to the NTS System.

9.2 Specific Requirements

9.2.1 The NTS scope of supply and delivery shall include (not limited to):

- Master clocks.
- Sub Master-clocks.
- GNSS antennas.
- Workstations/HMIs.
- Digital clocks.
- Analog clocks.
- Cabling and connectors.
- Racks.
- Software architecture, including full definition of all protocols used.
- Management System.
- SW licenses.
- Auxiliary elements, tools, and gear (lightning protectors, attachments, bindings, testing equipment, etc.).
- Spare parts.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.



13 SUBMITTALS

13.1 General Requirements

13.1.1 General submittal requirements are defined in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor and Supplier information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence NTS subsystem reliability, availability, and maintainability characteristics.



16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.



Schedule 5(m)

Operation Control Center (OCC)

California High-Speed Rail Authority



Standard Specifications

TSCC Specification

SPEC-0017 – Operation Control Center (OCC)

Rev. 0.0

A blue ink signature of Selma Duru.

Authored:

Selma Duru, TCS Engineer

10/15/2025

Date

A black ink signature of Thomas Newey.

Checked:

Thomas Newey, Telecoms Lead

10/15/2025

Date

A black ink signature of Bruno Comperat.

Checked:

Bruno Comperat, Deputy Director of Rail Engineering

10/16/2025

Date

A blue ink signature of Ryan Scott.

Approved:

Ryan Scott, Director of Rail Engineering

10/16/2025

Date

A blue ink signature of Amit Joshi.

Released:

Amit Joshi, Configuration Manager

10/16/2025

Date



Document Revision History – OCC Specifications**First Edition****September 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition



TABLE OF CONTENTS

1	INTRODUCTION	4
1.1	SCOPE OF THE TECHNICAL SPECIFICATION	4
2	REFERENCE STANDARDS AND DOCUMENTS.....	5
2.1	GENERAL	5
2.2	STANDARDS	5
3	TERMS, DEFINITION AND ABBREVIATION	7
4	OCC DESCRIPTION	8
4.1	PURPOSE OF THE OCC	8
4.2	OCC DEFINITION.....	8
5	CONTROL ROOMS	9
5.1	GENERAL REQUIREMENTS.....	9
5.2	ENVIRONMENTAL REQUIREMENTS.....	9
5.3	SYSTEM OPERATION	9
5.4	COMMON REQUIREMENTS FOR CONTROL ROOMS.....	9
5.5	OCC ROOMS.....	13
5.6	FACILITY ROOMS	14
5.7	STAFF AND CONTROLLERS RESPONSIBILITIES	15
5.8	CONTROL ROOMS WORKSTATION EQUIPMENT	15
5.9	WORKSTATION ALLOCATION RIGHTS	18



1 INTRODUCTION

1.1 Scope of the technical specification

- 1.1.1 The scope of this Technical Specification is to define The Authority's Requirements for the **Control Center Systems**, which includes the **Operational Control Center (OCC)** and **Facilities Control rooms**.
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of OCC is presented in Appendix A.
- 1.1.4 The requirements are formulated using the following words and their meanings:
 - "Shall": Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure).
 - "Should": Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents.
 - "Must": Indicates an obligation or a mandatory requirement.
 - "May": Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines and specifications provided in this chapter for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning and training.
- 2.1.2 All generic standards to be used are provided in: Technical Contract Requirements.

2.2 Standards

- 2.2.1 The following specific standards to be used for Control Centers are listed below.

ID	Code	Title
Control Room		
[R6]	ISO 11064	Ergonomic Design of Control Centers – Part 1 to 7
[R7]	EN 614 Part 1	Safety of machinery. Ergonomic design principles. Terminology and general principles
[R8]	EN 614 Part 2	Safety of machinery. Ergonomic design principles. Interactions between the design of machinery and work tasks
[R9]	BS 5940 Part 1	Office furniture. Specification for design and dimensions of office workstations, desks, tables and chairs
Displays / Workstations		
[R10]	ANSI/HFS 100	Human Factors Engineering of Computer Workstations
[R11]	ISO10075	ERGONOMIC PRINCIPLES RELATED TO MENTAL WORKLOAD - PARTS 2 & 3
[R12]	ISO9241	Ergonomic of Human System Interaction 210 – Human centered design for interactive systems 302 - Terminology for electronic visual displays 303 – Requirements for electronic visual displays 400 - Principles and requirements for physical input devices 3 – Visual display requirements 4 – Keyboard requirements 5 - Workstation layout and postural requirements 6 - Guidance on the working environment
[R13]	ISO9335	Ergonomic requirements for the design of displays and control actuators 2 - Displays
Auditory / Visual Signals		
[R14]	ISO7731	Danger Signals for workplaces – Auditory danger signals
[R15]	ISO11428	Ergonomics – Visual danger signals – Generic requirements, design and testing
[R16]	ISO11429	Ergonomics – System of auditory and visual danger and information signals



ID	Code	Title
[R17]	EEMUA 191	Alarm systems – A guide to design, management and procurement
[R18]	EEMUA 201	Process plant control desks utilizing human-computer interfaces - guide to design, operational and human computer interface issues.
[R19]	ANSI/ISA-18.2	Management of alarms for process industries
[R20]	EEMUA 201	Process plant control desks utilizing human-computer interfaces - guide to design, operational and human computer interface issues.
Lighting		
[R21]	CIBSE	Code for Lighting
[R22]	ISO8995	1 – Lighting of workplaces – Part 1: Indoor
Thermal Environment		
[R23]	ANSI/ASHRAE 55	Thermal Environmental Conditions for Human Occupancy
Acoustics		
[R24]	MIL-STD-1472F	Department of defense design criteria standard –Human engineering

TABLE 1 - LIST OF APPLICABLE STANDARDS

2.2.2 The Standards, regulations, codes and directives listed in TABLE 1 are applicable to the design of the Control Rooms, Systems, Workstations and Human Machine Interfaces and are in addition to those defined in the high-level tender documentation.



3 TERMS, DEFINITION AND ABBREVIATION

- 3.1.1 All the terms, definitions, and abbreviations are provided in the Glossary of Terms, Abbreviations and Definitions.



4 OCC DESCRIPTION

4.1 Purpose of the OCC

4.1.1 The overall rail shall be controlled through a hierarchical arrangement of rooms in the OCC at the following locations:

- Control Room
- Crisis Room
- Safety & Security Room
- Security Gatehouse
- Training Room
- Maintenance Room
- Equipment Room

4.2 OCC Definition

4.2.1 A proposed overview of the OCC layout is provided in the figure below:

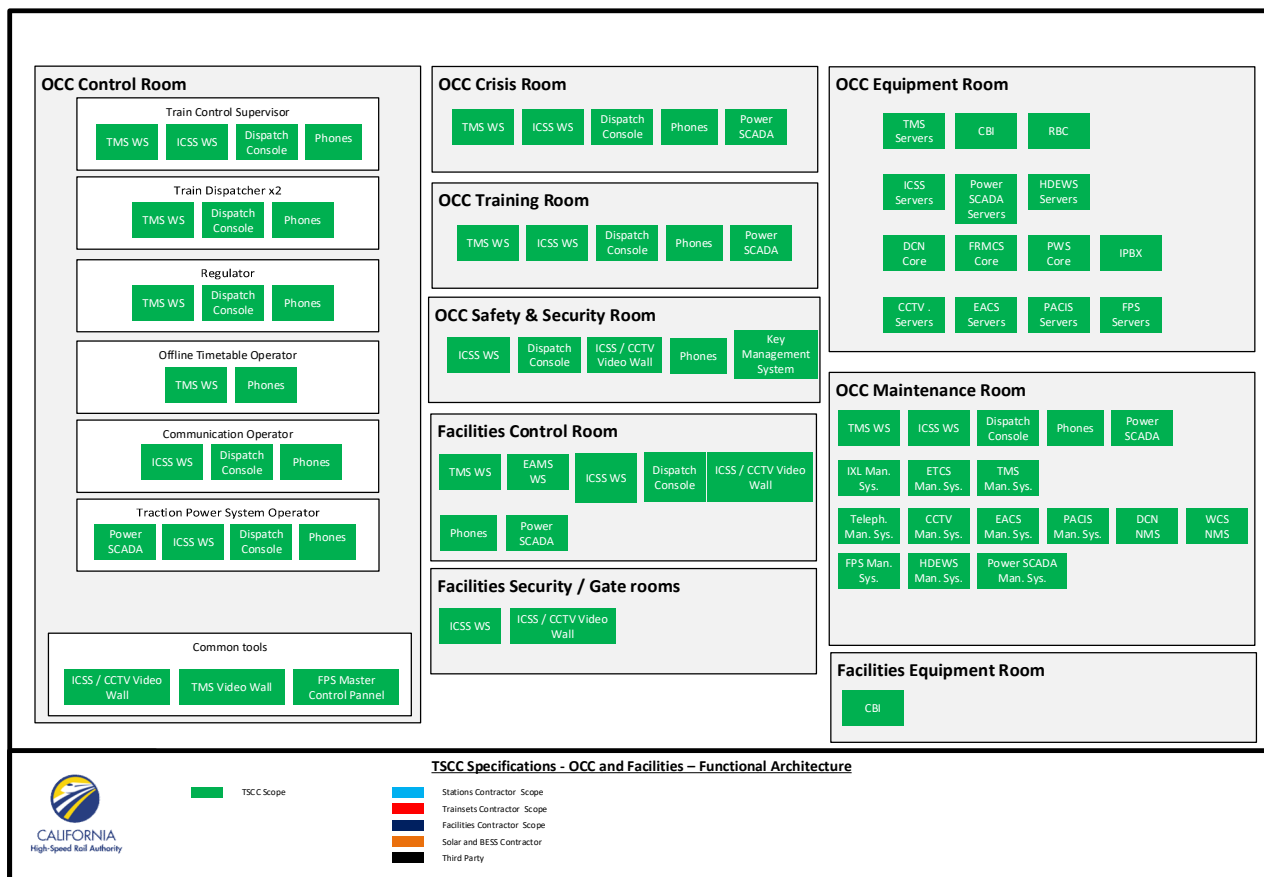


FIGURE 1 - GENERAL OVERVIEW OF THE OCC

4.2.2 The OCC shall be located in Fresno.

5 CONTROL ROOMS

5.1 General Requirements

- 5.1.1 The OCC and facility staff shall be able to control and monitor all equipment and functions for operations in the relevant area of control.
- 5.1.2 The TSCC Contractor shall supply all workstations, consoles, desks, furniture, fixtures and fittings to be in the various rooms that are required for operation of the railroad.
- 5.1.3 This specification shall be read in conjunction with the standards listed in the *Table 1 - List Of Applicable* Standards and TSCC Technical Specifications which describe in detail the requirements for the workstations, servers, networking equipment, peripheral equipment, computers, printers, telephones, handsets and other voice communications equipment to be installed in the various rooms.
- 5.1.4 While any future upgrades, modifications, or additions of equipment in the OCC, all new equipment, consoles, desks, furniture, fixtures, and fittings shall remain homogeneous with the originally installed consoles, desks, furniture, fixtures, and fittings. In case of space constraints arising from these upgrades or modifications, the TSCC Contractor shall rearrange the control room layout to accommodate the new assets of the CHSR line, subject to the Authority's approval.

5.2 Environmental Requirements

- 5.2.1 A detailed task analysis and human factors study shall be conducted by the TSCC Contractor for all control rooms.

5.3 System Operation

- 5.3.1 All traffic on the main line shall be controlled from the Operational Control Center (OCC) located in Fresno.
- 5.3.2 Movements between the main line and the facilities via the transfer tracks shall be coordinated by the train dispatchers at the OCC and the relevant local controller.

5.4 Common Requirements for Control Rooms

5.4.1 General Requirements

- 5.4.1.1 Requirements are subject to input from the Early Train Operator, and should be revised once a concept of operations for the OCC is approved by the Authority.
- 5.4.1.2 The OCC and facilities shall contain the necessary displays, control workstations, communications apparatus and operating personnel to control, monitor and maintain the CHSR line and facilities.
- 5.4.1.3 The TSCC Contractor shall perform a detailed task analysis to reconfirm the roles and responsibilities of controllers, equipment quantities and controller types.
- 5.4.1.4 The quantity/number of controllers/staff shown in this specification is indicative only and shall be subjected to change based on the detailed task analysis by the TSCC Contractor.
- 5.4.1.5 The Ergonomic & Human Factors Guidelines shall include detailed task analyses and collaborative design processes to support the optimization of control and display interfaces and engineering processes and systems, mitigating the risks of human error and optimizing human performance through design.



5.4.2 Human Machine Interface Guidelines

5.4.2.1 The TSCC Contractor shall prepare a set of Human Machine Interface (HMI) Guidelines, which should be applicable to all room workstations and equipment.

5.4.2.2 The HMI Guidelines shall set out requirements for:

- Use and display English. Multilingual support, including Spanish, should be considered based on operational and regulatory requirements defined by the Authority.
- Screen navigation
- Use of screen areas
- Menus
- Tabs
- Buttons
- Icons
- Schematics
- Graphs
- Alphanumeric text input fields
- Alphanumeric displays
- On screen keypads
- Sound
- Color
- Icon displays
- Use of backlighting
- Help functions
- Screen layout Alarms and Displays including Legends (explanation of icon)

5.4.2.3 The HMI Guidelines shall define the use of colors and sounds for alarms and warnings.

5.4.2.4 The HMI guidelines shall also define requirements for the following:

- Positioning of labels
- Positioning and types of actuators
- Positioning and type of indicators

5.4.3 Ergonomic & Human Factors Guidelines for control rooms

5.4.3.1 The TSCC Contractor shall prepare a set of Ergonomic & Human Factors Guidelines for control rooms that shall be applicable to the design and layout of all rooms.

5.4.3.2 The Ergonomic & Human Factors Guidelines for Rooms shall comply with the standards referenced in this specification.

5.4.3.3 The Ergonomic & Human Factors Guidelines for Rooms shall set out the Ergonomic & Human Factors requirements for the following:

- Console / desk furniture
- Seating design and posture
- CCTV placement



- Furniture location
- Line of sight recommendations
- Maintenance access
- Accessibility and human circulation
- Lighting levels
- Use of natural / artificial light
- Levels of vibration
- Room acoustics
- Temperature
- Air quality
- Indicators or actuators not already covered by the HMI Guidelines. Alarms and Displays

5.4.3.4 The Ergonomic & Human Factors Guidelines shall deliver a recommendation for the operational environment on the CHSR line. The TSCC Contractor shall provide the guidelines to facilities contractors for implementation.

5.4.3.5 The Ergonomic & Human Factors Guidelines shall look at the operational efficiency of the workstations and controller consoles or desks, and the visual interface with the Visual Display Units as primary impacts.

5.4.3.6 The Ergonomic & Human Factors Guidelines shall consider the suitability of the control rooms and operational environment for the operational hours of the railroad, namely 24/7/365 operations.

5.4.3.7 The guidelines shall recommend the ergonomic requirements to maximize the efficiency of operational interaction between controllers in the control rooms.

5.4.4 Provision of Equipment Storage Space

5.4.4.1 Two classes of storage space (Type 1 and Type 2) shall be provided in each room.

5.4.4.2 Type 1 storage space that is frequently accessed daily shall be placed under each Dispatcher's console.

5.4.4.3 Type 2 storage space that is infrequently accessed shall be provided in other areas of each room.

5.4.4.4 The TSCC Contractor shall provide storage spaces at controller consoles and in other areas of each room.

5.4.5 Hanging of Equipment and Items

5.4.5.1 The design and loading specifications for wall and ceiling brackets and fixings used to hang equipment or items shall be in accordance with relevant applicable international standards.

5.4.5.2 Wall and ceiling mounted equipment shall not impede controllers in carrying out their duties.

5.4.6 Environment and Console Design

5.4.6.1 The detailed design of each control room shall consider acoustic control, limitation of acoustic interference between controller's locations, environment, air quality, lighting level and controller's comfort.

5.4.6.2 The consoles design shall be submitted to the Authority for approval.

5.4.6.3 All console surfaces shall be durable and scratch resistant.

5.4.6.4 Double consoles, where applicable, shall have sufficient space between controllers to allow them to have their own space but allowing for ease of communication between them.



- 5.4.6.5 All console furniture shall be designed in accordance with ergonomic considerations.
- 5.4.6.6 There shall be sufficient provision made for air flow and cooling within each dispatcher's console so that the ambient temperature within the console furniture remains within the operating limits of all equipment located inside the console enclosures.
- 5.4.6.7 Controller's consoles shall be designed to accommodate all necessary equipment for CHSR line and facilities.
- 5.4.6.8 The interior of the console shall allow for spare capacity (e.g., 40%) to be provided for future equipment requirements, agreed with the Authority.
- 5.4.6.9 The use of natural and artificial lighting shall not induce glare or significant heat gain within OCC and facilities environments.
- 5.4.6.10 If windows or skylights are employed in the room, all materials shall be shatter proof.
- 5.4.6.11 Each control room shall be provided with digital display clock(s) to be visible by all controllers which are connected to the Network Timing System.
- 5.4.6.12 The TSCC Contractor shall propose layouts for each control room which shall be subject to approval by the Authority.
- 5.4.6.13 The consoles shall be designed such that the dispatcher is able to view and reach each screen from a static position.
- 5.4.6.14 All operational equipment within Consoles shall be fed by Uninterrupted Power Supply (UPS) from the Low Voltage Power System (LVPS).
- 5.4.6.15 Type A/B North American Power sockets shall be provided within the console providing both UPS or non-essential power for the dispatcher to use.

5.4.7 Video Wall Display (VWD)

- 5.4.7.1 The TSCC Contractor shall propose a dedicated VWD for the CHSR line.
- 5.4.7.2 The Video Wall Display shall be located at the front of the OCC Control Room.
- 5.4.7.3 The VWD software shall be built on a generic Graphic Display software platform which has been proven in use.
- 5.4.7.4 The Ergonomic & Human Factors Guidelines shall consider the ability to work at any workstation in the OCC and have a free and unrestricted view of the VWD.
- 5.4.7.5 The VWD shall be configurable to display the following, but not limited to:
 - Line Overview
 - CCTV feeds
 - Meteorological data
 - Critical Alarms
 - Other feeds as required by the operator.
- 5.4.7.6 The VWD shall provide a line overview including, but not limited to the following:
 - Track Layout
 - Location of HDEWS detectors
 - Location of trains
 - Train Identification



- Train route
- Switch status
- HDEWS Alarms
- Selected alarms from other systems such as power, fire and ventilation systems
- Traction power Distribution network

- 5.4.7.7 The VWD shall enable the operator to hide and unhide each information above individually.
- 5.4.7.8 The VWD equipment shall come with self-test and diagnostic capabilities, where possible. Self-tests shall be initiated each time the equipment is powered up.
- 5.4.7.9 Successive loading of full static and dynamic graphics on the VWD shall be presented within a maximum delay (e.g., 3 seconds), agreed with the Authority.
- 5.4.7.10 The VWD shall be positioned at the front of the OCC Control Room facing the controllers.
- 5.4.7.11 The VWD shall be sufficiently sized to allow all controllers in the Control Room to be able to view the screen and details on the screen from their positions.
- 5.4.7.12 The TSCC Contractor shall propose a set of pre-defined display layouts to be agreed with the Authority during detailed design. The controller shall be able to modify the display layout by rearranging the windows and adding / suppressing feeds.
- 5.4.7.13 The VWD shall be compliant with the requirements of the electronic visual display in ISO 9241-303.
- 5.4.7.14 The VWD brightness shall be automatically adjusted to the room, ambient lighting and manual override shall be possible.
- 5.4.7.15 The VWD controller shall not have a single point of failure.
- 5.4.7.16 The VWD shall be capable of performing zoom function.

5.5 OCC Rooms

- 5.5.1 The OCC Rooms and associated functions required to operate the system of the CHSR line can be estimated as per [Table 37](#) ~~Table 37~~, subject to a detailed task analysis by the TSCC Contractor. This is subject to the Authority's approval during detailed design.

Room	Quantity
Control Room	1
Crisis Room	1
Training Room	1
Maintenance Room	1
Safety & Security Room	1

TABLE 37 – OCC ROOMS

- 5.5.2 A Safety & Security room is recommended in the OCC. The exact location shall be agreed with the Authority during detailed design stage.
- 5.5.3 The OCC Safety & Security room shall contain an Electronic Key Management System and cabinet.
- 5.5.4 The quantity/number of operators/staff required to operate the system of the CHSR line can be estimated as follows, subject to a detailed task analysis by the TSCC Contractor. This is subject to the Authority's approval.



5.5.5 The final list of workstations and equipment's shall be based on the approved task analysis.

5.5.6 Staff workstations in OCC Control Room (CR)

5.5.6.1 The proposed roles and their intended functions are defined as follows:

- Train Dispatcher: Manages operations within a defined geographical sector, including tasks such as setting up or cancelling routes. Manages engineering possession.
- Train Control Supervisor: Responsible for the Dispatchers. They can, for example, reassign geographical sectors between dispatchers.
- Offline Timetable Operator: Build and load timetables into the system.
- Regulator: Ensures overall regulation of the CHSR line. They coordinate with dispatchers, has the Time-Distance Graph, and can decide to prioritize a train or force a train to pause for regulation purposes.
- TPS Operator: The Traction Power System Operator supervises the Traction Power/OCS system via SCADA network.

5.5.6.2 Extra desks shall be provisioned by the TSCC Contractor for future network extension.

Operator	Quantity
Train Control Supervisor	1
Train Dispatcher	2
Offline Timetable Operator	1
Regulator	1
Communication Operator	1
Traction Power System Operator	1

TABLE 38 – STAFF DESKS IN OCC CONTROL ROOM

5.6 Facility Rooms

5.6.1 Facilities Control Rooms

5.6.1.1 The Facilities Control room shall be located within their respective premises.

Operator	Quantity
Yard Controller	1

TABLE 39 – STAFF DESKS FACILITIES CONTROL ROOM

5.6.2 Security Rooms (SR) and Security Gatehouses:

- 5.6.2.1 A security room shall be in the facilities. The exact location shall be to be agreed with the Authority during the design stage.
- 5.6.2.2 The security rooms and security gatehouses shall provide CCTV, Electronic Access Control System functionality and Fire Protection functionality for the controller.



Operator	Quantity
Security Operator (CCTV, EACS, Fire Protection)	1

TABLE 40 - SECURITY ROOMS

Operator	Quantity
Security Operator (CCTV, EACS, Fire Protection)	1

TABLE 41 - SECURITY GATEHOUSES

5.7 Staff and Controllers Responsibilities

- 5.7.1 The TSCC Contractor shall liaise with the Authority to obtain a detailed list of tasks and responsibilities to be implemented within the control rooms.
- 5.7.2 Workstations and equipment shall be provided for the dispatcher to perform the activities in the task list.

5.8 Control Rooms Workstation Equipment

- 5.8.1 The TSCC Contractor shall as part of their design work carry out task and communications analyses to justify the allocation of workstations and equipment for each controller. This is subject to the Authority's approval during design.
- 5.8.2 The workstations for the sub-systems to be considered shall be as follows:
- TMS system including control and monitoring shall refer to the Technical Specification – TMS
 - ICSS system including control and monitoring shall refer to the Technical Specification – ICSS
 - FRMCS Dispatcher Terminal
 - Enterprise Asset Management System (EAMS)
 - Fallback PSTN Phones
 - Emergency Hotline Phones
 - Office Administration Laptop
 - Telephone
 - Power SCADA Workstation
- 5.8.3 Each Workstation shall be equipped with an office administration computer and a telephone.
- 5.8.4 **OCC Control Room**
- 5.8.4.1 The quantities of workstation equipment to be achieved for the CHSR line and for each controller type shall be as follows:



Equipment	Number of Equipment					
	TCS	TD	OTO	R	CO	TPSO
TMS Workstation	1	1	1	1	1	-
ICSS Workstation (incl. PACIS)	1	1	-	1	1	1
FRMCS Dispatcher Terminal	1	1	-	1	1	1
Emergency Hotline Phones	1	1	-	1	1	1
Fallback PSTN Phones	1	1	1	1	1	1
Power SCADA Workstation	-	-	-	-	-	1

TABLE 42 - WORKSTATION EQUIPMENT FOR CONTROL ROOM

- TCS – Train Control Supervisor
- TD – Train Dispatcher
- OTO – Offline Timetable Operator
- R - Regulator
- CO - Communication Operator
- “-” – Not provided

5.8.4.2 The TSCC Contractor shall identify and propose all equipment for the Authority’s approval to meet the CHSR OCC operational needs.

5.8.5 Crisis Room

5.8.5.1 A Crisis Room (CR) for the CHSR line shall be provided at the OCC.

5.8.5.2 The quantities of workstation equipment to be achieved for the CHSR line in the Crisis Room shall be as follows:

Equipment	Number of Equipment
TMS Workstation	1
ICSS Workstation	1
FRMCS Dispatcher Terminal	1
Emergency Hotline Phones	1
Fallback PSTN Phones	1
Power SCADA Workstation	1

TABLE 43 - WORKSTATION EQUIPMENT FOR CRISIS ROOM

5.8.5.3 The TSCC Contractor shall identify and propose all the equipment for the Authority’s approval to meet the CHSR’s crisis operational needs.

5.8.6 Training Room

5.8.6.1 A Training Room for the CHSR line shall be provided at the OCC.

5.8.6.2 The quantities of workstation equipment to be achieved for the CHSR line in the Training Room and for the Trainer and each Trainee shall be as follows:



Equipment	Number of Equipment	
	TR	TE
TMS Workstation	1	1
ICSS Workstation	1	1
FRMCS Dispatcher Terminal	1	1
EAMS workstation	1	1
Emergency Hotline Phones	1	1
Fallback PSTN Phones	1	1
Power SCADA Workstation	1	1

TABLE 44 - WORKSTATION EQUIPMENT FOR TRAINING ROOM

- *TR – Trainer*
- *TE – Trainee*

5.8.6.3 The TSCC Contractor shall identify and propose all additional equipment for the Authority's approval to meet the CHSR's line training needs.

5.8.7 Maintenance Room

5.8.7.1 Maintenance Rooms for the CHSR line shall be provided at the OCC.

5.8.7.2 The quantities of workstation equipment to be achieved for the CHSR line in the Maintenance Room shall be as follows:

Equipment	Number of Equipment
ICSS Workstation	1
EAMS Workstation	1
Power SCADA Workstation	1

TABLE 45 - WORKSTATION EQUIPMENT FOR MAINTENANCE ROOM

5.8.7.3 The TSCC Contractor shall identify and propose all equipment for the Authority's approval to meet the CHSR maintenance needs.

5.8.1 Facility Control Room (FCR)

5.8.1.1 The quantities of workstation equipment for each Facility Control Room shall be as follows:

Equipment	Number of Equipment – Yard Controller (YC)
Facility TMS Workstation	1
ICSS Workstation	1
FRMCS Dispatcher Terminal	1
EAMS Workstation	1
Emergency Hotline Phones	1
Fall-back PSTN Phones	1
SCADA Workstation	1



TABLE 46 - WORKSTATION EQUIPMENT FOR FCR**5.9 Workstation Allocation Rights**

5.9.1 The following are workstation access rights for each of the controllers in OCC's Rooms. Each Controller shall be provided with control (C) and display (D) rights for each type of function available in that room. The representations are as follows:

- D' – Display. A controller assigned display capability shall be presented with graphically displayed information regarding the status of this sub-system and shall be able to manipulate the system to obtain additional information.
- 'C' – Control. A controller assigned control capability shall be assigned the same rights as display and shall also be able to output commands from the system to control it. These commands shall be activated principally using icons, menus, on-screen buttons. Command line textual input shall only be used where other forms of HMI control are not efficient.
- '- ' – Not assigned.

5.9.2 The control and monitoring rights of each controller in the CHSR line control rooms are provided for indicative purposes only. The number of controllers, their assigned tasks and hierarchy shall be determined through a detailed operational task analysis to be conducted by the TSCC Contractor in the production of the Ergonomic & Human Factors Guidelines.

5.9.3 Control Room

5.9.3.1 The control and monitoring rights for the workstations in the Control Room shall be as follows:

Equipment	Allocation Rights					
	TCS	TD	OTO	R	CO	TPSO
TMS Workstation	C	C	D	C	D	-
ICSS Workstation	C	C	-	C	C	C
FRMCS Dispatcher Terminal	C	C	-	C	C	C
Emergency Hotline Phones	C	C	-	C	C	C
Fallback PSTN Phones	C	C	C	C	C	C
Power SCADA Workstation	-	-	-	-	-	C

TABLE 47 - WORKSTATION ALLOCATION RIGHTS FOR CONTROL ROOM

- TCS – Train Control Supervisor
- TD – Train Dispatcher
- OTO – Offline Timetable Operator
- R - Regulator
- CO - Communication Operator
- TPSO – Traction Power System Operator
- "- " – Not Provided

5.9.4 Crisis Room (CR)

5.9.4.1 The control and monitoring rights for the workstations in the Crisis Room shall be as follows:



Equipment	Allocation Rights User of CR
TMS Workstation	D
ICSS Workstation	C
FRMCS Dispatcher Terminal	C
Emergency Hotline Phones	C
Fallback PSTN Phones	C
Power SCADA Workstation	D

TABLE 48 - WORKSTATION ALLOCATION RIGHTS FOR CRISIS ROOM**5.9.5 Training Room**

5.9.5.1 The control and monitoring rights for the workstations between the trainer and the trainee in the Training Room shall be as follows:

Equipment	Allocation Rights	
	TR	TE
TMS Workstation	C	C
ICSS Workstation	C	C
FRMCS Dispatcher Terminal	C	C
EAMS workstation	C	C
Emergency Hotline Phones	C	C
Fallback PSTN Phones	C	C
Power SCADA Workstation	C	C

TABLE 49 - WORKSTATION ALLOCATION RIGHTS FOR TRAINING ROOM

- *TR – Trainer*
- *TE – Trainee*

5.9.6 Maintenance Room

5.9.6.1 The control and monitoring rights for the workstations in the Maintenance Room shall be as follows:

Equipment	Allocation Rights
ICSS Workstation	C
EAMS Workstation	C
Power SCADA Workstation	C

TABLE 50 - WORKSTATION ALLOCATION RIGHTS FOR MAINTENANCE ROOM**5.9.7 Facility Control Room**

5.9.7.1 The control and monitoring rights of each controller in the Facility Control Room shall be as follows:

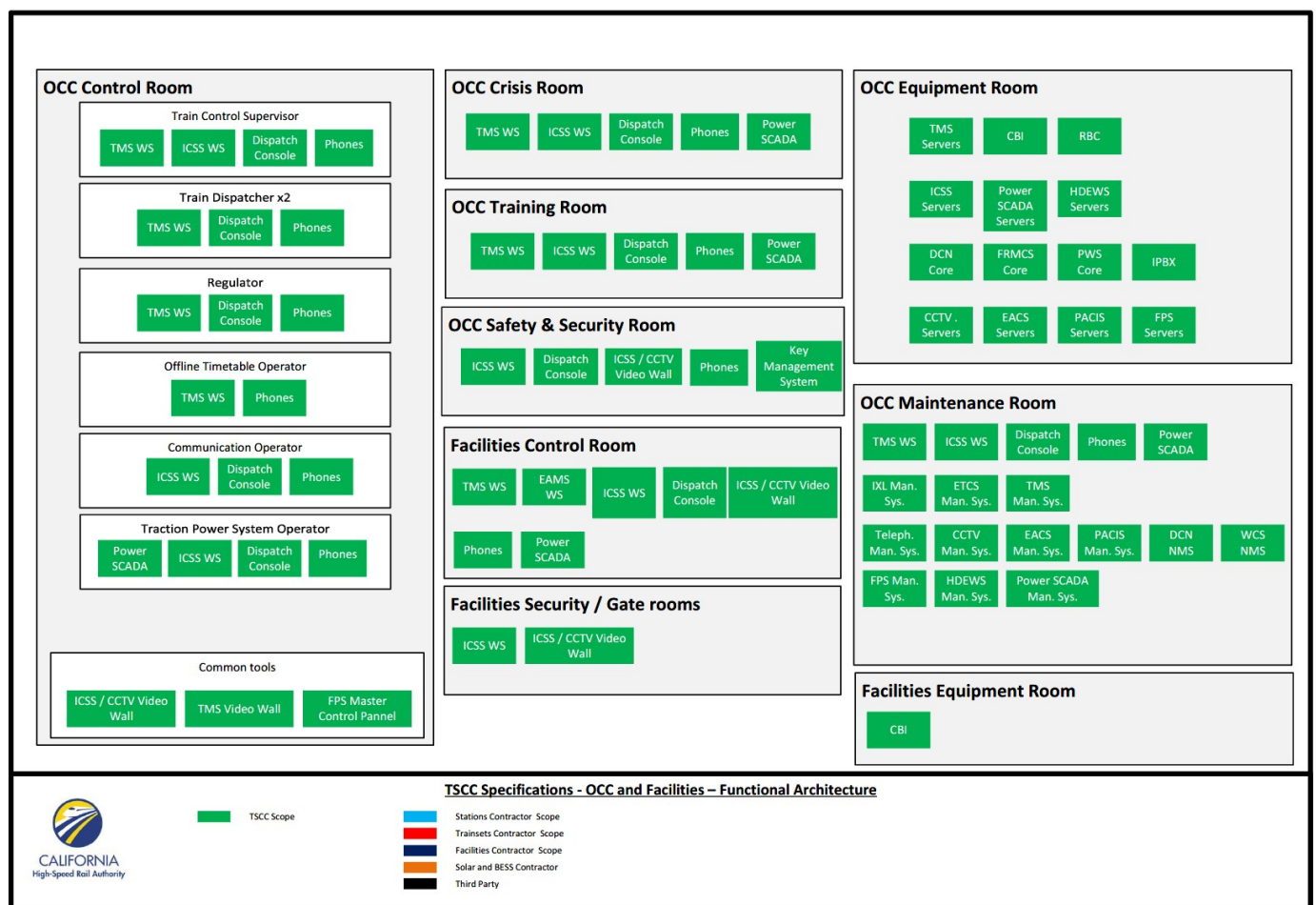
Equipment	Allocation Rights YC – Yard Controller (YC)
Facility TMS Workstation	C
ICSS Workstation	C



Equipment	Allocation Rights YC – Yard Controller (YC)
FRMCS Dispatcher Terminal	C
EAMS Workstation	C
Emergency Hotline Phones	C
Fall-back PSTN Phones	C
SCADA Workstation	C

TABLE 51 - WORKSTATION ALLOCATION RIGHTS FOR FACILITIES CONTROL ROOM

APPENDIX A TO EXHIBIT 5(M) OPERATION CONTROL CENTER (OCC)



Schedule 5(n)

Public Address and Customer Information System (PACIS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0018 – Public Address and Customer Information System
(PACIS)

Rev. 0.0

Authored:

A handwritten signature in black ink, appearing to read "Harshal Jadhav".

Harshal Jadhav, Telecom System Lead

10/15/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Thomas Newey".

Thomas Newey, Telecoms Lead

10/15/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Bruno Comperat".

Bruno Comperat, Deputy Director of Rail Engineering

10/16/2025

Date

Approved:

A handwritten signature in black ink, appearing to read "Ryan Scott".

Ryan Scott, Director of Rail Engineering

10/16/2025

Date

Released:

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Amit Joshi, Configuration Manager

10/16/2025

Date



Document Revision History – PACIS Specifications**First Edition****September 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION.....	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.1	GENERAL	6
2.2	DESIGN GUIDELINES.....	6
2.3	TSI	6
2.4	STANDARDS	6
2.5	OTHER DOCUMENTS	9
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	10
3.1	TERMS, DEFINITIONS AND ABBREVIATIONS	10
4	SYSTEM DESCRIPTION	11
4.1	PURPOSE OF THE PACIS	11
4.2	PACIS SYSTEM DEFINITION	11
4.3	PACIS SYSTEM OPERATIONAL CONTEXT	11
4.4	DESIGN LIFE	11
5	SYSTEM REQUIREMENTS.....	13
5.1	GENERAL REQUIREMENTS.....	13
5.2	ENVIRONMENTAL CONDITIONS REQUIREMENTS.....	14
5.3	OPERATIONAL REQUIREMENTS FOR PACIS	14
5.4	FUNCTIONAL REQUIREMENTS FOR PACIS	14
5.5	PERFORMANCE REQUIREMENTS FOR PACIS	22
5.6	CYBERSECURITY AND SECURITY REQUIREMENTS.....	23
6	INTERFACES REQUIREMENTS.....	24
6.1	GENERAL REQUIREMENTS.....	24
6.2	THIRD PARTY INTERFACE	24
6.3	EXTERNAL INTERFACES - TRAINSETS.....	24
6.4	EXTERNAL INTERFACES – FACILITIES CONTRACTOR	24
6.5	EXTERNAL INTERFACES – STATIONS CONTRACTOR	25
6.6	INTERNAL INTERFACES	25
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS	27
7.1	GENERAL REQUIREMENTS.....	27
7.2	SOFTWARE AND HARDWARE REQUIREMENTS	27
7.3	EMC REQUIREMENTS.....	27
8	TOLERANCES	28
9	SCOPE OF SUPPLY AND DELIVERY	29
9.1	GENERAL REQUIREMENTS.....	29
9.2	SPECIFIC REQUIREMENTS	29
10	MANUFACTURING.....	30
10.1	GENERAL REQUIREMENTS.....	30



11	INSTALLATION AND INTEGRATION.....	31
11.1	GENERAL REQUIREMENTS.....	31
12	TESTING & ACCEPTANCE	32
12.1	GENERAL REQUIREMENTS.....	32
12.2	SPECIFIC REQUIREMENTS	32
13	SUBMITTALS.....	33
13.1	GENERAL REQUIREMENTS.....	33
14	QUALITY MANAGEMENT	34
14.1	GENERAL REQUIREMENTS.....	34
15	ADDITIONAL INFORMATION REQUESTED	35
15.1	GENERAL REQUIREMENTS.....	35
16	LOGISTICS	36
16.1	GENERAL REQUIREMENTS.....	36



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Public Address and Customer Information System (PACIS) system, hereinafter: PACIS.
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of PACIS is presented in Appendix A.
- 1.1.4 The requirements are formulated using the following words and their meanings:
 - "Shall": Indicates a mandatory requirement that must be strictly implemented; a waiver from a mandatory requirement is permissible only with approval of a design variance.
 - "Should": Indicates a preferred course of action; a design variance is not required if it is not exercised.
 - "Must": Indicates an obligation or a mandatory requirement.
 - "May": Indicates a permissible course of action within the limits of the standards; a design variance is not required if it is not exercised.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines, and specifications provided in this chapter for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, and training.

2.2 Design Guidelines

- 2.2.1 The latest version of the following Design Guidelines shall be applied:

ID	Code	Title
[R1]	Design Criteria Manual	Chapter 12 – Communication Systems and Train Control
[R2]	AREMA Standards	Chapter 17 – High-Speed Rail Systems

TABLE 52 DESIGN GUIDELINES

2.3 TSI

- 2.3.1 There are no applicable TSIs for the PACIS.

2.4 Standards

- 2.4.1 The TSCC Contractor shall fully consider and apply the following standards, the in-force standards shall be applied.

ID	Standard	Title
[R3]	EN 11205	Acoustics - Noise emitted by machinery and equipment - Engineering method for the determination of emission sound pressure levels in situ at the workstation and at other specified positions using sound intensity
[R4]	EN 300 386	Telecommunication network equipment; Electro Magnetic Compatibility (EMC) requirements; Harmonized Standard covering the essential requirements of the Directive 2014/30/EU
[R5]	EN 50121	Railway Applications – Electromagnetic Compatibility
[R6]	EN 50121-3-2	Railway applications - Electromagnetic compatibility - Part 3-2: Rolling stock - Apparatus
[R7]	EN 50121-4	Railway applications - Electromagnetic compatibility - Part 4: Emission and immunity of the signaling and telecommunications apparatus
[R8]	EN 50121-5	Railway applications - Electromagnetic compatibility Emission and immunity of fixed power supply installations and apparatus
[R9]	EN 50122-1	Railway applications - Fixed installations - Electrical safety, earthing and the return circuit - Part 1: Protective provisions against electric shock
[R10]	EN 50124	Railway applications - Insulation coordination
[R11]	EN 50125	Railway applications - Environmental conditions for equipment
[R12]	EN 50125-3	Railway applications - Environmental conditions for equipment - Part 3: Equipment for signalling and telecommunications



ID	Standard	Title
[R13]	EN 50126	Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
[R14]	EN 50126-1	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
[R15]	EN 50126-2	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
[R16]	EN 50128	Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems
[R17]	EN 50159	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems
[R18]	EN 50164	Lightning Protection Components
[R19]	EN 50164-3	Lightning Protection Components (LPC) -- Part 3: Requirements for isolating spark gaps
[R20]	EN 50173	Information technology - Generic cabling systems
[R21]	EN 50174	Information technology - Cabling installation
[R22]	EN 50289-1-6	Communication cables - Specifications for test methods - Part 1-6: electrical test methods - Electromagnetic performance
[R23]	EN 50310	Application of equipotential bonding and earthing in buildings with information technology equipment
[R24]	EN 50849	Sound systems for emergency purposes
[R25]	EN 54-14	Fire detection and fire alarm systems - Part 14: Guidelines for planning, design, installation, commissioning, use and maintenance
[R26]	EN 54-16	Fire detection and fire alarm systems - Part 16: Voice alarm control and indicating equipment
[R27]	EN 54-24	Fire detection and fire alarm systems - Part 24: Components of voice alarm systems - loudspeakers
[R28]	EN 55024	Information technology equipment. Immunity characteristics. Limits and methods of measurement
[R29]	EN 60065	Audio, video and similar electronic apparatus - Safety requirements
[R30]	EN 60118-4	Hearing Aids - Part 4: Magnetic Field Strength in Audio-Frequency Induction Loops for Hearing Aid Purposes
[R31]	EN 60268-16	Sound system equipment - Part 16: Objective rating of speech intelligibility by speech transmission index
[R32]	EN 60297-3	Mechanical structures for electronic equipment - Dimensions of mechanical structures of the 482,6 mm (19 in) series - Part 3-100: basic dimensions of front panels, sub racks, chassis, racks and cabinets
[R33]	EN 60332-1-2	Tests on electric and optical fibre cables under fire conditions Part 1-2: Test for vertical flame propagation for a single insulated wire or cable - Procedure for 1 kW pre-mixed flame



ID	Standard	Title
[R34]	EN 60529	Degrees of protection provided by enclosures (IP Code)
[R35]	EN 60664-1	Insulation coordination for equipment within low-voltage systems -- Part 1: Principles, requirements and tests
[R36]	EN 60715	Dimensions of low-voltage switchgear and control gear. Standardized mounting on rails for mechanical support of switchgear, control gear and accessories
[R37]	EN 60754-2	Test on gases evolved during combustion of materials from cables – Part 2: Determination of acidity (by pH measurement) and conductivity
[R38]	EN 61000-6	Electromagnetic compatibility (EMC) - generic standards
[R39]	EN 61000-6-2	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity standard for industrial environments
[R40]	EN 61000-6-4	Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments
[R41]	EN 61034	Measurement of smoke density of cables burning under defined conditions
[R42]	EN 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
[R43]	EN 62262	Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (ik code).
[R44]	EN 62305	Protection against lightning
[R45]	ETSI EN 301 462	Human Factors (HF); Symbols to identify telecommunications facilities for deaf and hard of hearing people
[R46]	GTFS	General Transit Feed Specification
[R47]	IEC 60068	Environmental testing
[R48]	IEC 60331	Tests for electric cables under fire conditions
[R49]	IEC 60364	Low-voltage electrical installations (equivalent to HD 384 series)
[R50]	IEC 61000-3-6	Electromagnetic compatibility (EMC) - Part 3: Limits - Section 6: Assessment of emission limits for distorting loads in MV and HV power systems - Basic EMC publication
[R51]	IEC 61000-3-7	Electromagnetic compatibility (EMC) - Part 3-7: Limits - Assessment of emission limits for the connection of fluctuating installations to MV, HV and EHV power systems
[R52]	IEC 61000-5-2	Electromagnetic compatibility (EMC) - Part 5: Installation and mitigation guidelines - Section 2: Earthing and cabling
[R53]	IEC 61643	Low-voltage surge protective devices
[R54]	IEEE 1220	IEEE Standard for Application and Management of the Systems Engineering Process
[R55]	IEEE 1588	IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
[R56]	IEEE 60068-2-1	Environmental testing - Part 2-1: Tests - Test A: Cold
[R57]	IEEE 60068-2-30	Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)
[R58]	ISO 11064	Ergonomic design of control centers



ID	Standard	Title
[R59]	ISO 9001	Quality management systems — Requirements
[R60]	ISO/CEI 15288	Systems engineering - Systems life cycle processes
[R61]	NFPA 780	Standard for the Installation of Lightning Protection Systems
[R62]	RFC 7384	Security Requirements of Time Protocols in Packet-Switched Networks
[R63]	NFPA72	National Fire Alarm and Signaling Code
[R64]	NFPA 130	Standard for Fixed Guideway Transit and Passenger Rail Systems
[R65]	2010 ADA	2010 ADA Standards for Accessible Design
[R66]	UL2900 series	Cybersecurity for Network-Connectable Products
[R67]	TSA SD 1580/82-2022	Cybersecurity Requirements for High-Risk Rail Operators

TABLE 53 LIST OF APPLICABLE STANDARDS

2.5 Other Documents

2.5.1 The following documents shall be referred:

ID	Document	Title
[R68]	Schedule 16	Scope of Work
[R69]	Schedule 5(a) SPEC-0005	Cybersecurity Technical Specification
[R70]	Schedule 3	Safety, Security and RAM Requirements

TABLE 54 OTHER DOCUMENTS

3 TERMS, DEFINITIONS, AND ABBREVIATIONS

3.1 Terms, Definitions and Abbreviations

- 3.1.1.1 All the terms, definitions and abbreviations are provided in: Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of the PACIS

- 4.1.1 The PACIS consists of the Public Address System (PAS) and the Customer Information System (CIS).
- 4.1.2 The purpose of the Public Address System (PAS) is to provide audible information to facilitate the movement of passengers and inform them of operating conditions (arrivals, departures, hazards...) by means of broadcasting both manual and automated audio announcements. Announcements can also be emergency announcements, such as evacuation announcements, not only for passenger stations but also for any other facilities of the California High-Speed Rail System.
- 4.1.3 The purpose of the Customer Information System (CIS) is to provide visual information to passengers at station entrances, concourses, and platforms of the California High-Speed-Rail System.

4.2 PACIS System Definition

- 4.2.1 The PACIS provides users with audio announcements and visual messages for the following:
 - Train service information.
 - Safety and security information.
 - Emergency and evacuation information.
 - Information about user facilities at the station.
 - Local transit connection details.
 - Authority-controlled advertising.
- 4.2.2 The PACIS information, which is real-time and synchronized, shall be delivered to users via:
 - Audio announcements.
 - Visual messages
 - Digital content made available to apps and browsers on users' smartphones, computers, and other communicating devices and platforms.
 - Audio announcements accessible via T-coil receivers.
- 4.2.3 The PAS shall include, but not be limited to, the following equipment: loudspeakers, Dynamic Ambient Noise Sensors (DANS), interfaces, amplifiers, microphones, PA consoles, PAS NMS, necessary cables, and HMI functionality via ICSS workstation for both normal and emergency voice evacuation announcements and background music.
- 4.2.4 The CIS shall include, but not be limited to, the following equipment: Passenger Information Displays (PIDs), CIS NMS, necessary cables, and HMI functionality via ICSS workstation for both normal and emergency messages.

4.3 PACIS System Operational Context

- 4.3.1 The mission of the PACIS system is to provide reliable visual and audible information to the passengers and staff in compliance with the operational needs.
- 4.3.2 The PACIS shall be operated according to the CHSR operational procedures.

4.4 Design Life

- 4.4.1 The design life requirements of the PACIS shall be 30 years.
- 4.4.2 The design life requirements of the PACIS shall allow for the pertinent evolution and technological change of the PACIS system throughout its life to ensure it remains fit for purpose.



- 4.4.3 The TSCC Contractor shall ensure that PACIS system components with shorter design lifespans shall be managed by scheduled technology refresh strategies and spares management plans.
- 4.4.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce PACIS system components (with equal or compatible technical specifications) for the entire design life required.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

- 5.1.1 The PACIS shall be designed in accordance with the requirements described in this specification.
- 5.1.2 The Public Address System (PAS) shall be deployed in passenger stations, depots, OCC Building,, Stations, car parks, and any other facilities required for the California High-Speed-Rail System.
- 5.1.3 The Customer Information System (CIS) shall be deployed in passenger stations (station entrances, concourses, platforms, and any other place where there will be passengers waiting or in transit).
- 5.1.4 An integrated system for PACIS should be delivered by the TSCC Contractor, with redundant PACIS central servers in the OCC (i.e., No single points of failure) and connected with the PACIS station servers/controllers through the Digital Communications Network (DCN). Any other approach by the TSCC Contractor shall be properly justified, ensuring that a greater level of functionality, greater flexibility, reduced lifecycle cost, improved sustainability, etc. are provided.
- 5.1.5 The PACIS information shall be available in English and Spanish.
- 5.1.6 The PACIS design shall align with the California High-Speed-Rail branding, visual identity, signage system and graphical charts and shall be fully integrated in the overall station designs and shall take architectural constraints into account.
- 5.1.7 The TSCC Contractor's PACIS design shall respect and adapt to the architectural designs of stations and other facilities to avoid impacts in the constructive elements of the different facilities and shall fit and be installed harmoniously.
- 5.1.8 Ensuring compliance with the previous requirement, PACIS elements may be installed over existing station/facility infrastructure, ensuring that the overall performance of the PACIS is not compromised.
- 5.1.9 The PACIS design shall meet the ADA (Americans with Disabilities Act) requirements to guarantee the accessibility for persons with disabilities and persons with reduced mobility regarding ticketing, information desks, customer assistance points, visual information (signposting, pictograms, printed or dynamic information), spoken information, induction loops, etc.
- 5.1.10 The PACIS equipment shall be placed in locations that do not obstruct or encroach upon pedestrian access or movement paths.
- 5.1.11 The Passenger Information Displays (PIDs) at platforms shall be double-sided and legible from 25 meters under all ambient lighting conditions.
- 5.1.12 The distance between the PIDs shall be a maximum of 50 meters.
- 5.1.13 The lower edge of all PIDs shall be mounted at a minimum height of 2.5 meters above floor level.
- 5.1.14 Only PACIS systems with service-proven records for application on railway infrastructure shall be proposed by the TSCC Contractor.
- 5.1.15 Where integration with other public transport modes is planned at the California High-Speed-Rail stations (for example airport, metro, tram and bus), passenger information from this external transport modes shall be shown in separate displays from those used for railways.
- 5.1.16 PACIS shall display an accurate and up-to-date train timetable and scheduling information at all times. Real-time information shall be displayed to passengers that changes dynamically, based upon the status of the railway operations.
- 5.1.17 Time and date information shall be connected and received from the Network Timing System (NTS).
- 5.1.18 The PACIS shall be interfaced with the Fire Protection System to enable pre-recorded evacuation or emergency messages and hence shall meet the highest availability standards.
- 5.1.19 Emergency announcements shall take precedence and override normal live and pre-recorded announcements.



5.1.20 The PACIS shall be available and operational on a 24/7 basis.

5.2 Environmental Conditions Requirements

- 5.2.1 The TSCC Contractor's PACIS system design shall be appropriate for, and resilient to, the local environmental and climatic conditions at each installation site.
- 5.2.2 All equipment shall be protected from damage or degradation in performance due to shock or vibration as experienced in the railway environment.
- 5.2.3 The IP rating of the outdoor equipment shall be at least IP65.
- 5.2.4 All outdoor equipment that is directly exposed to the sun shall be UV-protected.
- 5.2.5 The PIDs shall be robust enough in design to ensure 100% protection from water, dust, lightning, rust, and any other environmental condition for the locations where each PID is to be installed.
- 5.2.6 The screens shall be protected against vandalism. The housing shall be vandal-resistant up to IK08 for indoor use and IK10 for outdoor use, and graffiti-resistant.
- 5.2.7 Bird repellent spikes shall be used for outdoor screens. The TSCC Contractor shall obtain prior approval from the Authority to ensure the locations of screens on which these spikes should be installed.
- 5.2.8 All PID and PAS equipment shall comply with Waste Electrical and Electronic Equipment (WEEE) and Restriction of Hazardous Substances (RoHS) directives for electronic waste and hazardous substances, and a component take-back or recycling plan shall be provided.

5.3 Operational Requirements for PACIS

- 5.3.1 The TSCC Contractor's PACIS design shall ensure compliance with station architecture design and the California High-Speed-Rail operational rules when:
 - Defining the locations required for the placement of the displays and the audio devices (speakers) to convey information to passengers and staff.
 - Establishing messages, alarms, warnings, and notification levels and thresholds.
 - Developing alarm triggering procedures that adhere to the California High-Speed-Rail System.
 - Implementing alarms, protocols, and procedures for the PACIS.
- 5.3.2 The PACIS shall allow the Operators to operate and maintain the main line and related local facilities as described in the concept of operations.

5.4 Functional Requirements for PACIS

5.4.1 General

- 5.4.1.1 The PACIS shall comply with the following minimum functional requirements.
- 5.4.1.2 Normal operation of the PACIS shall be performed via the Operator ICSS Workstation as part of the ICSS System.
- 5.4.1.3 The PACIS central servers shall be in the OCC, and the local servers shall be in stations.
- 5.4.1.4 A downgraded mode shall be considered in the event of a failure of connection with the OCC central server, so the local equipment at the station can take over.
- 5.4.1.5 Communication between the different PACIS of each station shall be done via the DCN aligned with the cybersecurity and operational policies of the California High-Speed-Rail System.
- 5.4.1.6 PACIS HMI on ICSS workstation shall have functionality of transmitting video/audio files to the display screens and PAS for public addressing, advertisement, and commercial purposes.
- 5.4.1.7 PACIS announcements shall be managed from the OCC.



- 5.4.1.8 The PACIS shall support the definition of different priorities for emergency messages. The emergency messages with higher priority shall interrupt any lower priority current announcements
- 5.4.1.9 Depending on the triggering input signals, pre-recorded/computerized emergency messages shall be automatically broadcast to pre-defined areas within the California High-Speed-Rail stations.
- 5.4.1.10 The PACIS shall be able to broadcast voice and display visual messages simultaneously when needed, depending on the type of information (e.g., evacuation and emergency messages, etc.).
- 5.4.1.11 The PACIS shall be synchronized appropriately to provide coherent passenger information (especially for the visually impaired people).
- 5.4.1.12 The PACIS shall comply with NFPA 130 - Standards For Fixed Guideway Transit and Passenger Rail Systems.
- 5.4.1.13 The PACIS system shall comply with Emergency Voice/Alarm Communication Systems (EVACS) requirements contained within the National Fire Alarm and Signaling Code (NFPA 72).
- 5.4.1.14 All audio announcements from loudspeakers shall provide good speech intelligibility as measured using the STI-PA metric and the STI-PA score shall meet the requirements of NFPA 72 in all locations for emergency announcements.
- 5.4.1.15 The PACIS shall be fed by the train control system and automatically updated. For this reason, interfaces to the train control system shall be provided to receive real-time traffic information using the General Transit Feed Specification (GTFS) format or a similar format agreed upon with the Authority.
- 5.4.2 Public Address System (PAS)**
- 5.4.2.1 The Public Address System (PAS) shall enable the Operator to address the passengers, the public, employees, and operation and maintenance staff with clearly understandable audio announcements on all areas of the CHSR System without disturbing the public unreasonably.
- 5.4.2.2 The PAS shall be installed at strategic locations such as OCC, stations, platforms, depots, maintenance facilities/workshops, traction power substations, and shelter sites, etc., aligned with stations and facilities' architectural design and shall support manual and automated audio announcements.
- 5.4.2.3 Various types of loudspeakers shall be installed throughout the railway line in accordance with the installation location. It is recommended that the speakers include the following types:
- Ceiling mount speaker.
 - Wall mount speaker.
 - Column mount speaker.
 - Sound projector.
 - Horn speaker.
- 5.4.2.4 The PAS shall cover the whole station building and the nearest outdoor area at the station building, where the main person flows and crowded areas are anticipated.
- 5.4.2.5 The PAS shall broadcast the following message types (not limited to):
- Automatic train announcements prior to the train's arrival at the station (configurable period).
 - Live, pre-recorded, and computerized messages (Text to speech).
 - Music and advertisements.
 - Gong and siren generator.
- 5.4.2.6 The PAS shall allow broadcasting automatic announcements as well as bursting/manual announcements when required and shall provide the facilities to support pre-recorded announcements



(verbal and speech synthesis) in English and Spanish from stations and/or OCC to the complete station public area (platforms and concourses).

- 5.4.2.7 The PAS information shall transit from the OCC to stations and other locations, making use of real-time protocols and multicast that shall control audio over IP across DCN. Thus, the PAS solution shall be IP-based.
- 5.4.2.8 Digital announcements shall be based on real voice recording and text-to-speech engines (TTS) or a combination of both, according to the number of languages to be managed and available TTS engines.
- 5.4.2.9 The TSCC Contractor shall incorporate the following priorities as a minimum for the PAS announcement:
- Priority 1 for emergency predefined audio announcements (for example- Fire evacuation announcement).
 - Priority 2 for live local announcements from the Station
 - Priority 3 for live announcements from the OCC.
 - Priority 4 for automatic announcements triggered by the Signaling system.
 - Priority 5 for music broadcast.
- 5.4.2.10 The PAS shall support the definition of at least ten (10) different PAS announcement priorities. The priorities shall be approved by the Authority and configurable by the Operator. Priorities shall be configurable without requiring special tools or a software update.
- 5.4.2.11 Activation of a pre-recorded, automatic, or live announcement shall automatically suppress the continuous music broadcast in the corresponding zones or locations.
- 5.4.2.12 The broadcast of an announcement from the OCC to a station shall not prevent the other stations from receiving music or advertising.
- 5.4.2.13 In stations with trains passing through without stopping (independently of the type and the speed of the train), and according to stations and passenger platforms, an audible warning system, as part of the PAS, shall notify audible announcements to passengers standing on the platform of approaching trains. Also, the CIS shall alert passengers on platforms by means of displaying the proper messages in the platform PID. The messages, in English and Spanish, shall follow the local regulations. ".s should be automatically triggered to broadcast and should be ranked as priority messages. Additional station generated messages shall notify when trains shall start moving or shall open/close doors.
- 5.4.2.14 Zone and multi-zone announcements, including environmental noise sensing, shall be supported.
- 5.4.2.15 PAS broadcast zones shall be configured by a system administrator.
- 5.4.2.16 PAS zone configuration shall support any combination of single or multiple zones as may be required for safety, operations, etc.
- 5.4.2.17 The PAS zone configuration shall enable overlapping between zones for redundancy purposes.
- 5.4.2.18 Dynamic Ambient Noise Sensors (DANS) shall be used to automatically adjust the audio level in each zone at any time, including during announcements.
- 5.4.2.19 All live PAS announcements from the OCC/Depots/Stations shall be recorded in a centralized Voice Recording System (VRS) with originator identification, duration, date, and time information. Refer to the Telephony System technical specification document, which includes VRS.
- 5.4.2.20 The PA Console shall be equipped with a standard range of operational accessories to support effective use by station/control room personnel, such as "gooseneck" microphone with a Push to Talk (PTT) button, a button keyboard to select audio zones, emergency announcements, alarm tones, or music.
- 5.4.2.21 The PAS shall be able to receive, amplify, and deliver PA announcements that originate from:
- ICCS workstation at OCC and Station.



- PA console/microphone.
- Authorized telephone extensions.
- Authorized Wireless Communication System mobile devices.

- 5.4.2.22 The TSCC Contractor shall provide an acoustical coverage study, to optimize the position and the gain of the loudspeakers in all the areas.
- 5.4.2.23 An acoustic coverage study shall be submitted by the TSCC Contractor for the Authority's approval in coordination with Architectural design.
- 5.4.2.24 The Sound Pressure Level (SPL) throughout the buildings shall comply with the requirements in the current local fire code for emergency broadcasting in the event of a confirmed fire alarm.
- 5.4.2.25 The SPL throughout the buildings shall ensure the achievement of the intelligibility of the broadcasts at a minimum specified Speech Transmission Index (STI) value.
- 5.4.2.26 The PAS Graphical User Interface (GUI) on the ICSS workstation shall be capable of displaying the zone occupied during the announcements.

5.4.3 Customer Information System (CIS)

- 5.4.3.1 The Passenger Information Displays (PIDs) shall be installed at strategic locations at stations and platforms where they can be legible from a reasonable distance for an average person.
- 5.4.3.2 The PIDs shall be in areas that provide sufficient queuing and dwell space for passengers to stop and view the displays without impeding pedestrian flow or obstructing access to station entrances, fare gates, vertical transport (e.g., escalators, stairs, lifts), or other circulation-critical areas. The TSCC Contractor shall demonstrate, through pedestrian flow analysis or station circulation modelling in accordance with applicable station design standards and human factors guidelines (e.g., ISO 11064, BS EN 894, or equivalent), that the placement of each PID supports safe, accessible, and efficient passenger movement under both normal and disrupted operating conditions.
- 5.4.3.3 The CIS shall keep the passengers well informed on the travel options, and additional real-time information shall be provided as well during the disruption of the operational services.
- 5.4.3.4 The CIS shall be capable of displaying timely and location-relevant notices to passengers, including:
- Service alerts, such as delays, cancellations, and diversions;
 - Information on planned maintenance activities affecting train services or station access;
 - Emergency or unplanned disruptions, including weather-related impacts or incidents;
 - Notices about upcoming public events (e.g., festivals, sporting events) that may affect passenger volumes or travel patterns.
- 5.4.3.5 The information provided (in English and Spanish) to the passengers shall consist of the following real-time information (not limited to):
- Train number.
 - Scheduled arrival and departure time (for all trains within the next two hours).
 - Expected arrival and departure time (for all trains within the next two hours).
 - Train origin and destination.
 - All intermediate stations.
 - Platform number (including highlighting platform changes).
 - Passenger facilities on the train.
 - Name of the train operator.
 - Clock displaying current local time.



- Operational, normal, and emergency (including evacuation) messages to passengers.
- Supplementary information like temperature.
- Service alerts and disruptions, including delays, cancellations, or changes to train services due to delays, incidents, adverse weather, or planned maintenance activities.

5.4.3.6 CIS shall be designed with features which include (not limited to):

- Auto-repeat of messages.
- Cycles of messages.
- Alternated messages.
- Scheduled pre-recorded messages.
- Scrolling left / right.
- Rolling up / down.
- Flashing.
- Variable message lengths and character size.
- IP based.

5.4.3.7 The CIS shall be able to provide different types of information (not limited to):

- Pre-recorded messages and textual display messages.
- Delivery of automated scheduled messages.
- Live Operator speech.
- Infotainment.
- Advertising.
- Video streams.
- Graphics.
- Live web content.
- Multi-lingual messaging (English and Spanish languages)

5.4.3.8 Individual and predefined messages capability shall be supported by the CIS.

5.4.3.9 CIS messages shall be (not limited to):

- Predefined messages.
- Pre-formatted data completed by adding words/parameters.
- Free text messages.

5.4.3.10 The information provided to the passengers shall be clear and coherent.

5.4.3.11 The TSCC Contractor shall design a system that allows the assignment of priority levels to the different types of information broadcast, for example, a way to treat advertising, infotainment, and music as optional features with lower priority.

5.4.3.12 If an emergency evacuation is triggered or an audible alert broadcast is made, in addition to Public Address System, and to enable a fast and efficient communication to passengers and staff to assist in evacuation scenarios, PIDs within the affected voice alarm zone shall automatically fill the entire display screens with an appropriate emergency messages, giving people in the danger zone both audible and visual alerts and direction, quickening response and evacuation times. Emergency



messages shall continue to be displayed on screens even if the system's server or the IP network has failed.

- 5.4.3.13 The information (including advertisements) shall be shown in PIDs placed at least at the station entrance, concourse, ingress automatic gates, and station platforms to advise passengers.
- 5.4.3.14 Each display technology shall be appropriate for its location, application, and high performance, with due regard to environment, lighting levels, and legibility.
- 5.4.3.15 Each display on platforms and in concourses shall be fully readable to a normal sighted individual when standing or sitting in a wheelchair.
- 5.4.3.16 The PIDs shall comply with the principles of EN 16584-2:2020 – Railway Applications – Design for Accessibility, ensuring that real-time and static information is legible from typical passenger approach paths. The displays shall meet the following minimum criteria:
- Characters shall be at least 20 mm high for sighting distances of up to 8 meters and scaled proportionally for greater distances.
 - Text and symbols shall have a minimum luminance contrast ratio of 70% against the background.
 - Displays shall be positioned to avoid glare and provide visibility from multiple angles, including for users with mobility or visual impairments.
 - Information shall be bilingual (English and Spanish), clear, concise, and unambiguous.
- 5.4.3.17 All PIDs shall conform to the accessibility and visibility provisions of the ADA Standards for Transportation Facilities (49 CFR Part 37, Appendix A), including:
- Text characters used in fixed or dynamic messages shall be sans-serif, uppercase or mixed-case, and of a height appropriate to the viewing distance and ambient conditions.
 - Displays shall be mounted at a height and angle that enables clear line of sight for both standing and seated users, including persons using wheelchairs.
 - Displayed content shall provide high contrast, non-reflective backgrounds, and remain visible under lighting conditions typical to indoor and covered station environments.
 - All dynamic information must be provided audibly via the Public Address system where required, to ensure compliance with multimodal accessibility principles.
- 5.4.3.18 The CIS shall be capable of creating and displaying passenger information in any combination of characters, numerals, animated graphics, punctuation & symbols.
- 5.4.3.19 The CIS shall incorporate a real-time digital clock, which must be synchronized with the Network Timing System (NTS), and the addition of a message display.
- 5.4.3.20 The CIS digital clocks shall show local time in the 24-hour format: HH:MM: SS and configurable to show local time in AM/PM format.
- 5.4.3.21 Displays that have dates shall use US customary format – MM:DD: YY.
- 5.4.3.22 The CIS shall be able to operate in all ambient artificial lighting conditions and outdoor lighting environments, including full sunlight conditions found throughout the station, and automatically adjust the display intensity/illumination/brightness to match ambient conditions.
- 5.4.3.23 Energy-saving modes shall be implemented, including brightness adjustment, and/or switching on or off hours before trains are expected.
- 5.4.3.24 The PIDs shall be professional high-performance displays with suitable housing used for public display applications.



- 5.4.3.25 The PID housing shall be adequate for the indoor and outdoor environments, depending on the location.
- 5.4.3.26 All displays shall be equipped with a status indication arrangement that is visible outside the panel enclosure, allowing maintenance personnel to check the PID status at a glance.
- 5.4.3.27 The CIS shall automatically coordinate PAS announcements with travel information shown on PIDs across the site.
- 5.4.3.28 All messages shall be displayed in English and Spanish, and/or blinking/flipping between the two languages as selected by the CIS operator.
- 5.4.3.29 Display information shall be sourced from the centralized control system, with the capability for manual override from ICSS workstations in the OCC.
- 5.4.3.30 Each CIS layout shall be easily configurable by authorized users, allowing them to choose which blocks and widgets, such as live news and travel feeds, videos, or graphics, are displayed where on each of the display screens.
- 5.4.3.31 The authorized users shall be able to create those templates to be used by the authorized operator, depending on the needs of each display location or even operational conditions (evacuation, alarms, operational incident, etc.).
- 5.4.3.32 The CIS shall continue normal operation and dissemination of information without interruption during template change.
- 5.4.3.33 The PIDs shall support the display of a defined template in degraded mode (loss of communication). This template shall display as a minimum, the local time, a predefined message, and an appropriate image.
- 5.4.3.34 The TSCC Contractor shall provide an ergonomic study to optimize the position of the PIDs in the stations.
- 5.4.3.35 The PID screen shall be based on LED technology.
- 5.4.3.36 The minimum size for the PID screen must be 42 inches diagonal.
- 5.4.3.37 The PIDs screen resolution shall be at least 4K, with an aspect ratio according to the purpose and location of the display within the station or facility.
- 5.4.3.38 The PIDs shall be capable of displaying commonly supported media file formats (e.g. MP4, MPEG-4) but shall not allow deprecated or insecure technologies such as Flash or DVD/Blu-ray playback. All media playback systems must be integrated into a secure content management platform that prevents unauthorized access or tampering.
- 5.4.3.39 It shall be possible to monitor the status as well as the current contents of any PID at any location.
- 5.4.3.40 All PIDs shall support secure remote monitoring, diagnostics, and update functionality, including retrieval of log files, firmware version, and current content status.
- 5.4.3.41 The CIS shall provide remote operator capability to shut down or blank out any or all PIDs in the event of cyber intrusion, inappropriate content display, or failure scenarios, without impacting emergency visual messaging systems.
- 5.4.3.42 The CIS shall support open APIs (e.g., GTFS-RT, SIRI-SM) for future integration with mobile apps, web portals, and third-party passenger information services.
- 5.4.3.43 The CIS shall support future integration with AI-powered analytics systems to enhance passenger communication, disruption handling, and system resilience.

5.4.4 **PACIS Management System**

- 5.4.4.1 The PACIS Management System shall include the following features (not limited to):
 - Friendly user GUI and remote web browser interface.



- Graphical display of the PACIS associated elements along the California High-Speed-Rail system.
- The status of the PACIS equipment shall be graphically shown.
- PACIS zone and multi-zone configuration and edition.
- Creation, loading and editing of PACIS messages and templates.
- Pre-programming system triggering events.
- Alarms and status information in both graphical and table formats.
- Alarms drill-down analysis to diagnose alarm root-cause.
- Message priorities assignment and pre-emption strategy when simultaneous messages are broadcasted.
- Co-ordinating PACIS messages.
- Retrieve event logs (creation of daily/weekly/monthly/annual log files of all events).
- Modifying pre-defined system information.
- System parameter configuration.
- Report generation.

5.4.4.2 The PACIS Management System shall be provided with administration capabilities as a minimum:

- Log-on Levels Control Functions.
- System administration, management, and housekeeping functions.
- System configuration and user data modifications, including resetting of passwords.
- Read only to system configuration and use data modification.
- Creation, configuration, and deletion of users and associated roles.
- Creation and deletion of designated functions and commands available to each log-on control access level.

5.4.4.3 The PACIS Management System shall monitor system alarm status on a real-time basis and allow alarm acknowledgment, filtering, and export at least in Excel format.

5.4.4.4 The PACIS Management system shall maintain for at least 90 days a historical record archive of system faults, including fault event timestamp, fault location, fault type, and fault cleared timestamp.

5.4.4.5 In addition to the alarms and status to be shown on the ICSS workstation in the OCC, the status of major equipment of the system shall be monitored and displayed with suitable indications to the local PACIS equipment.



5.5 Performance Requirements for PACIS

5.5.1 Public Address Systems (PAS)

- 5.5.1.1 Voice announcement latency to any location from any central facility shall not exceed 250ms.
- 5.5.1.2 The amplifier switching shall be automatic, seamless, without any intervention or interruption to the ongoing audio announcement dissemination.
- 5.5.1.3 Each zone shall be equipped with a sufficient number of speakers located throughout the zone to ensure uniform audio levels
- 5.5.1.4 The coverage variance shall be within the range of ± 3 dB for the whole coverage area.
- 5.5.1.5 Loudspeakers shall not be driven at more than 80% of their maximum allowable input rating.
- 5.5.1.6 Sufficient quantities of Digital Ambient Noise Sensor (DANS) shall be installed to fully detect the ambient noise within each zone.
- 5.5.1.7 The output level of the PA audio announcement shall be adjusted in a real-time manner according to the level of noise measured by DANS.
- 5.5.1.8 The PAS shall ensure that the broadcast sound level provided as necessary throughout the dedicated area is greater than the ambient noise level by a configurable value (typically 10dB) up to a maximum of 95dBA.
- 5.5.1.9 The PAS volume distribution at distances beyond 50 meters from the ROW (Right-of-Way) shall not exceed 65 dBA. During nighttime, in residential areas, the volume level shall be reduced by an additional 10 dBA. The TSCC Contractor shall verify that system specifications comply with all local noise regulations.
- 5.5.1.10 The reverberation time (RT60) at 500Hz shall be less than 1.5 seconds (Max RT).
- 5.5.1.11 The PAS shall provide STI > 0.5.
- 5.5.1.12 The TSCC Contractor shall perform acoustic testing to ensure audio performance of the PA system in each zone according to the latest revision of standard IEC 60268-16.
- 5.5.1.13 The PAS shall allow the operator to adjust manually the volume level, and automatic volume control shall not override the manual adjustment made unless further configuration setting is edited.
- 5.5.1.14 At the California High-Speed-Rail facilities, the distribution of the audio signals and cable route design shall be configured in redundant approach to ensure that failure of an amplifier, a cable and/or a speaker does not render the PA system inoperative or result in the total loss of PA facility in any part of any zone.

5.5.2 Customer Information System (CIS)

- 5.5.2.1 The PIDs shall use LED screen monitors with video display capability with a size and resolution consistent with viewing from a distance up to 25 meters and from the viewing angle of +/- 160 degrees or better from the horizontal and from the vertical.
- 5.5.2.2 PIDs shall be sized to show individual station names or words of messages. Each station's name, or words of messages, shall be displayed for a minimum of 2 seconds.
- 5.5.2.3 If scrolling information is shown (either horizontal or vertical), each complete word shall be displayed for a minimum of 2 seconds, and the horizontal scrolling speed shall not exceed 6 characters per second.
- 5.5.2.4 The time between the validation of any operator action in real time and the reception of it into PIDs shall not exceed 3 seconds.



5.5.3 Safety Requirements

- 5.5.3.1 PACIS shall comply with the safety requirements defined in Schedule 1 and the Authority's System Safety Plan.
- 5.5.3.2 Where PACIS supports evacuation, emergency messaging, or audible warning, these functions shall be assigned a minimum Safety Integrity Level (SIL) 1 as per EN 50126-2.

5.5.4 RAM Requirements

- 5.5.4.1 The TSCC Contractor shall be responsible for performing all the activities as specified in Schedule 1 and the Authority's RAM Management Plan.

5.6 Cybersecurity and Security Requirements

- 5.6.1 The PACIS design, configuration, and operation shall be fully compliant with the California HSR Cybersecurity Technical Specification. All generic security controls, roles, logging, patching cadence, incident-response procedures, and assurance measures are established within the California HSR Cybersecurity Technical Specification.
- 5.6.2 All PACIS components, including PIDs, PA controllers, servers, and media players, shall be treated as networked endpoints and subject to the Authority's cybersecurity compliance reviews, threat modeling, and supply chain risk assessments.
- 5.6.3 The TSCC Contractor shall ensure that all display and multimedia content sources are verified, approved, and distributed through a secure content management platform with appropriate user access controls and content validation mechanisms, including the usage of cryptographic hashes to verify the integrity of media files. Use of deprecated or insecure file formats (e.g., Flash, DVD media, or unauthorized codecs) is prohibited.
- 5.6.4 The PACIS network topology shall implement segmentation and security zoning such that a local compromise (e.g., ransomware attack) cannot propagate to other zones or affect other systems. Each system shall be capable of being logically or physically isolated without interrupting emergency override functions.
- 5.6.5 Controls shall be implemented to prevent and mitigate the potential for unauthorized messages to be displayed on any passenger facing visual displays.
- 5.6.6 PACIS and associated systems shall have a nominated System Owner who shall be accountable for cybersecurity risk ownership and mitigation.



6 INTERFACES REQUIREMENTS

6.1 General Requirements

6.1.1 The interfaces are classified as following:

- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR contractors)
- External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors)
- Internal Interfaces: Interfaces between systems within the TSCC scope

6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.

6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.

6.2 Third Party Interface

6.2.1 Interfaces between PACIS from and to any external database or external transport mode real-time traffic information should be aligned with and based on the General Transit Feed Specification (GTFS) format, or a similar format agreed with the Authority. In addition, other related standards and specifications to ensure future interoperability between external information systems through open interfaces.

6.2.2 For the implementation of those open interfaces, the TSCC Contractor shall ensure (not limited to) that adequate APIs are used or developed (e.g., SIRI-SM API for exchanging real-time information about public transportation services), the needed models are implemented, and a common codification is adopted. Moreover, integration tests shall be conducted to ensure the full interoperability of the information exchange between transport operators' information systems.

6.3 External Interfaces - Trainsets

6.3.1 The TSCC Contractor shall work together with the Trainset contractor to allow OCC to make live audio announcements and display videos/messages via the Future Railway Mobile Communication System (FRMCS) to the Rolling Stock onboard public address and passenger information display system(s).

6.4 External Interfaces – facilities contractor

6.4.1 The TSCC Contractor shall install all PACIS equipment in the OCC and facilities being provided by the facilities contractor.

6.4.2 Visible equipment shall be integrated harmoniously with the architecture of the stations.

6.4.3 The TSCC Contractor shall provide to the facilities contractor:

- Equipment dimensions
- Equipment clearances requirements
- Equipment mounting and fixings requirements
- Cable routes/containment requirements
- Equipment loadings
- Installation and maintenance requirements
- Equipment heating loads
- Equipment cooling loads
- Equipment hydraulic requirements



- 6.4.4 To be provided by facilities contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:
- Room dimensions and layouts
 - Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
 - Room raised floor system
 - Delivery access routes.
 - Maintenance access routes

6.5 External Interfaces – stations contractor

- 6.5.1 The TSCC Contractor shall install all PACIS equipment in the stations.
- 6.5.2 Visible equipment shall be integrated harmoniously with the architecture of the stations.
- 6.5.3 The TSCC Contractor shall provide to the station contractors:
- Equipment dimensions
 - Equipment clearances requirements
 - Equipment mounting and fixings requirements
 - Cable routes/containment requirements
 - Equipment loadings
 - Installation and maintenance requirements
 - Equipment heating loads
 - Equipment cooling loads
 - Equipment hydraulic requirements
- 6.5.4 To be provided by stations contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:
- Stations layouts
 - Room dimensions and layouts
 - Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
 - Room raised floor system
 - Delivery access routes.
 - Maintenance access routes

6.6 Internal Interfaces

- 6.6.1 **Interface with Digital Communications Network (DCN)**
- 6.6.1.1 The PACIS shall have an interface with the DCN for the transport of PACIS data in a secure and reliable way and the interconnection of all PACIS devices along the California High-Speed-Rail System.
- 6.6.2 **Interface with Traffic Management System (TMS)**
- 6.6.2.1 The PACIS shall have an interface with the TMS for real-time traffic information display, such as train identification, change of time, cancellation, mission/itinerary modification, and, in general, provide all required information to PACIS to ensure the functionalities and performance described in this specification for PACIS.



6.6.3 Interface with Telephony System

- 6.6.3.1 The PACIS shall have an interface with the Telephony System to allow announcements from authorized telephones to the PAS.
- 6.6.3.2 The PACIS shall have an interface with the Voice Recording System as a part of the Telephony System, to record all the live announcements made through the PAS.

6.6.4 Interface with Network Timing System (NTS)

- 6.6.4.1 The PACIS shall have an interface with the NTS to ensure an accurate current time of the day display and to provide time synchronization to the PACIS system.

6.6.5 Interface with Integrated Control and Supervision System (ICSS)

- 6.6.5.1 The PACIS shall interface with the ICSS to manage PAS and PIS audio announcements and visual messages from ICCS HMI.
- 6.6.5.2 The PACIS shall have an interface with the ICSS on standard protocols, e.g., SNMP (no vendor proprietary protocols shall be used), to allow status monitoring of the PACIS equipment.

6.6.6 Interface with Enterprise Asset Management System (EAMS)

- 6.6.6.1 The PACIS shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.

6.6.7 Interface with Wireless Communication System (WCS)

- 6.6.7.1 The PACIS shall have an interface with the FRMCS System (Future Railway Mobile Communication System) to allow OCC personnel to make announcements and distribute visual messages via the PACIS system on any Trainset or selected group of Trainsets.
- 6.6.7.2 PAS shall interface with FRMCS to allow live audio announcements from authorized FRMCS devices.
- 6.6.7.3 The PACIS shall interface with the Fire Alarm and Protection System to provide automatic announcements in emergency situations. The local Fire Alarm and Protection System at the station shall be directly connected to one of the station's PACIS elements to broadcast emergency pre-recorded audio announcements through PAS loudspeakers.

6.6.8 Interface with Low Voltage Power System (LVPS)

- 6.6.8.1 The PACIS shall have a redundant interface with the LVPS to ensure an uninterruptible power supply with battery backup of minimum 12 hours..



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied by the TSCC Contractor shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards. Refer to 2.4.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the design life requirements.

7.2 Software and Hardware Requirements

- 7.2.1 The PACIS design shall be based on COTS (Commercial Off-The-Shelf), open architecture, and modular system architecture, with standard non-proprietary interfaces.
- 7.2.2 The TSCC Contractor's design for central servers shall be on-premises, either physical, virtualized, or cloud, to ease systems evolution, complying with the Cybersecurity requirements defined in Cybersecurity Technical Specifications.
- 7.2.3 All cabling for PACIS shall be designed, supplied, installed, and commissioned by the TSCC Contractor.
- 7.2.4 The displays and speakers shall be maintenance-free.
- 7.2.5 PA loudspeakers located in external zones shall be compliant with IP66.
- 7.2.6 PACIS should adopt networked IP-based devices with PoE-type power supply, if possible, as soon as transmission distances allow it (typically less than 100m), i.e., in the presence of nearby network switches and according to the consumption of the devices. For longer distances, other technologies, such as Powered Fiber Cable systems, should be used to avoid the need for extra power-feeding cables and devices.
- 7.2.7 The PACIS servers/controllers shall have a redundant power supply.
- 7.2.8 The PACIS devices shall be connected to the UPS of the facility where they are located (OCC, station, etc.).
- 7.2.9 To simplify the PAS architecture, loudspeakers with built-in amplifiers can be considered for some locations.
- 7.2.10 The PIDs with at least 4K resolution displays shall be used due to their flexibility for passenger information purposes, video, infotainment, etc., by means of the possibility of defining multiple blocks or widgets within the screen area. Any other approach by the TSCC Contractor shall be properly justified, ensuring that a greater level of functionality, greater flexibility, reduced lifecycle cost, improved sustainability, etc., is provided.
- 7.2.11 The PIDs shall allow future extension and upgrading of native capabilities for display and management of graphics, animations, and digital video files playback.
- 7.2.12 PIDs shall be IP-based.
- 7.2.13 Low toxicity, low smoke emission, low flammability, zero halogen fire retardant cable shall be used for the distribution of broadcast signals to the speakers and signals to the displays.
- 7.2.14 Power consumption for each PACIS component type (PID, speaker, controller) shall be specified. Total system energy estimates shall be provided for normal, degraded, and standby modes.

7.3 EMC Requirements

- 7.3.1 The PACIS shall be fully immune and protected from any Electromagnetic Interference (EMI) with the traction power, multi-tubular cabling, and Radio Frequency Interference (RFI). The EMI emissions shall be mitigated in accordance with applicable standards (EN 50122 or equivalent)



8 TOLERANCES

Not applicable to PACIS.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 The TSCC Contractor shall supply and deliver all components related to the PACIS system scope of work.

9.2 Specific Requirements

9.2.1 The PACIS scope of supply and delivery shall include (not limited to):

- Central and local servers.
- Displays.
- Speakers.
- PA console.
- DANC.
- Controllers.
- Amplifiers.
- Cabling and connectors.
- Racks.
- Software architecture, including a full definition of protocols used.
- Management System.
- HW/SW licenses.
- Auxiliary elements and gear (cases, bird repellent spikes, attachments, bindings, testing equipment, etc.).
- Spare parts.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.

12.2 Specific Requirements

12.2.1 General test cases, Interface test cases, and the following information (not limited to) shall be recorded and reported during the test procedure:

- For commercial advertisement purposes, the CIS display scheduling template and content shall be tested in accordance with the configurable time duration, subject to approval from the Authority.
- Real-time information received from the train control system, its dissemination on PACIS equipment, e.g., destination, train arrival/departure, train passing through, etc. The test shall also be done by the actual operation of running trains on the mainline.
- Noise sensing and automatic gain control function by DANS.
- Emergency evacuation triggering test, display, and audible alert broadcasts made on PACIS equipment.

12.2.2 Functional test cases shall be defined to validate PACIS performance under degraded communications, server failover, emergency overrides, content switching delays, and alarm prioritization.

12.2.3 CIS template override scenarios and fail-safe displays (e.g., static message + time) shall be tested for network loss and emergency activation cases.



13 SUBMITTALS

13.1 General Requirements

13.1.1 General submittal requirements are defined in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence PACIS subsystem reliability, availability, and maintainability characteristics.



16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.



Schedule 5(o)

Signaling Engineering Rules (SER)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0019 – Signaling Engineering Rules (SER)

Rev. 1.0

Authored:	 _____ Gabriel Tyburcy, TCS Engineer	10/15/2025 _____ Date
Checked:	 _____ Andrew Clapham, Train Control Lead	10/15/2025 _____ Date
Checked:	 _____ Bruno Comperat, Deputy Director of Rail Engineering	10/16/2025 _____ Date
Approved:	 _____ Ryan Scott, Director of Rail Engineering	10/16/2025 _____ Date
Released:	 _____ Amit Joshi, Configuration Manager	10/16/2025 _____ Date



Document Revision History – SER Specifications**First Edition****September 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE DOCUMENT	5
1.2	APPLICATION OF THE DOCUMENT	5
1.3	RELEVANT INPUT DATA	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.1	REFERENCE STANDARDS.....	6
2.2	REFERENCE DOCUMENTS.....	6
3	TERMS, DEFINITION AND ABBREVIATION	8
4	MARKER BOARDS	8
4.1	GENERAL	8
4.2	MARKER BOARDS DEFINITION.....	8
4.3	VISIBILITY OF MARKER BOARDS	10
4.4	PROTECTION OF SUPERVISED LOCATION.....	10
4.5	OVERLAP	11
4.6	MARKER BOARD PLACEMENT	11
5	AXLE COUNTER	14
5.1	GENERAL	14
5.2	AXLE COUNTER PLACEMENT.....	14
6	BALISE.....	19
6.1	GENERAL	19
6.2	BALISE PLACEMENT	19
7	SHUNTING SIGNALS	24
7.1	GENERAL	24
7.2	SHUNTING SIGNALS PLACEMENT	24
8	DERAILERS	25
8.1	GENERAL	25
8.2	DISTANCE FROM FOULING POINT	25
8.3	DISTANCE FROM CATENARY SUPPORTS.....	25
9	SWITCH MACHINES	26
9.1	GENERAL	26
9.2	SWITCH MACHINES CONFIGURATION.....	26
10	WORK AREAS.....	27
10.1	GENERAL	27
10.2	TRACK LAYOUT SEGMENTATION	27
11	NAMING	28
11.1	GENERAL	28
11.2	MARKER BOARDS NAMING.....	28
11.3	AXLE COUNTERS NAMING.....	29



11.4	BALISE NAMING	29
11.5	SHUNTING SIGNALS NAMING.....	30
11.6	DERAILERS NAMING	30
11.7	SWITCH MACHINES AND SWITCH DETECTORS NAMING.....	31



1 INTRODUCTION

1.1 Scope of the document

1.1.1 This document specifies basic interlocking and ETCS engineering rules for the placement of the following signaling objects on a track layout:

- Marker Boards;
- Axle counters;
- Balises;
- Shunting signals;
- Derailers;
- Switch motors.

1.2 Application of the document

1.2.1 This document shall be used as an input for the TSCC Contractor Train Control Systems design of the California High-Speed Rail.

1.2.2 Engineering guidelines could also be used as input and high-level rules for the TSCC Contractor's detailed engineering rules. However, the TSCC Contractor will have to substantiate any changes related to rules specified in this document. The TSCC Contractor will have to develop its own engineering rules related to systems not scoped in this document in the frame of his design.

1.3 Relevant input data

1.3.1 The design shall consider ETCS system requirements which can be found in STS_ETCS [R21] (further ETCS technical specification).

1.3.2 The length of the passenger trainset according to HSR Design Criteria Manual (further HSR DCM) [R18] shall be considered – 205m (672.6 feet) for single-traction train and 410m (1,345.2 feet) for the double-traction train.

1.3.3 The useful length for the maintenance trains according to HSR Maintenance Facilities Specification [R19] shall be considered – 91,4m (300 ft).

1.3.4 Other relevant data shall also be considered by the TSCC Contractor in its design such as track geometry (gradient, fouling point location, track profile) and Trainset characteristics (deceleration rate, distances between axles, etc.).



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 Reference Standards

Standard No.	Standard Title	ID
EN 50126-1	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process	[R1]
EN 50126-2	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety	[R2]
EN 50129	Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling.	[R3]
EN 50159	Railway applications – Communication, signalling and processing systems.	[R4]
EN 50716	Railway Applications – Requirements for software development	[R5]
TSI CCS	Commission Implementing Regulation (EU) 2023/1695 of 10 August 2023 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union	[R6]
TSI CCS	List of ERTMS mandatory specifications as per Appendix/Annex A – Table A2 of CCS TSI 2022 which refer to: ETCS Baseline 4; RMR: GSM-R Baseline 1 Maintenance Release 1 + FRMCS Baseline 0; ATO Baseline 1	[R7]
TSI CCS	List of supporting informative specifications as per CCS TSI Application Guide	[R8]

TABLE 55 - REFERENCE STANDARDS

2.2 Reference Documents

Doc Code	Document Title	Reference	Author
SUBSET-036	FFFIS for Eurobalise	[R9]	Unisig
SUBSET-040	Dimensioning and Engineering rules	[R10]	Unisig
SUBSET-091	Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2	[R11]	Unisig
ERA/ERTMS/033281	Interface between CCS trackside and other subsystems	[R12]	ERA
ERA_ERTMS_OPE_AppA_5 / V 5.0	ERTMS Operational Principles and Rules	[R13]	ERA
EEIG 06E068	ETCS Marker Board definition	[R14]	EUG
EEIG 21E089	Engineering rules for harmonized marker boards	[R15]	EUG
011REC1053 V1.04	Harmonised ERTMS Marker Boards	[R16]	ERA
HSR DCM – Chapter 8	Design Criteria Manual Chapter 8: HSR Trainsets	[R17]	HSR



Doc Code	Document Title	Reference	Author
HSR MFS	HSR Maintenance Facilities Specification	[R18]	HSR
TCS Glossary	TCS Glossary of Terms, Abbreviations and Definitions	[R19]	TCS Engineer
10_STS_ETCS	TSCC Contract Requirements Part C - System Technical Specification of ETCS	[R20]	TCS Engineer
12_STS_IXL	TSCC Contract Requirements Part C - Interlocking	[R21]	TCS Engineer

TABLE 5 - REFERENCE DOCUMENTS

3 TERMS, DEFINITION AND ABBREVIATION

3.1.1 All the terms, definitions, and abbreviations are provided in the Glossary of Terms, Abbreviations and Definitions.

4 MARKER BOARDS

4.1 General

4.1.1 ETCS Marker Boards shall be designed according to the following documents:

- European standard EN 16494:2025: Railway applications – Requirements for ERTMS Trackside Boards;
- EEIG 06E068: ETCS Marker Board definition documents;
- EEIG 21E089: EEIG Engineering rules for harmonized marker boards;
- Harmonized ERTMS Marker Boards, European Union Agency for Railways, version 1.04;
- ERTMS Operational Principles and Rules, European Union Agency for Railways, version 5.

4.1.2 Marker Boards are located to give trains start and stop locations, which can have a significant impact on operational capacity. Several important aspects of marker board locations can be:

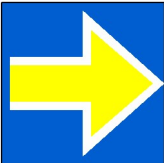
- Operational stopping points for trains;
- Needed safety distance to fouling point or conflicting routes / movement areas;
- Level transition, corresponding to transitions between ETCS levels;
- Operational needs for turning movements.

4.1.3 Marker Boards shall be installed in such a way that they clearly indicate the track to which it refers, and it may be mounted on a dedicated mast or, when possible (e.g., for line block sections), on existing structure (e.g., the catenary pole). There is not a reference standard that establishes the height from the ground/rail for Marker Boards installation. It will be defined according to infrastructure constraints, to optimize visibility and readability.

4.1.4 When locating Marker Boards, the right side of the track to which they refer shall be considered firstly as an area for installation.

4.2 Marker Boards definition

4.2.1 Below is a list (TABLE 6) of Marker Boards to be implemented for the HSR, according to European Standards.

Marker Board representation	Marker Board's name	Marker Board's location
	Stop Marker	In station: incoming and outgoing



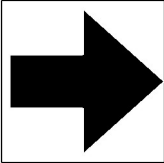
	Location Marker	In station (optionally): at the start/end of a shunting movement in OS mode
	Level Transition board	At each Level Transition border

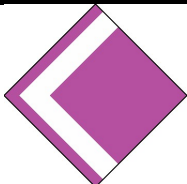
TABLE 6. STANDARD MARKER BOARDS

4.2.2 The following additional Marker Boards are provided (TABLE 7).

Marker Board representation	Marker Board's name	Marker Board's location
	Start of Mission	In station: at 30m/50m before the exit Stop Marker, only at places where trains will restart with a loss of valid position, departing from track accessible from depot/maintenance facility
	Mileage board	Located at every 660ft (1/8 mi for both directions). The blue arrow indicates increase or decrease of the MP, the black arrow indicates the track to which it refers

TABLE 7. ADDITIONAL MARKER BOARDS

4.2.3 For Shunting movements there is no standard equipment, so according to the ETCS Technical Specification [R21], the following Marker Boards could be used (TABLE 8).

Marker Board representation	Marker Board's name	Marker Board's location
	Start of Shunting area	In station: at the start of shunting movements

	End of Shunting area	In station: at the end of shunting areas

TABLE 8. SHUNTING MARKER BOARDS

4.2.4 Based on the definition from the “Harmonised ERTMS Marker Boards” [R17]:

- 4.2.4.1 ETCS stop markers and ETCS location markers may be used to unambiguously identify the end of a block section as an EOA where the driver requires supplementary information to identify the exact stopping location in addition to the display on the DMI;
- 4.2.4.2 ETCS stop markers and ETCS location markers serve to mark the location to where the driver has to drive under his responsibility (in SH/SR mode) before a possible MA in FS/OS is received.
- 4.2.4.3 The ETCS stop marker shall be used to unambiguously identify an EOA which protects one or a group of safety-critical points such as a switch, a conflicting route as entrance of a station, junctions, etc. where the driver requires supplementary information to identify the exact stopping location in addition to the display on the DMI (for instance where a release speed is provided);
- 4.2.4.4 The ETCS stop marker may be used to identify other points of the track the driver shall not overpass when an MA is not available, unless he has received a specific authorization by the Dispatcher;
- 4.2.4.5 The ETCS location marker may be used to unambiguously identify the end of a block section/OS section as an EOA where the driver requires supplementary information to identify the exact stopping location in addition to the display on the DMI (for instance where a release speed is provided);
- 4.2.4.6 The ETCS location marker may be used to identify other points of the track the driver can overpass when a MA in OS mode is not available;

4.3 Visibility of Marker boards

- 4.3.1 As instructed in the ETCS technical specification [R21], the visibility of the marker boards shall be the following:
- Main and block Marker boards $\geq 400\text{m}$ (200m on rough terrain);
 - Shunting boards $\geq 100\text{ m}$.

4.4 Protection of Supervised Location

- 4.4.1 The following Supervised Locations shall be considered:
- The entry point of an occupied block section (i.e. axle counter located ahead of the occupied section);
 - The fouling point of a switch, positioned for a route, conflicting with the current direction of movement of the train;
 - The derailer;
 - The end of shunting area;
 - End of platform or other planned stopping location of train rear end;
 - The head of a switch which is uncontrolled (heel joint of turnout).



4.5 Overlap

- 4.5.1 Overlap distance corresponds to the distance between the marker board (marking the end of EoA) and the Supervised Location. For details refer to ETCS technical specification [R21].
- 4.5.2 Note: If the overlap is timed, it will be configured as an ETCS Overlap in the MA packet definition. If the overlap is not (i.e. permanent) it will be associated to an ETCS Danger Point in the MA packet definition.

4.6 Marker board placement

- 4.6.1 Marker boards shall refer to the track to which it belongs as indicated in the following figure (FIGURE 1):

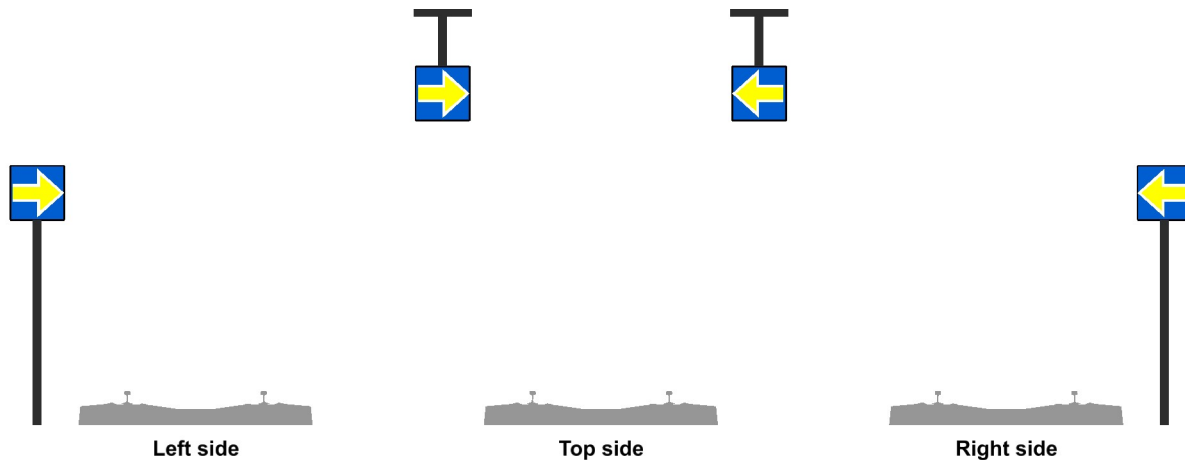


FIGURE 1. MARKER BOARD PLACEMENT

4.6.2 Marker boards at double track lines in the main line

- 4.6.2.1 In the main line, at double track lines, corresponding marker boards (FIGURE 2) should be aligned:

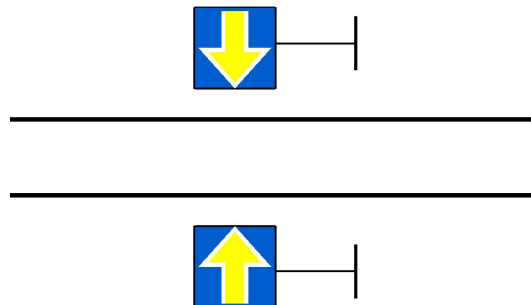


FIGURE 2. MARKER BOARDS AT DOUBLE TRACK LINES

4.6.3 Distance of the Marker board from the fouling point

- 4.6.3.1 The distance between the marker board and the fouling point (FIGURE 3) is given by the overlap distance indicated in ETCS technical specification [R21] and illustrated below:

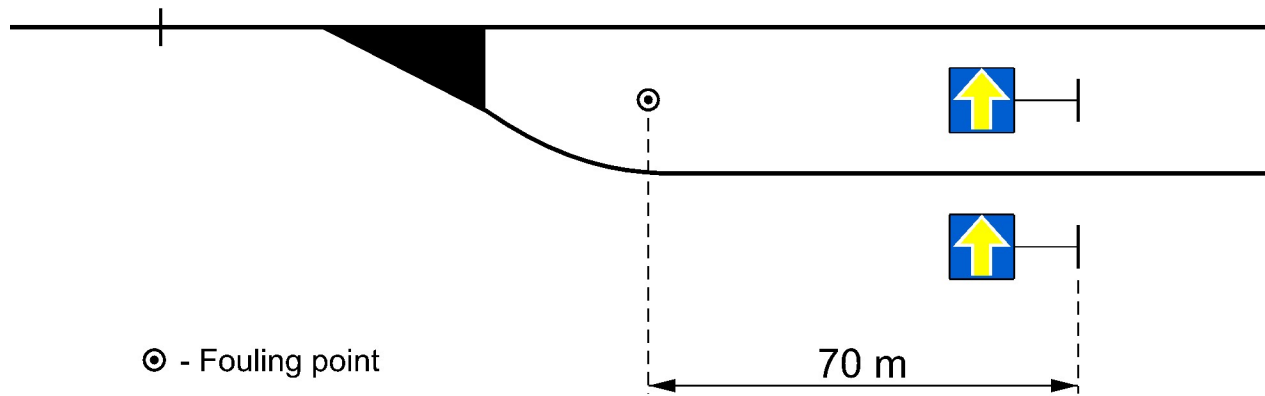


FIGURE 3. MARKER BOARD BEFORE FOULING POINT

4.6.4 Distance of the Marker board from the tip of the switch

- 4.6.4.1 The standard distance between the marker board (FIGURE 4) and the tip of a switch is given by the overlap distance from the ETCS specification [R21] and illustrated below:

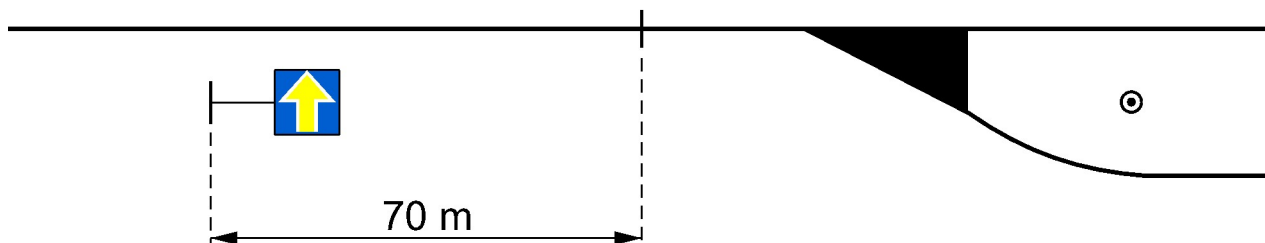


FIGURE 4. MARKER BOARD FROM THE TIP OF THE SWITCH

- 4.6.4.2 This distance can be adapted depending on the track layout and the operational needs but should not be less than 20m (refer to chapter 0).

4.6.5 Station with passing loop configuration

- 4.6.5.1 Based on the above principles, the following configuration for a station with passing loop configuration will be as following (**FIGURE 10**):

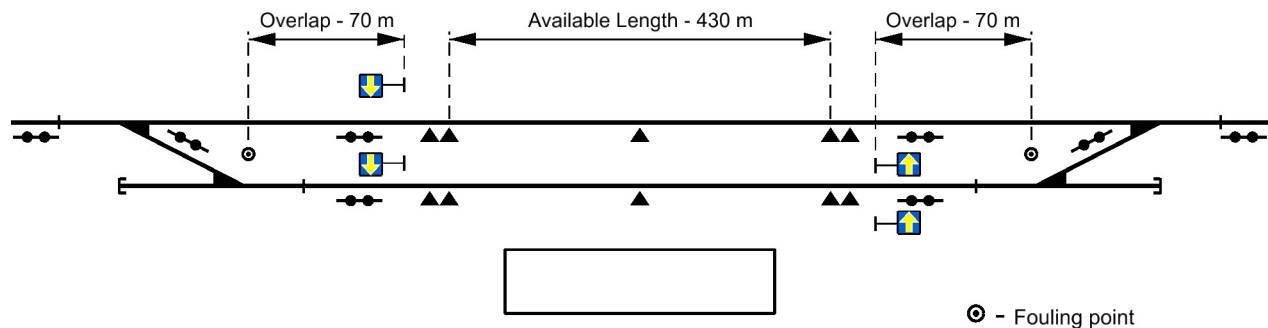


FIGURE 10. MAIN TRACK IN A STATION WITH PASSING LOOP CONFIGURATION

- 4.6.5.2 The available track length is defined as a distance between the first balise in “Stop if in SR” BG related to ETCS stop marker board for the specific direction and the first balise in “Stop if in SR” BG related to ETCS stop marker for the opposite direction.
- 4.6.5.3 The available track length shall be at least 430m for passenger trains, considering the following reserves:
- The reserve for braking inaccuracy shall consider possible inaccuracy of the end position of the train after braking - the distance of 5 m represents the regular value according to the European practice;
 - The reserve for indicator view is required in front of the ETCS marker board. It allows the train driver to see the respective indication and identification marking. The distance of 10-15 m represents the value recommended by ERTMS Users Group (Engineering rules for harmonised marker boards [R16]) and shall be considered by designer.
- 4.6.6 **Marker board on fixed bridges/viaducts**
- 4.6.6.1 Marker boards shall preferably be placed at the start of a bridge, and not on the bridge due to limited availability for maintenance of marker board and axle counters.
- 4.6.6.2 Also, as instructed in the ETCS technical specification [R21], from an interlocking perspective it is important not to place any ETCS stop markers on the bridge / viaduct, or at a nominal train length beyond the viaduct, so that trains will not be forced to stop on the viaduct when the preceding train stops or there is a fault in the signaling system.
- 4.6.7 **Marker boards in non-stopping**
- 4.6.7.1 The marker board shall not be placed inside a non-stopping area. Non-stopping areas are defined in ETCS technical specifications.



5 AXLE COUNTER

5.1 General

- 5.1.1 Occupancy of main-siding tracks, turnout and other station sections, as well as block sections, will be controlled by an axle counter system.

Note to reader: In this section, a TVP corresponds to a portion of track between 2 axle counters.

5.2 Axle counter placement

- 5.2.1 All requirements in TSI CCS [R7] regarding axle counter placement shall apply.

5.2.2 Section minimum distance

- 5.2.2.1 The minimum length of a signaling section is 20 000 mm for a 1435 mm track gauge. Indeed, as required in chapter 3.1.2.1 of ERA/ERTMS/033281 [R13], the maximum axle distance (for 1435 mm gauge) for a trainset shall not exceed 20 000 mm.

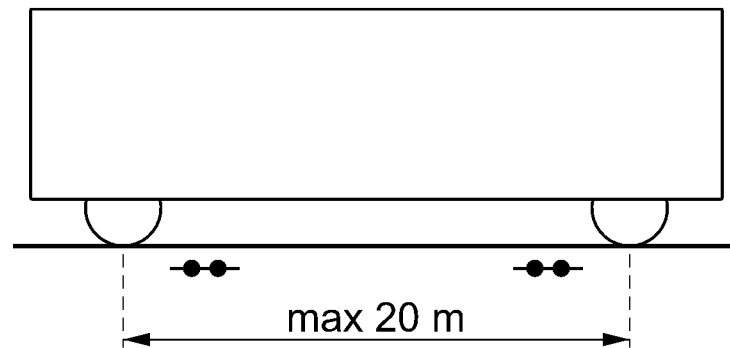


FIGURE 11. EXAMPLE OF INSUFFICIENT SECTION LENGTH - A VEHICLE OR CONSIST SHALL NOT BRIDGE A SIGNALING SECTION, MAKING THE TRAIN DETECTION SYSTEM REPORT ITS AS “UNOCCUPIED”

- 5.2.2.2 In addition, axle counter systems shall be able to distinguish the detection of an axle by 2 subsequent counters with sufficient resolution (to avoid any count-error). As per chapter 3.1.2.2 of ERA/ERTMS/033281 [R13], the minimum trainset axle distance could be as per the table below:

Maximum Speed v [km/h]	Minimum axle distances a_i [mm]
$v \leq 100$	720
$100 \leq 300$	$v \cdot 7,2$
$300 < v \leq 400$	2160

TABLE 9 - MINIMUM AXLES COUNTER DISTANCE

5.2.3 Axle counter at a signaling point

- 5.2.3.1 All marker boards, start / end of shunting areas and shunting signals shall have an associated axle counter.
- 5.2.3.2 The axle counter shall be placed a minimum of 15 meters beyond the EoA marker board, as shown in the following figure (FIGURE 12):

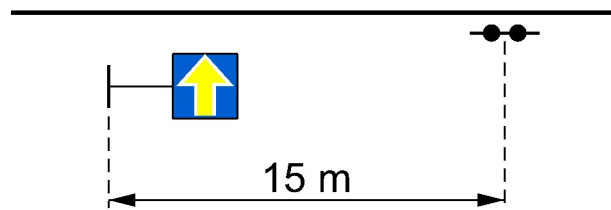


FIGURE 12. AXLE COUNTER AT A MARKER BOARD LOCATION

Note to reader: The rationale is the following:

When the actual train front passes the Stop / Location MB, the cumulative odometry error affecting the distance of the minimum safe front end from the actual front end is assumed to be about 15 m. Then the train drives the first axle on the axle counter, which triggers a Conditional Emergency Stop (further CES) message to the train to confirm correct occupation of the section beyond the MB.

The adopted distance will allow the on-board equipment to reject the new EoA included in the CES command (the minimum safe front end of the train will be behind the MB) which will influence the continuation of the train movement, without tripping (change mode into TR). The distance shall be sufficient to ensure that the train will not occupy the TVP, before its minimum safe front end pass Stop / Location MB. The following situation shall be avoided (Figure 8)

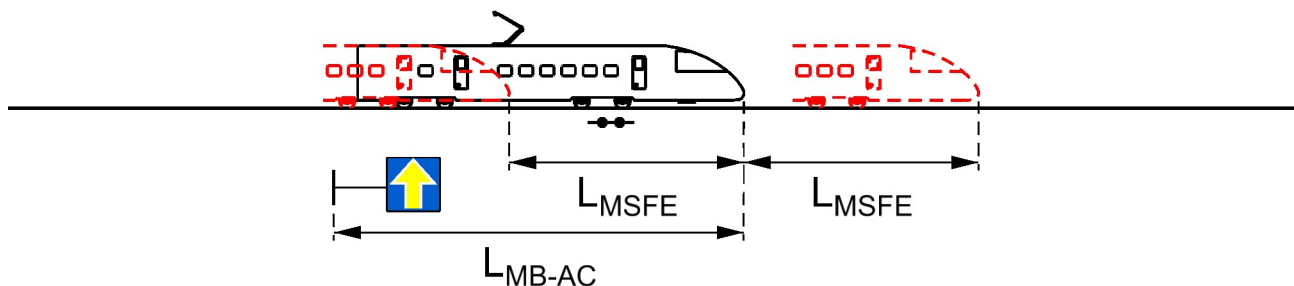


FIGURE 8. RATIONALE FOR MINIMUM DISTANCE BETWEEN MB AND AXLE COUNTER

L_{MSFE} – DISTANCE BETWEEN ACTUAL FRONT END AND MAXIMUM/MINIMUM SAFE FRONT END BASED ON CONFIDENCE INTERVAL (SUBSET-041 POINT 5.3.1.1)

L_{MB-AC} – DISTANCE BETWEEN STOP MARKER AND ACTUAL FRONT END

$L_{MB-AC} > L_{MSFE}$ WHILE FIRST AXLE IS PASSING AXLE COUNTER

- 5.2.3.3 The distance between EoA and axle counter shall not be too large to avoid having a non-detected vehicle between the marker board and the axle counter such as illustrated below (FIGURE 9). Indeed, in this case, the driver will see its movement authority ends at the previous marker board whereas he will see no train before the next marker.

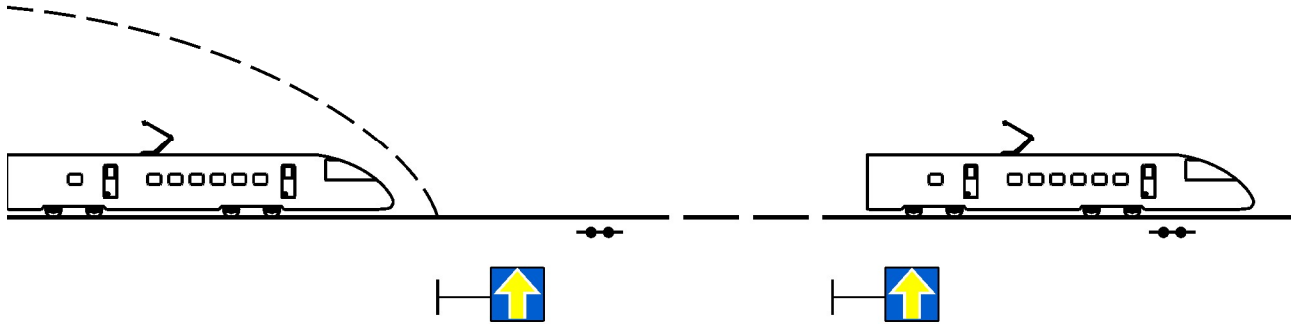


FIGURE 9. EXAMPLE OF TOO LONG DISTANCE

5.2.4 Distance from fouling point to axle counter

5.2.4.1 As described in TSI CCS [R7], a train detection system shall be able to detect:

- The first axle before the front of the train reaches the danger point ahead;
- The last axle until the end of the train has passed the danger point.

5.2.5 As required in chapter 3.1.2.4 of ERA/ERTMS/033281 [R13], the distance between the end of train and first axle on high-speed line will not exceed 5m.

5.2.6 Distance from switch blade toe to axle counter

5.2.6.1 The distance between the switch blade toe and the axle counter shall be sufficient to guarantee that the point is free to move after clearing the point's TVP section.

5.2.6.2 In addition, a 5 meters values will ensure that if a train is moving from the neighboring TVP section (that has not yet occupied the point's TVP section) simultaneously as the point receives a "switch point to opposite position" command, the train will not reach the switch blade before the point's switch blade moves.

5.2.6.3 The following figure is illustrating a typical axle counter location considering switch head

- when a 70m overlap is provisioned (as per section 4.6.4);
- for an intermediate switch of a route.

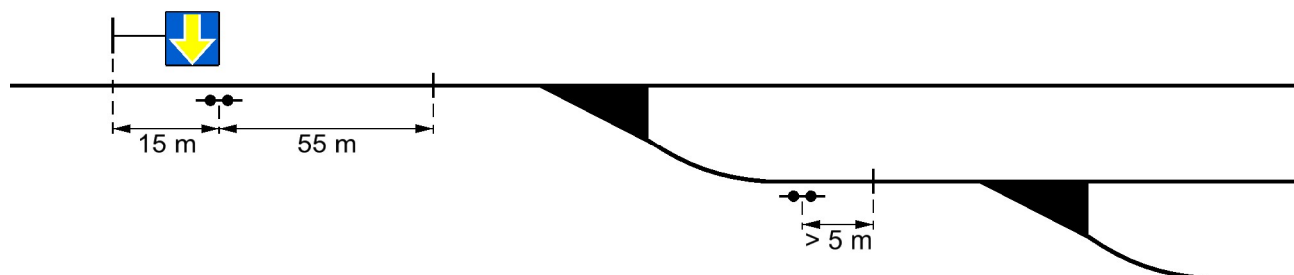


FIGURE 10. AXLE COUNTER FROM SWITCH BLADE TOE / TYPICAL LAYOUT

5.2.7 Cross over

5.2.7.1 Based on the principles exposed before in this document, a typical Axle Counter implementation for a cross over will be as following (FIGURE 11):

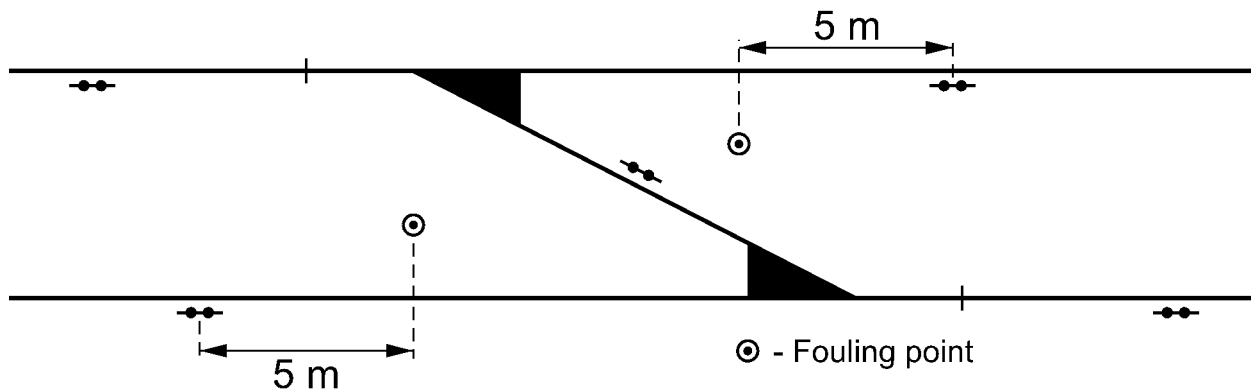


FIGURE 11. AXLE COUNTER ON CROSS OVER

5.2.8 Distance axle counter – derailer – fouling point

5.2.8.1 The axle counter shall be placed approximately 1 meter on approach to the derailer, or as close to the derailer as possible (FIGURE 17).

Note to reader: Rationale: To avoid that shunting movements up to the derailer are detected as occupied section over the switch.

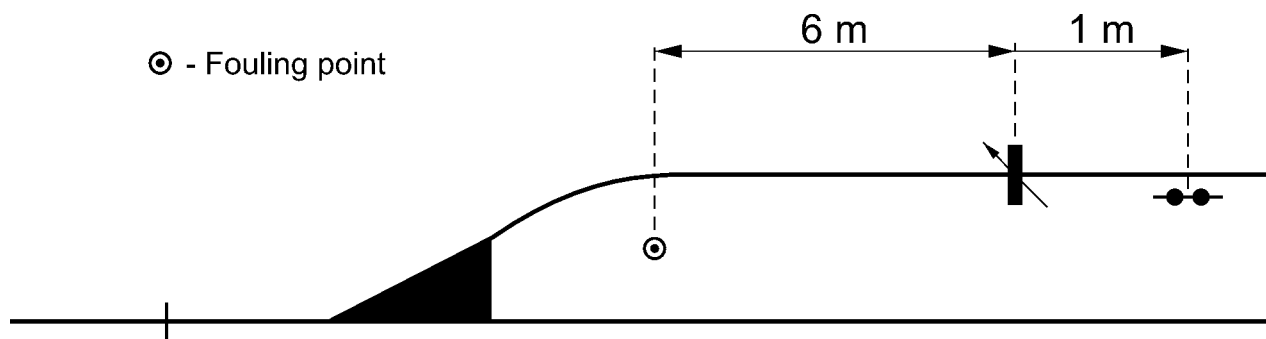


FIGURE 17. AXLE COUNTER FROM DERAILER AND FOULING POINT

5.2.9 Axle counter location additional requirements

5.2.9.1 Axle counters shall be installed:

- At all boundaries with tracks not equipped with track clearance detection or equipped with other means of train detection or equipped with different type of axle counter system;
- At the start of each train and shunting route, at the end of each train route (except for dead end track) and to locate the end of the train (in case this is not done at the exit signal (marker board) for opposite direction route;
- At all boundaries of a route section node (two or more adjacent turnouts) to ensure simultaneous train routes over it;

- At danger points to provide track clearance detection section between EoA and danger point. With regard to the principle of operation of the ETCS and the interlocking system, this principle may be changed at the next stage of design;
- At all boundaries of a flank protection area.



6 BALISE

6.1 General

- 6.1.1 All requirements in TSI CCS [R7] regarding balise engineering shall apply.
- 6.1.2 Eurobalise layout shall enable ETCS functionalities described in ETCS Technical Specification [R21].
- 6.1.3 For HSR CA project each Balises Group will be composed of one or more fixed eurobalises, distance between each one of them will be 3 m (according to SUBSET-036 chapter 5.6.3 [R10]).
- 6.1.4 The minimum distance between two balise groups, defined as the distance between closest balises of the two groups (i.e. between the Balise Reference Mark of the last one of the first group and the Balise Reference Mark of the first one of the second group) shall be calculated according to SUBSET-036 chapter 4.2.9. [R10].

6.2 Balise placement

- 6.2.1 In accordance with the assumptions made for the functionality of the system on the basis of ETCS technical specification [R21], a concept for the location of balises has been defined taking into account the TSI CCS specifications [R7], operational considerations and other guidelines necessary for the purpose of conducting traffic based on the indications of the ETCS L2 system.
- 6.2.2 This does not necessarily imply that dedicated BGs will be expected for each function described. The Telegrams length and the Balise size have to be considered in order to define if the same BG can have one or more functions, considering each BG has location related information to recalibrate the position of the train. Balise engineering will be in the scope of the future TCS contractor, which will be responsible for optimizing the number and location of BGs considering the BGs proximity.
- 6.2.3 **Start of Mission Balise Groups**
 - 6.2.3.1 Assuming that Cold Movement Detection equipment will be installed on the HSR fleet, but may be unavailable, additional BGs are considered to obtain an unambiguous train position for Start of Mission, in locations where SoM can take place e.g. main station tracks.
 - 6.2.3.2 Nominally, the train position information will be provided by the CMD devices.
 - 6.2.3.3 In the case of CMD failure obtaining an unambiguous train position will be provided by “Start of Mission” Balise Groups located near the probable front end of parked train.



6.2.4 “Stop if in SR” Balise Groups

- 6.2.4.1 A group of two balises shall be located in front of each Stop Marker. This Balise Group shall be able to send a “Stop if in SR” packet to the OBU equipment in case of Staff Responsible movement.

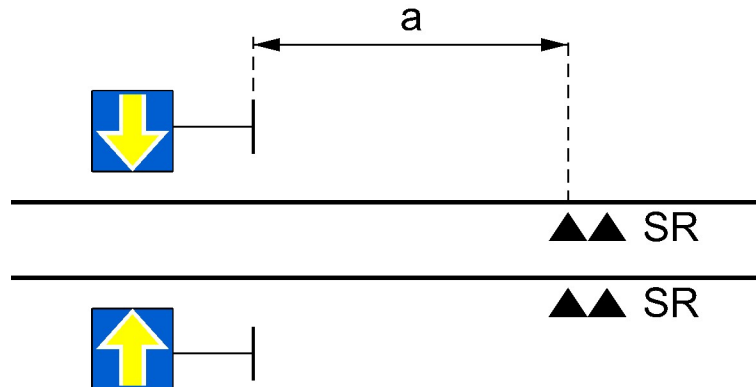


FIGURE 18. LOCATIONS OF “STOP IF IN SR” BALISE GROUPS

a – DISTANCE BETWEEN THE LRBG AND STOP MARKER, BASED ON SUBSET-040 P. 4.1.1.4, 5m IS ASSUMED

6.2.5 Relocation Balise Groups

- 6.2.5.1 Based on the ETCS L2 functionality assumptions from ETCS specification [R21] and TSI CCS specifications [R7], the non-switchable balises for recalibrating odometry shall be placed in the following locations:
- 6.2.5.2 According to the safety requirements of SUBSET-091 [R12], the maximum distance between two consecutive balise groups shall not exceed 2500 m;
- 6.2.5.3 Balise Groups made up of a single fixed balise placed to optimize braking curves during the braking to target:
- 200m before Marker Boards located in the main tracks;
 - Note: Considering optimization of number of balises in case of two Stop Markers placed in station for opposite movement's directions two BGs can be replaced by one located in the middle of distance between these MBs;
 - 200m before speed change points (changing from higher to lower speeds).

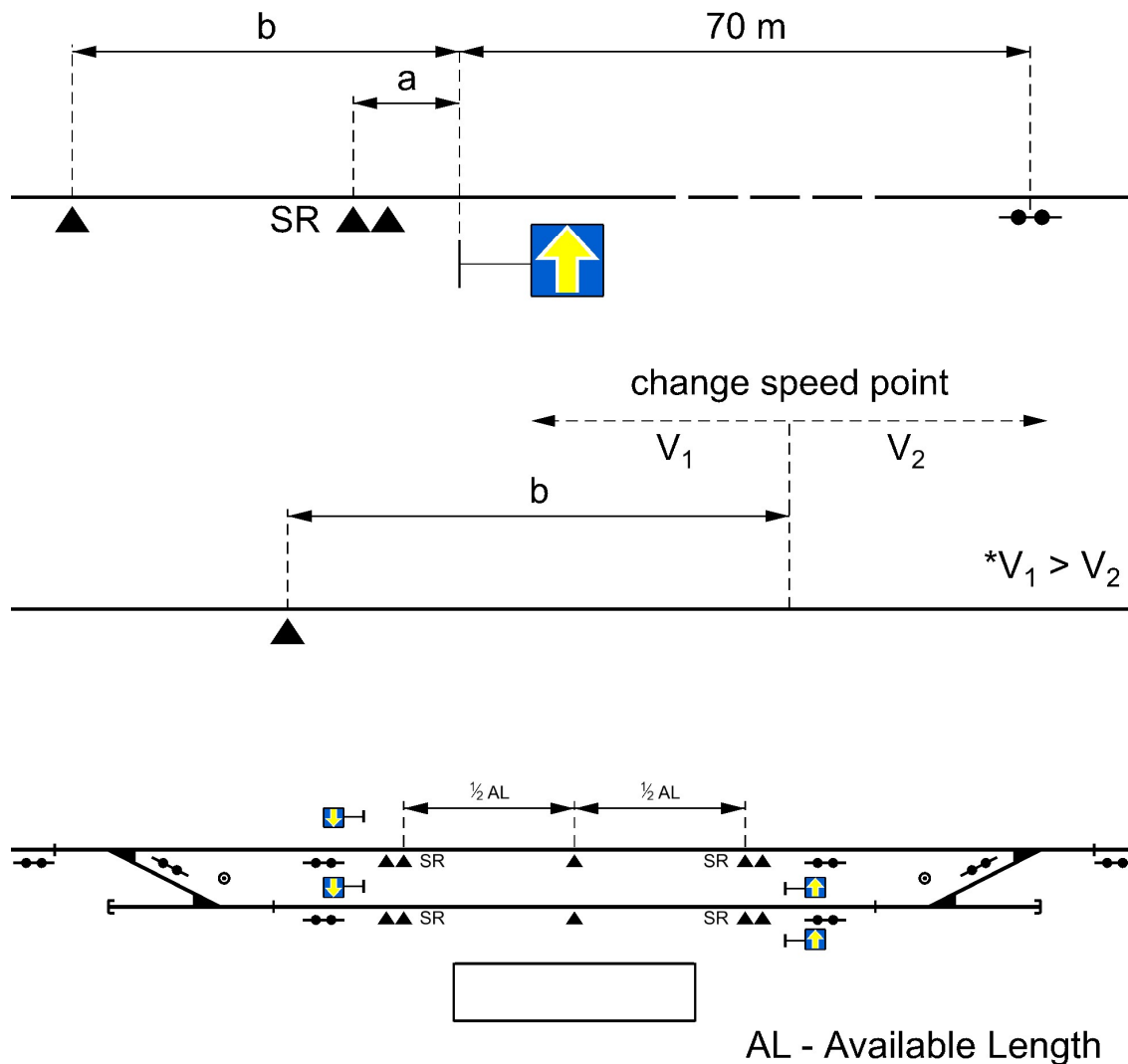


FIGURE 14 - LOCATIONS OF RELOCATION BALISE GROUPS IN FRONT OF EOA / SPEED CHANGES

a – distance of the "Stop if in SR" BGs from the EoA (in accordance with chap. 6.2.4);

b – the distance between the LRBG and the EoA / maximum speed change is assumed to be 200m for the purpose of calibrate odometry (odometry error x calculated on basis of SUBSET-041 point 5.3.1.1: $x = 0.05 * b + 5 = 0.05 * 200 + 5 = 15$ [m]);

V_1, V_2 – maximum permitted speed.

- 6.2.5.4 Balise Groups made up of a single fixed balise placed to minimize odometry error in front of points of change of track conditions located at a distance of 200 m from the beginning of the section with the given condition, e.g. regenerative braking, non-stopping area;

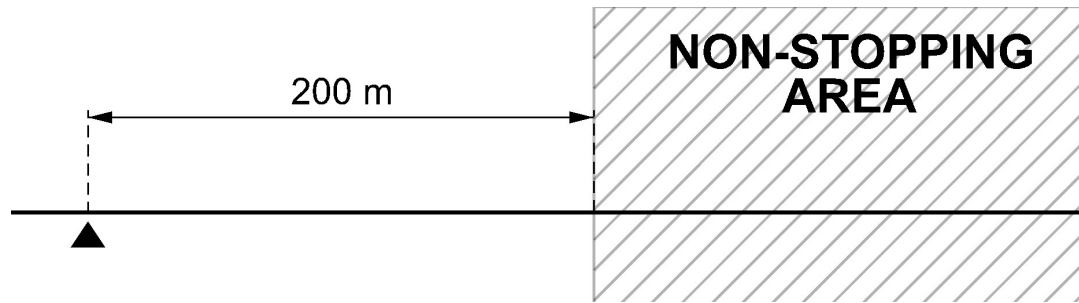


FIGURE 20. LOCATIONS OF RELOCATION BALISE GROUPS IN FRONT OF TRACK CONDITIONS

b – the distance between the LRBG and the EoA / maximum speed change is assumed to be 200m for the purpose of calibrate odometry (odometry error *x* calculated on basis of SUBSET-041 point 5.3.1.1: $x = 0.05 * b + 5 = 0.05 * 200 + 5 = 15$ [m]);

6.2.5.5 Balise Groups made up of a single fixed balise placed to determine the position of a train when passing a turnout located at a distance:

- min. 1 m from tip of the turnout;
- min. 1 m from the fouling point;
- min. 1,4 m between the balises placed in adjacent tracks due to ensure protection against cross-talk - SUBSET-036 pt. 4.2.5.

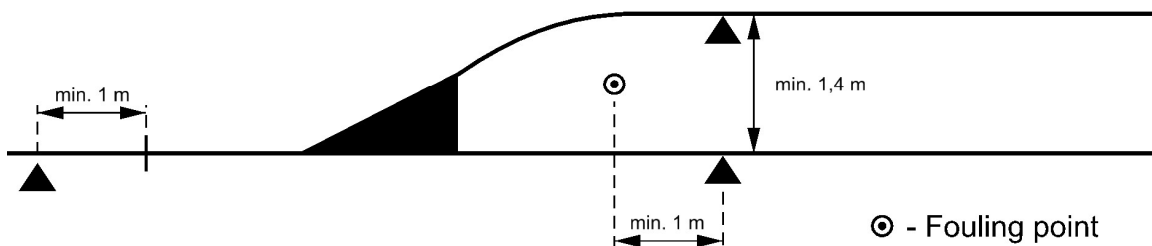


FIGURE 21. LOCATIONS OF RELOCATION BALISE GROUPS NEAR TURNOUT

d - the distance between the BG and the tip / fouling point of the turnout, assumed ~1m

6.2.6 Shunting areas borders

6.2.6.1 Within shunting areas, BGs shall be located to transmit package 132 "Danger for Shunting information" on the end of the shunting area.

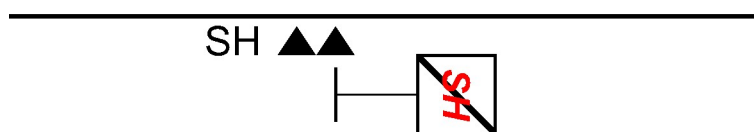


FIGURE 22. LOCATIONS OF "DANGER FOR SHUNTING INFORMATION" BALISE GROUPS

6.2.7 National Values

- 6.2.7.1 Balise Groups which transmit information about the National Values shall be placed at the boundaries between shunting yards / siding tracks and the RBC area;

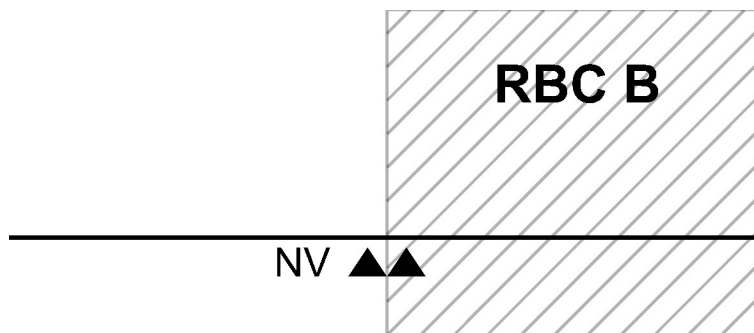


FIGURE 18. LOCATIONS OF BALISE GROUPS WITH NATIONAL VALUES

7 SHUNTING SIGNALS

7.1 General

- 7.1.1 Shunting signals are used to provide information about permission to move in SH mode with use of defined shunting routes when shunting movement is protected by interlocking as defined in [R22].
- 7.1.2 Shunting signals shall be used in the following cases:
- When shunting routes cross the main tracks;
 - At the point where a shunting route starts, e.g. from a rib or stabling track, from a depot, from a siding, etc;
- 7.1.3 Shunting signals shall be located to the right of the track to which they relate. In exceptional cases, it is allowed to set a shunting signal on the left side of the track.

7.2 Shunting signals placement

7.2.1 Distance to axle counter

- 7.2.1.1 Shunting signals shall be placed as close as possible to the axle counter, with a tolerance of -1 meter to +30 meters.

7.2.2 Distance to danger point

- 7.2.2.1 If the shunting signal is placed at the border of shunting area or in front of fouling point of turnout included in train routes, it shall be placed at a minimum distance of 15 meters from the danger point (FIGURE 19).

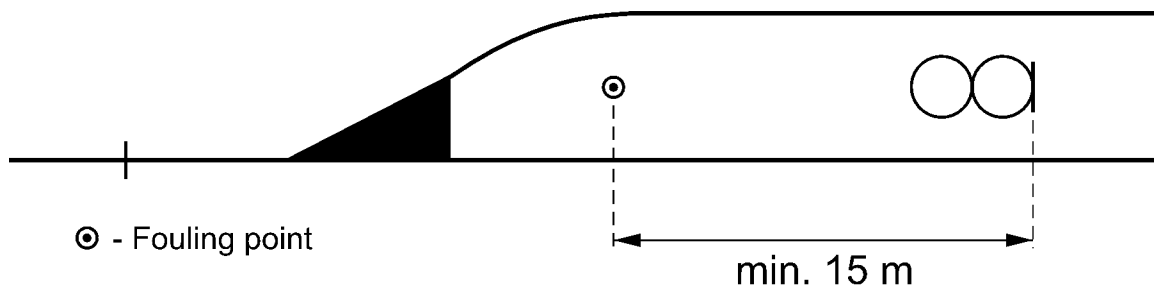


FIGURE 19. SHUNTING SIGNALS BEFORE FOULING POINT

8 DERAILERS

8.1 General

- 8.1.1 According to IXL technical specification [R22] derailleurs are used to protect the train route from trainset running away from a sidetrack.
- 8.1.2 Derailers should not be used on main tracks.
- 8.1.3 The installation location and direction of derailment shall be such that the derailed trainset causes the least possible risk to safety and damage to trackside equipment and facilities.
- 8.1.4 Beacons with signals indicating their position may be used for derailleurs. Derailer's signals shall be illuminated at night.

8.2 Distance from fouling point

- 8.2.1 Derailers shall be installed at a distance of 6 m in front of the fouling point of the protected turnout. This distance can be exceeded under condition of including derailer in turnout's TVP (FIGURE 25).

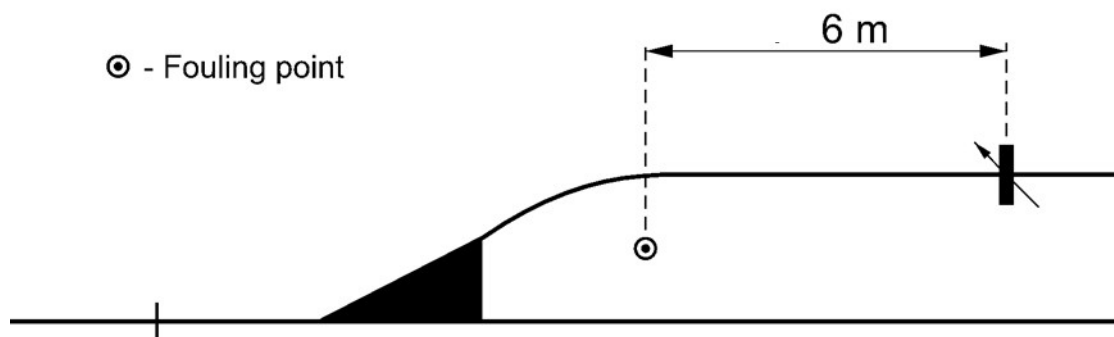


FIGURE 25. DERAILERS BEFORE FOULING POINT

8.3 Distance from catenary supports

- 8.3.1 Derailers shall not be located up to 5 m behind and 30 m in front of the catenary support looking in the direction of derailment.

9 SWITCH MACHINES

9.1 General

- 9.1.1 According to IXL technical specification [R22] switch and derailer machines are used to move and keep switch blades, derailers and moveable switch frogs in their final position.
- 9.1.2 The switch machine shall be installed in a location that ensures its proper operation. As far as possible, the aim shall be that:
- Convenient and safe access to the switch motor is provided;
 - There is a convenient cable connection.

9.2 Switch machines configuration

- 9.2.1 According to Technical Specification for IXL technical specification [R22] on straight track where speed is > 200 km/h, turnouts shall be equipped with swing nose crossings.
- 9.2.2 In the case of turnouts with more than one inside locking for the switch blades or the switch frogs, multi-drive systems are assumed to be implemented. The use of bar / hydraulic transmission is possible and is in scope of switch machines engineering by future contractors.
- 9.2.3 When multi-drive systems are used, the first drive (looking from the beginning of the switch) shall be of the non-trailable type, while the subsequent drives may beailable.



10 WORK AREAS

10.1 General

- 10.1.1 The work areas relate to the 'engineering ownership' of railway tracks. To ensure the safety of people involved in railway maintenance, access to work areas shall be adequately protected against unauthorized vehicles via the Staff Protection System.
- 10.1.2 According to IXL technical specification [R22] the CHSR railway network shall be divided into work areas consisting of one or few track clearance detection sections (subject of review and approval by the Authority).

10.2 Track layout segmentation

- 10.2.1 Division of work areas shall enable maximum functionality of movement during maintenance activities.
- 10.2.2 Catenary sectioning shall be considered in work areas segmentation process.
- 10.2.3 Crossovers shall be divided into work areas in a way to allow bidirectional movement on the maximum number of tracks.
- 10.2.4 In stations every track shall be included in a different work area. Grouping several tracks in one work area shall be agreed by the TSCC Contractor during the design stage.



11 NAMING

11.1 General

11.1.1 Generally signaling devices can be named using description:

- Alphabetic;
- Numerical;
- Alphanumeric.

11.1.2 Each device shall be uniquely labelled to enable easy location and referencing.

11.2 Marker boards naming

11.2.1 Stop Markers shall be named using number pool reserved for particular OCC.

11.2.2 Stop Markers shall be numbered according to increasing kilometrage/milage starting from left side to right side looking in the direction of movement, the first letter of the label specifies the OCC from which MA is provided to pass the MB.

11.2.3 Number shall be unique and considering number reserve for each indicator group.

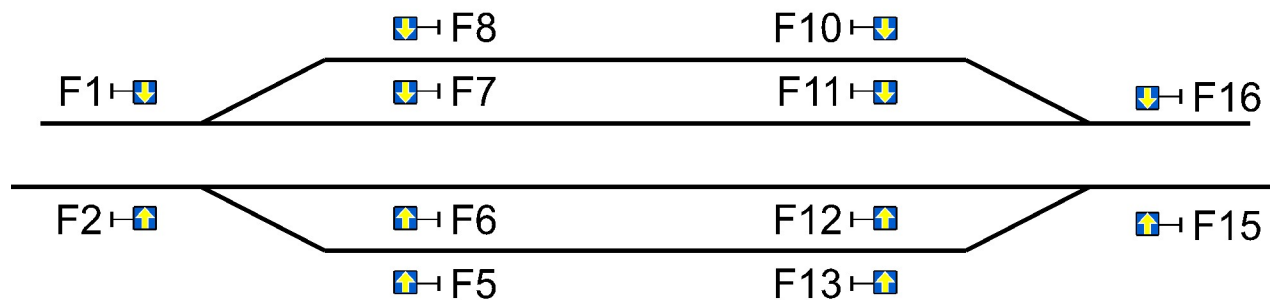


FIGURE 26. MARKER BOARDS NAMING

11.3 Axle counters naming

- 11.3.1 Axle counters shall be named using names of tangential TVPs e.g. s2-t2.
- 11.3.2 Turnout's TVP shall have alphanumeric description starting with the letter s (switch) and number of turnouts e.g. s2. If turnout's TVP includes several turnouts, then all switch numbers shall be considered with slash between them e.g. TVP for switches no. 4 and 6 shall be named s4/6. Axle counters at the ends of such a TVP may be numbered using a simplified TVP name – including only the nearest switch.
- 11.3.3 Station track's TVP shall have alphanumeric description starting with letter t (track) and number of tracks. Note: If on one track a few TVPs are designed a lowercase letter according to increasing kilometrage/milage shall be added to each TVP's name e.g. t4a, t4b, t4c etc.
- 11.3.4 Open line's TVP shall have alphanumeric description starting with letter t (track), number of track and acronym of tangential station / control point according to increasing kilometrage/milage e.g. for track no. 1 between Fresno (smaller kilometrage) and Fresno MOWF it may be t1FFM.

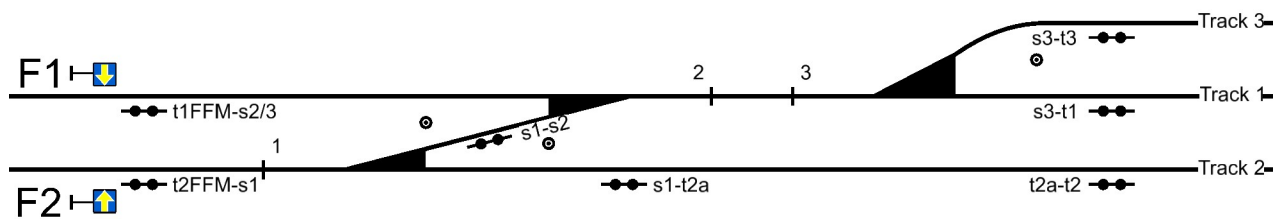


FIGURE 27. AXLE COUNTERS NAMING

11.4 Balise naming

- 11.4.1 Each balise group shall have its unique identification number. Identity numbers (NID_BG variable) will be engineered by the future TCS Contractor.
- 11.4.2 Balise groups which can send a "Stop if in SR" packet shall be numbered as follows: SR-MB number to which BG is associated-letter suffix (A/B/...) e.g. SR-F101-A. Letter suffix may be used in case there are few Balise Groups associated with the same Marker Board.
- 11.4.3 Balise Groups that are designated to SoM procedure (for obtaining an unambiguous train position) shall be named as follows: SM-MB number to which BG is associated-letter suffix (A/B/...) e.g. SM-F101-A. Letter suffix shall be used in the same way as described in requirement 10.4.2. Associated Marker Board means start location of the first route being set when Start of Mission occurs.
- 11.4.4 Relocation Balise Groups shall be numbered in accordance with the main engineering rule that was applied to locate them.
- 11.4.4.1 Balise groups used for relocation on open lines, before track conditions, speed changes shall be numbered as follows: RL-number of first reference mile in the nominal direction of movement-letter suffix (A/B/...) e.g. RL-23-A. Letter suffix shall be used in a similar way to that described in requirement 10.4.2. e.g. there are several relocation BGs before the same mile.
- 11.4.4.2 Balise groups used for relocation before Marker Boards shall be numbered as follows: RL-MB number-letter suffix (A/B/...) e.g. RL-F101-A. Letter suffix shall be used in a similar way to that described in requirement 10.4.2. If one BG is used for relocation before two MBs then for numbering purpose priority is given to the MB associated with nominal direction of movement.
- 11.4.4.3 Balise groups used for relocation near switches shall be numbered as follows: RL-switch number-letter suffix (A/B/...) e.g. RL-40-A. Letter suffix shall be used in a similar way to that described in requirement 10.4.2. e.g. there are several relocation BGs near the same switch.



- 11.4.5 Balise groups which can send a “Danger if in Shunting” packet shall be numbered as follows: SH-the nearest switch number-letter suffix (A/B/...) e.g. SH-40-A. Letter suffix shall be used in a similar way to that described in requirement 10.4.2. e.g. there are several BGs which can send a “Danger if in Shunting” packet near the same switch.
- 11.4.6 Balise groups which transmit information about the National Values shall be numbered as follows: NV-the nearest switch number-letter suffix (A/B/...) e.g. NV-40-A. Letter suffix shall be used in a similar way to that described in requirement 10.4.2. e.g. there are several BGs transmitting National Values near the same switch.

11.5 Shunting signals naming

- 11.5.1 Each shunting signal shall have numeric description from number pool reserved for particular e.g. 2.
- 11.5.2 Shunting signals shall be numbered according to increasing kilometrage/milage starting left side to right side looking in the direction of movement.
- 11.5.3 Number shall be unique and considering number reserve for each shunting signals group.

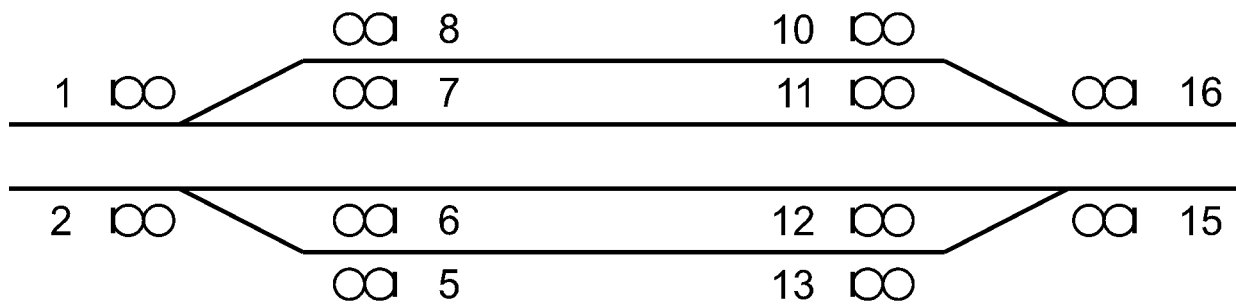


FIGURE 28. SHUNTING SIGNALS NAMING

11.6 Derailers naming

- 11.6.1 Each derailer shall have alphanumeric description starting with letters D (derailer) and number from number pool reserved for particular OCC e.g. D2.
- 11.6.2 Derailers shall be numbered according to increasing kilometrage/milage starting from track no. 1.
- 11.6.3 The number shall be unique and considering number reserve for each derailers group. Note: In purpose of better consistency derailers number group would be the same as switch machines number group.



11.7 Switch machines and switch detectors naming

- 11.7.1 Each turnout shall have a numeric description from the number pool reserved for a particular OCC. Each switch machine shall have a numeric or alphanumeric (multi-drive systems) description with the same number as turnout.
- 11.7.2 The alphanumeric description of the switch machine shall be composed of the number of the turnout on which the machine is mounted and the following Roman numerals.
- 11.7.3 Switch detectors shall be named in the same way as the switch machines, with the additional requirement that the letter d shall be added before the Roman numeral.
- 11.7.4 Turnouts numbers shall be unique and considering number reserve for each turnout's signals group.

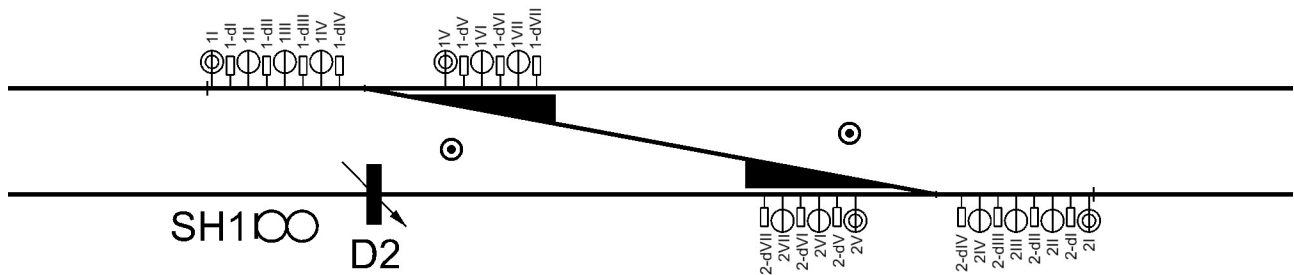


FIGURE 29. SWITCH MACHINES, SWITCH DETECTORS AND DERAILERS NAMING

Schedule 5(p)
Telephony System

California High-Speed Rail Authority



Standard Specifications TSCC Specifications SPEC-0020 – Telephony System Rev. 1.0

Authored:

A handwritten signature in black ink, appearing to read "Harshal Jadhav".

Harshal Jadhav, Telecommunication Systems Lead

12/22/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Thomas Newey".

Thomas Newey, Telecoms Lead

12/22/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Bruno Comperat".

Bruno Comperat, Deputy Director of Rail Engineering

12/23/2025

Date

Approved:

A handwritten signature in blue ink, appearing to read "Ryan Scott".

Ryan Scott, Director of Rail Engineering

12/23/2025

Date

Released:

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Amit Joshi, Configuration Manager

12/23/2025

Date



Document Revision History – Telephony System Specifications**Second Edition****December 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition
1.0	December 2025	Second edition for Addendum 2



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION.....	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.1	GENERAL	6
2.2	DESIGN GUIDELINES.....	6
2.3	STANDARDS	6
2.4	OTHER DOCUMENTS	10
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	11
3.1	TERMS, DEFINITIONS AND ABBREVIATIONS	11
4	SYSTEM DESCRIPTION	12
4.1	PURPOSE OF THE TELEPHONY SYSTEM	12
4.2	TELEPHONY SYSTEM DEFINITION	12
4.3	TELEPHONY SYSTEM OPERATIONAL CONTEXT	12
4.4	DESIGN LIFE	12
5	SYSTEM REQUIREMENTS.....	13
5.1	GENERAL REQUIREMENTS.....	13
5.2	ENVIRONMENTAL CONDITIONS REQUIREMENTS.....	13
5.3	OPERATIONAL REQUIREMENTS FOR TELEPHONY SYSTEM	13
5.4	FUNCTIONAL REQUIREMENTS FOR TELEPHONY SYSTEM.....	14
5.5	PERFORMANCE REQUIREMENTS FOR TELEPHONY SYSTEM.....	22
5.6	CYBERSECURITY AND SECURITY REQUIREMENTS.....	23
6	INTERFACES REQUIREMENTS.....	24
6.1	GENERAL REQUIREMENTS.....	24
6.2	THIRD PARTY INTERFACES	24
6.3	EXTERNAL INTERFACES – STATION CONTRACTOR.....	24
6.4	EXTERNAL INTERFACES – FACILITIES CONTRACTOR	24
6.5	INTERNAL INTERFACES	25
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS	27
7.1	GENERAL REQUIREMENTS.....	27
7.2	SOFTWARE AND HARDWARE REQUIREMENTS	27
7.3	EMC REQUIREMENTS.....	27
8	TOLERANCES	28
9	SCOPE OF SUPPLY AND DELIVERY	29
9.1	GENERAL REQUIREMENTS.....	29
9.2	SPECIFIC REQUIREMENTS	29
10	MANUFACTURING.....	30
10.1	GENERAL REQUIREMENTS.....	30



11	INSTALLATION AND INTEGRATION.....	31
11.1	GENERAL REQUIREMENTS.....	31
12	TESTING & ACCEPTANCE	32
12.1	GENERAL REQUIREMENTS.....	32
12.2	SPECIFIC REQUIREMENTS FOR TELEPHONY SYSTEM.....	32
13	SUBMITTALS.....	33
13.1	GENERAL REQUIREMENTS.....	33
14	QUALITY MANAGEMENT.....	34
14.1	GENERAL REQUIREMENTS.....	34
15	ADDITIONAL INFORMATION REQUESTED	35
15.1	GENERAL REQUIREMENTS.....	35
16	LOGISTICS	36
16.1	GENERAL REQUIREMENTS.....	36



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Telephony System.
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of the Telephony System is presented in Appendix A.
- 1.1.4 The requirements are formulated using the following words and their meanings:
 - **"Shall"**: Indicates a mandatory requirement that must be strictly implemented; a waiver from a mandatory requirement is permissible only with approval of a design variance.
 - **"Should"**: Indicates a preferred course of action; a design variance is not required if it is not exercised.
 - **"Must"**: Indicates an obligation or a mandatory requirement.
 - **"May"**: Indicates a permissible course of action within the limits of the standards; a design variance is not required if it is not exercised.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines and specifications provided in this technical specification for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, training, operations and maintenance.

2.1.2 All generic standards to be used are provided in: Technical Contract Requirements.

2.2 Design Guidelines

2.2.1 The latest version of the following Design Guidelines shall be applied:

ID	Code	Title
[R1]	Design Criteria Manual	Chapter 5 – Safety and Security
[R2]	Design Criteria Manual	Chapter 12 – Communication Systems and Train Control
[R3]	AREMA Standards	Chapter 17 – High-Speed Rail Systems

TABLE 61 DESIGN GUIDELINES

2.3 Standards

2.3.1 The TSCC Contractor shall fully consider and apply the following standards:

ID	Standard	Title
[R4]	EN 300 386	Telecommunication network equipment; Electromagnetic Compatibility (EMC) requirements; Harmonized Standard covering the essential requirements of the Directive 2014/30/EU
[R5]	EN 50121	Railway Applications – Electromagnetic Compatibility
[R6]	EN 50121-3-2	Railway applications - Electromagnetic compatibility - Part 3-2: Rolling stock - Apparatus
[R7]	EN 50121-4	Railway applications - Electromagnetic compatibility - Part 4: Emission and immunity of the signaling and telecommunications apparatus
[R8]	EN 50121-5	Railway applications - Electromagnetic compatibility Emission and immunity of fixed power supply installations and apparatus
[R9]	EN 50122-1	Railway applications - Fixed installations - Electrical safety, earthing and the return circuit - Part 1: Protective provisions against electric shock
[R10]	EN 50125	Railway applications - Environmental conditions for equipment
[R11]	EN 50126-1	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
[R12]	EN 50126-2	Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
[R13]	EN 50128	Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems



ID	Standard	Title
[R14]	EN 50159	Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems
[R15]	EN 50164	Lightning Protection Components
[R16]	EN 50164-3	Lightning Protection Components (LPC) -- Part 3: Requirements for isolating spark gaps
[R17]	EN 55024	Information technology equipment. Immunity characteristics. Limits and methods of measurement
[R18]	EN 60065	Audio, video and similar electronic apparatus - Safety requirements
[R19]	EN 60118-4	Hearing Aids - Part 4: Magnetic Field Strength in Audio-Frequency Induction Loops for Hearing Aid Purposes
[R20]	EN 60529	Degrees of protection provided by enclosures (IP Code)
[R21]	EN 61000-6	Electromagnetic compatibility (EMC) - generic standards
[R22]	EN 61000-6-2	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity standard for industrial environments
[R23]	EN 61000-6-4	Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments
[R24]	EN 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
[R25]	EN 62262	Degrees Of Protection Provided By Enclosures For Electrical Equipment Against External Mechanical Impacts (Ik Code).
[R26]	EN 62305	Protection against lightning
[R27]	ETSI EN 301 462	Human Factors (HF); Symbols to identify telecommunications facilities for deaf and hard of hearing people
[R28]	ETSI Q.SIG	ISDN Based Signaling Protocol
[R29]	IEC 60304	Standard colors for insulation for low-frequency cables and wires
[R30]	IEC 61000-3-6	Electromagnetic compatibility (EMC) - Part 3: Limits - Section 6: Assessment of emission limits for distorting loads in MV and HV power systems - Basic EMC publication
[R31]	IEC 61000-3-7	Electromagnetic compatibility (EMC) - Part 3-7: Limits - Assessment of emission limits for the connection of fluctuating installations to MV, HV and EHV power systems
[R32]	IEC 61000-5-2	Electromagnetic compatibility (EMC) - Part 5: Installation and mitigation guidelines - Section 2: Earthing and cabling
[R33]	IEC 61643	Low-voltage surge protective devices
[R34]	IEEE 60068-2-1	Environmental testing - Part 2-1: Tests - Test A: Cold
[R35]	IEEE 60068-2-30	Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)



ID	Standard	Title
[R36]	IEEE 802.1Q	IEEE Standard For Local And Metropolitan Area Networks--Bridges And Bridged Networks
[R37]	IEEE 802.1x	Port-based Network Access Control (PNAC)
[R38]	IEEE 802.3	10/100 BASE-T specification
[R39]	IEEE 802.3af	Power over Ethernet (PoE)
[R40]	IEEE 802.3at	Power over Ethernet Plus (PoE+)
[R41]	IETF RFC 1825 & RFC 1829	Internet Protocol Security (IPSec)
[R42]	IETF RFC 2131	Dynamic Host Configuration Protocol (DHCP)
[R43]	IETF RFC 2865	Remote Authentication Dial In User Service (RADIUS)
[R44]	IETF RFC 3261 & RFC 2543	SIP - Session Initiation Protocol
[R45]	IETF RFC 3411 & RFC 3418	Simple Network Management Protocol (SNMPv3)
[R46]	IETF RFC 4510	Lightweight Directory Access Protocol (LDAP)
[R47]	IETF RFC 5246	Secure Sockets Layer (SSL)
[R48]	IETF RFC 791	IP – Internet Protocol
[R49]	ITU-T G.652/G.655/G.656/G.657	Fiber Optic Cable Specification
[R50]	ITU-T G.703	G.703 Digital Interface
[R51]	ITU-T G.711/G.729/G.723	Audio Data Compression
[R52]	ITU-T G.8010	Architecture of Ethernet layer networks
[R53]	ITU-T G.803	Architecture of transport networks based on the synchronous digital hierarchy (SDH)
[R54]	ITU-T H.323	H.323 Call Signaling and Control Protocol
[R55]	ITU-T Q.23	Dual-tone multi-frequency signaling (DTMF)
[R56]	ITU-T Q.931	ISDN Connection Control Protocol
[R57]	ITU-T Y.1540	Internet protocol data communication service - IP packet transfer and availability performance parameters
[R58]	ITU-T Y.1541	Network performance objectives for IP-based services
[R59]	Microsoft Windows API	Telephony API (TAPI) and Java Telephony API (JTAPI)
[R60]	NFPA 130	Fixed Guideway Transit and Passenger Rail Systems
[R61]	NFPA 780	Standard for the Installation of Lightning Protection Systems
[R62]	TIA/EIA/TSB122-A	Telecommunications IP Telephony Equipment Voice Gateway Loss and Level Plan Guidelines



ID	Standard	Title
[R63]	ANSI A117.1	Accessible and Usable Buildings and Facilities
[R64]	2010 ADA	2010 ADA Standards for Accessible Design

TABLE 62 LIST OF APPLICABLE STANDARDS

2.4 Other Documents

2.4.1 The following documents shall be referred:

	Document	Title
[R65]	Schedule 16	Scope of Work
[R66]	Schedule 5(a) SPEC-0005	Cybersecurity specification
[R67]	Schedule 3	Safety, Security and RAM Requirements

TABLE 63 OTHER DOCUMENTS



3 TERMS, DEFINITIONS, AND ABBREVIATIONS

3.1 Terms, Definitions and Abbreviations

- 3.1.1 All the terms, definitions, and abbreviations are provided in the Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of the Telephony System

- 4.1.1 The purpose of the Telephony System shall be to ensure clear and reliable communication between all the locations involved in the California High-Speed Rail System operations for maintaining efficient and safe operations, coordinating emergency responses, ensuring effective staff communication, and providing aid to passengers.

4.2 Telephony System Definition

- 4.2.1 The Telephony System shall provide effective landline communication across the California High-Speed Rail (CHSR) System.
- 4.2.2 The Telephony System shall ensure CHSR staff's internal voice communications and links with the public network and emergency services.
- 4.2.3 The use cases for the Telephony System are as follows:
- Operational communication- To enable real-time voice communication for train operations, train control, traction, and control room activities that are critical to the safe and efficient running of trains.
 - Emergency communication- To allow instant communication during abnormal or dangerous situations to coordinate response and minimize impact on safety and service.
 - Passenger safety and security communication- To provide communication channels for passengers to request assistance or report safety/security concerns, and for staff to respond promptly.
- 4.2.4 The types of telephones based on their use cases to be provided shall include:
- Operational communication- Manual-dial IP telephones shall be used by all operational staff of the CHSR System for the operational railway traffic management in a safe and reliable way.
 - Emergency communication- An auto-dial telephone (blue light telephone) shall be provided to allow personnel to make emergency communication with the OCC.
 - Passenger safety and security communication- A Passenger Help Point (PHP) shall be provided at platforms to allow passengers to communicate with the OCC or Station operator.

4.3 Telephony System Operational Context

- 4.3.1 The mission of the Telephony System is to facilitate clear and reliable communication between the various stakeholders involved in the California High-Speed Rail System operations in compliance with the operational needs.

4.4 Design Life

- 4.4.1 The design life requirements of the Telephony System shall be 30 years.
- 4.4.2 The design life requirements of the Telephony System shall allow for the pertinent evolution and technological change of the Telephony System throughout its life to ensure it remains fit for purpose.
- 4.4.3 The TSCC Contractor shall ensure that Telephony System components with shorter design lifespans shall be managed by scheduled technology refresh strategies and spares management plans.
- 4.4.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce Telephony System components (with equal or compatible technical specifications) for the entire design life required.



5 SYSTEM REQUIREMENTS

5.1 General Requirements

- 5.1.1 The Telephony System shall be designed in accordance with the requirements described in this specification.
- 5.1.2 The Telephony System shall be comprised of the following sub-systems:
- Softphone (Telephony GUI on Integrated Control and Supervision System (ICSS) workstation).
 - Auto-Dial Telephones.
 - Passenger Help Points (PHPs).
 - Manual-Dial Telephones.
 - Voice Recording System (VRS).
 - Voice Mail System.
 - Telephony Management System.
- 5.1.3 The TSCC Contractor's Telephony System design shall support both voice and data. The data refers to all non-audio digital information the Telephony System must transmit — from call control signals to emergency alerts, device status, logs, and integration data for PA, CCTV, FRMCS, and ICSS.
- 5.1.4 The TSCC Contractor's Telephony System design shall consider on-premises solutions (physical, virtualized) bearing in mind that the proposals shall be based on state-of-the-art high-speed railroad technology.
- 5.1.5 The Telephony System equipment shall be placed in locations where it does not infringe the movement of people.
- 5.1.6 The Telephony System shall have direct dial access to and from the Public Switched Telephone Network (PSTN) for voice calls.
- 5.1.7 Government Emergency Telecommunications Service access shall be provided via the Telephony System.

5.2 Environmental Conditions Requirements

- 5.2.1 The TSCC Contractor's Telephony System design shall be appropriate for, and resilient to, the local environmental and climatic conditions at each installation site.
- 5.2.2 The equipment provided shall be protected from damage or degradation in performance due to shock or vibration as experienced in the railway environment.
- 5.2.3 The indoor telephone equipment shall have a minimum ingress protection rating of IP30 in accordance with EN 60529.
- 5.2.4 The outdoor telephone equipment shall have a minimum ingress protection rating of IP65 in accordance with EN 60529.
- 5.2.5 The outdoor telephones shall be weatherproof and vandal resistant.

5.3 Operational Requirements for Telephony System

- 5.3.1 The TSCC Contractor's Telephony System design shall ensure compliance with the California HSR planned operations and shall allow the operation and maintenance of the main line and related local facilities as per the Authority's concept of operations.



- 5.3.2 The Telephony System shall provide communications between CHSR alignment locations, and also to yards, depots, operation and maintenance facilities, passenger stations, OCC, and trains.
- 5.3.3 The Telephony System shall allow communications between, at least:
- Operation control center (OCC).
 - Stations.
 - Staff offices within maintenance workshops, depot, train care facilities.
 - Technical rooms.
 - Traction power facilities.
 - Wayside facilities and shelters.
 - Elevators.
 - any other facility as required by the Authority.
- 5.3.4 The different locations where Telephony System will be deployed, will be linked together via the DCN.
- 5.3.5 All types of traffic shall be recorded via the voice and data recording system.
- 5.3.6 The TSCC Contractor shall design a comprehensive numbering plan to ensure that any operational telephone set must be able to reach any other set wherever located.
- 5.3.7 The Telephony System shall provide facilities to protect against malicious activities on the network, both internally and externally, including attacks from viruses, hacking, hijacking, spoofing and other malicious activities that may compromise the integrity of the network.

5.4 Functional Requirements for Telephony System

5.4.1 General

- 5.4.1.1 The Telephony System shall provide communication for operational staff and emergency communication outlets for passengers.
- 5.4.1.2 The Telephony System shall be based on redundant and centralized Main IP PABXs at the OCC to manage all the internal (on-net) and external calls (off-net) for the CHSR System.
- 5.4.1.3 The Telephony System shall be provided with Satellite IP PABXs at Stations and Depot.
- 5.4.1.4 The Main IP PABXs and the Satellite IP PABX shall be connected together via the Digital Communication Network (DCN).
- 5.4.1.5 When the DCN or the Main IP PABXs are faulty, telephone sets at stations/facilities must be provided with local basic voice communication services via the Satellite IP PABX.
- 5.4.1.6 The Telephony System shall have access to the PSTN to make external calls as well as have access to 911 and the emergency services.
- 5.4.1.7 The capacity of the connection from the Telephony System to the PSTN and to other external systems shall be determined based on anticipated usage, both inbound and outbound, using standard traffic engineering principles.

5.4.2 Telephony Service Features

- 5.4.2.1 The services provided by the Telephony System shall support all communication types used by modern railway organizations and provided by modern professional telephone networks.



5.4.2.2 The Telephony System shall allow modification of services through an appropriate system software configuration.

5.4.2.3 The Telephony System shall support:

- Abbreviated dialing.
- Automatic callback.
- Call diversion/ call forward.
- Calling party name display.
- Call pick up, call recording, call transfer, call waiting, conference call.
- Direct Inward Dialing, Direct Outward Dialing.
- Distinctive Ringing.
- Do Not Disturb.
- Hands-free.
- Last Number Redial.
- Network Call Transfer.
- Voice Mail and voice mail retrieval.
- Call hold, speed dial, follow me, caller ID.

5.4.2.4 The Telephony System shall support QoS support.

5.4.2.5 The Telephony System shall be able to assign levels of service to network users and the facility for interconnection with other systems on the railway and to external networks.

5.4.2.6 The system shall provide facilities to implement call-type restrictions for designated telephone instruments, to meet the operational requirements of the Authority.

5.4.2.7 It shall be possible to manage user access to external networks by invoking call barring features.

5.4.2.8 Call barring shall be possible at individual user level for incoming and outgoing calls, as well as for national and international call barring requirements for individual locations and instruments.

5.4.2.9 The TSCC Contractor shall develop the call access matrix, Class of Services (CoS), and Quality of Service (QoS) together with the Authority.

5.4.2.10 The TSCC Contractor shall develop and prepare a comprehensive, flexible and well-defined numbering scheme and call routing facilities.

5.4.2.11 The TSCC Contractor shall propose a standard class of services for the Authority's approval.

5.4.2.12 The assignment of the Class of Services (CoS) to any telephone extension shall be configurable.

5.4.2.13 The final definition and configuration of CoS shall be subject to the approval of the Authority.

5.4.3 Softphone

5.4.3.1 The Softphone is a software-based telephone application that enables operators to initiate and receive voice calls from the operator workstation over the communication network.

5.4.3.2 The Softphone shall be integrated with the ICSS workstation. Once integrated, the Telephony System shall allow all the operator positions to perform all telephony functionalities in a similar manner.

5.4.3.3 The Softphone roles capability shall include (not limited to):

- Incoming access to a predetermined subset of telephones and outgoing access to a predetermined subset of telephones. Subsets may overlap.



- Allow calls to be made to endpoints by pressing a single speed dial button. Multiple screens of buttons are acceptable.
- Allow calls to be received, indicated by the flashing of the appropriate speed dial button and an audible alert.
- Allow different audible alerts to be associated with different incoming calls to provide a means of alerting the OCC to different priority calls.

5.4.3.4 The Softphone shall be configured for different operator workstation roles, which are accessible via separate logins to allow users to assume a particular pre-configured 'role' on the system via logging in to an ICSS HMI.

5.4.3.5 The pre-configured roles shall be designed to load a particular set of displays on an ICSS HMI, which shall allow calls to/from a pre-determined set of end-user devices.

5.4.3.6 Each role shall have access to the PSTN to make external calls as well as have access to 911 and the emergency services.

5.4.3.7 The following functionalities shall be supported (not limited to):

- An alphanumeric keyboard (including * and #).
- Functional buttons for short code calls.
- SMS functionalities.
- Push To Talk (PTT) button.
- Multiple simultaneous role handling.

5.4.3.8 Functional buttons for extended functions like:

- Call mute.
- Call hold.
- Call forward.
- Call transfer.
- Call history.
- Electronic directory / Phone book.
- Conference.
- Call wizard for simple composition of functional numbers.

5.4.4 Auto-Dial Telephone

5.4.4.1 Auto-dial or 'lift to call' telephones are devices that, when lifted, automatically dial one or more users, typically a specified telephone configured for a particular role.

5.4.4.2 Calls to auto-dial telephones shall only be permitted from the appropriate ICSS workstations.

5.4.4.3 Auto-dial telephones shall, at a minimum, be provided:

- At emergency access points and emergency egress locations.
- In safety refuge areas.
- On station platforms at the middle and ends of the length of each station platform.
- At traction power facilities.
- In a tunnel (if required according to NFPA 130).



- 5.4.4.4 Auto-dial telephones shall be marked by a blue light above each device.
- 5.4.4.5 Auto-dial telephones shall be weatherproof and vandal-resistant.
- 5.4.4.6 Auto-dial telephones shall be available for use, as required, without the need for access keys.
- 5.4.4.7 All auto-dial telephones shall be remotely monitored and report faults via the Telephony Management System.
- 5.4.4.8 Auto-dial telephones shall be available for use, as required, without the need for access keys.
- 5.4.4.9 The location and operational use of all auto-dial telephones shall be assessed to ensure that, once installed, users shall not be exposed to any safety risks.
- 5.4.4.10 Upon an Auto-dial telephone use, an alarm shall sound in the OCC, and the images of the CCTV camera monitoring that location shall be immediately displayed in the OCC.

5.4.5 Passenger Help Point (PHP)

- 5.4.5.1 As part of the Telephony System, all stations and elevators shall be equipped with Passenger Help Points (PHPs) to allow communication between the operators and passengers upon their request.
- 5.4.5.2 A single push of the activation button shall cause the PHP to dial a call automatically. A clear and highly intelligible voice communication shall be established between the PHP and the operator position.
- 5.4.5.3 Upon PHP use, an alarm shall sound in the OCC, and the images of the CCTV camera monitoring that location shall be immediately displayed in the OCC.
- 5.4.5.4 Calls arriving at the OCC, which are not answered within a user-defined, configurable period of 30 seconds to 120 seconds, shall be rerouted to the pre-defined operator position. The re-route destination shall be configurable.
- 5.4.5.5 A "Discrete Listening Function" shall be available to the OCC operator. The PHP shall be capable of a "discrete listening function" to be activated remotely by an operator. The audio transmission shall be one-directional from the PHP to the listener, and no visual indication is to be present for ambient listening on the PHP.
- 5.4.5.6 The PHPs shall support active noise cancellation and acoustic echo cancellation to ensure clear voice communication in noisy environments.
- 5.4.5.7 All PHPs shall be remotely monitored and report faults via the Telephony Management System.
- 5.4.5.8 The location and operational use of all PHPs shall be assessed to ensure that, once installed, no users shall be exposed to any safety risks.
- 5.4.5.9 The Height of installation for PHPs shall be adapted to people with disabilities.
- 5.4.5.10 The PHPs shall be fitted with an audio frequency induction loop (Telecoil or T-Coil) to provide better reception for hearing-impaired passengers wearing hearing aids. The audio frequency induction loops shall comply with EN 60118-4 standard.
- 5.4.5.11 Signage indicating the presence of Audio Frequency Induction Loop shall be compliant with ADA Accessibility Guidelines (ADAAG) and ANSI A117.1, including the appropriate internationally recognized symbol for induction loops where applicable.

5.4.6 Manual-Dial Telephones

- 5.4.6.1 Manual-Dial telephones shall be used by all operational and maintenance personnel of the CHSR System.



5.4.6.2 Manual-dial telephones shall be provided within all California High-Speed Rail facilities, including but not limited to:

- OCC.
- Station rooms.
- Staff offices within stations, Depot, Maintenance facilities, Train care facilities.
- Technical rooms.
- Traction power facilities.
- Wayside facilities and shelters.
- Meeting rooms.
- Ticketing offices.

5.4.6.3 Manual-dial telephones shall support a handset with 12 push-button keypad.

5.4.6.4 Manual-dial telephones shall support adjustable volume control for the speaker and ringer.

5.4.6.5 Manual-dial telephones shall support:

- minimum of 10 programmable function keys for assignment of features or additional extension circuits.
- minimum of 24 memories for speed dialing.
- Hands-free operation through built-in speaker and microphone.
- LCD display.
- Visual display of details for all simultaneous incoming and outgoing calls.
- display of call duration.
- Call waiting facility.
- Conference facility.
- System clock display.
- On-hook dialing.
- A visual notification for received messages.
- Automatic answering.

5.4.6.6 Manual-Dial telephones shall support HD video transmission for face-to-face communication.

5.4.6.7 Manual-Dial telephones shall be compliant with the right type of PoE standard, according to the telephone set consumption.

5.4.7 **Voice Recording System (VRS)**

5.4.7.1 The Telephony System shall function as the CHSR central platform for logging and recording voice and data communications across all interconnected communication systems, not limited to telephony services. This shall include integration with the Voice Recording System (VRS) to capture and store all relevant communications and associated metadata, including timestamps, source/destination identifiers, and call/session details, for operational, safety, and audit purposes.



- 5.4.7.2 The Voice Recording System (VRS) shall enable the recording and logging of the following as a minimum:
- All telephone conversations to/from the OCC.
 - Passenger Help Point calls.
 - All Future Rail Mobile Communication System (FRMCS) calls and data.
 - All Dispatch Console calls and data, including Emergency Responder Communication calls and data.
 - All live PA system announcements.
- 5.4.7.3 All calls involving operator positions shall be time-stamped at the start of the call, with time and date synchronized with the Network Timing System (NTS).
- 5.4.7.4 The recording system shall provide seamless recording 24 hours a day, 7 days a week for the IP-PABXs.
- 5.4.7.5 The VRS shall be sized sufficiently to accommodate any other systems that require voice recording.
- 5.4.7.6 The overall storage capacity shall be adequate for storage of a minimum of 90 days of voice and video recordings.
- 5.4.7.7 The VRS shall support different recording formats. In addition, all supported recording formats shall be compatible with COTS audio players.
- 5.4.7.8 The VRS shall be designed based on the optimal compression ratio for the voice recording. The compression ratio shall not degrade the quality of the recorded audio beyond the audibility to the human ear, and for digital voice profiling.
- 5.4.7.9 The VRS shall support centralized collection, indexing, and secure archival of all recorded media and metadata in a searchable format, accessible only to authorized users for incident investigation, compliance audits, and system diagnostics.
- 5.4.7.10 Authorized Operator selectable functions shall provide the facility to;
- View the call log.
 - Listen to the real-time ongoing call.
 - Listen to recorded calls.
 - Play, pause, stop, fast forward, rewind, skip forward, skip reverse.
 - Playback single or multiple calls simultaneously.
 - Fast search based on items including, but not limited to, channel number, incoming number, outgoing number, call type, date, and time.
 - It shall be able to search using partial incoming or outgoing numbers.
 - Replay the same recorded file on a continuous basis until stopped by the Operator.
 - Playback stored and archived recordings without affecting the normal recording process.
 - Enable playback to be listened to simultaneously by up to four additional local or remote Operators.
 - Allow the creation of audio sequences from multiple calls.
 - Depending on access rights, live monitoring of ongoing calls shall be possible.
 - Facility to 'bookmark' a call for later searches.
- 5.4.7.11 Managed user access and export functionality shall be provided.



- 5.4.7.12 The VRS shall provide the possibility to configure filters for searching and playback of stored recordings by relevant Call Detail Records (CDR).
- 5.4.7.13 Each Call Detail Record shall contain the following minimum information:
- Phone number of the subscriber originating the call (calling party, A-party).
 - Phone number receiving the call (called party, B-party).
 - Starting time of the call (date and time).
 - Call duration.
 - Identification of the telephone exchange or equipment writing the record.
 - A unique sequence number identifying the record.
 - Additional digits on the called number are used to route the call.
 - Disposition or the results of the call, indicating, for example, whether the call was connected.
 - Route (interface) by which the call entered the exchange.
 - Route (interface) by which the call left the exchange.
 - Call type (voice, SMS, video, data, etc.).
 - Any fault condition encountered/rejected calls/blocked calls.
 - Involved parties for any type of multiparty call.
 - Radio cell information (optional).
 - Other railway-related information based on FRMCS.
- 5.4.7.14 Recorded communications shall include a means of ensuring no tampering of each audio stream has taken place in a manner suitable for evidence in a court of law.
- 5.4.7.15 In accordance with California Government Code §34090.6 and guidelines issued by the California Secretary of State - Records Management Program, all recorded and logged data including voice, video, data, and metadata shall be retained for a minimum period of 2 years or longer if required by agency policy, regulatory obligations, or operational needs. The system shall also support secure deletion of records after the retention period expires, in accordance with approved records management practices.
- 5.4.8 Telephony Management System**
- 5.4.8.1 The telephony management system shall include a comprehensive software application with a graphical environment to allow operation, configuration, and monitoring of the Telephony System of each location.
- 5.4.8.2 The telephony management system shall manage all the telephony equipment performing the following actions (not limited to):
- Configuration of the Telephony System features.
 - Supervising the state of all the equipment.
 - Analyzing alarms and taking the necessary actions.
 - Managing the system modifications.
 - Providing statistics related to telephone traffic (general, or per position).
 - Coordinating the software upgrade.



- Creation, configuration, and removal of users and assigning roles and access permissions.

5.4.8.3 A database shall be built for defining the Telephony System configurations. Any change to the database shall automatically be updated onto suitable storage devices such that an updated version of the configuration shall be available should there be a system or power failure.

5.4.8.4 The telephony traffic management statistics shall be compiled and stored on a hard disk.

5.4.8.5 The telephony management system shall provide a real-time network statistics dashboard that presents key operational and performance indicators across all telephony subsystems, including but not limited to IP PABXs and telephony endpoints. The dashboard shall support customizable views and user-defined thresholds to highlight system health, alarms, and usage patterns.

5.4.8.6 The telephony management system shall support both automated and ad hoc reporting capabilities, including:

- Real-time metrics such as traffic volume, session status, and resource utilization.
- Periodic performance reports (e.g., hourly, daily, weekly, monthly) with trend analysis, peak usage statistics, and Service Level Agreement compliance indicators.
- Usage reports per subsystem, user category, and telephony location.
- Export of reports in common formats such as PDF, CSV, and XML for integration with external systems.

The TSCC Contractor shall ensure that reports and dashboards are accessible via a secure web-based interface, support role-based access controls, and retain historical data in accordance with the Authority's data retention policy.

5.4.8.7 Any failure of any element of the Telephony System shall be indicated without delay at the telephony management system, which shall allow gathering, classifying, and logging alarm events from any system element. This management system shall allow the configuration of user profiles, new extensions, permissions, etc.

5.4.8.8 All equipment shall be monitored to ensure that a failure at the card level can be detected and reported to the internal fault diagnostics system and the ICSS System.

5.4.8.9 The telephony management system shall provide the monitoring of the Telephony line for disconnection and faults.

5.4.8.10 The telephony management system shall provide the monitoring of hardware status of auto-dial telephones and PHPs, such as off-hook, damage to the microphone or speaker, etc.

5.4.8.11 The self-test feature shall be used to monitor the hardware status of auto-dial telephones and PHPs in a timely and real-time manner. The self-test feature shall identify the faulty components of auto-dial telephones and PHPs.

5.4.9 Voice Mail System

5.4.9.1 The voice mail system shall be integrated with the IP-PABXs such that access to the voice mail system shall be via the IP-PABX.

5.4.9.2 The voice mail system shall be provided for callers to leave voice messages if the call is not answered.

5.4.9.3 The voice mail system shall provide voice mailboxes for users to retrieve, record, playback, and broadcast voice messages.



- 5.4.9.4 Calls to extensions assigned with voice mail boxes shall be automatically forwarded to the voice mail system when the call is not answered or the called subscriber is busy.
- 5.4.9.5 Calls forwarded to the voice mail system shall be greeted by playing a greeting voice message. The default greeting message shall include the extension number of the called party.
- 5.4.9.6 The TSCC Contractor shall develop the voice mail system default greeting messages, which shall be submitted to the Authority for approval.
- 5.4.9.7 The caller shall be guided with the voice message playback to leave their message in the voice mail box assigned to the called party.

5.5 Performance Requirements for Telephony System

5.5.1 General

- 5.5.1.1 The Telephony System shall be 100% non-blocking for all calls.
- 5.5.1.2 The Telephony System shall support modern high-quality audio codecs, enabling wideband or higher voice fidelity to deliver high-definition (HD) voice communications.
- 5.5.1.3 The Telephony System shall present dial tone, where dial tone is to be presented, within 2 seconds.
- 5.5.1.4 The Telephony System shall signal internal calls within 5 seconds of dialing/autodialing.
- 5.5.1.5 The auto-dial telephone and PHP calls shall have a higher Grade of Service than the normal calls when calling between other telephone lines.
- 5.5.1.6 For calls to/from the OCC operator positions and emergency service through the PSTN, the Telephony System shall also be 100% non-blocking.
- 5.5.1.7 The audio quality of live calls and recorded calls that are replayed shall have a Mean Opinion Score (MOS) of 3.9 or greater as defined in ITU-T Recommendation P.800.
- 5.5.1.8 The Telephony System shall include the hardware, software, and licensing for the complete CHSR System requirements, plus 25 percent additional capacity for endpoints of all types being used.
- 5.5.1.9 The Telephony System shall be flexible to accommodate changes and expansions without service interruption.
- 5.5.1.10 The Telephony System shall be capable of establishing calls through different call routes to overcome any possible failure.
- 5.5.1.11 The Telephony System software maintenance and upgrades/updates/configuration shall be carried out over the Digital Communication Network (DCN) and not require the system to be taken out of operation.
- 5.5.1.12 The TSCC Contractor shall propose traffic capacity criteria for the Telephony System based on operational requirements of similar-sized projects.
- 5.5.1.13 The final call handling capacity shall be subject to the Authority's approval.
- 5.5.1.14 All voice recordings shall be captured in high audio quality and shall include accurate time and date stamps, synchronized with the Network Timing System (NTS).
- 5.5.1.15 The PHPs shall be equipped with an ambient noise level sensor for background noise cancellation. Noise cancellation shall reduce ≥ 15 dBA below background noise up to 75 dBA at a distance of ≤ 1.5 meters and at a height of 1.5 meters while supporting Speech Transmission Index ≥ 0.75 .



5.5.2 Safety Requirements

- 5.5.2.1 The Telephony System shall comply with the safety requirements defined in the Authority's System Safety Plan.

5.5.3 RAM Requirements

- 5.5.3.1 The TSCC Contractor shall be responsible to perform all the activities as specified in Schedule 1 and the Authority's RAM Management Plan.

5.6 Cybersecurity and Security Requirements

- 5.6.1 The TSCC Contractor's design and implementation plan for the Telephony System shall be in full compliance with the Cybersecurity Technical Specification
- 5.6.2 The Telephony System shall have a nominated System Owner accountable for the ownership and mitigation of identified cybersecurity risks.
- 5.6.3 The System Owner shall ensure that threat modelling and risk assessment activities include appropriate resources and SMEs.
- 5.6.4 The Telephony Systems design and implementation plan shall be co-engineered with the TSCC Contractor's cybersecurity team and interfacing system teams to ensure threats are identified and mitigated throughout the project's lifecycle
- 5.6.5 Common Voice Over IP vulnerabilities shall be considered during the design of security controls for the Telephony System, including:
- Caller spoofing
 - Eavesdropping
 - Denial of Service attacks
 - Social engineering
 - Infrastructure-based attacks, including ransomware, malware, and system compromise
- 5.6.6 Secure protocols shall be used to protect the confidentiality and integrity of Voice Over IP traffic; the protocols shall use the approved encryption algorithms defined in the cybersecurity specification; protocols such as SRTP or SIP shall leverage approved cryptographic key exchange protocols in conjunction with AES encryption.
- 5.6.7 Voice over IP endpoints, including phones and other connected devices, shall be authenticated in accordance with the authentication and cryptographic requirements outlined in the cybersecurity specification.



6 INTERFACES REQUIREMENTS

6.1 General Requirements

6.1.1 The interfaces are classified as following:

- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR contractors)
- External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors)
- Internal Interfaces: Interfaces between systems within the TSCC scope

6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.

6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.

6.2 Third Party Interfaces

6.2.1 The TSCC Contractor shall be responsible for connection to the incoming Public Switched Telephone Network (PSTN) lines, obtaining the necessary approvals, coordinating with the relevant local authorities, cabling, civil works, and any related works regarding the connections to the PSTN.

6.2.2 The Telephony System shall interface with the PSTN system to allow communication between the CHSR Telephony System and the external PSTN network (off-net calls), in both normal and emergency scenarios.

6.3 External Interfaces – station contractor

6.3.1 Visible equipment in public areas (auto-dial telephones or PHPs) shall be integrated harmoniously with the architecture of the station.

6.3.2 The TSCC Contractor shall interface with the station contractor regarding the installation of PHPs inside the elevators and ensure their connection to the interface control box through the elevator traveling cable.

6.4 External Interfaces – facilities contractor

6.4.1 Visible equipment (auto-dial telephones or PHPs) shall be integrated harmoniously with the architecture of the facilities.

6.4.2 The TSCC Contractor shall interface with the facilities contractor regarding the installation of PHPs inside the elevators and ensure their connection to the interface control box through the elevator traveling cable.

6.4.3 The TSCC Contractor shall install all Telephony core network equipment in the OCC being provided by the facilities contractor.

6.4.4 The TSCC Contractor shall provide to the facilities contractor:

- Equipment dimensions
- Equipment clearances requirements
- Equipment mounting and fixings requirements
- Cable routes/containment requirements
- Equipment loadings
- Installation and maintenance requirements
- Equipment heating loads



- Equipment cooling loads
- Equipment hydraulic requirements

6.4.5 To be provided by facilities contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:

- Room dimensions and layouts
- Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
- Room raised floor system
- Delivery access routes.
- Maintenance access routes

6.5 Internal Interfaces

6.5.1 Interface with Digital Communications Network (DCN)

6.5.1.1 The Telephony System shall have an interface with the Digital Communication Network (DCN) for connecting the Main IP-PABXs in OCC and the Satellite IP-PABXs in stations.

6.5.1.2 The Telephony System shall use DCN to transmit voice and video calls.

6.5.2 Interface with CCTV System

6.5.2.1 The Telephony System shall have an interface with the CCTV system, as any PHP and auto-dial telephone call shall activate the embedded and/or nearest CCTV camera to the location. The images of the CCTV camera monitoring that location shall be immediately displayed to the operators via the ICSS Workstation.

6.5.3 Interface with Integrated Control and Supervision System (ICSS)

6.5.3.1 The Telephony System shall have an interface with the ICSS system on standard protocols (e.g., SNMP) to allow status monitoring of the Telephony System equipment.

6.5.3.2 The Telephony System shall interface with ICSS to manage voice calls from manual-dial telephones, auto-dial telephones, and PHPs on the ICSS workstations.

6.5.3.3 The ICSS shall include a facility to enable the patching of calls between the Telephony System and programmed WCS devices.

6.5.4 Interface with Wireless Communication System (WCS)

6.5.4.1 The Telephony System shall interface with the WCS to allow calls between telephones and WCS devices.

6.5.4.2 The VRS, as a part of the Telephony System, shall have an interface with the WCS to record and securely store all voice communications and logging information.

6.5.4.3 The VRS shall store all voice communications, including talk group calls, emergency calls, and point-to-point calls. Recordings shall include all metadata, such as caller identity, timestamp, call duration, priority level, and associated talk group call ID.

6.5.5 Interface with Network Timing System (NTS)

6.5.5.1 The Telephony System shall have an interface with NTS for time synchronization and time display.

6.5.6 Interface with the Public Address and Customer Information System (PACIS)

6.5.6.1 The Telephony System shall have an interface with PACIS to allow announcements from authorized telephones to the Public Address System (PAS).



- 6.5.6.2 The VRS as a part of the Telephony System shall have an interface with the PACIS to record all the live announcements via the PAS.

6.5.7 Interface with Wireless Communication Systems (WCS)

- 6.5.7.1 The Telephony System shall have a redundant interface with the Future Radio Mobile Communication System (FRMCS, a subsystem of the WCS). Telephony System acts as the central switching system for phone calls. The telephony system handles internal traffic between stations and acts as the gatekeeper to the outside world.
- 6.5.7.2 The FRMCS Dispatch Consoles shall be integrated with the Telephony System, which acts as the central recording and logging system for all Dispatch Consoles and FRMCS voice, data and metadata.
- 6.5.7.3 The Telephony System shall provide the voice, data and metadata recording and logging capabilities of the FRMCS.

6.5.8 Interface with Enterprise Asset Management Systems (EAMS)

- 6.5.8.1 The Telephony System shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.

6.5.9 Interface with Low Voltage Power System

- 6.5.9.1 The Telephony System shall interface with an Uninterruptible Power Supply (UPS) with minimum 12 hours backup to get the required power to feed the Telephony System equipment.



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied by the TSCC Contractor shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards. Refer to 2.4.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the design life requirements.

7.2 Software and Hardware Requirements

- 7.2.1 The Telephony System IP-PABXs and/or servers shall have redundant architecture, including hardware, software, network, power supply, cabling, cooling, data backup, and disaster recovery planning and physical security, so that the Telephony System survives during any one failure of hardware, power supply, cabling, and software.
- 7.2.2 The TSCC Contractor's Telephony System design shall support the expansion and scalability requirements while meeting or exceeding its RAMS to include redundancy, availability, and degraded modes of operation requirements.
- 7.2.3 The Telephony System equipment and devices shall be connected to the UPS of the facility where they are located (OCC, station, etc.).
- 7.2.4 All central servers may be on-premises or virtualized machines to ease systems evolution, complying with the Cybersecurity requirements.
- 7.2.5 The operating system of all the network devices shall be provided with the latest stable release.
- 7.2.6 All the application software shall be upgraded to the latest stable release and shall support all the requirements specified.

7.3 EMC Requirements

- 7.3.1 The Telephony System shall be fully immune and protected from any Electromagnetic Interference (EMI) with the traction power, multi-tubular cabling, and Radio Frequency Interference (RFI). The EMI emissions shall be mitigated in accordance with applicable standards (EN 50122 or equivalent)



8 TOLERANCES

Not applicable to Telephony System.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 The TSCC Contractor shall supply and deliver all components related to the Telephony System.

9.2 Specific Requirements

9.2.1 The Telephony System scope of supply and delivery shall include (not limited to):

- Servers.
- Main IP PABXs.
- Satellite IP PABXs.
- Softphone application/software.
- Auto-Dial Telephones with blue light indicator.
- PHPs with audio frequency induction loops.
- Manual- dial IP telephones.
- Voice Recording System (VRS).
- Billing System (if required).
- Telephony Management System.
- Voice Mail System
- HW/SW licenses.
- Software architecture, including full specification of protocols used.
- Auxiliary elements, tools, and gear.
- Spare parts.
- Maintenance laptops

9.2.2 The TSCC Contractor shall provide the exact site locations of each Telephony System equipment, using layout drawings.

9.2.3 The cables used in the Telephony System shall be low-smoke, flame-retardant, halogen-free type.

9.2.4 The TSCC Contractor shall provide the Telephony System cable schedule and layout.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.

12.2 Specific Requirements for Telephony System

12.2.1 The TSCC Contractor shall perform an Erlang calculation study to dimension the Telephony System, IP PABXs capacity, and to determine the number of lines and channels to be requested in the PSTN connections.

12.2.2 Network failure and Main IP PABXs failure test cases shall be performed to validate the function of the local communication service via the Satellite PABX.

12.2.3 Integration test with interfacing systems shall be recorded and reported.



13 SUBMITTALS

13.1 General Requirements

13.1.1 General submittal requirements are defined in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor and Supplier information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railroad management aspects which may influence Telephony System reliability, availability, and maintainability characteristics.

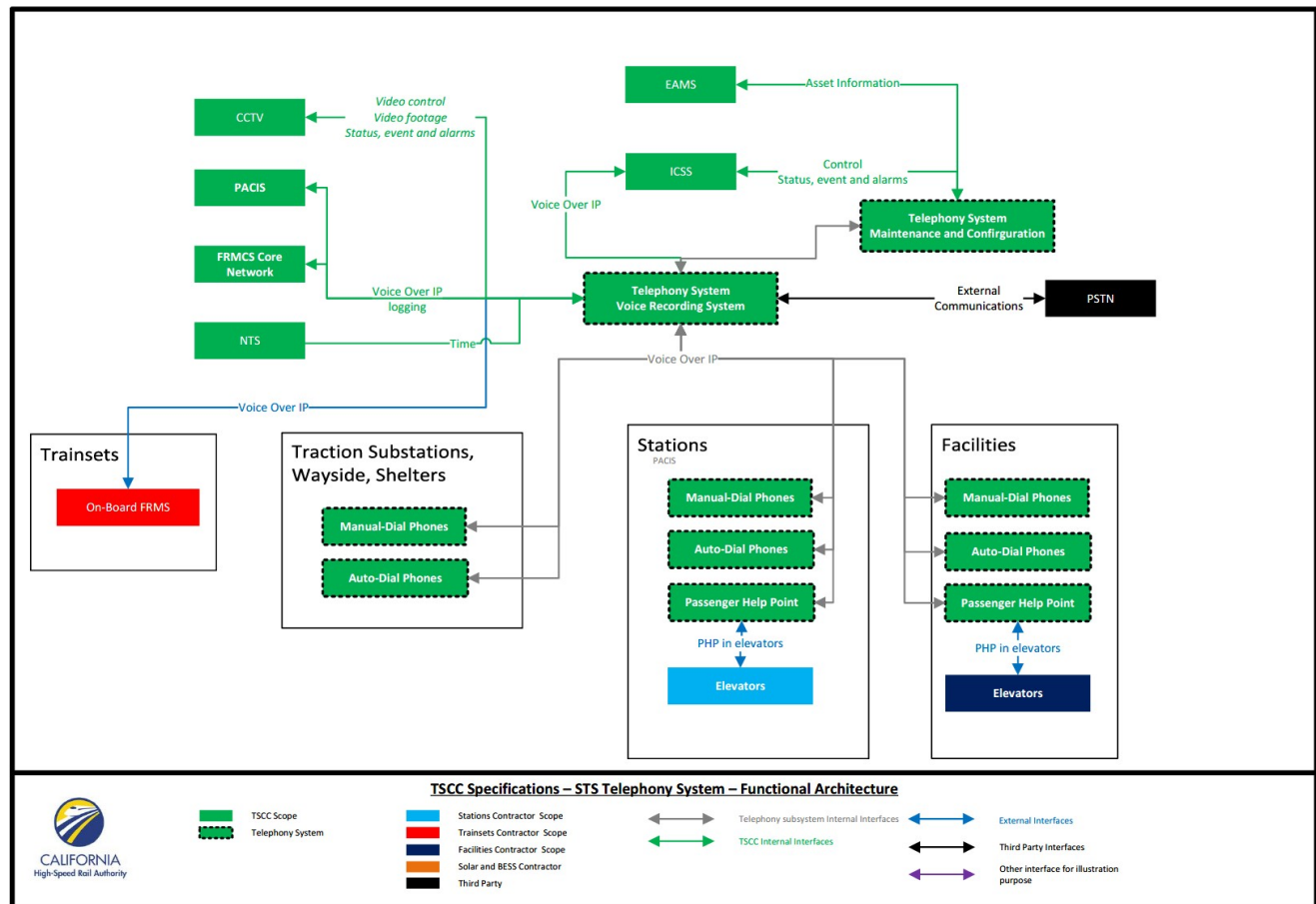


16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.

APPENDIX A TO EXHIBIT 5(P) TELEPHONY SYSTEM



Schedule 5(q)

Traffic Management System (TMS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0021 – Traffic Management System (TMS)

Rev. 0.0

A handwritten signature in blue ink, appearing to read "V. Decanter".

Authored:

Vincent Decanter / Selma Duru, TCS Engineer

10/15/2025

Date

A handwritten signature in blue ink, appearing to read "A. Clapham".

Checked:

Andrew Clapham, Train Control Lead

10/15/2025

Date

A handwritten signature in blue ink, appearing to read "Bruno Comperat".

Checked:

Bruno Comperat, Deputy Director of Rail Engineering

10/16/2025

Date

A handwritten signature in blue ink, appearing to read "Ryan Scott".

Approved:

Ryan Scott, Director of Rail Engineering

10/16/2025

Date

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Released:

Amit Joshi, Configuration Manager

10/16/2025

Date



Document Revision History – TMS Specifications**First Edition****September 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION	5
2	REFERENCE STANDARDS AND DOCUMENT	6
2.1	GENERAL	6
2.2	STANDARDS	6
3	TERMS, DEFINITION AND ABBREVIATION	7
4	SYSTEM DESCRIPTION	8
4.1	PURPOSE OF THE TMS	8
4.2	TMS DEFINITION	8
4.3	TMS AND ERTMS.....	8
4.4	TMS OPERATIONAL CONTEXT	9
4.5	DESIGN LIFE	9
5	SYSTEM REQUIREMENT	10
5.1	GENERAL REQUIREMENTS.....	10
5.2	ENVIRONMENTAL REQUIREMENTS.....	12
5.3	OPERATIONAL REQUIREMENTS	12
5.4	MAINLINE TMS FUNCTIONAL REQUIREMENTS.....	12
5.5	ENGINEERING POSSESSIONS FUNCTIONAL REQUIREMENTS.....	32
5.6	TRACTION POWER AND ELECTRICAL PROTECTION REQUIREMENTS.....	33
5.7	LOCAL FACILITIES (LF)	33
5.8	PERFORMANCE REQUIREMENTS.....	34
5.9	SECURITY AND CYBERSECURITY REQUIREMENTS.....	35
6	INTERFACE REQUIREMENTS	36
6.1	GENERAL REQUIREMENTS.....	36
6.2	EXTERNAL INTERFACES – FACILITIES CONTRACTOR	36
6.3	INTERNAL INTERFACES	36
7	MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS.....	40
7.1	TMS WORKSTATION	40
7.2	SERVERS	40
7.3	REDUNDANCY REQUIREMENTS	40
7.4	EMC REQUIREMENTS.....	40
8	TOLERANCES	41
9	SCOPE OF SUPPLY AND DELIVERY	42
9.1	GENERAL REQUIREMENTS.....	42
9.2	GENERAL REQUIREMENTS RELATED TO THE CONTRACTOR SCOPE OF WORK ARE DEFINED IN PART B – TECHNICAL CONTRACT REQUIREMENTS.	42
9.3	SPECIFIC REQUIREMENTS	42
10	MANUFACTURING.....	43



10.1	GENERAL REQUIREMENTS.....	43
11	INSTALLATION AND INTEGRATION.....	44
11.1	GENERAL REQUIREMENTS.....	44
12	TESTING & ACCEPTANCE	45
12.1	GENERAL REQUIREMENTS.....	45
12.2	SPECIFIC REQUIREMENTS	45
13	SUBMITTALS.....	46
13.1	GENERAL REQUIREMENTS.....	46
14	QUALITY MANAGEMENT.....	47
14.1	GENERAL REQUIREMENTS.....	47
15	ADDITIONAL INFORMATION REQUESTED	48
15.1	GENERAL REQUIREMENTS.....	48
16	LOGISTICS	49
16.1	GENERAL REQUIREMENTS.....	49



1 INTRODUCTION

1.1 Scope of the technical specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's requirements for the **Traffic Management System**, hereinafter: **TMS**.
- 1.1.2 The functional architecture of the TMS alongside other Train Control Systems is presented in Appendix A.
- 1.1.3 The requirements are formulated using the following words and their meanings:
- "Shall": Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure).
 - "Should": Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents.
 - "Must": Indicates an obligation or a mandatory requirement.
 - "May": Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.



2 REFERENCE STANDARDS AND DOCUMENT

2.1 General

2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines and specifications provided in this technical specification for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, training, operations and maintenance.

2.1.2 All generic standards to be used are provided in: Technical Contract Requirements.

2.2 Standards

2.2.1 The following specific standards to be used for TMS are listed below.

ID	Code	Title
[R25]	ISO 11064	Ergonomic design of control centers
[R26]	TAP TSI	Telematics Applications for Passenger Service TSI
[R27]	EN/ISO 62682 standard	Principles for managing alarms systems in process industries
[R28]	EULYNX Baseline Set 4 Release 4	EULYNX Baseline Set 4 Release 4

TABLE 13 – LIST OF APPLICABLE STANDARDS



3 TERMS, DEFINITION AND ABBREVIATION

- 3.1.1 All the terms, definitions, and abbreviations are provided in the Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Purpose of the TMS

4.1.1 The TMS system shall perform the following main functions:

- Timetable and simulation,
- Interface with other external timetable applications,
- Capacity management,
- Real-time traffic management in mainline and stations,
- Normal and degraded operation with predefined contingency plans
- Traffic Management at Facilities,
- Efficient coordination with national emergency / security authorities,
- Efficient coordination with the Train Dispatcher,
- Coordination of maintenance,
- Maintenance work monitoring and engineering possessions,
- Monitoring of energized track sections,
- Tool for training, playback and analysis of past operations,
- Diagnostic tool,
- Manual Routing of Trains
- Dispatching operations.

4.2 TMS Definition

4.2.1 The TMS shall be deployed in the Fresno OCC.

4.2.2 The TMS shall provide the Dispatcher HMI for all the traffic management tasks.

4.2.3 Yard Controller HMI shall be provided in the local facilities (LF), except for TCF.

4.2.4 Note: California HSR Project includes passenger stations, but also at a minimum trainset maintenance facility (LMF and HMF), Maintenance of Way Facility (MOWF) and Train Certification Facility (TCF) locations.

4.3 TMS and ERTMS

4.3.1 The Traffic Management System on main line shall include:

- Traffic Management System,
- Maintenance work monitoring and engineering possessions.

4.3.2 The TSCC Contractor shall propose its most efficient and secure solution for engineering possession and catenary protection.

4.3.3 TMS shall be interfaced with the following TCS subsystems for the purpose of following functions (list not limitative):

4.3.3.1 Radio Block Centre (RBC):

- Movement Authorities.
- Text message,
- Train Data (train running number, position and speed),



- Temporary Speed Restriction (TSR),
- RBC equipment status, alarms, and events.

4.3.3.2 Interlocking (IXL):

- Route setting,
- Trackside equipment monitoring and control,
- Temporary Shunting Area (TSA),
- IXL and TMS status, alarms, and events.

4.4 TMS Operational Context

4.4.1 The TMS system shall enable:

- 24h service all year round (with required traffic stops for maintenance work).
- Management of train movements along the line with the given headway.
- Bidirectional operation on main line.
- Management of interfaces with other subsystems of railway system.
- Recording of the traffic information and operational alarms.

4.4.2 The TMS system shall comply with the operational rules applicable on the CHSR line and shall allow safe movement of all trains for CHSR line at maximum operational speed.

4.4.3 The TMS system shall be deployed over the entire railway network on the CHSR line, managing all types of railway infrastructure, e.g., the main line and Facilities.

4.4.4 TMS shall support multiple operational roles based on operational needs, each role shall be open to configuration or re-configuration by the Authority. Example roles are defined in Chapter 5.4.5 *User Management (UM)*, functions and responsibilities will be defined by the operational procedure to be developed and approved by the Authority.

4.4.5 The examples of TMS operational roles are listed below:

- Supervisor,
- Dispatcher,
- Offline Timetable Operator,
- Regulator,
- Trainer (simulation)
- Yard Controller,
- TMS Administrator.

4.5 Design Life

4.5.1 The design life requirements of the TMS System shall be 30 years.

4.5.2 The TSCC Contractor shall ensure that the manufacturers will be able to produce TMS system components, with equal or better technical specifications, throughout the required operational lifetime, recognizing the potential for successive generations and evolving sensor technology.

4.5.3 Any equal or better technical specifications element should be able to be integrated “out of the box”, with no re-work of existing systems, components or other element’s part from the single item being replaced.



5 SYSTEM REQUIREMENT

5.1 General Requirements

- 5.1.1 The TSCC Contractor shall design, install, verify and validate, test and commission, organize the training, provide warranty services and provision of defect notification period services for the TMS roll out.
- 5.1.2 The TMS for mainline will be technically implemented into the Operational Control Centre (OCC) in Fresno.
- 5.1.3 The TMS shall conform to California legislation, to US Code of Federal Regulations (CFRs) and comply with agreed California High Speed Rail operations.
- 5.1.4 The TMS shall be deployed as follows:
- Main line TMS operation workstations in the OCC Operating Floor,
 - TMS servers in the OCC equipment rooms,
 - TMS workstation in local facilities. Traffic management for the following local facilities: MOWF/LMF/HMF shall be managed by a dedicated Yard Controller, who will be located at the facility.
- 5.1.5 The TMS shall implement functionalities and technologies with high level of flexibility, to allow easy modification, expansion and reconfiguration according to the traffic management organization and consistence of traffic (as it is expected that frequent adaptation of the operational control center and organizational structures may be required during the TCS subsystem lifetime), and be capable to adapt to different possible organizational and operational models that could be applied to CHSR line.
- 5.1.6 The TMS shall provide at least the following main functions which shall conform to the requirements of legislation of California and shall be implemented to ensure the process of operation of CHSR:
- Real-time image of the entire line,
 - Permanent control across the whole network,
 - Automatic and manual route setting,
 - Real timetable management
 - Supervision of train movements and train tracking,
 - Supervision of the whole line,
 - Timetable conflict resolution,
 - Priority management,
 - Regulation,
 - Temporary Speed Restriction management (TSR),
 - Visualization (no possibility of action) of the alarms which could impact the normal operation from the following systems: Hazard Detection and Early Warning Systems.
 - Works train movement route setting,
 - Engineering possessions management for maintenance and engineering works, (including indication of Maintenance works protection measures.)
- 5.1.7 The TMS shall be able to:
- Remotely control the computer-based interlocking system,
 - Generate route setting commands to the interlocking,
 - Process timetable data coming from both:



TMS internal timetable tool,

a different (external) timetable tool or application, that the Authority may elect to procure as a totally different timetable system, other than the TMS internal timetable tool,

- Perform capacity management,
- Perform traffic regulations to optimize the operation,
- Localize and identify trains by tracking all train movements,
- Record all relevant events of the operational day for later statistical evaluations and for post-incident analysis,
- Back up the overall supervision and control of all train movements by a data logging and playback system,
- Individual management of objects (turnouts for the various functions as turnout blocking, inhibition, individual control, or block sections),
- Provide real-time display,
- Provide alarms and associate fault diagnostic information for the entire Signaling System.

5.1.8 All stations should be remotely controlled from the Fresno OCC TMS.

5.1.9 The TMS shall be able to manage, at least, the following types of trains:

- High Speed Passenger trains,
- Maintenance trains,
- Testing trains,
- Emergency trains.

5.1.10 The TMS shall provide:

- Fully automatic route setting in the regular operation mode and partially automated in degraded modes,
- Manual route setting in case of emergency operation, or in the event of Automatic Route Setting functionality being unavailable.

5.1.11 The TMS shall be able to manage operation on CHSR main line, including:

- Passenger stations: Merced, Madera, Fresno, Kings/Tulare, Bakersfield.
- Transfer tracks to facilities (depending on the proposed solution for the track configuration and the operational needs).

5.1.12 Dedicated tracks separating the main line from facilities shall enable any train movement from the main line to the facilities and from the facilities to the main line. Those tracks are called "Transfer tracks". In case a train should enter the main line from the facilities, the Local Control shall request authorization from the main line Dispatcher.

5.1.13 The TMS shall ensure the following interfaces with other TSCC systems:

TCS Systems (other than TMS)	TMS		
	Receive, Process & Send Data	Monitor (visualization on Dispatchers HMI)	Command (actuate)
RBC	Yes	Yes	Yes



IXL - Interlocking	Yes	Yes	Yes
Power SCADA System	Yes	Possible	No
LVPD (Low Voltage Power Distribution)	Yes	No	No
DCN (Digital Communication Network)	Yes	No	No
Cybersecurity	Yes	No	No
Hazard Detection and Early Warning System (HDEWS) (incl. all Detectors and Sensors System)	Yes	Possible	No
Integrated Control and Supervision System	Yes	Possible	No
Passenger Information Display System / Public Address System	Receive & process	No	No
Network Synchronization and Time Distribution System (Master Clock System)	Yes	No	No

TABLE 14. TMS INTERFACES WITH OTHER TSCC SYSTEMS

5.2 Environmental Requirements

- 5.2.1 TMS's equipment is hosted in the OCC, passenger stations and facilities buildings. The relevant environmental requirements apply.
- 5.2.2 The TMS's equipment shall meet the environmental requirements described in the Scope of Work.

5.3 Operational Requirements

- 5.3.1 The TMS shall allow the Authority to operate the CHSR main line as described in this Technical Specification and in the CHSR Operational Concept in Nominal, Degraded and Emergency mode.
- 5.3.2 The TMS shall allow the Authority to maintain the CHSR main line as described in this Technical Specification and in the CHSR Maintenance Concept.
- 5.3.3 The operational requirements at the level of detail needed for TMS design will be specified later by the Authority, with coordination with the TSCC Contractor.

5.4 Mainline TMS Functional Requirements

5.4.1 Timetable, Infrastructure Construction and Simulation:

5.4.1.1 Offline Timetable

- 5.4.1.1.1 The TMS shall provide an offline timetable function allowing the construction and management of CHSR.
- 5.4.1.1.2 The TMS offline timetable shall meet the requirements of *TAP TSI [R2]*.
- 5.4.1.1.3 The Offline timetable function shall provide automatic timetable generation including automatic detection and automatic conflict resolution.
- 5.4.1.1.4 A dedicated HMI shall be provided for this activity. This HMI shall provide all the tools in an ergonomic and user-friendly environment, timetable construction and simulation shall



be realistic and based on the railway network topology, rolling stock characteristics and other parameters to be agreed prior to the design.

5.4.1.2 **Timetable Management (TTM)**

- 5.4.1.2.1 TMS shall provide an import function allowing timetable import from the Offline timetable function according to all requirements of *TAP TSI [R2]*.
- 5.4.1.2.2 The import function shall include a timetable consistency check step before timetable storage.
- 5.4.1.2.3 TMS shall include a Timetable Management function that support the management (creation, modification, selection...) of predefined electronic timetables.
- 5.4.1.2.4 TMS shall automatically select the timetable for the current operating day according to the calendar of operation.
- 5.4.1.2.5 TMS shall allow a manual selection of an operating timetable among the set of available timetables.
- 5.4.1.2.6 TMS shall allow the content of the current timetable to be adapted manually or automatically such as but not limited to:
 - Adjustment of departure time,
 - Addition of extra journeys,
 - Modification and cancelation of existing journeys.
- 5.4.1.2.7 TMS shall provide convenient functions and HMI to support offline timetable management, including but not limited to:
 - Generation of a complete and coherent timetable using a graphical time-distance chart,
 - Insertion into the timetable database,
 - Printing of timetables.
- 5.4.1.2.8 Timetables shall be the primary source of information for other functions typically Automatic Train Reporting, Automatic Route Setting, Automatic Train Regulation, certain features of Train Description function and also Passenger Information system.
- 5.4.1.2.9 The TTM function shall provide for the basic preparation, building, storage, editing, loading etc. of Base and Operational timetables.
- 5.4.1.2.10 The TTM function shall be able to adapt the timetable for seasonal, weekend, holiday and exceptional effects and shall enable Dispatchers to edit and modify the timetable information both off-line and online.
- 5.4.1.2.11 Timetable data shall include train identity, type, class, time profile, stopping pattern, routing information etc.
- 5.4.1.2.12 The TTM function shall provide the loading, activation, and editing of appropriate daily operational timetables.
- 5.4.1.2.13 The TMS shall provide an export function allowing export timetable according to the format required by *TAP TSI TAP TSI [R2]*.

5.4.1.3 **Integration of the external Timetabling data from other External applications**



- 5.4.1.3.1 In the beginning or throughout the Operations period and at any time, the Authority may elect to procure an independent timetable planning system, other than the TMS internal timetable tool.
- 5.4.1.3.2 TMS shall provide an import function allowing timetable import from the External timetable tool.
- 5.4.1.3.3 The import function shall be clearly specified in order to have a precise definition of the data format that will be imported.
- 5.4.1.3.4 The import function shall include a timetable consistency check step before timetable storage.
- 5.4.1.3.5 All other requirements stated above in this section are mandatory.

5.4.2 Traffic Operation and Real Time Traffic Management

5.4.2.1 Route Setting

- 5.4.2.1.1 The TMS shall allow at least the following commands:

Route setting (Main route, Shunting route, Call-on route),

Fleet mode (the route remains in a locked state),

Route cancel (Main route, shunting route, Call-on route), including partial cancellation,

Emergency Route Release and group replacement

Call-on route: certain locations are permitted to allow more than one train into a single section, e.g. to join trains or enable 2 trains to use one platform. The movement of the second train into an occupied section is authorized by setting a "call-on" route...

- 5.4.2.1.2 The TMS shall allow the management of the Shunting route allowing the authorized trains to move to permanent shunting areas or to temporary shunting areas as works (application and management of predefined shunting areas).
- 5.4.2.1.3 The TMS shall allow the management of call-on routes for the trains in On-Sight mode allowing these trains to enter occupied sections.
- 5.4.2.1.4 The TMS shall allow the management of Main routes for the trains in FS mode in normal operation.
- 5.4.2.1.5 The TMS shall allow setting "extended routes" (composed of several routes) within an interlocking by selection of the route entrance and the route exit limits.
- 5.4.2.1.6 It shall be possible to place certain routes into "Fleet Mode" such that, on passage of a train, route normalization is inhibited (route is dynamically (partially) released, and the new route could be set when conditions ahead allow).
- 5.4.2.1.7 TMS shall enable Dispatcher to execute emergency route release and group replacement controls.
- 5.4.2.1.8 Overrun alarms (i.e. when informed by the RBC that a train entered in trip mode when passing a Marker Board at danger) shall be raised on the TMS for the dispatcher to take appropriate actions.
- 5.4.2.1.9 The TMS shall perform a preventive check to avoid setting a route, if the OCS is not powered (if so, trains shall be stopped in the appropriate section),



- 5.4.2.1.10 These checks shall be performed in manual and automatic (ARS) mode.
- 5.4.2.1.11 Detailed functionality and graphical user interface of Route Setting function to be proposed by TSCC Contractor prior to the detailed technical design and approved by the Authority.
- 5.4.2.2 Automatic Route Setting (ARS)**
- 5.4.2.2.1 The TMS shall provide Automatic Route Setting functionality (ARS).
- 5.4.2.2.2 The ARS function shall automatically provide route setting requests to the interlocking for routes throughout the controlled area and shall provide the following facilities:
- Be capable of operating any booked service to its planned path from the point of Inception to the point of termination,
 - Be capable of automatically changing a Train Identification (TI) where a train has completed one booked path and is about to embark on another booked path, and
 - Be able to regulate path conflicts that arise from perturbed running of booked services, minimizing the overall delay.
- 5.4.2.2.3 The ARS function shall be sub-divided into "areas" which may be related to interlocking areas.
- 5.4.2.2.4 It shall be possible for Dispatchers to either enable or dis-enable ARS for each track area separately via HMI. An indication of the status of each area shall be given to the Dispatcher.
- 5.4.2.2.5 The train service data for the ARS will be derived from the timetable in real time and shall be updated automatically to consider regulation information.
- 5.4.2.2.6 The ARS function shall be provided with the identity and location of each train by the Train Identification (TI) function.
- 5.4.2.2.7 The ARS function shall be capable of performing route setting and train regulation for the whole area under control of the TMS.
- 5.4.2.2.8 Route settings shall match the planned timetable when all trains are running as scheduled.
- 5.4.2.2.9 When train services are disrupted the ARS function shall make decisions to regulate the service to achieve minimum overall delay to trains.
- 5.4.2.2.10 Means shall be provided to enable such ARS decisions to be automatically referred to the Dispatcher for vetting and acknowledgement prior to implementation.
- 5.4.2.2.11 When the ARS function is not able to bring an optimum solution, it shall keep trains running in line with the general timetable plan or contingency plan.
- 5.4.2.2.12 ARS action shall be taken on the basis that trains shall only have routes set for them once they have been recognized by the ARS system and are included in the timetable data.
- 5.4.2.2.13 When the ARS function is enabled, manual route settings shall also be available and shall always take priority over automatic operation.



- 5.4.2.2.14 The Dispatcher shall be able to deactivate the ARS function at least for:
A train,
A station,
Several stations.
- 5.4.2.2.15 Should communication to one or more interlocking be unavailable, ARS shall continue to operate in all areas not affected by the failure.
- 5.4.2.2.16 The Dispatcher shall be able to:
Operate the ARS function and receive information from it,
Selectively signal individual trains by ARS or manual means and be able to determine by which method each train is operated,
Determine the next forecasted route of the train by the ARS,
Ascertain the timetable under ARS control,
Engage and disengage ARS areas.
- 5.4.2.2.17 The system shall be interlinked with the Train Identification function such that display of Train Identification for ARS and non-ARS trains shall be clearly distinguishable by use of distinctive colors.
- 5.4.2.2.18 The ARS function shall be able to implement the regulation decisions including real-time timetable adjustment.
- 5.4.2.2.19 The TSCC Contractor shall provide the most efficient Automatic Route Setting function avoiding unnecessary delays of trains.
- 5.4.2.2.20 The ARS function shall appropriately route an identified train to the correct destination.
- 5.4.2.2.21 Manual route setting, and cancellation, shall be available in parallel with ARS and shall not cause additional activity for the Dispatcher because of the ARS being present.
- 5.4.2.2.22 Routes set by ARS function shall be displayed in an identical manner to those set manually.
- 5.4.2.2.23 Routes may only be set by ARS functions when all the following conditions are satisfied:
The train is approaching a point where route setting is required,
The train has an entry in the timetable or is running to a standard pattern,
The train is progressing along a scheduled route or a permitted alternative route,
The train type is suitable to enter the route,
The next route required is designated as requiring setting by the ARS strategies,
The train is a designated ARS train.
- 5.4.2.2.24 Commands to set a route shall only be sent to an interlocking by ARS where such a route:
is available to be set,
is an ARS route,
lies in an area which is enabled for ARS operation.
- 5.4.2.2.25 Oversetting of routes shall not be permitted by the ARS system even where this facility is available manually.



- 5.4.2.2.26 In the event of any of the following occurring within an ARS area, then such an area shall immediately be dis-enabled and shall revert to manual control:
- manual cancellation of a route,
 - identification of an incorrect sequence of axle counter's operation based on information received from interlocking,
 - initiation of Workstation control,
- ARS working may only then be re-established by the Dispatcher.
- 5.4.2.2.27 The ARS function shall set routes ahead of train movements to the following criteria:
- Routes shall be set far enough ahead of train movements to ensure that drivers will not receive restrictive signals unnecessarily,
 - Routes shall not be set unnecessarily far ahead to not impair the efficiency of the train regulation.
- 5.4.2.2.28 Suitable ARS alarms shall be generated for each of the following circumstances:
- Changes of state of the ARS function or of any area within it becoming either available or unavailable,
 - The inability to correlate train descriptions in the timetable with those of trains in the Train Identification's function,
 - Trains being run to a path not prescribed to them in the timetable,
 - The inability to set a route for any train,
 - Trains which have had a route set for them fail to move within 5 minutes.
- 5.4.2.3 After TMS is put in operation, the Authority shall be able to configure and adjust the ARS function parameters determining the route preparation.
- 5.4.2.3.1 Detailed functionality and graphical user interface of ARS function to be proposed by the TSCC Contractor prior to the detailed technical design and approved by the Authority and train dispatchers.
- 5.4.2.4 **Automatic Train Reporting (ATR)**
- 5.4.2.4.1 The principal functions of the Automatic Train Reporting (ATR) system shall be:
- To monitor real-time train running performance against timetable,
 - To provide statistical data for analysis and timetable preparation.
- 5.4.2.4.2 As trains progress through the system their actual progress shall be monitored and compared with the operational timetable data.
- 5.4.2.4.3 For the purpose of monitoring station stops, the arrival time at a station is the time when the track detection system preceding the loop line or passing road is occupied and then cleared (usually a point track).
- 5.4.2.4.4 The departure time from the station is the time when the first track beyond the loop line or passing road is occupied (usually a point track).
- 5.4.2.4.5 System outputs shall be in the form of Workstation's displays, hardcopies and storage devices in respect of:
- Time-Distance Graphs,
 - Train Run Reports, Schedules etc.,



Stored ATR data.

- 5.4.2.4.6 The Automatic Train Reporting function shall provide exports to Transmodel standards.
- 5.4.2.4.7 Displays of Train Graphs shall incorporate pan and zoom techniques in both axes.
- 5.4.2.4.8 The ATR function outputs shall contain information in respect of train running, which is planned, actual, future and predictive and each shall be shown in a distinctive manner.
- 5.4.2.4.9 Outputs shall be available on a routine basis and on demand.
- 5.4.2.4.10 Dispatchers shall be able to call up information by exception using selection criteria. This shall include the ability to select the extent of variance from the timetable for specific reports.
- 5.4.2.4.11 The ATR function shall interlink with the Train Identification function such that TD displays are able to highlight the extent of delay, i.e. variance from the timetable.
- 5.4.2.4.12 Delay criteria and form of display shall be subject to the specific approval of the Authority.
- 5.4.2.4.13 Online data storage shall be provided, enabling users to access and browse the previous 60 months' records at any time. It shall be possible to extend the storage time for specific types of data if required.
- 5.4.2.4.14 The ATR function shall also store records in a suitable manner to permit the transfer of each month's records to external processors or to suitable media for archival storage.
- 5.4.2.4.15** Detailed functionality and graphical user interface of ATR function to be proposed by the TSCC Contractor prior to the detailed technical design and approved by the Authority.

5.4.2.5 Signaling Commands (SIG)

- 5.4.2.5.1 The TMS shall be able to operate with different types of interlocking and RBC using the EULYNX standard protocols.
- 5.4.2.5.2 The operation of the Signaling System (TMS+ IXL+RBC + Wayside) shall be unified within TMS, no specific HMI shall be required, and it shall be possible to issue commands to all parts of the Signaling System, RBC and IXL, in the same HMI view.
- 5.4.2.5.3 The Safety critical commands shall be defined and implemented by the TSCC Contractor during design stage and follow the RAMS process.
- 5.4.2.5.4 Inhibit, Blocking or protection functions (of turnouts, etc.), when initiated by the TMS, shall be managed as vital functions (SIL2 at least, the definition of the appropriate security level will be the responsibility of the TSCC Contractor).
- 5.4.2.5.5 Dispatchers shall have the possibility to issue a route command by interacting on the presentation of the start and end signal/markerboard of the route. In case more than one route is possible to be set between the start and end signal/markerboard, all possible routes shall be displayed for selection.
- 5.4.2.5.6 TMS shall generate requests to the IXL, to enable individual or group management of signaling objects (turnout blocking, inhibition, individual control, block sections, Signal replacement....).
- 5.4.2.5.7 TMS shall enable to manage emergency stops using a Signal group replacement command to set a group of signaling Marker Boards to a Stop aspect.



5.4.2.6 Double and simple commands

5.4.2.6.1 The commands can be done:

Double command with confirmation (safety related command),
Simple command.

5.4.2.6.2 All safety-related commands shall be done with confirmation.

5.4.2.6.3 Safety related commands shall be at least, but not limited:

Engineering possession,
TSR,
Cancellation of emergency stop,
Section liberation (axle counter reset-restore operation),
Train index modification,
Track condition cancellation (low adhesion, radio hole etc.),
Emergency route release,
Individual management of the objects,
Remote control authorization,
SR, OS and SH mode authorization,
ETCS markerboards unblocked.

5.4.2.6.4 The TSCC Contractor shall define all safety related commands, and the solution put in place in order to manage these commands. Graphical user interface prior to the detailed technical design shall be approved by the Authority.

5.4.2.7 Train Identification (TI)

5.4.2.7.1 The Train Identification function (Ti) shall meet all requirements of the *TAP TSI*.

5.4.2.7.2 Train identifications shall generally be subject to the following characters criteria:

A letter followed by numbers,
A directional arrow is positioned at the beginning or end of the TI as appropriate.

5.4.2.7.3 The TSCC Contractor shall propose the train description rules for the Authority's approval.

5.4.2.7.4 Dynamic TI displays shall be presented on screens and follow the progress of the trains.

5.4.2.7.5 The identification shall be displayed by replacement of a short section of track mimic with the TI at the location concerned, which shall then revert to normal track mimic as the TI moves on.

5.4.2.7.6 The TI function shall be capable of dealing with joining and separation of trains, more than one train occupying a track section etc.



- 5.4.2.7.7 Comprehensive command facilities shall be provided including:
Enter, delete, replace, or modify TIs,
Edit manually and system generated TI,
Search for the location of a specific TI; and
Identify the TI at a specific location.
- 5.4.2.7.8 The TI function shall continue to operate under degraded and/or unusual input conditions:
Train detection system failures (unknown, non-connected trains or train has lost the connection),
Turnout indication failures,
Trains passing End of Authority,
Detection of the incoherence between TD and train running number entered by the driver;
and
Several trains on the same track section.
- 5.4.2.7.9 When the system detects the presence of an unknown or non-connected train, it shall first allocate a system generated identification to the train and then generate a prompt/alarm for the Dispatcher.
- 5.4.2.7.10 The system generated train identification shall be linked to train movement until the Dispatcher responds to the unknown train prompt or otherwise alters the train number.
- 5.4.2.7.11 Where a blocked track becomes occupied, the unidentified train identifier shall be replaced by an appropriate train identification.
- 5.4.2.7.12 Early transfer and display queuing of TIs for approaching trains is required to assist train regulation etc.
- 5.4.2.7.13 At borders with non-equipped sections, if any, or in other areas where trains enter the TMS area, TIs shall be entered manually or automatically via a Timetable Management system with appropriate confirmation by the Dispatcher. Where manual entry is required manual train queue display facilities shall be provided to automate assigning of TIs as trains enter the area.
- 5.4.2.7.14 The train numbers (all equipped with onboard ETCS) shall be displayed on the Workstation's displays and the Video Wall Display next to the marker of the exact train position.
- 5.4.2.8 Time-Distance Graph (TDG)**
- 5.4.2.8.1 The Time-Distance Graph function (TDG) serves as the main user interface for the operation management.
- 5.4.2.8.2 The TDG function presents graphically all train movements controlled by the TMS in real time.
- 5.4.2.8.3 The TDG function shall present all relevant planned data and the real time data for the railway operation.
- 5.4.2.8.4 Planned data shall be retained in the time-distance train graph when modified.
- 5.4.2.8.5 In the TDG seamless scrolling in both directions (time and position axis) shall be possible.



- 5.4.2.8.6 Within the TDG, it shall be possible to indicate/display the area of responsibility.
- 5.4.2.8.7 Within the TDG, the Dispatcher shall have the possibility to switch the indication of the area of responsibility on and off.
- 5.4.2.8.8 Train identifications shall be displayed in the time-distance graph.
- 5.4.2.8.9 The following information shall be displayed as a minimum:
Train progress,
Conflicts (routes, platforms, etc.),
Each type of train identified with dedicated color; and,
Differentiation between the train run and extrapolated path.
- 5.4.2.8.10 Detailed functionality and graphical user interface of TDG function to be proposed by the TSCC Contractor prior to the detailed technical design and approved by the Authority.
- 5.4.2.9 Temporary Speed Restrictions (TSR)**
- 5.4.2.9.1 The TMS shall allow the management of Temporary Speed Restriction (TSR) on the entire CHSR main line to limit the maximum speed allowed by infrastructure.
- 5.4.2.9.2 The TSR function shall allow:
To insert the TSR in the timetable,
Automatic setting of the planned TSR. These shall be submitted to Dispatcher's approval,
TSR manually set by the TMS Dispatcher; and
Modification/Cancelation of the planned TSR.
- 5.4.2.9.3 The Dispatcher shall have the possibility to define, store, re-load, modify and delete TSRs.
- 5.4.2.9.4 The Dispatcher shall have the possibility to define TSR by defining a start and end using operational kilometers (miles) or track section(s).
- 5.4.2.9.5 The cancelation or revocation of the TSR shall be done in a safe way. At least the Dispatcher shall confirm the cancelation of the TSR.
- 5.4.2.9.6 TMS shall support the Dispatcher during the definition of a TSR by entering known information and standard values in related input menus.
- 5.4.2.9.7 The standard values of the TSR shall be predefined for the Dispatcher and be adjustable only by the system administrator.
- 5.4.2.9.8 Within ETCS areas, the TMS shall command the definition and deletion of TSRs to the ETCS and receive from it the acknowledgement/rejection of TSR application.
- 5.4.2.9.9 The Dispatcher shall have the possibility to display all free-defined and pre-defined TSRs including the current status of the TSRs per track, per station, per line, per area.
- 5.4.2.9.10 Within the TMS, it shall be possible to plan the processing of TSRs as tasks within the timetable management (TTM).
- 5.4.2.9.11 TMS shall transmit the defined or re-loaded free-defined TSRs to the relevant Interfaced systems.



- 5.4.2.9.12 The Dispatcher shall have the possibility to activate and deactivate a TSR manually.
- 5.4.2.9.13 Within the TMS, it shall be possible to activate a TSR automatically. These shall be submitted to Dispatcher's approval.
- 5.4.2.9.14 The TSCC Contractor shall propose a method for entering TSR limiting as possible human error.
- 5.4.2.9.15 TSR shall be applied automatically in case of high wind.
- 5.4.2.9.16 The TMS function of the TSR shall be at least SIL2, the definition of the appropriate security level will be the responsibility of the TSCC Contractor.
- 5.4.2.10 Regulation (REG)**
- 5.4.2.10.1 The Regulation function shall automatically compute the real-time schedule of trains and raise an alarm to the Dispatcher in case of critical delays (it shall be possible to configure parameters of the critical delay by the Authority for different types of trains).
- 5.4.2.10.2 The Regulation function shall include the following functions:
- Figure out in real time optimal estimated schedule, including the regulation measures allowing the best operation,
 - Put in place in real time this optimal schedule,
 - Detection of the conflicts at points of convergence,
 - Display to the Dispatcher information as well as the tools allowing them to modify schedule and anticipate any major perturbations.
- 5.4.2.10.3 The Regulation function shall also perform:
- Conflicts resolution between the trains including considering the train priority,
 - Conflicts resolution over single line sections between opposing trains including sections of single line working in respect of booked maintenance work,
 - Departure management of the trains from the stations.
- 5.4.2.10.4 The Regulation function shall detect and display real-time and extrapolated conflicts, including:
- Time-Distance Graph,
 - Traffic regulation alarms displayed on the workstation of the Dispatcher.
- 5.4.2.10.5 The train regulation function shall process the following commands from the Dispatcher:
- Add or remove a train from the regulation process,
 - Assignment of a journey to a train,
 - Enable or disable the traffic regulation alarms,
 - Identification of delays.
- 5.4.2.10.6 The TMS shall identify a train as ahead or delayed in accordance with the timetable when the train is ahead or delayed after departing from a station.
- 5.4.2.10.7 The TMS shall clearly display to the Dispatcher, train identified as ahead or delayed.
- 5.4.2.10.8 The TMS shall be able to display countdown information before train departure.



- 5.4.2.10.9 The ARS function must regulate, at least but preferably better, a competent and experienced Dispatcher.
- 5.4.2.10.10 The system shall resolve all day-to-day regulation conflicts between trains whose route setting is under ARS control.
- 5.4.2.10.11 Calculations must consider all trains affected by a predictable regulation.
- 5.4.2.10.12 Regulation of trains shall be based on the following principles:
- When all trains are running in accordance with the timetable.
 - When running out of course the ARS system must minimize delay to all trains affected (e.g., where two trains are approaching a point of conflict in one direction the delay experienced by the second train as a result of ARS regulation must be factored into the delay calculation).
 - Each train's delay shall be weighted according to priority using an appropriate weighting system.
 - Timetable order shall be maintained where the weighted delays incurred in doing so are minimal.
- 5.4.2.10.13 The Regulation function shall process an updated schedule considering at least the following information:
- Theoretical schedule,
 - Train's location in real time,
 - Train mode information (ETCS mode, etc.).
- 5.4.2.10.14 Infrastructure information (wayside equipment failure, occupied tracks, TSR, ...).
- 5.4.2.10.15 The regulation shall satisfy at least the following objectives:
- Minimum headway,
 - Punctuality,
 - Minimum energy consumption,
 - Minimum client waiting time.
- 5.4.2.10.16 To respect the minimum headway objective, the forecasted optimal schedule shall be as close as possible to the theoretical headway defined for CHSR line. The TSCC Contractor shall define the criteria with their ponderation and parameters allowing them to evaluate this objective.
- 5.4.2.11 Conflict Detection**
- 5.4.2.11.1 The conflict detection function shall forecast the development of railway operation regularly in forecasted interval.
- 5.4.2.11.2 The conflict detection forecast is based at least on the status of the current railway operation, the status of the current resource base and the current operational timetable.
- 5.4.2.11.3 The timeframe used by the conflict detection function shall be adjustable per area by the Dispatcher.
- 5.4.2.11.4 It shall be adjustable by the Authority whether the conflict detection forecast uses the remaining driving time reserves.



- 5.4.2.11.5 The conflict detection function shall detect any conflict along the forecasted railway operation.
- 5.4.2.11.6 At least the following situations shall be detected as conflicts by the conflict detection function:
- Any allocation of a resource to more than one task for a time period exceeding the conflict time threshold,
 - Any allocation of a not appropriate resource to a task for a time period exceeding the conflict time threshold,
 - Any forecasted scheduled train mission exceeding the Deviation time threshold.
- 5.4.2.11.7 The conflict timeframe threshold shall be adjustable by the Dispatcher per area, per resource type and per specific resource.
- 5.4.2.11.8 The Deviation time threshold shall be adjustable by the Dispatcher per area, per train category and per specific train.
- 5.4.2.12 Emergency Stop Management**
- 5.4.2.12.1 The Dispatcher shall have the possibility to issue an emergency stop message via the Signaling System:
- To a train selected by Dispatcher,
 - To several trains selected by the Dispatcher,
 - To all trains within a specific station or line,
 - To all trains within the area of responsibility of Dispatcher/to all lines.
- 5.4.2.12.2 The emergency messages can be conditional or unconditional. In case of conditional emergency stop, the TMS shall wait for signaling feedback and alert the Dispatcher if conditional emergency stop is rejected by the Signaling system.
- 5.4.2.12.3 The command of emergency stops shall be done in a safe way, i.e. such a way that the emergency stop command does not cause damage to the people on the train and the train stops in a safe location (not on the bridge, etc..).
- 5.4.2.13 ETCS Modes and Authorization**
- 5.4.2.13.1 The TMS shall, at least, display the following information:
- RBC-train link state,
 - ETCS mode,
 - Adhesion factor activation (command available for the Dispatcher),
 - MA status,
 - TSR status
- 5.4.2.13.2 The TMS shall be able, at least, to supervise the following train modes:
- Trains running in nominal mode (Full Supervision),
 - On-Sight mode,
 - Staff Responsible mode,
 - Shunting mode (SH, in engineering works areas).
 - Emergency mode (TRIP mode).



Sleeping mode (SL) in case of non-leading cab.

Automatic Driving (AD) mode (GoA2)

Note: For other modes, please refer to *ETCS Technical Specification*.

5.4.2.13.3 The TMS shall also manage "Low Adhesion" areas that alter train braking distance/speed profile in its parameters.

5.4.2.13.4 The Dispatcher shall authorize the Staff Responsible mode (SR) to the driver. This authorization shall be sent to the RBC.

5.4.2.13.5 The TMS shall enable the Dispatcher to authorize the On-Sight mode to the driver if all conditions are satisfied.

5.4.2.13.6 The TMS shall allow the management of the following track conditions:

Adhesion reduced (can be chosen by Dispatcher),

Non-stopping points (information displayed).

5.4.2.14 Temporary Services

5.4.2.14.1 The TMS shall have the possibility to establish temporary services, as follows:

Unavailability of a portion of one or both tracks

Unavailability of one or several stations

Works on the tracks

Restrictions or external events of any kind that reduce temporarily the availability and/or the operating conditions of a portion of one or both tracks

5.4.2.14.2 The temporary services, shall be:

Either predetermined scenario

Or manually defined by the operations personnel upon occurrence

5.4.2.14.3 The temporary services can be of:

Prohibition of trains operation into a specific portion of one or both tracks

Prohibition to authorize trains to stop in a specific station

Speed restrictions

Etc....

5.4.2.15 Automatic Set Up of Operating Restrictions

5.4.2.15.1 The TMS shall have the possibility to establish automatically speed restrictions, upon receipt of alarms from detectors and sensors:

Wind detectors

Hot box detectors (speed restriction, or route cancelations according to the gravity of the alarm)

Flooding detectors

High Temperature detectors

Broken Rail Detection sensors

5.4.2.15.2 The TMS shall have the possibility to cancel routes automatically and close all the corresponding signals, upon receipt of alarms from detectors and sensors:



- Hot boxes detectors (speed restriction, or route cancelations according to the gravity of the alarm)
- Road Vehicle detectors (from bridges)
- Etc...

5.4.2.15.3 The complete list of safety hazards and HDEWS alarms to consider for automatic reaction shall be defined by the TSCC Contractor during detailed design and safety analysis.

5.4.2.16 Human Machine Interface (HMI)

5.4.2.16.1 A line layout allowing an overview of the whole line or sections under Dispatcher's responsibilities as well as detailed pictures shall be available.

5.4.2.16.2 Detailed pictures shall be available to Dispatcher to facilitate the operation and control functions.

5.4.2.16.3 The design of the Overview and Detailed pictures shall be subject to the specific approval of the Authority.

5.4.2.16.4 The arrangements shall be versatile such that it shall be possible for Dispatchers to call up any display on any screen.

5.4.2.16.5 Overview pictures shall contain information consistent with that required to set main routes and effect train regulation including at least, in correct geographical relationship:

Geographical track layout together with major geographical features including stations, viaducts etc.,

Names of all operational points (stations, stopping points, junctions, crossovers, etc.),

Marker boards together with marker board identity,

Route status indication,

Track section status,

Turnout status and position,

Block occupation and status indications,

Train description for all trains in the area of control,

Timetable deviation,

Temporary speed restriction,

Engineering possession (working area) status,

Shunting area status,

Local operation status,

HDEWS equipment status.

HMI ergonomics studies and human factors shall be studied according to *ISO 11064*.

5.4.2.16.6 The best international practices shall be applied and considered in the relevant design for space utilization.

5.4.2.16.7 The TSCC Contractor shall perform detailed ergonomic studies dealing with the following aspects:

Workstations and furniture,

Best strategy for information display on Dispatcher's workstations,



Working environment and OCC adjustment**Dispatcher workload (Human Factors)**

- 5.4.2.16.8 The results of the studies shall be submitted to the Authority. The comments and suggestions shall be incorporated in the design up to the final approval of ergonomic studies.
- 5.4.2.16.9 HMI interactions shall be object oriented.
- 5.4.2.16.10 The HMI interaction shall also be possible via menu-based interaction or typing of commands.
- 5.4.2.16.11 The following HMI view types shall, at least, be implemented:
- Main menu
 - Specific menu adapted to context (will be detailed during design stage)
 - Box and list views
 - Distance-time graph
 - Schematic track layout
 - Administration view
 - Task management view
 - Infrastructure view for engineering possessions management
 - Alarms and events dedicated displays
- 5.4.2.16.12 The Dispatcher shall have the possibility to call HMI object related help and explanatory information for any HMI object directly in relation to that HMI object.
- 5.4.2.16.13 The information to be displayed in any HMI view shall depend on the TMS role and area of responsibility of the Dispatcher.
- 5.4.2.16.14 The structure of Main menus and sub-menus shall be adjustable by HMI configuration per HMI view type.
- 5.4.2.16.15 For every HMI object a specific menu should become available when selecting the HMI object.
- 5.4.2.16.16 The menu shall be placed in such a way that no vital information is hidden.
- 5.4.2.16.17 HMI shall ensure that for display of all text, alarms, indications, menu and other written information are displayed in English.

5.4.3 Analysis Tools to Improve and Optimize the Operations**5.4.3.1 Archiving and Reporting**

- 5.4.3.1.1 The TMS shall provide an Archiving function allowing data to be recorded and stored for a period of at least 60 months.
- 5.4.3.1.2 The Archiving system shall be easily extended.
- 5.4.3.1.3 It shall be possible to replace a storage unit during the operation with no impact on the operation and Dispatcher's work.



- 5.4.3.1.4 The recorded data shall allow:
Reports edition,
Secure files transfer via external telecommunication network or media, and
Report printing.
- 5.4.3.1.5 The TMS shall provide tools to improve and optimize day-to-day operations.
- 5.4.3.1.6 The TMS shall provide a record function for all relevant data, at least for the following functions:
Playback,
Juridical data recording,
Statistics.
- 5.4.3.1.7 The Juridical recorded data shall be also available in a separate standalone JRU (Juridical Recording Unit) for a minimum of 90 days, or a longer period if required by the Code of Federal Regulations (CFRs).
- 5.4.3.2 Simulator and Training**
- 5.4.3.2.1 The TMS shall provide a TMS training mode.
- 5.4.3.2.2 Training mode shall include:
playback of recorded situations,
a simulator with simulated environment including signaling, train movements and TMS interfaces.
- 5.4.3.2.3 The TMS shall provide a simulation environment to validate any change of the timetable, simulate different scenarios of train delays.
- 5.4.3.2.4 The TMS shall allow the use of the recorded occurrences in the network to be analyzed and to simulate possible resolution scenarios.
- 5.4.3.2.5 Within the TMS training system, it shall be possible to carry out several training sessions at the same time.
- 5.4.3.2.6 A dedicated workstation shall be provided for the Trainer.
- 5.4.3.2.7 During the training mode playback of recorded situation, it shall be possible to adjust the playback speed.
- 5.4.3.2.8 The TMS simulator shall be able to allow programmed scenarios.
- 5.4.3.2.9 The trainer shall have the possibility to use recorded operational situations to define new simulation scenarios using the scenario editor.
- 5.4.3.2.10 The trainer shall have the possibility to modify existing scenarios using the scenario editor.
- 5.4.3.2.11 The trainer shall have the possibility to simulate a real timetable within the training mode of the simulator.
- 5.4.3.2.12 The simulation module shall be further detailed and included during project design.

5.4.4 Alarms



5.4.4.1 Alarms general requirements

- 5.4.4.1.1 Alarms and events shall be displayed and timestamped.
- 5.4.4.1.2 The TSCC Contractor shall design TMS alarms in accordance with *EN/ISO 62682 standard*.
- 5.4.4.1.3 All alarm indications shall be flashing when requiring immediate attention and steady if less urgent attention is necessary.
- 5.4.4.1.4 The alarm attributes shall be at least:
 - the type: Operational or Synthesis,
 - the severity: emergency, alert, critical, error, warning, notice, info, debug,
 - the origin subsystem(s): PIDS, ...
 - the recipient: OCC Supervisor, Dispatcher ... They are the responsible users intended to react/respond to the alarm occurrence.
- 5.4.4.1.5 The TSCC Contractor shall submit alarm management and design to the Authority for approval.

5.4.4.2 Alarm Type

- 5.4.4.2.1 The following alarm types shall be at least managed by the TMS:
 - Operational alarms are alarms that potentially impact the service,
 - Synthetic alarms correspond to the subset of maintenance alarms.
- 5.4.4.2.2 The qualifications of alarms as Operational and Synthesis shall be done by the TSCC Contractor and submitted to the Authority for approval.

5.4.4.3 Alarm Management

- 5.4.4.3.1 The TSCC Contractor shall provide an alarm management function including alarm routing for the subsystems interfaced with the TMS.
- 5.4.4.3.2 Alarm management should be designed in such a way that TMS Dispatcher's workload is never exceeded.
- 5.4.4.3.3 There shall be an alarms priority ladder to avoid wrong execution of Dispatcher's actions on the TMS system.

5.4.5 User Management (UM)

- 5.4.5.1 The TMS shall provide a centralized User Right Management function for each area of responsibility. Within the TMS, the user right management function centralizes user management for all functions.
- 5.4.5.2 The User Right Management function shall be based on the differentiation between TMS roles, areas of responsibilities and the TMS user:
 - A TMS role is a specific set of interaction rights and information access rights within TMS, independently from a real TMS user and an area of responsibility.
 - An area of responsibility defines the area where a TMS user can execute the assigned TMS role(s).
 - A TMS user is a specific Dispatcher, for whom an account has been created. Within the TMS User Right Management function, a specific user must be assigned to one or several TMS roles and to one or several areas of responsibility. When logging into TMS the user takes over the assigned TMS role(s) and area(s) of responsibility.



- 5.4.5.3 Within User Right Management, the number of managed TMS roles, users, areas of responsibilities and combinations of these shall not be limited.
- 5.4.5.4 The User Right Management function shall allow predefining some TMS configurations which are used frequently (for example day, night, facilities controlled locally or by OCC, etc.).
- 5.4.5.5 The Administrator shall have the possibility to define and manage TMS roles independently from specific users and areas of responsibility of the Authority.
- 5.4.5.6 The Administrator shall have the possibility to define and manage roles at least along the following dimensions:
 - Availability of functions,
 - Access to information,
 - Availability of communication channels,
 - Availability of HMI types.
- 5.4.5.7 The Administrator shall be, at least, able to manage a role through the following actions:
 - Create a role,
 - Delete a role,
 - Modify a role,
 - Replace existing role by another role,
 - Copy a role,
 - Suspend a role.
- 5.4.5.8 The Administrator shall be, at least, able to manage a user and its rights through the following actions:
 - Create a user,
 - Delete a user,
 - Modify a user,
 - Assign a user to one or several areas of responsibility,
 - Re-assign a user to one or several areas of responsibility,
 - Copy an existing user.
- 5.4.5.9 The User Right Management function shall ensure that only known users can login.
- 5.4.5.10 All personal data of the users shall be secured against unauthorized access inside TMS and outside TMS.
- 5.4.5.11 Every user who is logged in to TMS shall be identified unambiguously.
- 5.4.5.12 Every user who logged in to TMS is only assigned to TMS role(s) defined for that specific user.
- 5.4.5.13 Every user logged in to TMS shall be able to interact in its assigned area of responsibility and role.
- 5.4.5.14 The change of users through the Log off from the previous user and the Log in of the succeeding user on the same HMI shall be possible without closing any window and without interruption of operation.
- 5.4.5.15 Any area and role necessary for operation are covered by users logged in at any time during the operation.
- 5.4.5.16 An alarm shall be raised in case an area and/or a role is not covered by a user.



- 5.4.5.17 Area of responsibility means the area that a user/Dispatcher is controlling or operating in the scope of his TMS role when logged in.
- 5.4.5.18 The Administrator shall have the opportunity to assign areas of responsibility to two or more users performing the same role at the same time.
- 5.4.5.19 The controlled area is assigned completely at least one user for every role required at any time.

5.4.6 Video Wall Display (VWD)

- 5.4.6.1 The TSCC Contractor shall supply, install, configure, and test a large Video Wall Display (VWD) system in the OCC. Installation, configuration and testing shall be coordinated with the Authority.
- 5.4.6.2 The VWD system shall be built up by the arrangement of a sufficient number of display screens to be consistent with operational requirements.
- 5.4.6.3 The VWD system shall also include the necessary equipment (server, video cards, ...) to receive, manage and display different video streams from different sources.
- 5.4.6.4 The VWD system shall be sufficient in size and shall be positioned within the control room so that the displayed details can be clearly seen, and textual details are legible from any of the workstations in the control room.
- 5.4.6.5 The VWD system shall include dedicated software for the management of the system.
- 5.4.6.6 The following details shall be on constant display but not limited to:
 - The track layout of the entire network, including the trainset maintenance facility,
 - All stabling areas,
 - The trains running currently on the network and their movements (direction),
 - The train identification and operating mode of each train,
 - The routes set,
 - The track sections with imposed temporary speed restriction,
 - Engineering possessions,
 - Temporary speed restrictions,
 - Traction Power Supply status,
 - The day of the week and the date in dd-mm-yyyy format,
 - The accurate time in 24-hour mode and in hh:mm:ss format.
- 5.4.6.7 The VWD system shall have the ability to display any desired image and the ability to configure the amount and placement of images on the screen. The ability to change shall be flexible and simple.
- 5.4.6.8 The TMS shall provide input for displaying Main Line panoramic images such that they are independently standalone from TMS. When the dispatcher or the Yard Controller zooms in or zooms out the TMS HMI on their own workstation, the Main Line TMS overview being shown on the panoramic display shall still show the status of the whole Main Line.
- 5.4.6.9 In addition to the constant display, it shall be possible to display CCTV images on the VWD.
- 5.4.6.10 The TSCC Contractor shall coordinate with the TCS subsystems for connection rights and video streams access.



5.5 Engineering Possessions Functional Requirements

- 5.5.1 The TMS shall help the Dispatcher in the management of engineering possession (section(s) of track) to ensure the safety of staff and protection of equipment when working within the engineering possession (Working Area). This function shall allow:
- Automatic setting of engineering possession (planned). These are submitted to the Regulator's approval,
 - Engineering possession manually set by the Dispatcher from the OCC or the maintenance staff on-site,
 - Definition of the Working Area.
- 5.5.2 The TSCC Contractor shall propose a solution as described in requirement 4.3.2
- 5.5.3 The engineering possession function shall enable exclusion from operations of a part of the railway network or a single element of it (i.e. section of the track, any specific turnout).
- 5.5.4 The timetable management shall allow the planning of the engineering possessions.
- 5.5.5 The Regulator shall have the possibility to activate and deactivate an engineering possession manually.
- 5.5.6 In case an engineering possession extends over more than one area of responsibility, TMS shall ensure the correct split of the engineering possessions between these areas of responsibility and transmit it to Interlocking.
- 5.5.7 The engineering possession management shall be done in a safe way (especially engineering possessions cancellation). The verifications shall be implemented in order to check the validity of orders received. If the Dispatcher chooses the forbidden or invalid possession, the TMS shall block forbidden or incoherent actions, alert the Dispatcher and suggest valid available engineering possessions.
- 5.5.8 The TSCC Contractor shall describe and implement features enabling safe management of Engineering possessions, in manual mode and in planning mode. Engineering possession management shall be submitted to the Authority for approval.
- 5.5.9 The TMS shall treat the engineering possession as activated / deactivated only after receiving the status information of the activation / deactivation of the engineering possession from the Signaling System.
- 5.5.10 The TMS shall report the current status of the engineering possession to the relevant Interfaced systems for further distribution to all relevant stakeholders after receiving the status report of the activation / deactivation of the engineering possession from the Signaling System.
- 5.5.11 The TMS shall automatically update the train route setting conditions according to activated / deactivated engineering possessions.
- 5.5.12 In case a catenary switch-on is planned related to an engineering possession, a task request shall be raised to the Power SCADA System or to the TPS Operator to switch-on the catenary after the engineering possession is deactivated.
- 5.5.13 In case a catenary switch-off is planned related to an engineering possession, the activation of that engineering possession shall only be processed when the catenary switch off is reported by the Power SCADA system or by the TPS Operator to the Dispatcher for the catenary sections concerned.
- 5.5.14 The TSCC Contractor shall define its solution for the management of engineering possessions and catenary protections, including at least:



- Mapping specification of engineering possession vs catenary protections (and vice versa).
- Specification of the management function for engineering possessions vs catenary protections (including sequence diagrams).

These specifications will be submitted to the Authority for approval.

- 5.5.15 The commands sent from the TMS to the Signaling System for blocking and unblocking of an engineering possession or for activation and deactivation of a planned engineering possession shall be processed independently in the TMS.
- 5.5.16 Engineering possessions and catenary protections shall be displayed on TMS HMIs and Time-Distance Graph.

5.6 Traction Power and Electrical Protection Requirements

- 5.6.1 Even though the control and command of the traction power will be handled by another system (TPS), TMS shall have an interface with the Power SCADA System.
- 5.6.2 TMS HMI shall give the possibility to the Dispatcher to visualize and acknowledge the energized and non-energized track portions.
- 5.6.3 The TMS shall prevent a Dispatcher establishing a route, should part or all of this route not be energized. Should the Operator attempt to establish a route along a non-energized portion of track, the TMS shall reject the route and emit a sound and visual alarm.
- 5.6.4 The establishment of routes along non-energized track portions shall however be possible following double confirmation.

5.7 Local Facilities (LF)

- 5.7.1 This section provides general information, assumptions, and requirements on TMS principles in the Local Facilities.
- 5.7.2 The TSCC Contractor shall provide a Local TMS control system for the following facilities: LMF (Light Maintenance Facility), HMF (Heavy Maintenance Facility) and MOWF (Maintenance of Ways Facility). Each facility will have its own dispatcher(s).
- 5.7.3 Within previous facilities, the TMS control system shall at least allow:
- Display of TCS trackside equipment status and alarms (routes, signals, track sections, axle counter, turnouts, etc.)
 - Control of routes,
 - Local management of the exchange tracks,
 - Shunting train composition activities where needed.
- 5.7.4 The TSCC Contractor shall provide a Local TMS workstation for each facility.
- 5.7.5 The Local TMS control system of facilities shall at least interface with:
- Interlocking managing the facilities,
 - Main Line TMS.
- 5.7.6 Depending on the proposed solution for the track configuration and the operational needs, the exchange tracks shall either be managed by the main line TMS or the local TMS control system.



Note: Dedicated tracks separating the main line from facilities shall enable any train movement from the main line to the facilities and from the facilities to the main line.

Those tracks are called “exchange tracks”.

5.7.7 Modification of track configuration and/or operation in facilities operated locally shall not affect the main line TMS configuration and logic.

Note: There shall be segregated data and configuration between main line and the facilities ensuring software integrity / no re-validation and no safety re-demonstration of main line when changing facilities data.

5.8 Performance Requirements

5.8.1 The performance targets and performance requirements of the TMS are closely related to line performance and capacity.

5.8.2 The performance targets definition shall be based on the following assumptions:

- TMS is working in normal operating mode.
- TMS and all its components are working properly.
- Established operating rules and procedures allow the headways defined in the performance targets.
- The performance of the trains operating on the line is compatible with the headways defined by the performance targets.

5.8.3 The TMS shall be able to manage trains running at a maximum operational speed up to 355 km/h (220 mph).

5.8.4 It is required that once a control is initiated by the Regulator that the field equipment receives command and responds to it with minimum delay. The maximum time between activation of a command at the TMS workstation and the interlocking responding shall be lower than 500 ms.

5.8.5 The TMS shall have sufficient processing capacity to process, record and store all necessary information.

5.8.6 The maximum initialization time (from the power on and till the system allowing the Dispatcher to send a command) shall be lower than five (5) minutes.

5.8.7 When a new graphic picture is called up for display on a color screen, the response time from the finish of the entry of the command requesting the display until the conclusion of the drawing of the display, including all data items, must not exceed 4 seconds. Where several pictures are called simultaneously, then the maximum response must not be greater than 8 seconds for five (5) displays. These displays may be either identical or different in content.

5.8.8 Where text Information is called, the screen shall start writing within 2 seconds from the entry of the command and be completed with a screen containing 1000 characters including blanks in not more than 4 seconds. Again, multiple screen requests are possible, and this shall be such that all screens complete writing within 8 seconds.

5.8.9 Safety requirements

5.8.10 The TMS system shall comply with the safety requirements defined in the *System Safety Plan*.

5.8.11 The TSCC Contractor shall demonstrate that their proposal is a safe reliable and proven technical solution used on operated HSR program for at least 5 years without any issues.



5.8.12 RAM Requirements

5.8.13 The TMS system shall comply with the RAM requirements defined in the Schedule 1.

5.9 Security and Cybersecurity Requirements

5.9.1 The TMS system shall be in full compliance with CHSR cybersecurity controls specified in Technical Specifications for Cybersecurity.

5.9.2 The TMS shall conform to federal, state, and local governing rules, requirements, and regulations.

5.9.3 A System Owner shall be nominated for the TMS, the System Owner shall be accountable for cybersecurity risk ownership and mitigation.

5.9.4 The System Owner shall ensure that appropriate resources are in attendance during threat modelling and risk assessment activities.

5.9.5 User Access control roles defined in the TMS shall be mapped to roles in the centralized directory services, this solution shall be co-engineered with the Cybersecurity Lead and Cybersecurity Services Lead, as defined in the CHSR Cybersecurity Technical Specification and be compliant with the identity, access management, and authentication controls defined in the specification.

5.9.6 Interfaces with other systems shall be authenticated and use secure protocols as defined in the Cybersecurity Specification.

5.9.7 All remote access and inbound or outbound connectivity with systems on the internet or in an IT network (such as a cloud-based EAMS), must comply with the requirements outlined in the Cybersecurity Specification.



6 INTERFACE REQUIREMENTS

6.1 General Requirements

6.1.1 The interfaces are classified as following:

- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR TSCC Contractors)
- External interfaces: interface between TSCC systems and systems provided by CHSR contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors)
- Internal Interfaces: Interfaces between systems within the TSCC scope

6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.

6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.

6.2 External Interfaces – facilities contractor

6.2.1 The TSCC Contractor shall install all TMS equipment in the OCC and facilities being provided by the facilities contractor.

6.2.2 The TSCC Contractor shall provide to the facilities contractor:

- Equipment dimensions
- Equipment clearances requirements
- Equipment mounting and fixings requirements
- Cable routes/containment requirements
- Equipment loadings
- Installation and maintenance requirements
- Equipment heating loads
- Equipment cooling loads
- Equipment hydraulic requirements

6.2.3 To be provided by facilities contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:

- Room dimensions and layouts
- Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
- Room raised floor system
- Delivery access routes.
- Maintenance access routes

6.3 Internal Interfaces

6.3.1 Interface with Power SCADA System

6.3.1.1 The TMS shall interface with the Power SCADA System.

6.3.1.2 This interface shall be realized at a central level through a redundant connection to the Digital Communication Network (DCN).



- 6.3.1.3 The TMS shall receive from Power SCADA System at least the following status for operational purposes:

Electrical status of catenary sections,
Limited traction power capacity (emergency mode of operation).
Catenary protections requesting engineering possessions to be set by the TMS

- 6.3.1.4 The TMS shall send to Power SCADA System at least the following information:

Train follow-up information (trains' Ids and location),
The status of engineering possessions when catenary protection for maintenance purposes is requested by Power SCADA System.

6.3.2 Interface with ETCS

- 6.3.2.1 The interface with the RBC shall be realized at a central level through a redundant connection to the Digital Communication Network (DCN).

- 6.3.2.2 The interface with RBC shall respect the ERTMS specification Baseline defined in the contract.

- 6.3.2.3 Note: The SCI-CC interface specification of EULYNX is currently used to interface TMS with CBI; it may also be used to interface RBC to TMS for some specific functions.

- 6.3.2.4 TMS shall be interfaced with the RBC to exchange the following information:

- Movement Authorities,
- ERTMS Train modes,
- Text message,
- Train running numbers, position and speed,
- RBC equipment status, alarms, and events,
- Temporary Speed Restriction (TSR),
- Low Adhesion Factor activation.

6.3.3 Interface with Interlocking (IXL)

- 6.3.3.1 The TMS interface with the IXL shall be realized at a central level through a redundant connection to the Digital Communication Network (DCN).

- 6.3.3.2 The TMS shall enable the control of the 171Miles Early Operating Segment (EOS) of CHSR Merced – Bakersfield.

- 6.3.3.3 The TMS shall interface by means of EULYNX standard communication protocol (RaSTA) and application layer (SCI-CC) with the IXL system.

- 6.3.3.4 The EULYNX Baseline Set 4 Release 4 shall be applicable for this interface.

- 6.3.3.5 The TMS shall be interfaced with the IXL, at least, to exchange the following information:

Route setting,
Trackside equipment monitoring and control (when needed),
IXL and TMS status, alarms, and events,
Temporary Shunting Area (TSA).

6.3.4 Interface with FRMCS

- 6.3.4.1 TMS shall interface FRMCS to manage the assignment of voice talk group communication according to Area of Responsibility boundaries.



6.3.5 Interface with ICSS

- 6.3.5.1 The TSCC Contractor shall provide a TMS interface with ICSS.
- 6.3.5.2 The interface with ICSS shall be realized at central level through a redundant connection to the Digital Communication Network (DCN).
- 6.3.5.3 ICSS alarms and statuses (only the ones that are necessary for the Dispatcher) shall be routed to the TMS. Depending on the contractor solution, the following alarms may be included:
 - Rail temperature monitoring system alarms.
 - Broken rail detection system alarms.
 - Alarms related to flood monitoring system.
- 6.3.5.4 The TSCC Contractor shall provide status and alarm list to the Authority for approval.

6.3.6 Interface with DCN

- 6.3.7 The TMS interface with the Digital Communication Network (DCN) shall be achieved through a redundant connection.
- 6.3.8 As the Digital Communication Network (DCN) is the main TMS communication link with its interfaces, it shall be designed to offer optimum bandwidth to the TMS.

6.3.9 Interface with Network Timing System (NMS)

- 6.3.9.1 The TMS interface with the NMS shall be realized at central level through the Digital Communication Network (DCN).
- 6.3.9.2 The NMS shall provide the TMS with time reference allowing TMS equipment to be synchronized with all TCS systems.

6.3.10 Interface with Public Address and Customer Information System (PACIS)

- 6.3.10.1 The TMS shall be interfaced with the PACIS to automatically update traffic information (e.g., arrival times, departure times, destinations, etc.) displayed at platforms and stations).
- 6.3.10.2 The TMS shall be interfaced with the PAS to automatically update traffic information (e.g., train arrival, train departure, delay, etc.) for audio messages played at platforms and stations.

6.3.11 Interface with EAMS

- 6.3.11.1 The TMS shall interface with the EAMS.
- 6.3.11.2 This interface shall be realized at a central level through a redundant connection to the Digital Communication Network (DCN).
- 6.3.11.3 The TMS shall send the status of engineering possessions, information on incidents and delays.
- 6.3.11.4 The TMS shall provide static Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.

6.3.12 Interface with Hazard Detection and Early Warning System (HDEWS)

- 6.3.12.1 The TMS shall interface with the HDEWS.
- 6.3.12.2 This interface shall be realized at a central level through a redundant connection to the Digital Communication Network (DCN).
- 6.3.12.3 Through this interface, the TMS receives operational alarms coming from all the HDEWS detectors.



6.3.12.4 The TMS shall monitor, at least, the following information:

- Connection status to each subsystem,
- HDEWS alarms.

6.3.12.5 **Interface with Low Voltage Power System (LVPS)**

6.3.12.6 The TMS shall be interfaced with LVPS system for power supply.

6.3.12.7 The TMS shall be connected to LVPS as an Emergency Load.

6.3.12.8 In case of nominal power outage, the LVPS shall be able to supply power to The TMS equipment for at least 12 hours.



7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 TMS Workstation

- 7.1.1 The number of Dispatcher's Workstations shall be confirmed by the TSCC Contractor according to the operational needs defined by the Authority.
- 7.1.2 Workstation position arrangements shall employ fully integrated systems with the minimum number of Operator interface units, displays, Keyboards etc. consistent with efficient operation of all systems and facilities.
- 7.1.3 Ergonomic studies shall be performed by the TSCC Contractor to organize Dispatcher workstations and HMI. These studies shall be submitted to the Authority for approval.
- 7.1.4 The operation of the TMS shall enable the signaling system to be controlled and operated in any combination of stations.
- 7.1.5 The workstation centralized units shall be located in the technical room of OCC to reduce the noise in the control room.

7.2 Servers

- 7.2.1 The TMS shall be provided with central servers in the OCC configured for Non interrupted service.
- 7.2.2 The TMS servers' cabinets shall be designed in a way to simplify the maintenance.
- 7.2.3 The server architecture shall allow centralized architecture of the whole TMS and dimensioning of the system (RAM, telecommunication network etc.) considering the used applications.
- 7.2.4 The administrator shall be able to request the switch off or reinitialization of the servers of TMS:
 - From each workstation,
 - Maintenance workstation.
- 7.2.5 Server's reinitialization shall be imperceptible by the operation, it shall not cause:
 - Any display interruption,
 - Any communication loose (commands, requests and verification/validation process shall still be continuous without any interruption).

7.3 Redundancy Requirements

- 7.3.1 The redundancy of the servers located in the OCC shall be of "hot standby" type.
- 7.3.2 The physical destruction of one server shall not affect the operation of the CHSR line.
- 7.3.3 All TMS configurations and data shall be retrievable even upon destruction of one server.

7.4 EMC Requirements

- 7.4.1 The TMS and associated electrical and electronic devices shall be designed to the requirements defined in the *EN 50121-4 standard (Rail Applications - Electromagnetic Compatibility - Part 4: Emission and Immunity of Signalling and Telecommunications apparatus)*.
- 7.4.2 All equipment shall be provided with its own electromagnetic interference free enclosure where necessary to ensure correct operation and avoid permanent degradation.



8 TOLERANCES

Not applicable to Traffic Management System.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.2 General requirements related to the TSCC Contractor Scope of Work are in the Scope of Work.

9.3 Specific Requirements

9.3.1 The TMS scope of supply and delivery shall include (not limited to):

- Servers.
- Workstations/Displays /HMI's.
- Video Wall Display.
- Cabling, connectors, switches/patch panels.
- Racks.
- Software architecture including full specification of protocols used.
- SW licenses.
- Maintenance tools.
- Any necessary supporting structures for TMS.
- To consider test configuration to be delivered:
 - for Authority's testing purposes and
 - for Authority's training purpose
- Any auxiliary elements needed for TMS.
- Training.
- As-built documentation.
- List of parts and components.
- Spare parts.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.



12 TESTING & ACCEPTANCE

12.1 General Requirements

12.1.1 General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.

12.2 Specific Requirements

12.2.1 The TSCC Contractor shall develop a simulated environment to conduct all tests that can be performed using the simulated environment for the equipment and interfaces, before the on-site testing phase. The main goals are as follows:

- Test the TMS functionalities,
- Integrate TMS with TSCC subsystems CBI, RBC, PACIS, etc.,
- Test of the EULYNX interfaces,
- Test operational scenarios,
- Redundancy and robustness test,

12.2.2 The TMS simulation environment(s) shall confirm that the Operational Principles are fully implemented on the prototypes, and this implementation complies with the expected behavior.

12.2.3 The TSCC Contractor shall propose and fulfil a set of functional and operational tests that comply with all the functionality of CHSR signaling principles. These tests scenario shall be accepted by the Authority.



13 SUBMITTALS

13.1 General Requirements

13.1.1 The submittals required for the Interlocking system are defined in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor and related Suppliers, information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence TMS system reliability, availability and maintainability characteristics.

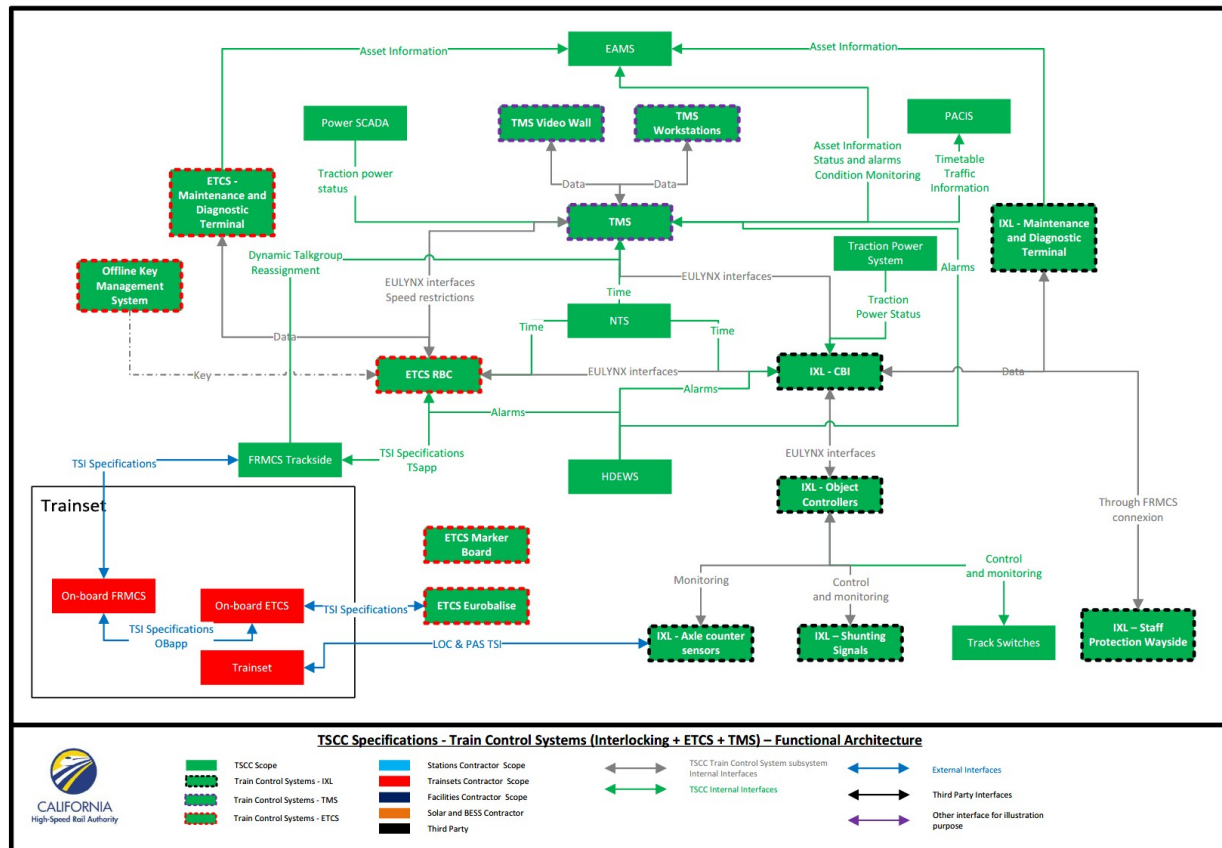


16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.

APPENDIX A TO EXHIBIT 5(Q) TRAFFIC MANAGEMENT SYSTEM (TMS)



Schedule 5(r)

Wireless Communication System (WCS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0022 – Wireless Communication Systems (WCS)

Rev. 1.0

Authored:

A handwritten signature in black ink, appearing to read "Nick Ashby".

Nick Ashby, Wireless Systems Lead

12/22/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Thomas Newey".

Thomas Newey, Telecoms Lead

12/22/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Bruno Comperat".

Bruno Comperat, Deputy Director of Rail Engineering

12/23/2025

Date

Approved:

A handwritten signature in blue ink, appearing to read "Ryan Scott".

Ryan Scott, Director of Rail Engineering

12/23/2025

Date

Released:

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Amit Joshi, Configuration Manager

12/23/2025

Date



Document Revision History – WCS Specifications**Second Edition****December 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition
1.0	December 2025	Second edition for Addendum 2



TABLE OF CONTENT

1	INTRODUCTION	5
1.1	SCOPE OF THE TECHNICAL SPECIFICATION.....	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.1	GENERAL	6
2.2	DESIGN GUIDELINES.....	6
2.3	TECHNICAL SPECIFICATIONS FOR INTEROPERABILITY	6
2.4	STANDARDS	6
2.5	UIC SPECIFICATIONS	11
2.6	OTHER DOCUMENTS	11
3	TERMS AND DEFINITIONS	13
3.1	GENERAL	13
4	SYSTEM DESCRIPTION	14
4.1	BACKGROUND	14
4.2	PURPOSE OF WIRELESS COMMUNICATION SYSTEMS.....	14
4.3	DEFINITION OF WIRELESS COMMUNICATION SYSTEMS.....	15
4.4	OPERATIONAL CONTEXT	16
4.5	DESIGN LIFE	17
5	SYSTEM REQUIREMENTS.....	17
5.1	GENERAL REQUIREMENTS.....	17
5.2	ENVIRONMENTAL REQUIREMENTS.....	24
5.3	OPERATIONAL REQUIREMENTS	26
5.4	FUNCTIONAL REQUIREMENTS.....	29
5.5	PERFORMANCE REQUIREMENTS.....	41
5.6	SECURITY AND CYBERSECURITY REQUIREMENTS.....	44
6	INTERFACE REQUIREMENTS	48
6.1	GENERAL REQUIREMENTS.....	48
6.2	THIRD PARTY INTERFACES	48
6.3	EXTERNAL INTERFACES - TRAINSETS.....	50
6.4	EXTERNAL INTERFACES – STATIONS CONTRACTOR	50
6.5	EXTERNAL INTERFACES – FACILITIES CONTRACTOR	51
6.6	INTERNAL INTERFACES	51
7	MATERIAL, PRODUCT AND COMPONENT REQUIREMENTS.....	54
7.1	GENERAL REQUIREMENTS.....	54
7.2	SOFTWARE AND HARDWARE REQUIREMENTS	54
7.3	RADIO SITE PREPARATION REQUIREMENTS.....	54
7.4	RADIO TOWER REQUIREMENTS	55
7.5	RF EXPOSURE REQUIREMENTS.....	55
8	TOLERANCES	57
9	SCOPE OF SUPPLY AND DELIVERY	58
9.1	GENERAL REQUIREMENTS.....	58



9.2	SPECIFIC REQUIREMENTS	58
10	MANUFACTURING	60
10.1	GENERAL REQUIREMENTS.....	60
11	INSTALLATION AND INTEGRATION.....	61
11.1	GENERAL REQUIREMENTS.....	61
12	TESTING & ACCEPTANCE	62
12.1	GENERAL REQUIREMENTS.....	62
12.2	SPECIFIC REQUIREMENTS FOR FRMCS	62
12.3	SPECIFIC REQUIREMENTS FOR ETCS	64
12.4	SPECIFIC REQUIREMENTS FOR PWS	64
13	SUBMITTALS.....	67
13.1	GENERAL REQUIREMENTS.....	67
14	QUALITY MANAGEMENT	68
14.1	GENERAL REQUIREMENTS.....	68
15	ADDITIONAL INFORMATION REQUESTED	69
15.1	GENERAL REQUIREMENTS.....	69
16	LOGISTICS	70
16.1	GENERAL REQUIREMENTS.....	70



1 INTRODUCTION

1.1 Scope of the Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Wireless Communication Systems, hereinafter: WCS.
- 1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.
- 1.1.3 The functional architecture of the WCS is presented in Appendix A of this specification.
- 1.1.4 The requirements are formulated using the following words and their meanings:
 - **"Shall"**: Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure).
 - **"Should"**: Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents.
 - **"Must"**: Indicates an obligation or a mandatory requirement.
 - **"May"**: Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

- 2.1.1 The TSCC Contractor shall apply the in-force standards, guidelines and specifications provided in this technical specification for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning, training, operations and maintenance.
- 2.1.2 All generic standards to be used are provided in: Technical Contract Requirements.

2.2 Design Guidelines

- 2.2.1 The latest version of the following Design Guidelines shall be applied:

No	Code	Title
[R2]	DCM_01	Design Criteria Manual Chapter 1: Overview
[R3]	DCM_12	Design Criteria Manual Chapter 12: Communication Systems and Train Control
[R4]	AREMA_17	AREMA Standards Chapter 17 – High-Speed Rail Systems
[R5]	DCM_12	Design Criteria Manual Chapter 26: Roadways and Site Works
[R6]	DCM_2	Design Criteria Manual, Chapter 2: Basis of Design
[R7]	DCM_35	Design Criteria Manual, Chapter 35: Environmental
[R8]	DCM_07	Design Criteria Manual, Chapter 7: Electromagnetic Compatibility

TABLE 66 : DESIGN GUIDELINES AND PROCEDURES.

2.3 Technical Specifications for Interoperability

- 2.3.1 The applicable Technical Specifications for Interoperability (TSIs) are listed below:

No	TSI	Title
[R9]	CCS TSI	COMMISSION IMPLEMENTING REGULATION (EU) 2023/1695 of 10 August 2023 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union and repealing Regulation (EU) 2016/919

TABLE 67 : LIST OF TSI AND REGULATIONS.

2.4 Standards

- 2.4.1 The relevant standards to be used for WCS are listed below.
- 2.4.2 The TSCC Contractor shall fully consider and apply the following standards.

No	Standard	Title
[R10]	ADA Section 307	Americans with Disabilities Act (ADA) Standards for Accessible Design, Section 307 – Protruding Objects
[R11]	NFPA 101	National Fire Protection Association (NFPA), 101: Life Safety Code



No	Standard	Title
[R12]	CBC Section 11B-404.2.3	2019 California Building Code (CBC), Chapter 11B, 11B-404.2.3 – Clear Width (Doorways)
[R13]	NFPA 1225	National Fire Protection Association (NFPA), 1225: Standard for Emergency Services Communications
[R14]	CFC S510	California Fire Code Section 510 – Emergency Responder Radio Coverage in Buildings
[R15]	IEC 60529	International Electrotechnical Commission (IEC), 60529: Degrees of protection provided by enclosures (IP Code)
[R16]	IEC 60068	International Electrotechnical Commission (IEC), 60068: Environmental Testing
[R17]	EN 50164-3	European Norm (EN), 50164-3: Lightning Protection Components (LPC) – Part 3: Requirements for Isolating Spark Gaps
[R18]	IEC 61643	International Electrotechnical Commission (IEC), 61643: Low-voltage surge protective devices
[R19]	IEC 60715	International Electrotechnical Commission (IEC), 60715: Dimensions of Low-Voltage Switchgear and Controlgear – Standard Mounting Rails for Mechanical Support of Electrical Devices
[R20]	EN 62305	European Norm (EN), 62305: Protection Against Lightning
[R21]	NFPA 780	National Fire Protection Association (NFPA), 780: Lightning Protection Standard
[R22]	EN 50121-5	European Norm (EN), 50121-5: Railway Applications – Electromagnetic Compatibility – Part 5: Emission and Immunity of Fixed Power Supply Installations
[R23]	EN 55024	European Norm (EN), 55024: Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement
[R24]	EN 300386	European Norm (EN), 300386: Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunications network equipment; Electromagnetic compatibility requirements
[R25]	EN 50122-1	European Norm (EN), 50122-1: Railway Applications – Fixed Installations – Electrical Safety, Earthing and the Return Circuit – Part 1: Protective Provisions against Electric Shock
[R26]	EN 61000-6-2	European Norm (EN), 61000-6-2: Electromagnetic Compatibility (EMC) – Part 6-2: Generic Standards – Immunity for Industrial Environments
[R27]	EN 61000-6-4	European Norm (EN), 61000-6-4: Electromagnetic Compatibility (EMC) – Part 6-4: Emission Standard for Industrial Environments
[R28]	IEC 61000-3-6	International Electrotechnical Commission (IEC), 61000-3-6: Electromagnetic Compatibility (EMC) – Part 3-6: Limitation of Emission of Harmonic Currents in Medium and High Voltage Power Systems
[R29]	IEC 61000-3-7	International Electrotechnical Commission (IEC), 61000-3-7: Electromagnetic Compatibility (EMC) – Part 3-7: Limits – Assessment of Emission Limits for Fluctuating Loads in MV and HV Power Systems



No	Standard	Title
[R30]	IEC 61000-5-2	International Electrotechnical Commission (IEC), 61000-5-2: Electromagnetic Compatibility (EMC) – Part 5-2: Installation and Mitigation Guidelines – Earthing and Cabling
[R31]	EN 50121-3-2	European Norm (EN), 50121-3-2: Railway Applications – Electromagnetic Compatibility – Part 3-2: Rolling Stock – Apparatus
[R32]	EN 50121-4	European Norm (EN), 50121-4: Railway Applications – Electromagnetic Compatibility – Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus
[R33]	EN 1991-1-4	European Norm (EN), 1991-1-4: Eurocode 1 – Actions on Structures – Part 1-4: General Actions – Wind Actions
[R34]	EN 50126	European Norm (EN), 50126: Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
[R35]	EN 50128	European Norm (EN), 50128: Railway Applications – Communication, Signalling and Processing Systems – Software for Railway Control and Protection Systems
[R36]	EN 50129	European Norm (EN), 50129: Railway Applications – Communication, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling
[R37]	3GPP TS 22.179	3 rd Generation Project Partnership (3GPP), Technical Specification 22.179: Service Requirements for the Future Railway Mobile Communication System (FRMCS)
[R38]	ETSI TR 103 459	European Telecommunications Standards Institute (ETSI), Technical Reference: 103 459 “System Reference Document - Future Railway Mobile Communication System (FRMCS)
[R39]	ISO/IEC 27001	International Standards Organization (ISO) / International Electrotechnical Commission (IEC), 27001: Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements
[R40]	NIST SP 800-53	National Institute of Standards and Technology (NIST), Special Publication 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations
[R41]	IEC 62443-2-4	International Electrotechnical Commission (IEC), 62443-2-4: Security for Industrial Automation and Control Systems – Part 2-4: Requirements for IACS Solution Suppliers
[R42]	IEC 62351	International Electrotechnical Commission (IEC), 62351: Power Systems Management and Associated Information Exchange – Data and Communications Security
[R43]	EN 50125-3	European Norm (EN), 50125-3: Railway applications - Environmental conditions for equipment - Part 3: Equipment for signaling and telecommunications
[R44]	eCPRI	eCPRI Specification Group, Enhanced Common Public Radio Interface
[R45]	IEEE 1914.3	Institute of Electrical and Electronics Engineers (IEEE) 1914.3: Standard for Radio over Ethernet (RoE) Encapsulations and Mappings
[R46]	EN 50159	European Norm (EN), 50159: Railway Applications – Communication, Signalling and Processing Systems – Safety-related Communication in Transmission Systems



No	Standard	Title
[R47]	3GPP TS 23.379	3 rd Generation Project Partnership (3GPP), Technical Specification 23.379: Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2
[R48]	3GPP TS 23.282	3 rd Generation Project Partnership (3GPP), Technical Specification 23.282: Functional architecture and information flows to support Mission Critical Data (MCDData)
[R49]	3GPP TS 23.281	3 rd Generation Project Partnership (3GPP), Technical Specification 23.281: Functional architecture and information flows to support Mission Critical Video (MCVideo)
[R50]	3GPP TS 23.283	3 rd Generation Project Partnership (3GPP), Technical Specification 23.283: Mission Critical Communication Interworking with Land Mobile Radio Systems
[R51]	IEC 61508	International Electrotechnical Commission (IEC), 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
[R52]	IEEE 802.11be	Institute of Electrical and Electronics Engineers (IEEE), 802.11be: Extremely High Throughput (aka "Wi-Fi7")
[R53]	3GPP TS 23.228	3 rd Generation Project Partnership (3GPP), Technical Specification 23.228: IP Multimedia Subsystem (IMS); Stage 2
[R54]	3GPP TS 24.302	3 rd Generation Project Partnership (3GPP), Technical Specification 24.302: Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3
[R55]	3GPP TS 24.229	3 rd Generation Project Partnership (3GPP), Technical Specification 24.229: IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
[R56]	3GPP TS 33.402	3 rd Generation Project Partnership (3GPP), Technical Specification 33.402: 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses
[R57]	IETF RFC 6442	Internet Engineering Task Force (IETF), Request for Comments (RFC) 6442: Location Configuration Information for GEOPRIV
[R58]	3GPP TS 23.167	3 rd Generation Project Partnership (3GPP), Technical Specification 23.167: IP Multimedia Subsystem (IMS) emergency sessions
[R59]	3GPP TS 23.179	3 rd Generation Project Partnership (3GPP), Technical Specification 23.179: Functional architecture and information flows to support mission critical communication services; Stage 2
[R60]	3GPP TS 23.203	3 rd Generation Project Partnership (3GPP), Technical Specification 23.203: Policy and charging control architecture
[R61]	3GPP TS 22.280	3 rd Generation Project Partnership (3GPP), Technical Specification 22.280: Mission Critical Services Common Requirements (MCCoRe); Stage 1
[R62]	3GPP TR 36.942	3 rd Generation Project Partnership (3GPP), Technical Report 36.942: Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (RF) system scenarios
[R63]	ITU-R P.1238	International Telecommunication Union Radiocommunication Standardization Sector (ITU-R) P.1238: Propagation data and prediction methods for the planning of indoor



No	Standard	Title
		radiocommunication systems and radio local area networks in the frequency range 300 MHz to 450 GHz
[R64]	ITU-R P.1812	International Telecommunication Union Radiocommunication Standardization Sector (ITU-R) P.1812: A path-specific propagation prediction method for point-to-area terrestrial services in the frequency range 30 MHz to 6 GHz
[R65]	3GPP TS 28.313	3rd Generation Project Partnership (3GPP), Technical Specification 28.313: Management and orchestration; Self-Organizing Networks (SON) for 5G networks
[R66]	NFPA 70	National Fire Protection Association (NFPA), 70: National Electrical Code
[R67]	47 CFR §1.1307	Title 47 of the Code of Federal Regulations (CFR), §1.1307: Environmental Considerations — Actions that May Have a Significant Environmental Effect, for Which Environmental Assessments (EAs) Must Be Prepared
[R68]	47 CFR §1.1310	Title 47 of the Code of Federal Regulations (CFR), §1.1310: Radiofrequency Radiation Exposure Limits
[R69]	ANSI/IEEE C95.1	American National Standards Institute (ANSI) / Institute of Electrical and Electronics Engineers (IEEE), C95.1: Standard for Safety Levels with Respect to Human Exposure to Electric, Magnetic, and Electromagnetic Fields, 0 Hz to 300 GHz
[R70]	IEC 60297	International Electrotechnical Commission (IEC), 60297: Mechanical structures for electronic equipment – Dimensions of mechanical structures of the 482.6 mm (19 in) series.
[R71]	3GPP TS 23.501	3rd Generation Project Partnership (3GPP), Technical Specification 23.501: System architecture for the 5G System (5GS)
[R72]	3GPP TS 23.503	3rd Generation Project Partnership (3GPP), Technical Specification 23.503: Policy and Charging Control Framework
[R73]	3GPP TS 26.114	3rd Generation Project Partnership (3GPP), Technical Specification 26.114: IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction
[R74]	3GPP TS 26.116	3rd Generation Project Partnership (3GPP), Technical Specification 26.116: Speech and audio coding; Performance characterization of speech and audio codecs
[R75]	EN 50701	European Norm (EN), 50701: Railway applications – Cybersecurity.
[R76]	TIA-102	Telecommunications Industry Association (TIA), 102: Project 25 (P25) Land Mobile Radio Communications
[R77]	IEEE 1588	Institute of Electrical and Electronics Engineers (IEEE), 1588: Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
[R78]	EN 14067-4	European Norm (EN), 14067: Railway applications – Aerodynamics, Part 4: Requirements and test procedures for aerodynamics on open track

TABLE 68 : LIST OF APPLICABLE STANDARDS.

2.5 UIC Specifications

No	Version	Title
[R79]	v2.0.0 (Dec-24)	FRMCS Functional Requirements Specification
[R80]	v2.0.0 (Dec-24)	FRMCS System Requirements Specification
[R81]	v2.0.0 (Dec-24)	FRMCS Telecom On-Board Architecture (TOBA) Functional Requirements Specification
[R82]	v2.0.0 (Dec-24)	FRMCS Functional Interface Specification
[R83]	v2.0.0 (Dec-24)	FRMCS Form-Fit-Functional Interface Specification

TABLE 69 : LIST OF APPLICABLE UIC SPECIFICATIONS.

2.6 Other Documents

2.6.1 The following documents shall be referred to:

No	Document	Title
[R84]	Schedule 16	Scope of Work
[R85]	Schedule 5	Digital Communication Network Technical Specification
[R86]	Schedule 5	Medium Voltage and Low Voltage Power Systems Technical Specification
[R87]	Schedule 5	Network Timing System Technical Specification
[R88]	Schedule 5	Cybersecurity Technical Specification
[R89]	Schedule 5	Telephony System Technical Specification
[R90]	Schedule 5	ETCS Technical Specification
[R91]	Schedule 5	CCTV Technical Specification
[R92]	Schedule 5	Electronic Access and Control System Technical Specification
[R93]	Schedule 5	Integrated Control and Supervision System Technical Specification
[R94]	Schedule 5	Public Address and Customer Information System Technical Specification
[R95]	-	<i>PPDR Rugged Handheld Device for heavy use v1.0 Whitepaper</i> , NCCOM
[R96]	Schedule 3	Safety, Security and RAM Requirements
[R97]	PLAN-1022 (Rev00, Apr-25)	Interface Management Plan
[R98]	DD-SY-Set	DD-SY-011 TSCC Sites Typical Configuration
[R99]	COPPA	Children's Online Privacy Protection Act (US Federal Act)



No	Document	Title
[R100]	CCPA	California Consumer Privacy Act
[R101]	CalECPA	California Electronic Communications Privacy Act
[R102]	RoHS Directive	Restriction of Hazardous Substances in Electrical and Electronic Equipment

TABLE 70 : OTHER REFERENCE DOCUMENTS.

3 TERMS AND DEFINITIONS

3.1 General

- 3.1.1 All the terms, definitions, and abbreviations are provided in the Glossary of Terms, Abbreviations and Definitions.



4 SYSTEM DESCRIPTION

4.1 Background

Note to reader: This Background section provides contextual information to provide clarity when reading this Specification. While this information is documented elsewhere in the train control and telecommunications specifications, it is important to reiterate these principles the WCS are built upon.

- 4.1.1 This Technical Specification (*this Specification*) provides the TSCC Contractor with the required information to design and construct the WCS on infrastructure that forms the CHSR System (*the System*).
- 4.1.2 The Authority requires WCS to be capable of supporting mission-critical high-speed rail operations, business-critical operational functions, as well as non-critical services for passenger comfort and connectivity.

Criticality Level	Description	Examples	Failure Consequence
Mission-critical	Essential for safe and continuous train operations	Train control radio, SIL4 signaling, interlocking systems	Cessation of network-wide operations. Major passenger disruptions. Immediate reputational and revenue impact. Requires activation of contingency or recovery plans.
Business-critical	Potentially impacts revenue or customer service	Ticketing, CCTV, Passenger Information System	Delays or degradation in service delivery. Major inconvenience to passengers or staff. Timely resolution is required to prevent reputational and revenue impact.
Non-critical	No impact on safety or operations	Passenger Wi-Fi, Infotainment, Digital advertising displays	Minor inconvenience. No impact on train movement or safety.

TABLE 20 : DESCRIPTION AND EXAMPLES OF CRITICALITY LEVELS.

- 4.1.3 The Authority shall utilize the European Train Control System (ETCS) Level 2 without signals to provide Movement Authority to trainsets on the CHSR right-of-way.
- 4.1.4 This ETCS system shall utilize FRMCS to provide voice and data communication between trainsets and wayside equipment.
- 4.1.5 The Authority shall utilize a dedicated telecommunication systems comprising of an IP-based Digital Communications Network (DCN), fiber optic network, wireless communication systems as well as multiple systems used to provide management, oversight and control of the Authority's infrastructure. The systems will be connected via a fiber optic backbone cabling system along the Right-of-Way interconnecting all wayside systems, stations, facilities and the Operational Control center (OCC).
- 4.1.6 The CHSR OCC will be located at Fresno.

4.2 Purpose of Wireless Communication Systems

- 4.2.1 The purpose of the WCS is to provide secure voice, data and video communications in a high-speed rail environment:
- 4.2.2 To and from the following user groups:
- Engineers, Operators, Drivers;
 - Conductors;
 - Attendants, Crew, Staff;
 - Ticket Inspectors / Revenue Protection Officers;
 - Transit Security / California Highway Patrol;
 - Controllers, Dispatchers, Managers;



- Cleaning & Service Crew;
- Maintenance & Incident Response Crews;
- Emergency Responders, Emergency Response Coordinator;
- Passengers;
- Any other persons authorized to perform work in the CHSR System;
- Other Californian railroad operators;
- Automated wireless and wireline systems.

4.2.3 At or within the following locations:

- Trainsets;
- Station Complexes;
- Control Centers;
- Wayside Shelters / Cabinets;
- Traction Power Facilities;
- Stabling Yards;
- Maintenance Facilities;
- Right-of-Way;
- Designated Emergency Evacuation Areas;
- Any other area where wireless communications can be reasonably expected.

4.2.4 Between fixed and handheld devices, and to access internet, telephony, and corporate and operational networks.

4.2.5 The Authority reserves the right to include additional user groups and locations that can be reasonably expected to be considered part of the CHSR System or required to integrate and/or interoperate with the CHSR System.

4.3 Definition of Wireless Communication Systems

4.3.1 The WCS shall consist of separate subsystems which provide both common and unique capabilities. The WCS subsystems are:

- Future Radio Mobile Communication System;
- Emergency Responder Communication System;
- Passenger Wi-Fi System.

4.3.2 The TSCC Contractor shall be responsible for all components, systems, interfaces, and activities necessary to fully design, deliver, integrate, test, and operationalize the WCS to the standard required for high-speed rail operations and for CHSR to enter revenue service.

This includes, but is not limited to design, procurement, sourcing, supply, construction, installation, configuration, integration, verification, validation, training, documentation, operations, maintenance and handover of all WCS subsystems, in accordance with the requirements of this and other technical specifications, and subject to acceptance by the Authority.

4.3.3 Future Radio Mobile Communication System

4.3.3.1 The Future Radio Mobile Communication System (FRMCS) provides mission-critical voice and data communication between all operational user groups and operational locations across the rail network.

4.3.3.2 The FRMCS ensures that communications essential to the safe and efficient operation of CHSR are maintained under normal, degraded, and emergency conditions, enabling safe train movement, coordination, and response during all possible scenarios, and to mitigate operational disruptions.



4.3.4 **Emergency Responder Communication System**

- 4.3.4.1 The Emergency Responder Communication System (ERCS) enables OCC personnel to interoperate with Emergency Responders via non-public network communications.

4.3.5 **Passenger Wi-Fi System**

- 4.3.5.1 The Passenger Wi-Fi System (PWS) is a non-critical subsystem of the WCS that provides a seamless, reliable, secure, high-capacity, and high-speed wireless internet service accessible to passengers via their personal devices.
- 4.3.5.2 The purpose of the PWS is to allow authorized passengers to access the internet for work and entertainment purposes in a safe and secure manner from personal digital devices with Wi-Fi capabilities during their journey.

4.4 **Operational Context**

- 4.4.1 The Wireless Communications Systems (WCS) shall be used operationally by various user groups to support high-speed rail operations, and by passengers during their journey.
- 4.4.2 The WCS FRMCS shall be able to be utilized from any location within the CHSR System.
- 4.4.3 All designs shall include provisions for the future expansion of the WCS, beyond the EOS, towards San Francisco, Los Angeles, and Sacramento without substantial re-work and with minimal impact on the operational infrastructure.
- 4.4.4 The WCS shall be designed and constructed to meet the requirements of the FCS system capacity of 1-2 trains per hour in each direction.
- 4.4.5 The WCS shall be designed to meet the requirements of the final CHSR service capacity of 12 trains per hour in each direction.
- 4.4.6 The WCS shall maintain reliable and continuous service performance at train speeds of up to 220mph (354 km/h).
- 4.4.7 The WCS shall support a diverse set of operational use cases including but not limited to:
- Real-time communication between train crews, station staff and train controllers / dispatchers;
 - Emergency response coordination;
 - Maintenance coordination;
 - Trackside condition monitoring;
 - Onboard diagnostics and condition monitoring;
 - Passenger entertainment and communication services.
- 4.4.8 The WCS FRMCS shall provide communication services to mobile users (e.g., train drivers, onboard staff, field maintenance crews), fixed users (e.g., signalers, OCC personnel, security staff), and automated systems. The FRMCS shall ensure consistent coverage, availability, and service quality across the full extent of all the facilities that make up the FCS of the CHSR System (*the System*).
- 4.4.9 The WCS shall enable seamless interoperability between user groups, and automated systems, supporting the exchange of voice, data, and control signals as required for safe and efficient CHSR operations.
- The WCS shall enable the OCC personnel to perform the centralized coordination, supervision, and control of all rail operations across the CHSR System.
- 4.4.10 To support these functions, the OCC shall utilize WCS Dispatch Consoles, which shall provide authorized personnel with integrated, full featured, real-time access to Mission-Critical, and emergency communications across all WCS subsystems.



- 4.4.11 The WCS shall support positive CHSR customer satisfaction by enabling the reliable operation of systems that contribute to on-time train performance and functioning passenger facilities. This includes, but is not limited to:
- Providing communication support for systems involved in train control, diagnostics, and fault reporting to minimize service disruptions;
 - Ensuring consistent operation of passenger-facing services such as onboard Wi-Fi, information displays, and station connectivity;
 - Facilitating timely communication between staff, OCC, and maintenance teams to support proactive issue resolution and service recovery.
- 4.4.12 The WCS shall enable interoperability between CHSR user groups and third-party user group networks, such as Emergency Responders and other Railroad Operators (e.g., Caltrain, BNSF, Amtrak, LA Metro and Brightline West).
- 4.4.13 The WCS shall be operated, maintained, and supported in accordance with the operational procedures, rules, and protocols defined by the Authority.

The TSCC Contractor shall ensure that all operational modes, fault management workflows, change control processes, and access protocols for the WCS are fully aligned with the Authority's documented procedures and operational governance framework.

No deviations from these procedures shall be permitted without prior written approval from the Authority.

4.5 Design Life

- 4.5.1 The Design Life requirements of the WCS shall be 30 years.
- 4.5.2 The TSCC Contractor shall provide an equipment lifecycle plan demonstrating how all WCS components will be maintained to meet the specified design life.
- 4.5.3 The TSCC Contractor shall ensure WCS components with shorter design lifespans (e.g., fixed and mobile devices, computing hardware, etc.) shall be managed by scheduled technology refresh strategies and spares management plans.
- 4.5.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce, supply and support WCS components, or provide replacements with equal or compatible technical specifications, for the entire lifetime required.

5 SYSTEM REQUIREMENTS

5.1 General Requirements

- 5.1.1 The WCS shall be designed in accordance with the requirements described in this specification, other relevant documents listed in Section 2 of this specification, other CHSR technical specifications and the full CHSR documentation. In the event of any conflict between these documents, the requirements of this specification shall take precedence.
- 5.1.2 The WCS shall provide secure voice, data and video communication between user groups, locations and network as described in 4.2.1.

WCS Subsystems

- 5.1.3 The WCS shall comprise multiple subsystems that deliver both shared and subsystem-specific capabilities. These include:
- Future Mobile Radio Communication System (FMRCS);
 - Emergency Responder Communication System (ERCS);
 - Passenger Wi-Fi System (PWS).



- 5.1.4 The TSCC Contractor may propose subsystem implementations using separate or combined communication systems, including shared use of wireless technologies (e.g., 4G, 5G, mmWave, Wi-Fi, P25, proprietary) or infrastructure components (e.g., towers, shelters, backhaul, or radio access nodes). The proposal may include alternative delivery or commercial models, such as Public-Private Partnerships or X-as-a-Service, provided all criticality, technical, operational, and compliance requirements are fully satisfied.
- 5.1.5 Where WCS subsystems are integrated or share infrastructure, the most stringent or mission-critical requirement applicable to any individual subsystem shall govern the combined solution. The TSCC Contractor shall clearly identify shared elements, justify compliance with all relevant subsystem requirements, and demonstrate that no degradation in performance, safety, or reliability will occur.

Note to reader: The Authority encourages innovative system architectures that minimize physical infrastructure and environmental footprint, provided they maintain the independence, integrity, and availability expected of each WCS subsystem's criticality level.

Radio Frequency Spectrum

- 5.1.6 The TSCC Contractor may utilize the Authority's owned 'Upper 700MHz Block A Guard Band' spectrum (757–758 MHz uplink / 787–788 MHz downlink) across the entire geographical area of the Los Angeles to San Francisco CHSR Right-of-Way.

Note to reader: The Authority acknowledges that this spectrum is not ideally suited to meet the requirements of WCS. The Authority encourages innovative spectrum strategies and active network sharing architectures (e.g., MORAN, MOCN, roaming, MVNO, FirstNet) that minimize the need for exclusive spectrum holdings and reduce overall spectrum use, provided they maintain the independence, integrity, and availability expected of each WCS subsystem in accordance with its criticality level.

- 5.1.7 The TSCC Contractor shall be responsible for the identification, acquisition, and ongoing cost of any additional radio frequency spectrum required to satisfy the technical, operational, and regulatory requirements of the WCS subsystems.
- 5.1.8 All licenses or spectrum usage rights acquired by the TSCC Contractor for the purpose of delivering WCS services shall be transferred or assigned to the Authority upon commissioning, in accordance with applicable regulatory and licensing conditions.

Design, Construct, Operate & Maintain

- 5.1.9 The design and implementation of the WCS shall incorporate provisions for future expansion to support additional project stages, increased system capacity, and evolving operational requirements. This shall include allowances for physical space, power, network connectivity, core network capacity, software scalability, and licensing. The WCS shall constitute a system that is scalable for future growth and capacity expansion. Software licensing models shall be scalable to accommodate future increases in user numbers, trainset numbers, service frequency, functional modules, and integration with new subsystems, without requiring re-procurement or significant system reconfiguration.
- 5.1.10 The TSCC Contractor's scope shall include all phases of the WCS including design, source, supply, construct, deploy, install, integrate, test, commission and maintenance to operate a seamless, reliable and secure WCS to support the CHSR System.

Backhaul and Fronthaul

- 5.1.11 The TSCC Contractor **shall** utilize the optical fiber infrastructure and the associated Digital Communications Network (DCN) for all inter-site connectivity between CHSR locations. Refer to Digital Communications Network Technical Specification.
- 5.1.12 The use of this existing optic fiber and IP-based DCN shall apply to WCS subsystems requiring backhaul, fronthaul, interconnection, or integration across stations, control centers, equipment shelters, and other designated facilities, unless otherwise approved by the Authority.



- 5.1.13 The TSCC Contractor shall utilize the existing optical fiber infrastructure where it is possible to provide fronthaul, and where not possible it shall install drop-off (distribution) optic fiber between splice closures and radio transmitters. Splice closures may need to be installed at locations where optic fiber coils have been placed.
- 5.1.14 Each WCS subsystem backhaul and fronthaul should operate independently but must not interfere with the operation or performance of any other subsystem. Where applicable, shared infrastructure (e.g. antenna systems, cabling) must support multi-service use with defined quality-of-service parameters.

Accessibility

- 5.1.15 All WCS equipment, enclosures, and associated cabling shall be installed so as not to obstruct pedestrian passageways, emergency egress routes, or required access paths to doors, equipment cabinets, or panels. Equipment shall not protrude into accessible routes in violation of ADA Section 307, and sufficient space shall be maintained to ensure door clearances conform to NFPA 101 (Section 7.2.1.5.3) and CBC Section 11B-404.2.3. All installations shall preserve the clear width and height requirements as defined by NFPA, ADA, and CBC standards for safety and accessibility.
- 5.1.16 Where additional access roads are required, the TSCC Contractor shall design these access roads to WCS equipment shelters in accordance with the requirements set out in Design Criteria Manual, Chapter 26 Roadways and Site Works. Refer to drawing set DD-SY-Set [R97] for typical site layouts.

Low Voltage Power Supply

- 5.1.17 All fixed WCS subsystem locations shall be powered by the Low Voltage Power System (LVPS). This requirement applies to all non-trainset and non-OCC WCS infrastructure. Refer to Medium Voltage and Low Voltage Power Supply Technical Specification.
- 5.1.18 All WCS subsystems installed at the OCC shall be powered from the facility's critical power infrastructure, which shall include uninterruptible power supply (UPS) systems and standby generators, to ensure continuous operation during mains power disruptions. Refer to Medium Voltage and Low Voltage Power Supply Technical Specification.
- 5.1.19 All WCS core network equipment at the OCC shall use Dual Power Supply Architecture with A-plane and B-plane redundant power supply.

Future Mobile Radio Communication System

- 5.1.19.1 The Future Mobile Radio Communication System (FRMCS) shall provide mission-critical voice communications primarily between trainset engineers and controllers / dispatchers in the OCC and secondarily be utilized by other operational user groups, as well as mission-critical data communications (e.g., ETCS) between trainset onboard train control equipment and the train control system controlling equipment at the OCC throughout the CHSR System.
- 5.1.19.2 The FRMCS shall ensure that communications are maintained under normal, degraded, and emergency conditions, enabling safe train movement, coordination, and response during all scenarios.
- 5.1.19.3 The TSCC Contractor shall design, source, construct, integration test and commissioning, provide training, operate, maintain and warranty all required radio transmission sites to deliver continuous and reliable FRMCS coverage throughout the CHSR System, including stations, tunnels, aerial structures, trenches, at-grade corridors, viaducts and operational facilities, in accordance with the defined coverage and performance requirements.

Note to reader: The EOS (Merced to Bakersfield) segment does not have any tunnels but does have trenches. It can be assumed that viaducts near residential areas will have noise walls (aka 'sound walls') – The specifics are under development. The contractor must request the latest information from the Authority before starting detailed design. It is the contractor's responsibility to take these items into consideration during radio network planning.

- 5.1.19.4 The FRMCS shall be designed for high availability with appropriate redundancy, fault-tolerant components, and self-healing network capabilities to support uninterrupted service delivery, suitable for high-speed rail operations.



- 5.1.19.5 The TSCC Contractor shall provide a FRMCS compliance report to the Authority that details compliance against Mandatory and Optional requirements from the current version of UIC FRMCS specifications, as per Section 2.5.
- 5.1.19.6 The TSCC Contractor shall ensure that all components of the FRMCS are upgraded to achieve full compliance with the finalized FRMCS standards within five (5) years of their formal ratification and publication by the UIC and associated 3GPP specifications. The TSCC Contractor shall monitor the development of the FRMCS standards and submit a compliance report, including compliance roadmap, for approval by the Authority within twelve (12) months of FRMCS standards ratification.
- 5.1.19.7 The TSCC Contractor shall design and supply an FRMCS that is fully software upgradable, such that no hardware replacement will be required to achieve full compliance with the finalized FRMCS standards once they are formally ratified.
- 5.1.19.8 The TSCC Contractor shall provide a FRMCS that consists of 5G Radio Access Network (RAN), geographically redundant 5G Standalone / FRMCS / MCX Core Network, Inter-Working Function (IWF), Dispatch Consoles, Compact Dispatch Consoles, handheld devices, Network Management System (NMS), NMS workstations, integration with other systems, all required software and licensing.
- 5.1.19.9 The FRMCS 5G RAN shall include all components required for operational FRMCS service, including but not limited to, such as:
- Equipment shelters, cabinets, and sun shelters for housing RAN infrastructure;
 - Equipment accommodation support services such as internal power distribution, climate control, fire protection, lighting, electronic access and physical security provisions;
 - Conduit extensions to the accommodation from existing pits, manholes, duct banks, and towers to support fiber, power, and RF cabling;
 - Optic fiber extensions, hauling and splicing, to provide backhaul and fronthaul;
 - Towers, foundations, cableways, antenna platform, earthing, bonding, antennas, feeders, jumpers, and associated cabling for the deployment of the FRMCS radio equipment;
 - All required FRMCS RF equipment, transmission equipment (e.g., switches, routers, multiplexers), and telepower systems including rectifiers, batteries, DC distribution, alarming and power monitoring components;
 - Supporting infrastructure like racking and cableways for other TSCC systems required (e.g., FPS, CCTV, EACS, DCN, LVPS, NTS).
- 5.1.19.10 The FRMCS 5G RAN base stations shall be connected to a 5G Standalone (SA) Core Network infrastructure, which includes all core network functions and IP Multimedia Subsystem, to enable full support for FRMCS-compliant mission-critical features and performance capabilities, as defined by 3GPP and UIC specifications (refer to section 2.5).
- 5.1.19.11 The FRMCS 5G Standalone (SA) Core Network architecture shall utilize a cloud-native, containerized, and orchestrated Service-Based Architecture, supporting Network Function Virtualization (NFV) principles. The architecture shall support all 5G Core Network Functions and their interactions, including authentication, security, session and mobility management, and service provisioning, in accordance with 3GPP specifications. This architecture will ensure the FRMCS core network is scalable, resilient, portable, and automatable.
- 5.1.19.12 The FRMCS core infrastructure shall comprise a primary and a secondary 5G Core Network, including FRMCS core network elements, each located at geographically separate sites to provide fault tolerance and service continuity. The system design shall ensure seamless, uninterrupted FRMCS service in the event of a failure or outage at either core location, with no loss of service, session drops, or degradation during automatic core switching. The primary and secondary 5G Core Networks shall be interconnected via standardized 3GPP interfaces.
- 5.1.19.13 The FRMCS shall be designed with no single point of failure and shall implement an active-active redundancy architecture. All critical network elements - including core functions, transport, and access



components - shall operate in parallel and independent instances capable of load sharing and seamless failover.

- 5.1.19.14 The FRMCS primary core infrastructure shall be located within the communications room of the OCC.
- 5.1.19.15 The FRMCS secondary core infrastructure shall be located at a California State Government data center, as approved, or otherwise agreed, by the Authority.
- 5.1.19.16 The FRMCS may utilize passive and active network sharing arrangements with Mobile Network Operators (Cellular Carriers), including neutral host, MOCN, and MORAN infrastructure sharing.

Note to reader: *The Authority welcomes innovative solutions that leverage existing infrastructure and alternate commercial delivery models (e.g., Public Private Partnerships, X-as-a-Service), while meeting their business requirements for a high availability train control system that is suitable for high-speed rail operations.*

- 5.1.19.17 The Trainset contractor shall be responsible for the sourcing of trainset radios, but the TSCC Contractor will provide all required information and be jointly responsible for system performance. Refer to Section 6.3 External Interfaces - Trainsets for details of interface and demarcation of responsibilities.

Fixed and Mobile Devices

- 5.1.19.18 The TSCC Contractor shall provide a range of FRMCS compatible fixed and mobile handheld device options suitable to the operational requirements of the CHSR operational user groups.
- 5.1.19.19 The TSCC Contractor shall provide FRMCS handheld devices that "PPDR Rugged Handheld Device for heavy use v1.0" NCCOM whitepaper.
- 5.1.19.20 The TSCC Contractor shall draft and submit a fixed and mobile device catalogue that outlines which devices and accessories are designated for which user groups and user roles for the Authority's approval. The TSCC Contractor shall provide a 'demonstration day' where all catalogue items are able to be tested to assist the Authority to determine which items are best fit for operations.
- 5.1.19.21 The TSCC Contractor shall provide FRMCS ruggedized handheld devices, with accessories, belt holders, remote speaker microphones, multi-bay chargers, single chargers, spare batteries, etc.
- 5.1.19.22 The TSCC Contractor shall provide a sample of each type of FRMCS device and accessories to the Authority for testing and approval.
- 5.1.19.23 The Authority reserves the right to initiate a fixed and mobile device 'true-up' process to reconcile proposed device models, configurations, and quantities with evolving operational requirements. This may include substituting device types, adjusting order volumes, or rebalancing allocations between fixed and mobile devices. The TSCC Contractor shall accommodate such changes without delay and shall update pricing, delivery schedules, and inventory records accordingly. Any financial adjustments resulting from the true-up shall be reflected in the subsequent invoicing cycle, subject to mutual agreement.
- 5.1.19.24 While in-trainset (inside trainset) handheld FRMCS coverage from terrestrial radio sites is excluded from the scope, the business requirement for wireless handheld voice communication between the train driver and onboard crew remains. The TSCC Contractor shall propose and implement a suitable solution to meet this requirement, subject to approval by the Authority (e.g., Wi-Fi, repeater, direct radio-to-radio simplex, etc.).

Network Planning

- 5.1.19.25 The TSCC Contractor shall perform FRMCS radio network planning, including propagation modelling and candidate site evaluation, to determine optimal locations for radio sites along the CHSR Right-of-Way.
- 5.1.19.26 As part of the radio network planning exercise, the TSCC Contractor shall include ETCS RBC boundary limit analysis. The TSCC Contractor shall demonstrate how the radio site locations have



been selected to avoid FRMCS radio handover in the ETCS RBC/RBC boundary areas along the CHSR Right-of-Way.

- 5.1.19.27 The TSCC Contractor's design shall detail the site evaluation and selection process used to determine optimal locations for radio sites.
- 5.1.19.28 FRMCS radio sites shall be located within the CHSR Right-of-Way by default but can be within the CHSR System.

Note to Reader: *Radio site locations shall be prioritized, with stations being the first preference, then signaling equipment rooms, Traction Power locations, BBU Hotel locations, before/after viaducts/trenches, etc. It is intended that radio sites be placed at the end of station platforms, but there may be instances where other locations could be considered (e.g., car parks).*

- 5.1.19.29 The final number, location, and configuration of FRMCS radio sites shall be determined through the TSCC Contractor's detailed radio propagation study. This study shall account for local topography, land use, coverage, and factors like accessibility, power and backhaul, structural suitability, safety and compliance, environmental factors, security, hazards, co-location and interference, future expandability, and total cost of ownership.
- 5.1.19.30 The TSCC Contractor shall draft and submit FRMCS Concept Design and Coverage Study to the Authority for review and approval prior to detailed design and deployment. The Coverage Design shall demonstrate how the operational and performance requirements are met.

Note to reader: *The network design should demonstrate the CHSR operational and performance requirements can be met by the FRMCS network designs. E.g., Appropriate network architecture for the railway traffic control communication and ETCS needs along the track.*

5.1.20 Dispatch Consoles

- 5.1.20.1 The WCS Dispatch Consoles shall support the operational needs of OCC personnel, managers, supervisors, dispatchers and train controllers responsible for the safe and efficient management of train operations, and coordination and control of train movements across the CHSR System.
- 5.1.20.2 The WCS shall support, and the TSCC Contractor shall provide, two types of dispatch consoles to meet the differing operational needs across the rail network:
- Dispatch Console: The Dispatch Console shall be a full-feature, fixed-location dispatch console intended for use within the OCC. It shall support the complete range of WCS functionality, including voice group management, priority call handling, call recording, incident coordination, and integration with other operational systems.
 - Compact Dispatch Console (CDC): The CDC shall be a lightweight, cost-effective, and portable console designed for use by field personnel or secondary user groups such as maintenance teams, emergency coordinators, or station supervisors. It shall provide essential dispatch functionality with support for FRMCS connectivity, group voice communication, user presence/status monitoring, and basic call management. The CDC may be implemented as a tablet-based or compact form-factor solution with a simplified user interface suitable for mobile and semi-fixed deployment in non-OCC facilities.
- 5.1.20.3 The WCS Dispatch Consoles and Compact Dispatch Console shall be COTS hardware and shall have touch-screen operation. WCS Dispatch Console workstation layout, including hardware and accessories, will be codeveloped with the Authority to meet the OCC operational requirements.



- 5.1.20.4 The WCS Dispatch Consoles shall be integrated directly into the FRMCS core network and can be considered FRMCS Dispatch Consoles, and part of the FRMCS system for the purposes of this Specification. The two terms may be used interchangeably within this Specification.
- 5.1.20.5 The WCS Compact Dispatch Consoles shall either wirelessly connect to the FRMCS or Wi-Fi via VPN, or hardwired via the DCN. The Compact Dispatch Console will have the same operational, functional and performance requirements as FRMCS mobile devices and thus can be considered as FRMCS mobile devices for the purposes of this specification.
- 5.1.20.6 The WCS Dispatch Consoles should be implemented as 'Universal Consoles' that provide the required OCC workstation services and capabilities of all the train control and telecommunications sub-systems from one workstation, specifically the Integrated Control and Supervision System (ICSS) workstation/console. The intent is to minimize physical hardware and desk space requirements by consolidating functionality into shared, integrated workstations. There is no requirement for WCS Dispatch Consoles to be deployed on dedicated or physically separate hardware from other systems, provided operational performance, security, and availability requirements are maintained.
- 5.1.20.7 The TSCC Contractor shall provide Dispatch Consoles with accessories and all required hardware and software to function as per requirements.
- 5.1.20.8 The TSCC Contractor shall provide Compact Dispatch Consoles with accessories and all required hardware and software to function as per requirements.
- 5.1.20.9 The WCS Dispatch Console functions shall align with the defined roles and responsibilities of OCC personnel as documented in the Authority's operational procedures and manuals, and be compliant with the Controller Equipment requirements of the UIC FRMCS specifications (refer to section 2.5).
- 5.1.20.10 The TSCC Contractor shall design, source, provide, install, test, commission, operate, and maintain WCS Dispatch Consoles that enable OCC personnel to initiate and manage voice and data communications in accordance with their operational roles and system integration requirements.
- 5.1.20.11 The TSCC Contractor shall engage in a co-design process with the Authority's OCC personnel to ensure that the WCS Dispatch Consoles meet operational workflows, Human Factors principles, and ergonomic best practices. The TSCC Contractor shall incorporate user feedback throughout the design lifecycle and shall provide early and ongoing access to functional console environments to support user training, familiarization, and operational readiness.

5.1.21 Emergency Responder Communication System

- 5.1.21.1 The Emergency Responder Communications System (ERCS) is exempt from the duplicate core infrastructure requirement.
- 5.1.21.2 The ERCS shall enable secure, direct, and interoperable communication between OCC personnel and Emergency Responders using non-public networks, such as P25 and FirstNet.
- 5.1.21.3 The ERCS shall be integrated into the WCS Dispatch Consoles to allow OCC personnel to communicate with Emergency Responders and Dispatchers.
- 5.1.21.4 The ERCS shall include all equipment required to interconnect the WCS with external Emergency Responder radio communication networks like P25 and FirstNet.
- 5.1.21.5 The ERCS shall be designed in compliance with applicable public safety communications codes, including:
- NFPA 1225 – Standard for Emergency Services Communications;
 - California Fire Code Section 510 – Emergency Responder Radio Coverage in Buildings;
 - Any additional requirements mandated by the Authority Having Jurisdiction (AHJ).



5.1.22 Passenger Wi-Fi System

- 5.1.22.1 The PWS shall provide a non-critical seamless, reliable, secure, high-capacity and high-speed Wi-Fi service that is easily accessible to passengers via their personal devices throughout their train journey.
- 5.1.22.2 The PWS shall utilize mmWave (60GHz unlicensed band) Trainset-to-Trackside (mmWave TtT) architecture to provide the highest possible bandwidth and data rates, and to align with similar solutions provided by other comparable Railroad Operators (e.g., Caltrain).
- 5.1.22.3 The TSCC Contractor shall design, construct, commission, operate and maintain all required radio transmission sites to deliver continuous and reliable PWS mmWave Trainset-to-Trackside (mmWave TtT) coverage throughout the CHSR Right-of-Way, including tunnels, aerial structures, trenches, at-grade corridors, viaducts where passenger in-revenue services traverse, in accordance with the defined coverage and performance requirements.
- 5.1.22.4 PWS mmWave transmitters shall be installed on Overhead Contact System (OCS) masts. No requirement for dedicated PWS radio towers.
- 5.1.22.5 The PWS mmWave TtT transmitters shall be parented back to dedicated PWS edge switches, prior to interfacing with DCN, at FRMCS BBU Hotel locations via fronthaul optic fiber.
- 5.1.22.6 The PWS shall be designed to minimize the required number of optic fibers required to interconnect mmWave TtT transmitters.
- 5.1.22.7 The PWS core infrastructure shall be located within the communications room of the OCC.

Network Planning

- 5.1.22.8 The TSCC Contractor shall perform PWS radio network planning, including propagation modelling and site evaluation, to determine optimal locations for PWS transmitters along the CHSR Right-of-Way.
- 5.1.22.9 The final number, location, and configuration of PWS mmWave TtT transmitters shall be determined through the TSCC Contractor's detailed radio propagation study. This study shall account for local topography, land use, coverage, and factors like accessibility, power and backhaul, structural suitability, safety and compliance, environmental factors, security, hazards, co-location and interference, future expandability, and total cost of ownership.
- 5.1.22.10 The TSCC Contractor shall perform PWS in-train Wi-Fi coverage planning, including propagation modelling and antenna location evaluation, to determine optimal locations for PWS antennas within trainsets to ensure highest levels of Wi-Fi coverage are available to passengers.
- 5.1.22.11 The TSCC Contractor shall submit PWS Concept Design and Coverage Study, both TtT transmitters and in-train Wi-Fi, to the Authority for review and approval prior to detailed design and deployment. The Coverage Design shall demonstrate the operational and performance requirements are met.

5.2 Environmental Requirements

- 5.2.1 The WCS shall be designed in accordance with the Design Criteria Manual, Chapter 2: Basis of Design, section 2.2.10 Environmental, and Chapter 35: Environmental.
- 5.2.2 The WCS shall be designed in accordance with the requirements described in EN50125-3 Railway applications - Environmental Conditions for Equipment - Part 3: Equipment for Signaling and Telecommunications, Section 4: Environmental Conditions.
- 5.2.3 The WCS shall be designed in accordance with the Design Criteria Manual, Chapter 7: Electromagnetic Compatibility, section 7.1.2 Regulations, Codes, Standards, and Guidelines.
- 5.2.4 The WCS design should minimize the environmental impact of the WCS and of the entire CHSR operations during O&M phase.
- 5.2.5 All WCS designs for equipment in the Right-of-Way shall be suitable for electrified territory operations with appropriate mitigations in place to negate the possible safety and WCS performance risks.
- 5.2.6 The WCS equipment shall be designed and constructed to withstand the environmental conditions applicable to its installed location for the WCS design life. The level of protection shall comply with the



following Location Specific Requirements. The design shall demonstrate suitability of the selected equipment location categories.

- 5.2.7 The TSCC Contractor shall ensure that all electrical and electronic equipment supplied and installed complies with the requirements of the RoHS Directive (2011/65/EU as amended by 2015/863/EU) on the Restriction of Hazardous Substances in Electrical and Electronic Equipment [R101]. The TSCC Contractor shall retain records demonstrating RoHS compliance for all applicable equipment and components and make them available for inspection upon request.

Location Specific Requirements

- 5.2.8 WCS equipment locations shall be defined as:

- Indoor: A fully enclosed, climate-controlled environment protected from external weather conditions. Examples include control rooms, equipment rooms, trackside equipment shelters and occupied buildings.
- Outdoor Sheltered: A non-climate-controlled environment that provides partial protection from direct exposure to weather. Examples include covered platforms, tunnels, and ventilated enclosures.
- Outdoor Fully Exposed: An environment with no protection from external elements, subject to full weather exposure. Examples include trackside areas, open rooftops, and freestanding equipment.

- 5.2.9 The Indoor WCS equipment shall be compliant with the following environmental requirements:

- Data Center equipment Ingress Protection: IP 30 minimum (IEC 60529 [R14]);
- Temperature range: 0 to 40 °C (IEEE 60068-2-1 [R15]);
- Relative Humidity: 5%-95% Non-Condensing (IEEE 60068-2-30/78 [R15]);

- 5.2.10 The Outdoor Sheltered WCS equipment shall be compliant with the following environmental requirements:

- Ingress Protection: IP 54 minimum (IEC 60529 [R14]);
- Temperature Range: -20 °C to +50 °C (without direct solar load);
- Relative Humidity: 5%-95% Non-Condensing (IEEE 60068-2-30/78 [R15]);
- Wind Load: Sustained wind speed: 20 m/s; gusts: 30 m/s;
- Rain Exposure: Drip and splash protection only (equipment must not be directly exposed to rainfall);
- Seismic Considerations: Equipment and mounting structures shall meet applicable seismic anchorage and structural requirements of the California Building Code (CBC);
- Vibration & Shocks: IEC 60068-2-27 (Shocks), IEC 60068-2-6 (Vibration) [R15];

- 5.2.11 The Outdoor Fully Exposed WCS equipment shall be compliant with the following environmental requirements:

- Ingress Protection: IP 67 minimum (IEC 60529 [R14]);
- Temperature Range: -35 °C to +50 °C (without solar load; must tolerate California desert extremes), to +70 °C (with solar load);
- Relative Humidity: 5%-95% Non-Condensing (IEEE 60068-2-30/78 [R15]);
- Wind Load: Sustained wind: 24 m/s (approx. 54 mph); gusts: 40 m/s (approx. 89 mph) per CBC wind loading provisions;
- Rain Intensity: Minimum 50 mm/hour (per Caltrans design storm assumptions);
- Ice and Sleet: 12.5 mm (for northern and mountainous California regions);
- Seismic Considerations: Equipment and mounting structures shall meet applicable seismic anchorage and structural requirements of the California Building Code (CBC);
- Vibration & Shocks: IEC 60068-2-27 (Shocks), IEC 60068-2-6 (Vibration);
-



5.2.12 All WCS equipment locations shall be compliant with:

- Lightning Protection: EN 50164-3, IEC 61643, EN 60715, EN 62305, NFPA 780 (installed in accordance with the California Fire Code and local AHJ requirements);
- EMC: EN 50121-5, EN 55024, EN 300386, EN 50122-1, EN 61000-6-2, EN 61000-6-4, IEC 61000-3-6, IEC 61000-3-7, IEC 61000-5-2, EN 50121-3-2, EN 50121-4.

5.2.13 All Outdoor Fully Exposed WCS equipment cabinets that are exposed to direct sunlight shall be fitted with sun shelters or protective overhead covers designed to shield the cabinets from direct solar radiation. The sun shelter shall be engineered to reduce the impact of solar heat gain and assist in maintaining internal cabinet temperatures within the equipment's specified operating range.

Sun shelters shall:

- Extend beyond all sides of the cabinet by a minimum of 300 mm;
- Be constructed from UV-resistant, non-combustible, and weather-resistant materials;
- Be structurally rated for local environmental conditions including:
 - Sustained wind speeds up to 24 m/s and gusts up to 40 m/s (per general design standards);
 - Aerodynamic pressure and suction forces generated by passing high-speed trains operating at speeds up to 220mph (354 km/h), including transient crosswinds and turbulence;
 - Train-induced pressure loads of at least 1.5 kPa, based on dynamic pressure from high-speed train passage in close proximity, consistent with railway aerodynamic standards such as EN 14067-4 or equivalent;
 - Comply with applicable wind load factors for railway proximity as specified in the California Building Code (CBC) and relevant railway design standards (e.g. EN 1991-1-4 where applicable);
- Not obstruct ventilation, access, or maintenance activities;
- Be integrated into the overall equipment grounding, bonding and lightning protection scheme, where applicable;
- Be designed and constructed to achieve a design life of 30 years with appropriate corrosion and UV resistance, subject to appropriate maintenance.

5.3 Operational Requirements

5.3.1 The TSCC Contractor shall be responsible for the configuration, management, provisioning, maintenance and planning of all operational aspects of the WCS, including but not limited to coverage, capacity, performance, periodic reporting, user roles, prioritization and communication talkgroup matrix (Fleetmap) structures. All proposed configurations shall be documented and submitted to the Authority for review and approval prior to implementation.

5.3.2 Future Mobile Radio Communication System

5.3.2.1 The FRMCS shall function as the communications system of last resort for safety-related and time-critical operational communications. In the event of a partial or complete failure of other communications subsystems, the FRMCS shall remain operational and capable of supporting essential voice and data communication between train drivers and OCC personnel, and other user groups such as maintenance personnel. The FRMCS shall support the coordination of activities required to restore degraded or failed systems, ensuring safe and continuous CHSR operations under abnormal or emergency conditions.

Note to reader: The FRMCS voice communications will be required by crews to restore other failed systems and/or rescue passengers during an outage. Hence, the FRMCS system needs to be operational during all possible outage scenarios.



- 5.3.2.2 The FRMCS shall allow all train drivers and the OCC to maintain communications while the trainset is in operation throughout the complete CHSR Right-of-Way, including stabling yards and maintenance facilities.
- 5.3.2.3 The FRMCS shall allow all CHSR operational personnel to communicate from all locations throughout the full CHSR System, including indoor locations where coverage is not meeting performance criteria and enhancement is required. Preference will be given to terrestrial FRMCS radio sites to address inbuilding coverage where possible.
- 5.3.2.4 In indoor areas where outdoor radio coverage does not meet the required performance levels for the FRMCS, the TSCC Contractor shall provide dedicated indoor radio coverage solutions. Indoor coverage shall be delivered using appropriate technologies such as Distributed Antenna Systems (DAS), small cells, or other solutions suitable for the specific building type, usage, and radio environment. The indoor coverage design shall ensure seamless connectivity and service continuity for CHSR operational personnel in accordance with the overall system performance requirements.
- 5.3.2.5 The FRMCS shall incorporate sufficient redundancy, independence, and coverage to remain operational during communications outages, including support for maintenance teams accessing infrastructure or trainsets during fault rectification and service recovery.
- 5.3.2.6 The FRMCS shall support the operation of ETCS Level 2, including integration with safety-critical functions rated to SIL 4 in accordance with relevant CENELEC standards (EN 50126, EN 50128, and EN 50129). The implementation shall comply with the applicable requirements of the European Union Agency for Railways Control Command and Signaling TSI (CCS TSI), particularly those relating to the interoperability of FRMCS and ETCS systems. Refer to ETCS Technical Specification.
- 5.3.2.7 The FRMCS shall maintain continuous service availability in the event of hardware, software, link or power failure, consistent with high-availability targets suitable to support SIL 4 compliant systems.
- 5.3.2.8 The FRMCS design shall support operational functionality in accordance with the service requirements specified in 3GPP TS 22.179 "Service Requirements for the Future Railway Mobile Communication System (FRMCS)" and ETSI TR 103 459 "System Reference Document - Future Railway Mobile Communication System (FRMCS)". The design shall ensure that all operational communications align with the functional and performance expectations outlined in these specifications.
- 5.3.2.9 The FRMCS shall enable OCC personnel and authorized operational staff to transmit operational data and service updates to trainset systems including, but not limited to, the Public Address and Customer Information System (PACIS), and train crew devices and terminals. This capability shall support:
- Real-time service announcements (e.g. delays, disruptions, platform changes);
 - Scheduled or dynamic passenger information updates (e.g. next stop, arrival times, transfer connections);
 - Remote coordination with train crew and conductors for service instructions and incident management.
- 5.3.2.10 Refer to Public Address and Customer Information System Technical Specification for further details.
- 5.3.2.11 The FRMCS shall support continuous voice talkgroup communication between Train Drivers and Train Dispatchers as trainsets cross Dispatch Area boundaries. Dispatch Area's are also known as Target Areas or Areas of Responsibility.
- 5.3.2.12 The FRMCS shall ensure that trainset voice talkgroup communication with the correct Train Dispatcher is maintained, based upon location, without requiring driver intervention during transitions between Dispatch Areas.
- 5.3.2.13 The FRMCS shall dynamically reassign talkgroups as trainsets cross Dispatch Area boundaries based upon requests from other TSCC subsystems, such as the Traffic Management System.
- 5.3.2.14 The FRMCS shall enable authorized operational user groups to access core system functionality, such as Asset Management Systems (AMS) and corporate information, through mobile applications or web-based interfaces on FRMCS devices. This capability will provide efficiencies for mobile user groups.



E.g., Train crew and station personnel could have tablets with range of applications to support their operational duties.

- 5.3.2.15 The TSCC Contractor shall develop a comprehensive fleetmapping plan (configuration and talkgroup matrix) to define the logical organization of users and communication groups within the WCS that meets the Authority's operating requirements. The fleetmap shall address user role definitions, talkgroup structures, call priority levels, communication access rules, and device provisioning requirements. The plan shall support operational scenarios and role-based communications and shall be submitted to the Authority for review and approval prior to implementation.
- 5.3.2.16 The FRMCS should include a Test Network that duplicates all elements of the FRMCS production network that can be utilized for pre-deployment testing of proposed software, hardware and configuration changes prior to implementation on the FRMCS production network.
- 5.3.2.17 The FRMCS shall support all the required WCS Dispatching Consoles functionality.

5.3.3 Dispatch Consoles

- 5.3.3.1 The WCS Dispatch Consoles shall allow OCC train controllers / dispatchers to interoperate with other Railroad Operator train controllers / dispatchers for the purposes of traffic coordination and emergency scenarios (e.g., Caltrain, BNSF, Amtrak, LA Metro and Brightline West).
- 5.3.3.2 The WCS Dispatch Consoles shall allow OCC personnel to coordinate mission-critical and emergency communications with all relevant CHSR user groups, including train drivers, train crew, maintenance crews, station staff, and emergency responders.
- 5.3.3.3 OCC personnel shall be able to automatically configure all WCS Dispatch Consoles based on a preconfigured user profiles and dispatcher 'areas of responsibility' activated in TMS (as well automatically adjust the Location Dependent Addressing area in the Dispatch Console according to the changed dispatcher are of responsibility in TMS).
- 5.3.3.4 The WCS Dispatch Consoles shall remain fully operational under normal, degraded, and emergency conditions, with automatic failover to redundant paths, dual UPS power and standby generating plant mains power in the event of any primary system failure.
- 5.3.3.5 For the purposes of OCC business continuity - In the event of degraded operating scenarios, WCS Dispatch Consoles shall retain operational capability by being able to connect into the core network over the internet via a secure Virtual Private Network (VPN).
- 5.3.3.6 The FRMCS Test Network should replicate the WCS Dispatch Console capabilities to provide training functions for OCC dispatchers and train controllers.

5.3.4 Emergency Responder Communication System

- 5.3.4.1 The ERCS shall remain operational under normal, degraded, and emergency operating conditions, including infrastructure power loss, partial communications failures, or disaster scenarios.
- 5.3.4.2 The ERCS shall allow OCC personnel to initiate and maintain voice and data communications with public safety agencies during emergency incidents.
- 5.3.4.3 The ERCS shall allow OCC personnel to interconnect (aka 'patch' or 'bridge') ERCS and FRMCS talkgroups calls, to facilitate emergency responder communications with any FRMCS end user.
- 5.3.4.4 The ERCS shall support integration into the incident command structure managed by the Authority Having Jurisdiction (AHJ) during response efforts.
- 5.3.4.5 The ERCS shall allow OCC operators to monitor, communicate, and exchange information with multiple responder units simultaneously. The ERCS shall interoperate with:
- Emergency Responder Control Centers;
 - Portable responder radios;
 - Mobile units;
 - Incident command vehicles;



- Regional PSAPs;
- Inter-agency gateways and mutual aid radio systems.

5.3.5 Passenger Wi-Fi System

- 5.3.5.1 The Passenger Wi-Fi System (PWS) shall provide continuous coverage and consistent passenger user experience inside trainsets while stationary and in motion, including tunnels, cuttings and trenches.
- 5.3.5.2 The PWS shall allow passengers to maintain digital connectivity to the internet via their personal devices throughout their train journey from within the trainsets.

5.4 Functional Requirements

Network Timing Synchronization

- 5.4.1 The WCS shall utilize the Network Timing Systems to provide accurate and consistent time synchronization across all WCS fixed and onboard subsystems. Refer to Network Timing System Technical Specification for further details.

Network Monitoring System

- 5.4.2 The TSCC Contractor shall deliver a Network Management System (NMS) that provides a centralized, secure, and standards-aligned network monitoring and management system, including OCC workstations, for all WCS subsystems, including the FRMCS, ERCS, PWS and WCS Dispatch Consoles, excluding Compact Dispatch Consoles.
- 5.4.3 This NMS shall provide the following features:
- Network element access – The NMS shall provide connectivity to all core network elements and RAN elements in the WCS;
 - User management – The NMS shall control user access and distinguish user roles;
 - Alarm management – The NMS shall enable users to configure, capture, log and report alarms through a centralized user interface;
 - Performance management – The NMS shall enable users to view real-time, periodic, and historical data of network element performance for troubleshooting and optimization, including field-based analysis tools or probes;
 - Configuration management – The NMS shall enable users to automatically manage system backup configurations, track configuration changes to network elements, and enable mass updates of configuration settings;
 - License management – The NMS shall enable users to update operating licenses that govern core and field network elements;
 - Inventory management – The NMS shall enable users to explicitly know and understand each element of the WCS to track individual components and parts, including software and firmware identification;
 - Storage capability – The NMS shall capture the configuration and performance data with adequate storage for backup configuration checks;
 - Provisioning – The NMS shall enable users to commission, upgrade, or decommission network elements;
 - Service provisioning – The NMS shall support service provisioning workflows, including the configuration of subscriber profiles, QoS policies, network slice assignments, and policy rules by interfacing with 5GC functions such as UDM, PCF, SMF, and NSSF;
 - SIM/eSIM provisioning – The NMS shall interface with the operator's or Authority's SIM provisioning platform to enable the secure download, activation, and lifecycle management of eSIM profiles in accordance with GSMA Remote SIM Provisioning architecture (e.g., SM-DP+, SM-SR);
 - Cybersecurity – The NMS shall include robust cyber security measures that meet the recommendations of the Cybersecurity Technical Specification.



- 5.4.4 To manage all these different elements, the NMS will provide a Graphical User Interface (GUI) with three independent windows: a network topology status and health map, a performance dashboard and an alarm dashboard.
- 5.4.5 The NMS shall provide a real-time network statistics dashboard that presents key operational and performance indicators across all WCS subsystems, including but not limited to core network elements, RAN nodes, transmission systems, and service endpoints. The dashboard shall support customizable views and user-defined thresholds to highlight system health, alarms, and usage patterns.
- 5.4.6 The NMS shall support both automated and ad hoc reporting capabilities, including:
- Real-time metrics such as traffic volume, session status, user load, latency, jitter, packet loss, and resource utilization;
 - Periodic performance reports (e.g., hourly, daily, weekly, monthly) with trend analysis, peak usage statistics, and Service Level Agreement compliance indicators;
 - Usage reports per subsystem, network slice, user category, radio site or location;
 - Export of reports in common formats such as PDF, CSV, and XML for integration with external systems.
- 5.4.7 The TSCC Contractor shall ensure that reports and dashboards are accessible via a secure web-based interface, support role-based access controls, and retain historical data in accordance with the Authority's data retention policy.
- 5.4.8 The NMS shall support secure remote interrogation capabilities to enable authorized support personnel, including escalated third-level or vendor support teams, to access diagnostic tools and system telemetry for fault isolation and performance analysis.
- Remote access shall be provided exclusively via a secured Virtual Private Network (VPN) connection that meets the Authority's cybersecurity requirements, as per Cybersecurity Technical Specification. All remote sessions shall enforce multi-factor authentication (MFA/2FA).
- 5.4.9 The NMS shall ensure that:
- Remote interrogation access is restricted to defined user roles and scoped permissions;
 - All access attempts, successful logins, commands executed, and session durations are logged and auditable;
 - Remote access can be revoked in real-time by the Authority if required;
 - All remote data exchanges are end-to-end encrypted and comply with relevant cybersecurity standards (e.g., ISO/IEC 27001, NIST 800-53, or local equivalents).
- 5.4.10 The NMS alarm, performance and status monitoring capabilities shall be integrated into the Integrated Control and Supervision System (ICSS). The ICSS performs the 'manager of managers' function, so only high level and high priority information is required to be passed between subsystems. The ICSS can obtain data directly from the WCS subsystems, rather than via the NMS if this is more practical.
- 5.4.11 **Performance Reporting**
- 5.4.12 The TSCC Contractor shall deliver monthly WCS subsystem performance and maintenance reports, aligned with system assurance and cybersecurity standards. Reports shall include:
- Usage statistics, including:
 - Passenger Wi-Fi sessions service use;
 - Operational subsystem traffic volumes (e.g. FRMCS & Dispatch Console voice/data loads);
 - Performance metrics, including:
 - Throughput, latency, jitter, packet loss, and session duration;
 - Radio coverage gaps and signal strength trends;



- Availability and reliability reporting aligned with RAMS metrics from EN 50126 / EN 50129, including Mean Time Between Failures (MTBF) and incident frequency;
- Service Level Agreement (SLA) and Key Performance Indicators (KPIs) tracking, including compliance summaries and trend analysis;
- Security and access audit summaries, as required under IEC 62443-2-4 and IEC 62351, including:
 - Configuration changes;
 - Intrusion detection alerts;
 - Access violations;
- Documentation of:
 - Preventive maintenance activities and results;
 - Firmware/software patch deployments;
 - Hardware lifecycle events (e.g. replacements, EOL notices).

5.4.13 Equipment Racking

5.4.14 Where required, the TSCC Contractor shall provide equipment racks to house all WCS equipment in accordance with applicable standards. Equipment racks shall comply with IEC 60297 for mechanical dimensions and mounting, and shall be suitable for the environmental conditions defined in EN 50125-3 where applicable (e.g. trackside shelters, equipment rooms).

5.4.15 Each rack shall be supported by a dedicated power circuit, with circuit breakers installed in a clearly labeled and readily accessible local distribution panel within the same equipment room or enclosure. All power cabling shall be hardwired and comply with the National Electrical Code (NEC) and other applicable electrical codes.

5.4.16 Where required, the TSCC Contractor shall provide outdoor-rated telecommunications cabinets to house all required network, power, and support equipment in external environments, including along the railway Right-of-Way, at stations, and at other operational facilities. Outdoor cabinets shall be designed to meet the environmental, electrical, and mechanical protection requirements appropriate for their deployment conditions and shall comply with EN 50125-3 and the applicable Location Specific Requirements (5.2.8).

5.4.17 Future Mobile Radio Communication System

5.4.17.1 All functional requirements defined in the latest version of the Future Railway Mobile Communication System (FRMCS) Functional Requirements Specification (FRS), as published by the UIC FRMCS Functional Working Group (FWG), shall be implemented by the TSCC Contractor.

5.4.17.2 The TSCC Contractor shall submit a detailed compliance statement mapping the FRMCS design to the FRMCS FRS requirements, identifying any deviations, partial implementations, or non-compliant items, for review and approval by the Authority.

5.4.17.3 The FRMCS shall be capable of supporting FRMCS-compliant mission-critical voice, data, and video services (MCX), and shall enable future integration with FRMCS-based infrastructure and equipment, including support for standardized interfaces, functional architecture, and radio access technologies as specified in 3GPP Release 17 or later and UIC FRMCS specifications.

5.4.17.4 The FRMCS design shall comply with all system requirements defined in the latest version of the FRMCS System Requirements Specification (SRS) published by the UIC, ensuring alignment with international railway communication standards and future interoperability.

5.4.17.5 The FRMCS shall provide the full voice, data and video feature set, including Railway Emergency Communication (Emergency Duress), as detailed in the 3GPP MCX and UIC FRMCS specifications. The TSCC Contractor shall highlight any non-compliance or missing features.



Radio Access Network Architecture

- 5.4.17.6 The FRMCS shall implement a Centralized Radio Access Network (C-RAN) architecture, whereby Baseband Unit (BBU) processing is consolidated at a central facility (“BBU Hotel”), and Remote Radio Heads (RRHs) are installed at the top of radio towers. The RRHs shall connect to the centralized BBUs via high-speed fronthaul links to enable enhanced coordination, cost efficiency, and optimized resource utilization. Refer to *Figure 25*.

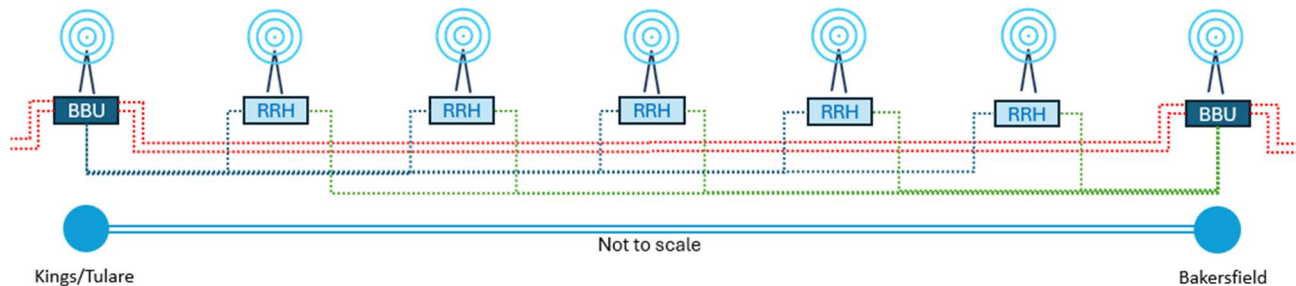


Figure 25 : Example of Centralized Radio Access Network (C-RAN) architecture, with a flat DCN ring (red) providing backhaul connectivity to BBU Hotel sites and with redundant fronthaul fiber from BBU to RRH sites (blue/green). If the fronthaul connectivity or the BBU fails, the RRH radio sites utilize the secondary BBU to maintain operations. NB: The BBU Hotels also have RRH for the tower collocated. In this example, all fiber is within the same cable run, providing a single point of failure.

- 5.4.17.7 This architecture shall be employed to minimize the physical footprint, and power requirements of radio sites along the CHSR Right-of-Way, reduce environmental impact, and support centralized resource pooling, simplified maintenance, and improved network scalability and resiliency.
- 5.4.17.8 The TSCC Contractor shall ensure the use of standards-based fronthaul interfaces (e.g., eCPRI or IEEE 1914.3) to interconnect RRHs and BBUs, and shall provide suitable protection, synchronization, and transport performance to support all FRMCS requirements.
- 5.4.17.9 The TSCC Contractor shall deploy BBUs at centralized, secure locations referred to as “BBU Hotels”, where multiple Remote Radio Head (RRH) sites along the Right-of-Way are logically and physically parented to shared redundant BBUs.
- 5.4.17.10 BBU Hotels may be notionally located at locations designated as “Communication Site” on the CHSR “Schematic Track Layout and System Sites” . documentation. These sites have been prepared with space, power, and civil infrastructure suitable to accommodate towers, equipment shelters and related telecommunications facilities.
- 5.4.17.11 The TSCC Contractor shall dual parent (or dual-homed) RRH's to BBU Hotel locations to provide redundancy to address BBU equipment or fronthaul failure risk.
- 5.4.17.12 The BBU Hotels shall be designed to support:
- Fronthaul connectivity to all associated RRHs using high-capacity, low-latency links;
 - Redundancy and survivability consistent with subsystem criticality;
 - Future traffic growth.
- 5.4.17.13 The TSCC Contractor shall submit a BBU Hotel deployment plan identifying all parent-child RRH relationships, fronthaul link specifications, site readiness conditions, degraded operation scenarios and proposed system integration, subject to Authority review and approval.
- 5.4.17.14 The FRMCS shall utilize a redundant Radio Access Network architecture providing either:
- Double Coverage, where every operational zone is served by at least two overlapping base stations within the same FRMCS network. Refer to Figure 26; or
 - Duplicated Coverage, where two logically and functionally independent FRMCS radio access systems provide overlapping coverage using separate radio, transmission, and DC power system

(including batteries), while allowing shared use of non-electronic physical assets such as towers, shelters, conduits, optic fiber cables and utility power supply. Refer to Figure 27.

The FRMCS design shall ensure that the failure of any individual radio site, equipment node, or backhaul path does not result in service interruption for safety-critical voice or data.

Note to reader: Double coverage results in no loss of coverage during a single site outage due to completely overlapping coverage from adjacent site. Duplicated coverage results in no loss of coverage during equipment failure. Duplicated coverage does not provide the same level of availability but can provide near the same level and reduce the number of radio sites required.

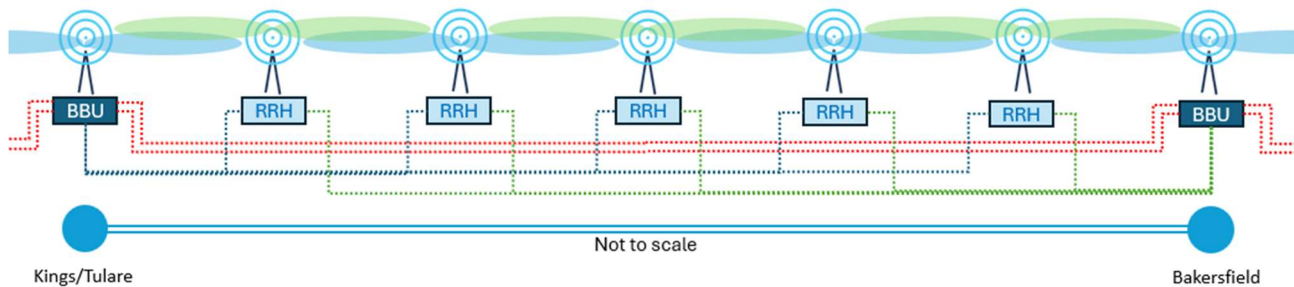


Figure 31 : Example of Centralized Radio Access Network (C-RAN) architecture, with 'Double Coverage'. Each adjacent radio site provides completely overlapping coverage. If any radio site fails, there is no loss of coverage.

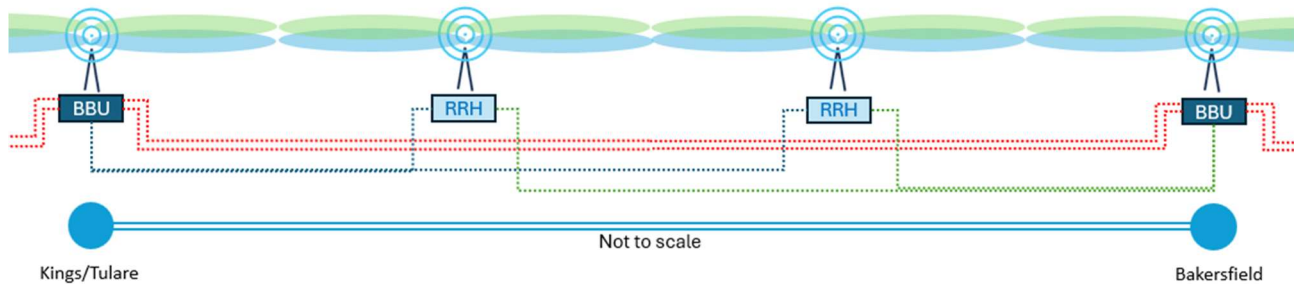


Figure 27 : Example of Centralized Radio Access Network (C-RAN) architecture, with 'Duplicated Coverage'. Each radio site has duplicated equipment, effectively two radio sites at one location. If any radio component fails, there is no loss of coverage, and there is battery backup and deployable generators to address loss of power.

FRMCS Feature Set

- 5.4.17.15 The FRMCS shall align with UIC FRMCS Functional Use Cases, 3GPP MCX redundancy principles, and safety-critical system design practices under EN 50159.
- 5.4.17.16 The FRMCS shall provide mission-critical Push-to-Talk (MCPTT) voice communication, as per 3GPP Mission-Critical Services: MCPTT (TS 23.379) and including:
- Individual and talkgroup calling;
 - Emergency call initiation with pre-emption and override;
 - Call priority management and call queuing;
 - Support for late join and ambient listening (subject to policy).
- 5.4.17.17 The FRMCS shall enable Mission-Critical Data (MCData) communication, as per 3GPP Mission-Critical Services: MCData (TS 23.282) and including:
- Reception and acknowledgement of control instructions and timetables;
 - Transmission of diagnostic and fault data from onboard systems to the OCC;
 - Support for Cab Display Systems receiving text messages from OCC personnel.

- 5.4.17.18 The FRMCS should provide Mission-Critical Video (MCVideo) capability, as per 3GPP Mission-Critical Services: MCVideo (TS 23.281), to support:
- On-demand video transmission from the train cab to the OCC;
 - Streaming of predefined onboard CCTV or event camera feeds during incidents.

Note to reader: The Authority acknowledges that the Authority's spectrum limitations (5.1.6), the Authority requires streaming CCTV capability from trainsets. This alternatively could be provided by the PWS. The Authority encourages innovative alternative proposals to be submitted that meet the underlying business requirement to provide the streaming CCTV capability.

- 5.4.17.19 The FRMCS shall support Dynamic Group Management, enabling OCC personnel, via Dispatch Consoles and other TSCC subsystems, to:
- Create, modify, and dissolve mission-critical voice talkgroups in real time;
 - Assign drivers/trainsets, maintenance teams, and field staff to specific talkgroups as required for operations or emergencies.
- 5.4.17.20 The Dynamic Group Management capability shall allow OCC personnel to interconnect (aka 'patch' or 'bridge') other systems that have been integrated into the WCS Dispatch Consoles.
- 5.4.17.21 The FRMCS shall support dynamic talkgroup reassignment requests, and confirm completion of reassignment, from WCS Dispatch Consoles and other TSCC subsystems.
- 5.4.17.22 The FRMCS shall support user configurable rules-based reassignment of trainset talkgroups based on location, train ID, or section transitions (i.e., As trainsets crosses a Dispatcher's Area of Responsibility boundaries).
- 5.4.17.23 The FRMCS shall maintain support for emergency override calls that can reach multiple Dispatcher Areas regardless of dynamic talkgroup affiliation.
- 5.4.17.24 The FRMCS shall support end-to-end prioritization of all mission-critical communications, ensuring that safety-critical data (e.g. ETCS messages) and emergency voice calls are assigned the highest levels of QoS and priority across all network domains, including RAN, Core Network, and Transport Network. The system shall also support the configuration and enforcement of differentiated priority levels for other voice, data services (e.g. operational voice, maintenance data), in accordance with 3GPP QoS Class Identifiers (QCI or 5QI), pre-emption capabilities, and local operational policies.
- 5.4.17.25 The FRMCS shall have the capability to store location data from FRMCS handheld devices. This data shall be able to be retrieved by the WCS Dispatch Consoles.
- 5.4.17.26 **Interoperability**
- 5.4.17.27 The TSCC Contractor shall provide an Interworking Function (IWF) to enable interoperability between the FRMCS-based communications system and existing or third-party Land Mobile Radio (LMR) systems, including but not limited to P25, TETRA, and analog conventional radio networks.
- 5.4.17.28 The IWF shall support voice interoperability to allow Operations Control Centre (OCC) dispatchers to:
- Initiate and receive group and individual voice calls between FRMCS and LMR users
 - Participate in emergency calls initiated from LMR or FRMCS terminals
 - Maintain Push-to-Talk (PTT) control behavior across systems
 - View the caller identity and source system for all interworked calls
 - Monitor, record, and replay interworked communications via the telephony logging system
- 5.4.17.29 The IWF shall support signaling and media translation in accordance with 3GPP TS 23.283 and applicable FRMCS and MCX specifications. The solution shall ensure interoperability without compromising the call priority, preemption, or quality-of-service mechanisms defined for FRMCS.



- 5.4.17.30 The TSCC Contractor shall provide interoperability between the FRMCS-based communications system and the FirstNet public safety broadband network (FirstNet), allowing authorized users, including OCC dispatchers, to communicate with FirstNet users via standards-based Mission Critical Services (MCX).

The interoperability solution shall support:

- Group and individual voice calls between FRMCS and FirstNet users using MCPTT (Mission Critical Push-to-Talk);
- Emergency call support across both networks, including priority and preemption;
- Location transparency, allowing OCC dispatchers to view the identity and affiliation (FRMCS or FirstNet) of the user;
- SIP/IMS-based interconnection and service-level interoperability in accordance with 3GPP TS 23.283 (LMR Interworking) and TS 23.379;
- End-to-end QoS control, ensuring MCX bearer traffic maintains service integrity and priority when traversing between the FRMCS and FirstNet environments.

- 5.4.17.31 The TSCC Contractor shall ensure that any interconnection with FirstNet complies with applicable cybersecurity, authentication, and identity federation policies as mandated by the Authority and by the FirstNet Authority.

- 5.4.17.32 Public Help Points shall provide two-way voice communication between the public and authorized railway personnel. Where required, Public Help Points shall be capable of operating over the FRMCS, utilizing its voice transport and call routing capabilities to establish reliable, prioritized connections with station staff, OCC personnel, or emergency responders. The system shall support integration with the Telephony System logging environment, including caller identification, location tagging, and call recording and logging. Refer to Telephony System Technical Specification.

Handheld Devices

- 5.4.17.33 FRMCS handheld devices shall support location reporting using multiple Global Navigation Satellite Systems (GNSS), including but not limited to GPS, Galileo, GLONASS, and BeiDou. Devices shall allow for programmable location reporting intervals (cadence) to suit operational requirements. All reported location data shall be transmitted to and captured by a centralized location server for real-time monitoring and historical tracking.

- 5.4.17.34 FRMCS handheld devices **should** support man down detection, lone worker monitoring, and ambient listening capabilities to enhance the safety of operational personnel. These features shall integrate with Mission Critical Push-to-Talk (MCPTT) emergency procedures as defined in 3GPP standards, enabling automatic emergency alerts, location update, and remote microphone activation under defined conditions. These capabilities are defined as:

- **Man Down:** An automatic emergency alert triggered by device sensors detecting that the user is motionless or in an abnormal posture (e.g., horizontal position) for a defined period;
- **Lone Worker:** A safety feature that monitors user activity and requires periodic check-ins, by pushing the PTT button in response to an alert. Failure to respond within a set timeframe triggers an emergency alert;
- **Ambient Listening:** The remote activation of a device's microphone, typically during an emergency call, to allow dispatchers or supervisors to hear the surrounding environment without user intervention.

FRMCS Recording and Logging

- 5.4.17.35 All FRMCS voice, data and metadata shall be recorded and logged for a minimum of 90 days. Refer to Telephony System Technical Specification for further information about logging requirements.



5.4.18 Dispatch Consoles

5.4.18.1 WCS Dispatch Consoles and Compact Dispatch Consoles shall provide authorized users with the full 3GP MCX and FRMCS feature set, such as, but not limited to:

- One to many push-to-talk (PTT) voice talkgroup communications;
- Simultaneous talkgroup communications;
- Broadcast talkgroup communications;
- Private / General call communications;
- Prioritized talkgroup and individual calling;
- Emergency Duress (Railway Emergency Call) functionality;
- Messaging, alerts, and acknowledgments;
- Interoperability between subsystems;
- Location-based user identification (FRMCS handheld devices);
- Patching within and between subsystems.

5.4.18.2 WCS Dispatch Consoles shall support user authentication, dynamic and multi-role assignment, and customizable UI profiles based on the assigned role of the operator (e.g., Train Dispatcher, Emergency Coordinator). That is, upon authenticating users shall be presented with the console configuration based upon their profile and role. Supervisors / managers shall be able to dynamically change the roles of users.

5.4.18.3 The WCS Dispatch Consoles shall display a real-time list of all active trainsets (identified by running train numbers) currently located within the Dispatch Area (Area of Responsibility) of the assigned dispatcher/operator. The console shall support direct voice communication with a specific trainset by allowing the dispatcher to initiate a call through a simple touch selection of the train number on the touch screen interface. As each Dispatch Area is associated with a dedicated talkgroup, and trainsets are dynamically reassigned to the appropriate talkgroup based on their location, the console shall ensure the dispatcher has visibility and calling capability for all trainsets currently affiliated with their designated Dispatch Area talkgroup.

5.4.18.4 WCS Dispatch Consoles and / or the dispatch workstation shall be integrated with other train control and telecommunications sub-systems, such as the Telephony System.

5.4.18.5 WCS Dispatch Consoles shall be designed to support integration with the FRMCS, which supports the ETCS SIL 4 subsystem. The WCS Dispatch Consoles components and their associated interfaces shall be developed, verified, and maintained in accordance with the safety requirements necessary to support a SIL 4 environment, in alignment with IEC 61508 and applicable railway safety standards.

5.4.19 Interoperability between WCS subsystems

5.4.19.1 The WCS shall support interoperable voice and data communication between FRMCS, PWS and Dispatch Console subsystems and Authority's corporate IT network (where required).

5.4.19.2 This WCS interoperability shall ensure that:

- Authorized users across different subsystems can exchange critical voice, data, and control messages securely and without degradation;
- Interfaces between subsystems comply with relevant open standards (e.g., 3GPP, IEEE, IETF) to enable seamless integration and future extensibility;
- Data can be accessed between WCS subsystems and Authority's corporate IT network (e.g., via DCN Firewall);



- Where subsystems operate on separate logical or physical infrastructure, appropriate interworking gateways, Inter-Working Functions, APIs, or middleware shall be implemented to maintain functionality and service continuity.

5.4.19.3 The TSCC Contractor shall demonstrate interoperability through system integration testing and provide documentation showing interface compatibility and user-level communication flows between subsystems, and demonstrate that this interoperability facilitates CHSR operations.

5.4.20 ETCS Support

5.4.20.1 The FRMCS shall provide the radio access bearer services for ERTMS/ETCS ensuring the overall safety of the end-to-end transmission between trainset and trackside ERTMS/ETCS applications. Refer to ETCS Technical Specification [R89] for further information.

5.4.20.2 The FRMCS shall ensure that ETCS safety-critical data is assigned the highest end-to-end priority level across all network segments, including the RAN, Core Network, and Transport Network. The system shall guarantee low latency, high reliability, and zero tolerance for pre-emption of ETCS traffic, using dedicated QoS parameters aligned with 3GPP-defined 5QI 75 or equivalent, and shall implement appropriate traffic marking, bearer selection, and resource reservation to support continuous and uninterrupted ETCS operation.

5.4.21 Emergency Responder Communication System

5.4.21.1 The ERCS shall be integrated into the WCS Dispatch Consoles system.

5.4.21.2 The ERCS shall support the following communication capabilities from WCS Dispatch Consoles:

- P25 radio voice interoperability with local, regional, and state responders;
- FirstNet LTE/5G data access (e.g., for video streaming, file sharing);
- Push-to-Talk (PTT) integration between OCC and responder teams;
- Support for unit ID, talkgroup assignment, and incident-specific channels.

5.4.21.3 The TSCC Contractor may utilize the FRMCS IWF to integrate ERCS with external Emergency Responder systems.

5.4.21.4 The specific agencies, channels and talkgroups will be determined in consultation with the Authority and each of the Authority Having Jurisdiction (AHJ) for emergency response within the CHSR System.

5.4.22 Passenger Wi-Fi System

5.4.22.1 The Passenger Wi-Fi System (PWS) shall provide a reliable, secure data communication between passenger devices and the internet, and operational personnel devices.

5.4.22.2 Profiling of network traffic shall be developed in detail for proper network dimensioning.

5.4.22.3 The PWS shall support uninterrupted session handover (unnoticeable to end users) between station and train W-Fi networks to preserve user sessions during boarding and alighting.

Note to reader: At the time of drafting is it unknown if passenger wi-fi service will be provided at stations.

5.4.22.4 If no station wi-fi service is initially implemented, the TSCC Contractor shall produce guidance for future reference on how to support uninterrupted session handover to mitigate the scenario where station Wi-Fi is introduced in future.

PWS User Experience and Accessibility

5.4.22.5 The PWS shall use a unified web browser-based authentication portal across stations and trains, offering:

- Fast user onboarding via captive portal, QR scan, and CHSR mobile app;
- Onboarding portal will be plain, simple, intuitive, free of advertising and branded as specified by the Authority;



- New users shall be able to establish an initial connection and access the internet within 30 seconds of selecting the Wi-Fi network, under normal network conditions;
- Authentication shall support federated identity and third-party sign-on using widely adopted providers such as Google, Apple ID, and Facebook;
- Accepted authentication protocols include OAuth 2.0, OpenID Connect, and SAML 2.0;
- Tiered access options (e.g., free basic, paid premium) with session persistence;
- Accessibility-compliant design (WCAG 2.1 AA or higher);
- Recognizing returning users and automatically re-establishing sessions to minimize reconnection time and improve user experience;
- Privacy policy and Fair Use policy confirmation during onboarding.

5.4.22.6 The PWS shall include a tiered passenger access model comprising:

- A **complimentary Wi-Fi** service access will be included with the passenger's train ticket, offering basic connectivity with configurable speed and daily data restrictions (specific volume to be defined during implementation planning). This basic tier shall support general web browsing, messaging, and email.
- A **premium Wi-Fi** service will be available for purchase, designed to support high-bandwidth applications including HD video streaming, cloud collaboration tools, and real-time video communications, including priority over 'basic tier' users.

5.4.22.7 The PWS tiering scheme may be changed by the Authority prior to or following the commencement of revenue service. The PWS shall support changing the number, naming, branding, pricing, access rights, data limits, quality-of-service levels, and feature sets of passenger Wi-Fi service tiers, including additional tiers, through a configurable management interface, without requiring hardware modifications or service disruption.

5.4.22.8 The PWS shall provide an integrated and secure digital payment gateway to enable access to the premium Wi-Fi service. The gateway shall support multiple forms of secure digital payment, including but not limited to:

- Credit/debit card payments (e.g., Visa, Mastercard, Amex);
- Mobile wallets (e.g., Apple Pay, Google Pay);
- QR code-based payments and carrier billing (where available);
- Integration with existing rail ticketing applications or passenger account systems.

5.4.22.9 All transactions shall be processed in compliance with the Payment Card Industry Data Security Standard (PCI DSS) and applicable consumer protection regulations.

5.4.22.10 The PWS premium service shall be able to be purchased as an additional service during CHSR ticket purchasing via all the CHSR ticket purchasing mechanisms. Activation of PWS service will be by the authentication portal.

5.4.22.11 The PWS shall allow users to seamlessly upgrade from the basic service to the premium Wi-Fi service during the journey without requiring session termination or loss of connectivity.

PWS Network Architecture and Technology

5.4.22.12 The PWS proposed architecture shall utilize high-bandwidth, low-latency backhaul technologies, with a strong preference for mmWave-based Train-to-Tracksides (TtT) communications as the primary backhaul solution, particularly leveraging the unlicensed 60 GHz band for fixed wireless access at stations and along the rail corridor.

To augment coverage, availability, or performance, the solution may also incorporate or be supported by:



- 5G NR, including network slicing to optimize the passenger experience;
- Tracksides wireless, hybrid satellite-mmWave solutions, or equivalent technologies for onboard connectivity;
- WAN bonding or aggregation techniques to increase backhaul capacity and resilience;
- An access point antenna architecture appropriate for the physical train environment and concurrent user demand.

All proposed technologies shall be interoperable, scalable, and optimized for the railway operational and passenger environment.

5.4.22.13 The PWS shall feature:

- Wi-Fi 7 (IEEE 802.11be) access points and backward compatibility with Wi-Fi 6/6E/5;
- Intelligent session management and aggregation of available backhaul technologies as defined in 5.4.22.12;
- Seamless user roaming and load balancing across station and train networks.

5.4.22.14 The PWS RF components must be optimized for rail environments and shall not interfere with critical operational systems (e.g., TPS, FRMCS, ETCS).

5.4.22.15 The PWS shall implement full network traffic segregation between:

- Passenger traffic (public internet access);
- Backhaul, Network Management Systems and other control plane systems.

5.4.22.16 This segregation shall be enforced through VLANs, firewalls, and access control lists (ACLs) to prevent unauthorized lateral movement or eavesdropping between networks.

Voice-over-Wi-Fi (VoWiFi) Support

5.4.22.17 The PWS shall support Voice over Wi-Fi (VoWiFi) services in accordance with 3GPP TS 23.228 (IP Multimedia Subsystem - IMS), 3GPP TS 24.302 (IMS registration over untrusted non-3GPP access), and 3GPP TS 24.229 (IMS core network signaling) [R54].

5.4.22.18 The PWS shall enable seamless access to VoWiFi for passenger devices registered with major U.S. carriers, including at least AT&T, Verizon, T-Mobile, and UScellular, without any user device configuration changes. The system shall also support VoWiFi access for international roaming subscribers whose home operators support IMS-based Wi-Fi calling.

5.4.22.19 The PWS shall:

- Provide IPv4 and IPv6 support for IMS signaling and media traffic;
- Support IPsec encapsulation and tunneling of IMS traffic in accordance with 3GPP TS 33.402 [R55] for non-3GPP access security;
- Enable Quality of Service (QoS) classification and marking for IMS signaling and RTP media (e.g., via DSCP);
- Prioritize VoWiFi bearer traffic to maintain acceptable Mean Opinion Score (MOS) and minimize latency, jitter, and packet loss.

5.4.22.20 The PWS shall support Network Address Translation (NAT) traversal and appropriate firewall configurations to ensure VoWiFi signaling and media flows are not blocked or degraded.

5.4.22.21 The PWS shall support emergency VoWiFi calls (e.g., E911) by:

- Allowing device-originated emergency SIP calls to reach the mobile operator's IMS core;
- Supporting Location Information Server (LIS) interaction and/or enabling the device to transmit location metadata over Wi-Fi (e.g., via IETF RFC 6442 or 3GPP TS 23.167);



- Not impeding compliance with operator obligations to provide emergency services via VoWiFi.

PWS Usage Restrictions and Content Protection

- 5.4.22.22 The PWS shall implement content filtering mechanisms to restrict access to websites and online services that fall under any of the following categories:
- Malicious or phishing domains;
 - Known sources of malware, spyware, or ransomware;
 - Illicit content (e.g., child exploitation, illegal drug sales, human trafficking);
 - Violent or extremist material;
 - Gambling and explicit adult content;
 - Parental controls will be enabled.
- 5.4.22.23 The content filtering solution shall use a regularly updated threat intelligence feed and shall be configurable to comply with jurisdictional requirements, including those of schools or family-focused services.
- 5.4.22.24 The TSCC Contractor shall ensure compliance with applicable regulations concerning the protection of minors online, including COPPA (Children's Online Privacy Protection Act) and equivalent state legislation where applicable.
- 5.4.22.25 Attempts to access restricted content shall be intercepted with a branded informational page that clearly states the reason for the restriction.
- 5.4.22.26 The system shall log access attempts to restricted content for security auditing purposes, while ensuring compliance with privacy legislation (e.g., CCPA).

PWS Data Logging and Retention

- 5.4.22.27 The PWS shall log user traffic metadata for all active sessions. This includes, but is not limited to:
- Timestamp of session start and end;
 - Source and destination IP addresses;
 - MAC address of the connecting device;
 - Access point and train/station identifier;
 - Protocol type (e.g., HTTP, HTTPS, DNS);
 - Volume of data transmitted and received.
- 5.4.22.28 Logged metadata shall be logically associated with the authenticated user account, session token, or device identifier (e.g., MAC address) for traceability and auditing purposes.
- 5.4.22.29 Full packet inspection or payload capture shall not be performed, except for network diagnostics or legal interception purposes, and only under strict access control and authorization.
- 5.4.22.30 All logged data shall be retained securely for a period of 6 months, where the retention period shall be defined in accordance with applicable legal, regulatory, and operational requirements (e.g., CALEA compliance, internal security policies).
- 5.4.22.31 Access to log data shall be restricted to authorized personnel and protected through:
- Role-based access control (RBAC);
 - Audit trails of access and retrieval;
 - Multi-factor authentication for privileged users.



- 5.4.22.32 All retained data shall be stored in encrypted form (at rest and in transit) and in compliance with data protection laws including the California Consumer Privacy Act (CCPA) [R99], the California Electronic Communications Privacy Act (CalECPA) [R100], and any applicable federal regulations.
- 5.4.22.33 Upon expiry of the retention period, logs shall be securely deleted or anonymized in accordance with documented data disposal procedures.
- 5.4.22.34 Users shall be notified via the Wi-Fi login portal or privacy policy that metadata logging is performed and retained, along with a summary of their data rights under CCPA [R99].

5.5 Performance Requirements

- 5.5.1 The WCS FRMCS and PWS shall support all required voice, data, and control communications with no degradation in quality, latency, or handover performance at train speeds up to 220 mph (354 km/h) and dynamic integration testing at 242 mph. The system shall ensure uninterrupted connectivity for mobile users and onboard systems during all high-speed operations, while meeting performance targets.
- 5.5.2 All WCS coverage requirements shall be evaluated under peak revenue service conditions, including during passenger peak hour periods. Coverage verification assessments shall account for body absorption and crowd density effects, ensuring that signal strength and quality meet specified performance thresholds in fully occupied environments. The TSCC Contractor shall prepare and submit a detailed coverage verification report to the Authority, including methodology, measurement results, analysis, and any identified non-compliances or remedial actions.
- 5.5.3 The WCS shall comply with the RAM requirements defined in Schedule 1 – Safety, Security and RAM Requirements.

5.5.4 Future Mobile Radio Communication System

- 5.5.4.1 All FRMCS voice, data, and video shall meet the 3GPP MCX performance targets, as per TS 22.179:
- MCPTT call setup time ≤ 300 ms (95% of attempts);
 - MCPTT end-to-end voice latency ≤ 300 ms;
 - MCPTT speech intelligibility: Maintain intelligible voice under packet loss up to 5% and variable bitrates;
 - MCPTT Mean Opinion Score (MOS): ≥ 4.0 under nominal network conditions using POLQA for AMR-WB or EVS codecs;
 - MCPTT Codec Support: System shall support AMR-WB and optionally EVS, with forward error correction as per 3GPP TS 26.114 and TS 26.116 MCDATA transfer latency ≤ 1 second for 1 kB control message;
 - MCVideo start-up time ≤ 1 second, with video latency ≤ 500 ms;
 - Guaranteed QoS class identifiers (QCI) per 3GPP TS 23.203 or 5QI per TS 23.501.

Performance shall be validated through objective testing (e.g., POLQA, E-model, or equivalent) and documented in the TSCC Contractor's System Test and Verification Plan which will be submitted to the Authority for approval.

- 5.5.4.2 The FRMCS shall provide seamless radio coverage for MCX services (voice, video, and data) in all areas where trainset movement, operational control, and maintenance activities take place, in accordance with the coverage expectations outlined in 3GPP TS 22.179, TS 23.179, and TS 22.280.
- 5.5.4.3 The FRMCS shall ensure, under normal, degraded, and emergency operating conditions:
- 100% geographical FRMCS coverage across the EOS CHSR System;
 - Signal strength of -95 dBm or better RSRP (for 5G) with a coverage probability of 95% at the antenna input of end-user devices in all operational areas;



- Coverage design shall assume an antenna height of 4 meters above rail level for train-mounted rooftop antennas operating within the railway Right-of-Way, and 1 meter above ground level for handheld radio devices used in stations, yards, maintenance facilities, and operational areas;
 - Indoor FRMCS coverage (if required) in OCC and stations via DAS, repeaters, or base station coverage;
 - Signal availability shall be maintained during typical propagation impairments, including body blockage, high-speed movement up to 220 mph (354 km/h), and multipath fading.
- 5.5.4.4 FRMCS coverage performance shall be validated via drive testing, walk testing, or trainset testing consistent with 3GPP TR 36.942, ITU-R P.1238, and P.1812.
- 5.5.4.5 The FRMCS shall be dimensioned to support peak concurrent usage of mission-critical services, including MCPTT, MCVideo, and MCData, during normal operations, planned events, and emergency scenarios. The system shall support the maximum operational train frequency without degradation in service performance. Performance shall align with 3GPP-defined KPIs for latency, availability, and call setup times as specified in TS 22.179, TS 23.179, and TS 28.313, and shall support simultaneous talkgroup communications, emergency call handling, and dynamic resource allocation under congested or degraded conditions.
- 5.5.4.6 The TSCC Contractor shall determine the minimum effective per-user downlink and uplink throughput required to support the full suite of services, including MCX and ETCS, at maximum train frequency. The FRMCS shall be designed to meet or exceed these throughput levels across the entire alignment, including in tunnels, trenches, cuttings, and viaducts, under both normal and degraded network conditions.
- 5.5.4.7 The FRMCS network shall also be dimensioned to support all operational and safety-critical communications across the CHSR System. OCC traffic controllers shall be able to maintain uninterrupted communication with all trainsets in their jurisdiction at all times. Baseline capacity shall include reasonable headroom for future extensions or reconfigurations, without requiring major capital investment.
- 5.5.4.8 All capacity planning assumptions, service profiles, and dimensioning models shall be documented in the TSCC Contractor's System Design and Performance Plan. Compliance with capacity and throughput requirements shall be validated during Factory and Site Acceptance Testing under simulated peak-load conditions.
- 5.5.4.9 The FRMCS shall be designed and optimized to achieve a handover success rate of at least 99.5% under normal operational conditions. Handover procedures shall maintain active sessions for all mission-critical services, including voice, video, and data, without perceptible service degradation or dropouts.
- 5.5.4.10 The FRMCS shall be configured to avoid unnecessary handovers and cell reselections, including so-called "ping-pong" effects, through appropriate parameter tuning (e.g., hysteresis, time-to-trigger). Cell mobility behaviors shall be optimized for high-speed train movements, including in coverage overlap areas, tunnels, and viaduct transitions.
- 5.5.4.11 The FRMCS shall support configurable prioritization of voice, data, and video communications in accordance with the operational requirements defined by the Authority. The system shall:
- Enable assignment and enforcement of QoS, Priority, and Pre-emption parameters on a per-service and per-user basis;
 - Support dynamic configuration and policy control using mechanisms defined in 3GPP TS 23.501 and TS 23.503;
 - Ensure that Mission-Critical services such as MCPTT, MCData, and MCVideo are mapped to appropriate 5QI (5G QoS Identifier) values, with support for guaranteed bit rate (GBR) and non-GBR flows as required;
 - Allow the Authority to define priority levels for specific user roles (e.g., drivers, controllers, maintenance staff) and use cases (e.g., emergency, routine, background);



- Ensure that all prioritization policies are enforced consistently across the 5G/FRMCS Core, RAN, and DCN segments;
- Provide the Authority with the capability to update prioritization policies through a secure configuration management interface.

5.5.4.12 If 3rd party infrastructure sharing is utilized (e.g. 5G Slicing), the FRMCS shall provide call prioritization, preemption, and quality-of-service control to maintain communication integrity during congestion under normal, degraded, and emergency conditions.

5.5.4.13 If Time Division Duplexing (TDD) is used within the FRMCS, all base stations shall maintain an absolute time alignment with a common time reference, with a maximum network-wide time deviation not exceeding 1.5 microseconds. This synchronization requirement ensures proper frame alignment and mitigates inter-cell interference in TDD-based deployments.

Backup Power

5.5.4.14 FRMCS BBU Hotel locations shall be equipped with standby generators capable of supporting full system load for a minimum of 24 hours. Fuel storage and refueling provisions shall be sufficient to maintain continuous operation for the specified duration under normal and emergency conditions. The BBU hotel locations will have sufficient battery backup for the standby generator to operate efficiently.

5.5.4.15 FRMCS RRH locations shall be equipped with rectifiers and battery backup systems capable of sustaining operations for a minimum of 12 hours in the event of Medium/Low Voltage Power System (LVPS) failure. The battery systems shall be appropriately rated, monitored, and maintained to ensure reliable performance under all environmental conditions. The batteries shall be dimensioned for 12 hours autonomy at the end of their serviceable lifetime.

5.5.4.16 All FRMCS locations shall be provided with an external connection point for a backup generator to enable temporary power supply during outages of the LVPS, including BBU Hotel in case of on-site standby generator failure or maintenance. This provision shall ensure uninterrupted operation of all critical WCS functions during LVPS failures, planned maintenance, or emergency situations. At shared locations, like Traction Power or Signaling, standby generators can be shared.

5.5.4.17 All FRMCS backup power systems will have alarming and monitoring integrated into either the WCS NMS and/or the Integrated Control and Supervisory System (ICSS), to ensure power, generator and battery status and optimal performance can be monitored at all times. Refer to Integrated Control and Supervision System Technical Specification.

5.5.5 Dispatch Consoles

5.5.5.1 WCS Dispatch Consoles in the OCC shall be designed to maintain 99.999% availability (five-nines) and be connected via redundant paths to the WCS core infrastructure.

5.5.6 Emergency Responder Communication System

5.5.6.1 The ERCS shall maintain:

- Voice communication latency ≤ 300 milliseconds round-trip;
- System availability $\geq 99.99\%$ annually in all emergency-critical locations;
- Uptime during grid outages through backup power (minimum 2 hours per code).

5.5.7 Passenger Wi-Fi System

5.5.7.1 The Passenger Wi-Fi System (PWS) shall be designed, delivered, and operated with the objective of achieving high levels of customer satisfaction and becoming a valued service offering of the train operator. To this end:

- The TSCC Contractor shall implement all reasonable measures to ensure the service is perceived as fast, reliable, and easy to use by the majority of passengers;



- The TSCC Contractor shall maintain a minimum Passenger Satisfaction Rating of 85% (as measured through periodic user surveys or feedback mechanisms approved by the Authority) and shall demonstrate continuous improvement in response to passenger feedback;
 - Failure to maintain this satisfaction threshold over two consecutive reporting periods may trigger remedial action, including the submission of a formal Service Improvement Plan, subject to Authority approval.
- 5.5.7.2 At a minimum, the end user experience of PWS performance (in terms of reliability, speed, ease of access, and media streaming capability) shall be comparable to that provided on leading commuter and intercity rail services such as Caltrain, Amtrak, Brightline West or equivalent high-speed rail international benchmarks. Submissions should clearly outline how proposed solutions meet or exceed and ability to maintain these benchmarks.
- 5.5.7.3 The end-to-end network should support a minimum aggregate backhaul capacity of 2 Gbps per trainset with higher performance solutions preferred.
- 5.5.7.4 Each active passenger device shall experience:
- Sustained minimum download speed of 20 Mbps;
 - Latency less than 50 milliseconds to common public internet endpoints;
 - Jitter less than 20 milliseconds when using common public internet services;
 - Ability to stream HD video (Netflix/YouTube), use real-time communication (VoIP/video calls/messaging services), and cloud-based applications (Microsoft Teams/Slack/Webex).
- 5.5.7.5 The PWS shall support a minimum of 450 concurrent users per trainset. Two trainsets may be coupled together for service. A double-traction train will carry a minimum of 900 passengers.
- 5.5.7.6 The PWS shall provide 99.5% monthly uptime per trainset.
- 5.5.7.7 There are no additional backup power requirements for PWS.

5.6 Security and Cybersecurity Requirements

- 5.6.1 All WCS equipment locations shall have CCTV coverage to mitigate the risk of theft of copper, batteries, generators, and other critical infrastructure. This includes installing CCTV on radio towers to provide additional coverage. CCTV systems shall be designed and installed in accordance with the CCTV Technical Specification [R90]. CCTV footage from these locations shall be transmitted to the OCC in real-time for monitoring, recording, and incident response purposes.
- 5.6.2 The WCS system shall nominate a System Owner that is accountable for cybersecurity risk ownership and mitigation.
- 5.6.3 All WCS equipment locations shall utilize the Electronic Access and Control System. Refer to Electronic Access and Control System Technical Specification.
- 5.6.4 The design of the security systems for the WCS radio sites shall be compliant with the CCTV System and Electronic Access and Control System Technical Specifications .
- 5.6.5 The WCS design shall be in full compliance with the Authority's cybersecurity policies specified in Cybersecurity Technical Specification.
- 5.6.6 The WCS security requirements shall mature over time based upon national and international standards and guidelines. Submissions should clearly outline how proposed solutions meet or exceed and the ability to maintain best industry practice security compliance.

Network Management System

- 5.6.7 The WCS Network Management System (NMS) shall enforce strict access control measures. All user access shall require individual credentials and be authenticated via role-based access control (RBAC) mechanisms. Administrator access shall require multifactor authentication (MFA). Default credentials must be changed prior to commissioning. Authentication, authorization, and access control requirements



shall be compliant with the Cybersecurity Technical Specification, specifically the least-privilege design principle and access review requirements.

- 5.6.8 The NMS shall generate and securely retain audit logs of all user activity, configuration changes, login attempts, and system events. Logs shall include timestamps, user IDs, IP addresses, and event types. Logs shall be protected against tampering and accessible only by authorized personnel.
- 5.6.9 All management communications between the NMS and network elements shall be encrypted using TLS 1.3. Remote access to the NMS shall be centrally managed and must be compliant with the remote access requirements defined in the Cybersecurity Technical Specification.
- 5.6.10 The NMS operating environment shall be hardened in accordance with vendor or industry security guidelines / best practices. All unnecessary services and ports shall be disabled. The operating system and application software shall be regularly updated with security patches. Patching shall be completed in accordance with change management processes and vulnerability and patch management requirements outlined in the Cybersecurity Technical Specification.
- 5.6.11 The NMS shall enforce session timeouts and automatic logoff for inactive sessions. Concurrent sessions shall be logged and optionally restricted by policy. Session Management, including session timeouts, shall be implemented and configured in compliance with the Cybersecurity Technical Specification, including remote access or local access to NMS systems.
- 5.6.12 The NMS shall support integration with external Security Information and Event Management (SIEM) systems via syslog or equivalent protocols that are supported by the target SIEM. The NMS TSCC Contractor shall be responsible for coordinating with the SIEM configuration team to ensure that adequate and relevant security event information is correctly formatted and ingested. The system shall support anomaly detection and alerting for suspicious behavior. Refer to Cybersecurity Technical Specification.
- 5.6.13 The NMS platform shall include or support the integration of endpoint protection tools. The system shall be regularly scanned for known threats, and alerts shall be generated for any detected issues.
- 5.6.14 Configuration data and logs from the NMS shall be regularly backed up to a secure, access-controlled storage location. Backup integrity shall be tested periodically, and recovery procedures shall be defined and documented. Backup and restoration technology, processes, and procedures shall align with the backup and restoration requirements defined in the Cybersecurity Technical Specification.
- 5.6.15 The TSCC Contractor shall implement a documented process for assessing, testing, and applying security patches to the NMS software and operating system, in line with a defined patching schedule and risk profile.
- 5.6.16 The NMS cybersecurity controls shall comply with applicable standards, including ISO/IEC 27001, NIST SP 800-53, and relevant rail cybersecurity guidance (e.g., EN 50701 where adopted). The TSCC Contractor shall provide evidence of security compliance during system design review and acceptance testing.
- 5.6.17 The NMS shall be configured to support the network security and network segmentation design as defined in the Cybersecurity Technical Specification by monitoring and verifying network configurations and producing alerts where non-compliance or anomalies are detected.
- 5.6.18 **Future Mobile Radio Communication System**
 - 5.6.18.1 The FRMCS shall implement end-to-end encryption, mutual authentication, and user role verification as defined in 3GPP mission-critical service specifications and UIC FRMCS security guidance. Refer to Cybersecurity Technical Specification for further details on access controls, encryption, and mutual authentication.
 - 5.6.18.2 Access to FRMCS devices, WCS Dispatch Consoles, and network interfaces shall require user and device authentication, with support for Role-Based Access Control (RBAC) and audit logging.
 - 5.6.18.3 The FRMCS shall be implemented with Control Plane and User Plane network segmentation, firewall protection, and intrusion detection mechanisms to isolate operational communications from non-critical services.



- 5.6.18.4 All ingress and egress traffic between the FRMCS network and any external or interconnected networks (including but not limited to the NMS/ICSS, SIEM, TMS, etc.) shall be explicitly controlled through stateful firewalls. The default policy for all firewall rules shall follow a deny-by-default approach, permitting only traffic that is explicitly defined and authorized in accordance with the Cybersecurity Technical Specification.
- 5.6.18.5 Each interconnection point between the FRMCS network and external networks shall be protected by a firewall or security gateway that supports granular packet filtering, deep packet inspection, logging, and intrusion detection/prevention capabilities. These firewalls shall be configured to restrict traffic to the minimum set of required ports, protocols, and IP addresses necessary for each interface's operational function.
- 5.6.18.6 An Intrusion Detection System (IDS) shall be deployed at key points within the FRMCS architecture to monitor network traffic for signs of malicious activity or policy violations. The IDS shall be integrated with the Security Operations Centre (SOC) and Security Information and Event Management (SIEM) platform to enable real-time alerting, forensic analysis, and correlation with other network events. At a minimum, IDS sensors shall be placed at:
- The boundary between the FRMCS core network and external systems;
 - Within the FRMCS core network to monitor control and user plane traffic;
 - At network aggregation points where traffic from the Radio Access Network enters the transport/core network.
- 5.6.18.7 The design and configuration of the IDS shall follow the segmentation, zoning, and threat detection principles defined in the Cybersecurity Technical Specification.

5.6.19 Dispatching Consoles

- 5.6.19.1 WCS Dispatch Consoles shall enforce role-based access control, session timeout, and two-factor authentication for all OCC users accessing WCS systems. Shared or generic user accounts shall not be able to be utilized.
- 5.6.19.2 The WCS Dispatch Consoles shall support federated identity authentication and single sign-on (SSO) in accordance with industry-standard protocols such as SAML 2.0, OAuth 2.0, or OpenID Connect (OIDC). The system shall enable dispatch personnel to authenticate using credentials from CHSR Authority corporate accounts, and shall allow seamless access to all authorized FRMCS functions and integrated applications without requiring repeated logins.
- 5.6.19.3 All communications between dispatch consoles and WCS infrastructure shall be encrypted using FIPS 140-2 compliant cryptographic algorithms, with audit logging enabled for all access, configuration changes, and communication events.

5.6.20 Emergency Responder Communication System

- 5.6.20.1 The ERCS shall use secure, encrypted communication protocols conforming to public safety standards:
- AES-256 encryption for P25 and FirstNet services;
 - Compliance with NIST 800-53 and FirstNet security frameworks.
 - **Passenger Wi-Fi System**
 - The PWS shall implement:
 - WPA3 encryption or higher on all access points;
 - TLS-based secure authentication and data encryption;
 - Logical and physical network segmentation between passenger and operational systems, including the use of distinct SSIDs for each network to ensure isolation of traffic, enforce access control policies, and prevent cross-network interference or compromise.



5.6.20.2 The PWS must comply with:

- Local data protection laws (e.g., California Consumer Privacy Act (CCPA));
- FCC radio frequency licensing and telecommunications regulations.



6 INTERFACE REQUIREMENTS

6.1 General Requirements

6.1.1 Interfaces are classified as below:

- Third Party interfaces: interfaces between TSCC systems and systems provided by Third Party (excluding CHSR contractors);
- External interfaces: interface between TSCC systems and systems provided by CHSR TSCC Contractors (Civils Packages, stations contractor, facilities contractor, Solar PV and BESS contractors);
- Internal interfaces between systems within the TSCC scope.

6.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.

6.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.

6.1.4 The identified WCS Third Party, External and Internal interfaces are represented in [Figure 28](#) below.

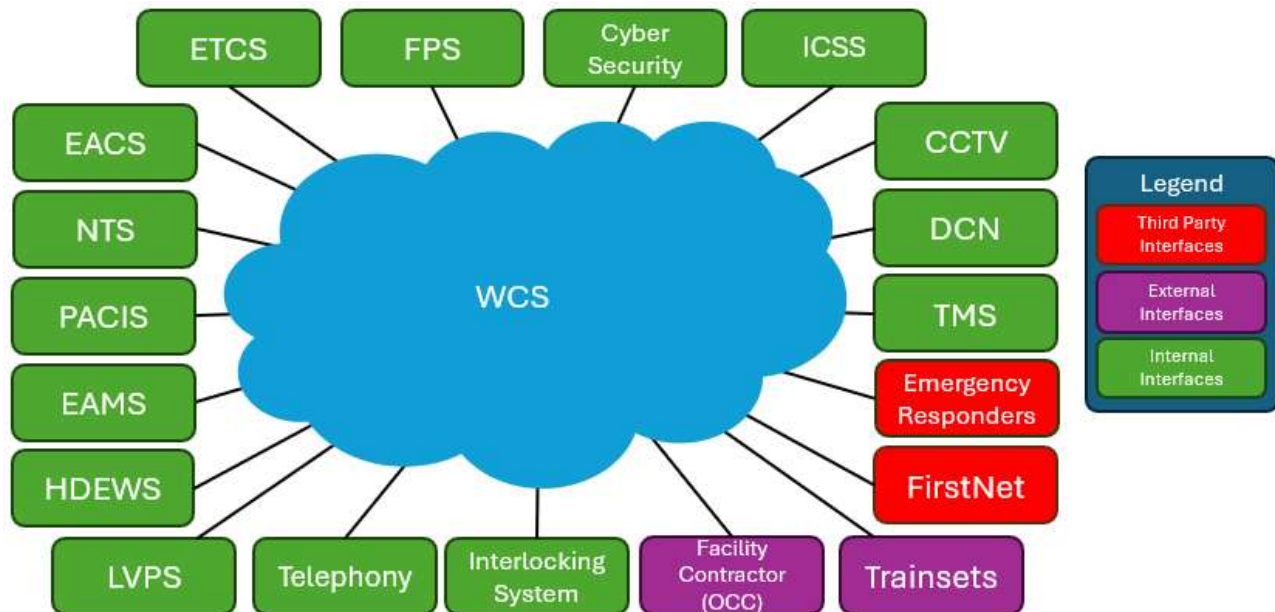


FIGURE 28: WCS THIRD PARTY, EXTERNAL AND INTERNAL INTERFACES.

6.2 Third Party Interfaces

The following section provides requirements associated with the Third Party interfaces between WCS and other systems.

6.2.1 With regard the Third Party interface, the TSCC Contractor shall follow the process defined in the Authority Interface Management Plan and shall support the Authority in developing the requirements and a scope split with related stakeholders. The TSCC Contractor shall execute the Third Party interfaces based on defined requirements and scope split.

6.2.2 The TSCC Contractor shall implement an external interface to enable interoperability between the FRMCS/MCX system and external Project 25 (P25) Land Mobile Radio (LMR) networks used by Emergency Responders during normal and emergency operations via the IWF.

6.2.3 The interface shall:



- Connect to external P25 systems via standardized interfaces, including but not limited to the Inter-RF Subsystem Interface (ISSI) and/or Console Subsystem Interface (CSSI) as defined in TIA-102;
 - Support exchange of group and individual voice calls between FRMCS/MCX users (e.g., train drivers, OCC dispatchers) and P25 radio users, with transparent PTT behavior and call continuity;
 - Enable emergency call bridging and participation in inter-agency talkgroups, including dynamically assigned talkgroups during coordinated incident response;
 - Apply appropriate identity mapping and alias translation, ensuring P25 user identifiers are visible and meaningful to FRMCS/MCX users and vice versa;
 - Maintain QoS, call priority, and preemption behavior across the interface in accordance with the priority schemes used in both systems;
 - Include all necessary physical, protocol, and security configurations to support the interface, including encryption handling, firewall rules, IP routing, and port configurations.
- 6.2.4 The TSCC Contractor shall work collaboratively with the Authority and relevant Emergency Responders to define interface parameters, talkgroup mappings, testing protocols, and failover behavior during the integration planning phase.
- 6.2.5 The TSCC Contractor shall provide an external interface between the FRMCS and FirstNet, to support interoperable mission-critical communications between railway operational users and external emergency responders.
- 6.2.6 The interface shall support the following capabilities:
- Mission-Critical Services interworking, including MCPTT, MCVideo, and MCData, in accordance with 3GPP TS 23.283 (LMR/MCX interworking) and TS 23.379 (inter-PLMN MCX service interworking);
 - Use of a Security Edge Protection Proxy to enable secure inter-PLMN signaling exchange over the N32 interface, with end-to-end integrity, encryption, and topology hiding;
 - User authentication, identity federation, and QoS coordination, allowing authorized FirstNet users to participate in railway-specific talkgroups or receive real-time incident communications during joint operations;
 - Support for dynamic group creation, inter-agency call patching, and roaming or guest access subject to policy-based control by the Authority;
 - Compliance with all applicable cybersecurity, privacy, and interoperability requirements, including adherence to PCI DSS, FIPS 140-2, and relevant federal or jurisdictional public safety interconnection standards.
- 6.2.7 The TSCC Contractor shall work with the Authority, FirstNet Authority and FirstNet operator to define interconnection parameters, network trust models, and service-level expectations prior to deployment.
- 6.2.8 The TSCC Contractor shall co-ordinate with the other D&B contractors to include but not limited to planning approvals.
- 6.2.9 The WCS shall interface with the on-board system of trains (scope of trainset contractor, to enable voice / data traffic, emergency calls, selected on board alarm/status information and on-board public address announcements).
- 6.2.10 The WCS core networks and Dispatch Consoles shall be located at the OCC. The TSCC Contractor shall liaise with the OCC TSCC Contractor to ensure that the OCC meets the WCS requirements.
- 6.2.11 The TSCC Contractor shall ensure that the WCS integrates, where required, with the Asset Management System being provided under a different CHSR contract.
- 6.2.12 The WCS, PWS and FRMCS (5G Core) shall interface with the internet firewalls/gateway at the OCC via the DCN.



6.3 External Interfaces - Trainsets

The following section provides requirements associated with the External Interface between the TSCC Contractor and Trainset contractor to deliver the onboard WCS components.

- 6.3.1 The TSCC Contractor shall be responsible for providing the Trainset contractor, in a timely manner and in alignment with the approved project schedule, all high-level designs, interface designs, technical specifications, and technical documentation necessary to support the integration of onboard WCS subsystems. This shall include, but not be limited to:
- Equipment specifications;
 - Physical and electrical interface specifications;
 - Equipment power requirements;
 - Space and mounting requirements;
 - Environmental and cooling requirements;
 - Antenna placement guidelines and RF cable routing information;
 - Data connectivity and signal interface details;
 - Installation and commissioning procedures.
- 6.3.2 All documentation shall be sufficiently detailed to enable the Trainset Contractor to proceed with detailed design, procurement, and installation activities without delay.
- 6.3.3 The Trainset Contractor shall be responsible for the installation design, procurement and supply of onboard WCS equipment (as specified by the TSCC Contractor), provision of power and cabling, mounting provisions, installation, and integration with other trainset systems. The Trainset Contractor shall also perform onboard commissioning and testing in accordance with the interface documentation and requirements provided by the TSCC Contractor.
- 6.3.4 The TSCC Contractor shall provide comprehensive support for the integration and commissioning of the onboard WCS subsystems. This includes:
- Bench and factory testing of WCS equipment;
 - Supervision and technical support during installation;
 - Integration and configuration of systems onboard;
 - Functional verification and interoperability testing;
 - Coordination with the Trainset Contractor to ensure compliance with the Technical Specifications and interface requirements.
- 6.3.5 Support shall be provided both remotely and onsite as requested by the Trainset Contractor and/or the Authority to ensure successful system integration.
- 6.3.6 The TSCC Contractor and Trainset Contractor shall share joint responsibility for verifying the correct operation of the onboard WCS subsystems during dynamic testing, including full end-to-end system functionality. Any non-conformances or integration issues identified during testing shall be investigated and resolved collaboratively, in accordance with the project's integration, test, and defect resolution procedures. Final handover shall not proceed until both parties have confirmed resolution of all critical issues affecting system performance or compliance.

6.4 External Interfaces – stations contractor

- 6.4.1 The TSCC Contractor shall ensure that the PWS core network shall allow the integration of station contractor's Wi-Fi access network.
- 6.4.2 The TSCC Contractor shall provide all required information to station contractor to facilitate the design and integration.



6.5 External Interfaces – facilities contractor

- 6.5.1 The TSCC Contractor shall install all WCS core network equipment in the OCC being provided by the facilities contractor.
- 6.5.2 The TSCC Contractor shall provide to the facilities contractor:
- Equipment dimensions
 - Equipment clearances requirements
 - Equipment mounting and fixings requirements
 - Cable routes/containment requirements
 - Equipment loadings
 - Installation and maintenance requirements
 - Equipment heating loads
 - Equipment cooling loads
 - Equipment hydraulic requirements
- 6.5.3 To be provided by facilities contractor to accommodate the TCSS equipment installation and operational/maintenance requirements:
- Room dimensions and layouts
 - Room facilities (Plumbing, HVAC, Lighting, Fire Protection Systems, Doors, electricity)
 - Room raised floor system
 - Delivery access routes.
 - Maintenance access routes

6.6 Internal Interfaces

6.6.1 Interface with Digital Communications Network (DCN)

- 6.6.1.1 The FRMCS core network infrastructure shall have redundant interface with the DCN to ensure secure and reliable transport of FRMCS data and to provide resilient interconnection between all FRMCS BBU Hotel and RRH sites and the core network infrastructure.
- 6.6.1.2 The FRMCS and DCN shall be integrated in a manner that enables FRMCS fixed and handheld devices to securely and reliably access data and services provided by other systems connected to the DCN.
- 6.6.1.3 The FRMCS DCN backhaul transmission shall be implemented with a ring-based architecture to enable automatic rerouting of communications to the core network in the event of a DCN transmission link or node failure. This design shall ensure continuity of service by utilizing redundant DCN transmission paths between FRMCS radio sites, specifically BBU Hotels, and between FRMCS and the DCN, maintaining full network connectivity and resilience along the CHSR Right-of-Way.
- 6.6.1.4 The FRMCS core network shall have redundant interface with the DCN Firewall and/or Broadband Network Gateway.
- 6.6.1.5 The PWS trackside transmitters shall interface with the DCN switches at trackside equipment shelters via dark fiber, and the PWS core network infrastructure shall interface with the DCN at the OCC, via dedicated VLAN.
- 6.6.1.6 The PWS shall interface with the DCN management VLANs to support remote monitoring, configuration, and performance logging of PWS components.
- 6.6.1.7 The PWS core network shall interface with the DCN firewall to manage secure access to internet-hosted services, including cloud-based content filtering and system updates.



- 6.6.1.8 The PWS transmitters shall connect to the DCN via managed trackside Ethernet switches capable of supporting VLAN segmentation and Quality of Service (QoS) for PWS traffic.
- 6.6.2 Interface with European Train Control System (ETCS)**
- 6.6.2.1 The onboard FRMCS radios shall interface with the onboard ETCS system to enable the exchange of safety-critical signaling data, including the transmission of train position reports from the ETCS to the RBC and the reception of Movement Authority messages from the RBC via FRMCS. This interface shall support the establishment and maintenance of a dedicated and secure communication session between the train and the trackside ETCS infrastructure.
- 6.6.2.2 The interface between the FRMCS and ETCS systems, both onboard and core network, shall meet Safety Integrity Level 4 (SIL 4) as defined in EN 50126, EN 50128, and EN 50129, to ensure the safe transmission and reception of signaling information critical to train operation. Compliance shall be demonstrated through appropriate safety case documentation and certification.
- 6.6.2.3 The FRMCS shall have redundant interface with the ETCS Radio Block Center (RBC) system for enabling exchange of signaling information (Movement Authority). The RBC receives the train position from the onboard ETCS via FRMCS and sends the authorization for the train to continue running. The authorization is sent to the train through a dedicated and safe communication session.
- 6.6.3 Interface with Telephony System**
- 6.6.3.1 The FRMCS shall have a redundant interface with the Telephony System, which acts as the central switching system for phone calls. The telephony system handles internal traffic between stations and acts as the gatekeeper to the outside world.
- 6.6.3.2 The Dispatch Consoles shall be integrated with the Telephony System, which acts as the central recording and logging system for all Dispatch Consoles and FRMCS voice, data and metadata.
- 6.6.3.3 The Telephony System shall provide the voice, data and metadata recording and logging capabilities of the FRMCS.
- 6.6.4 Interface with Network Timing System (NTS)**
- 6.6.4.1 The FRMCS shall have redundant interface with the NTS for accurate current time display and for precise calculations required for time estimation.
- 6.6.4.2 The NTS shall integrate with the FRMCS BBU Hotels to provide precise time and frequency synchronization using IEEE 1588v2 Precision Time Protocol and/or Synchronous Ethernet, ensuring coordination of time-sensitive functions such as radio resource management, handover, and TDD frame alignment across the FRMCS Radio Access Network.
- 6.6.4.3 The PWS core system shall interface with the NTS provided by the DCN to ensure time synchronization across all PWS components for logging, monitoring, and coordination purposes.
- 6.6.5 Interface with Integrated Control and Supervisory System (ICSS)**
- 6.6.5.1 The WCS NMS shall integrate with the ICSS to enable end-to-end monitoring, fault management, and performance reporting of the WCS infrastructure. This integration shall support standard interfaces and protocols to ensure compatibility with ICSS subsystems, and allow for centralized visibility and control within the broader operational management environment.
- 6.6.6 Interface with Train Management System (TMS)**
- 6.6.6.1 The FRMCS shall accept MCX Application Server API calls, such as Dynamic Talkgroup Reassignment, from the Train Management System and other TSCC subsystems interconnected via the DCN.
- 6.6.7 Interface with Medium/Low Voltage Power System**
- 6.6.7.1 All FRMCS RAN infrastructure, BBU Hotel and RRH cabinet locations, shall be powered by the MV+LV Power System.
- 6.6.7.2 All PWS trackside transmitters shall be powered by the MV+LV Power System.



- 6.6.7.3 All WCS core network equipment at the OCC shall be powered by the MV+LV Power System.
- 6.6.8 **Interface with Passenger Announcement and Customer Information System (PACIS)**
 - 6.6.8.1 The FRMCS shall integrate with the PACIS at the core network and on the trainset, to allow Passenger Announcements to be made in the OCC and broadcast in the trainset, and for Customer Information System onboard the trainset to be updated from the OCC.
- 6.6.9 **Interface with Cybersecurity**
 - 6.6.9.1 The FRMCS shall integrate with all Cybersecurity infrastructure and follow all implementation guidance as specified in the Cybersecurity Technical Specification
- 6.6.10 **Interface with Fire Protection System (FPS)**
 - 6.6.10.1 All WCS equipment shelters shall be protected by the FPS.
- 6.6.11 **Interface with Electronic and Access Control System (EACS)**
 - 6.6.11.1 All WCS equipment locations, apart from trackside cabinets and transmitters, shall have access controls provided by the EACS.
- 6.6.12 **Interface with Interlocking System (IXL)**
 - 6.6.12.1 The FRMCS shall provide wireless communication between Trackside Worker Protection Devices, that are in a handheld ruggedized tablet form factor, and the Interlocking System. The FRMCS shall provide high priority for mission-critical (safety-critical) communications.
- 6.6.13 **Interface with Enterprise Asset Management Systems (EAMS)**
 - 6.6.13.1 The FRMCS shall provide wireless communication between official handheld devices and the Enterprise Asset Management Systems to allow CHSR personnel to access core system functionality through mobile or web browser-based applications.
 - 6.6.13.2 The WCS shall provide static WCS Asset Information and dynamic Asset Information to the EAMS for maintenance activities and asset lifecycle management activities.
- 6.6.14 **Interface with other TSCC Sub-systems (TSCC's)**
 - 6.6.14.1 The FRMCS core network shall be integrated with other TSCC's via the DCN, to support secure connectivity between fixed and mobile FRMCS devices and other TSCC's. This capability shall enable authorized users to access core system functionality through mobile applications or web-based interfaces on FRMCS devices. This capability shall also enable automated systems to access core system functionality, such as Hazard Detection and Early Warning System.
- 6.6.15 **Interface with other WCS Sub-systems**
 - 6.6.15.1 The FRMCS Core Network, specifically the Inter-Working Function, shall integrate into the ERCS to facilitate the interface between the WCS Dispatch Consoles and external Emergency Responder systems.
 - 6.6.15.2 The WCS NMS shall integrate with and monitor the WCS subsystems.



7 MATERIAL, PRODUCT AND COMPONENT REQUIREMENTS

7.1 General Requirements

- 7.1.1 All materials supplied by the TSCC Contractor shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards. Refer to 2.4.
- 7.1.2 All materials supplied shall be of sufficient grade and quality to meet the design lifetime requirements.

7.2 Software and Hardware Requirements

- 7.2.1 The FRMCS and ERCS design shall be based on COTS, open architecture, and modular system architecture, with standard 3GPP non-proprietary interfaces.
- 7.2.2 The PWS design shall be based on COTS, open architecture, and modular system architecture, with standard non-proprietary interfaces for the subcomponents that are supported by standardized interfaces (e.g., Wi-Fi7, IP, etc.). It is acknowledged that mmWave trainset to track solutions are not standardized.
- 7.2.3 The FRMCS servers shall have redundant architecture including hardware, power supply, cabling and software so that FRMCS functionality remains available during any one failure of hardware, power supply, cabling and software.
- 7.2.4 All WCS cabling shall be designed, supplied, and installed and commissioned by TSCC Contractor.
- 7.2.5 All WCS cabling shall operate in the temperature range from -35 °C to 85 °C and comply with section 5.2 Environmental Requirements.
- 7.2.6 All WCS cabling shall comply with applicable U.S. standards and codes, including the National Electrical Code (NEC), NFPA 70, and relevant UL or ASTM standards for fire resistance, smoke propagation, and installation in commercial and transportation environments. Cabling shall be listed or certified by a Nationally Recognized Testing Laboratory.
- 7.2.7 The coaxial cables connecting the RRH to the antennas shall be dimensioned to guarantee the maximum transfer of power to the antennas.
- 7.2.8 All WCS antennas shall be designed, supplied, and installed and commissioned by TSCC Contractor. FRMCS antenna pans and tilts shall be validated post construction to ensure optimal operation.
- 7.2.9 All antennas for FRMCS shall support electronic tilt.
- 7.2.10 All RRH for FRMCS shall operate in the temperature range from -35 °C to +70 °C and shall have a minimum IP67 design, and comply with section 5.2 Environmental Requirements.
- 7.2.11 All WCS core network infrastructure for shall be designed, supplied, and installed and commissioned by TSCC Contractor.
- 7.2.12 All WCS core network infrastructure shall be dimensioned and licensed to guarantee the performance of the services needed for the complete functioning of the WCS.
- 7.2.13 The TSCC Contractor shall supply all necessary software licenses required for the operation, management, and maintenance of the WCS. All licenses shall include sufficient headroom to accommodate expected future capacity growth, as defined by the Authority's forecasted system expansion, without requiring additional procurement or renegotiation within the initial operational period.

7.3 Radio Site Preparation Requirements

- 7.3.1 All the requirements concerning the site preparation, e.g., civil works, fencing, access and technical buildings are described in the Scope of Work.
- 7.3.2 The FRMCS radio sites shall be designed, constructed, operated and maintained as per the requirements in section 5.1.22.7 Environmental Requirements.
- 7.3.3 FRMCS radio site locations shall be selected and designed to ensure safe, secure, and practical operation and maintenance. Site selection shall avoid hazard areas like flood-prone areas and vehicular crash risk



zones. Adequate provisions shall be made for access by maintenance vehicles, including space for crane or Mobile Elevating Work Platform operations, as well as parking. Each site shall be designed to include appropriate fencing, access control, and physical security measures in accordance with applicable standards and operational requirements.

7.4 Radio Tower Requirements

- 7.4.1 The FRMCS radio towers shall be a self-standing monopole structure made from concrete and/or metal and shall have the less environmental impact and require the minimum footprint as possible.
- 7.4.2 The FRMCS radios towers height shall be 100 foot / 30.48 meters from top of the running rails. No antennas shall be higher than this height limit.
- 7.4.3 The TSCC Contractor shall supply and install all foundations, lightning protection, earthing, and bonding systems required for masts and towers at standalone radio sites.
- 7.4.4 At sites co-located with traction power facilities, tower/mast foundations, earthing, and bonding systems shall be provided by Traction Power Contractors. The TSCC Contractor shall define and communicate all relevant technical and interface requirements to the Traction Power Contractors to ensure compliance with WCS system needs.
- 7.4.5 All equipment installed on radio towers shall incorporate appropriate bird-proofing measures tailored to local wildlife conditions, to prevent damage, maintain operational reliability, and ensure compliance with environmental protection requirements.
- 7.4.6 The TSCC Contractor shall design each radio tower to support the installation of multiple cellular carrier antennas, including provision for mounting infrastructure such as an antenna platform or equivalent structure. The design shall allow for sufficient structural capacity, antenna separation, cabling pathways, and access to accommodate current and future multi-operator deployments in accordance with relevant structural and safety standards.
- 7.4.7 At station locations or other high-demand sites, the TSCC Contractor shall design the radio tower compound with adequate space, access, and utility provisions to accommodate additional equipment huts or shelters for third-party Mobile Network Operators (e.g., Verizon, AT&T, T-Mobile). The design shall include appropriate foundations, power supply, cabling pathways, and physical security measures to enable future co-location of carrier equipment without requiring significant civil modifications or service disruption.
- 7.4.8 The TSCC Contractor shall ensure that all radio tower designs, equipment, and installations comply with all applicable local, state, and national codes, regulations, and standards. The TSCC Contractor shall provide evidence of such compliance, including but not limited to certifications, test reports, and design documentation, as required by the Authority or relevant regulatory bodies.
- 7.4.9 The FRMCS radio towers shall be designed, constructed, and maintained to exceed its minimum design life, ensuring continued structural integrity, operational reliability, and compliance with applicable standards throughout its lifecycle. The TSCC Contractor shall implement maintenance and inspection regimes, aligned with relevant codes and manufacturer recommendations, to proactively manage degradation and extend service life beyond the nominal design period.

7.5 RF Exposure Requirements

- 7.5.1 The WCS, including all transmitting infrastructure such as cellular, Wi-Fi, and radio antennas, shall be designed, installed, and operated in full compliance with Federal Communications Commission (FCC) regulations governing human exposure to radiofrequency (RF) electromagnetic fields.
- 7.5.2 All WCS antenna installations shall:
 - Comply with RF Exposure limits as specified in 47 CFR §1.1307, §1.1310, and related FCC guidance (e.g., OET Bulletin 65).
 - Be evaluated for Maximum Permissible Exposure compliance, accounting for both occupational and general population exposure zones.



- Implement appropriate signage, physical barriers, and administrative controls where exposure may exceed general population Maximum Permissible Exposure thresholds.
- Ensure that co-located transmitters are considered in cumulative exposure assessments.
- Provide site-specific RF exposure compliance documentation prior to system activation or commissioning.

RF Exposure evaluations shall follow procedures outlined by the FCC Office of Engineering and Technology, and where applicable, adhere to exposure limits defined in ANSI/IEEE C95.1. The TSCC Contractor shall coordinate with facility owners and safety personnel to ensure proper RF safety training and signage in accordance with FCC regulations.

- 7.5.3 The TSCC Contractor shall provide a complete RF Exposure Compliance Package demonstrating that all WCS transmitting infrastructure complies with FCC regulations (47 CFR §1.1307 and §1.1310) and ANSI/IEEE C95.1 exposure limits.

The package shall include:

- Site-specific RF exposure evaluation reports, including Maximum Permissible Exposure calculations and RF hazard contour diagrams;
- Antenna inventory with transmit power, frequency, gain, and FCC certifications;
- Evidence of RF safety signage and physical barrier implementation;
- Photographic evidence and annotated as-built drawings;
- Confirmation of RF safety training for relevant personnel;
- A signed compliance statement confirming adherence to FCC and industry standards.

The documentation shall be submitted and accepted prior to commissioning.



8 TOLERANCES

Not applicable to Wireless Communications Systems.



9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 General requirements are described in the Scope of Work document.

9.2 Specific Requirements

9.2.1 The TSCC Contractor shall supply, deliver, install, test, and commission all components necessary for a fully functional WCS, as specified in this Technical Specification.

9.2.2 The TSCC Contractor shall be responsible for the design, manufacture, factory acceptance testing (FAT), delivery, site installation, integration, site acceptance testing (SAT), and commissioning of the WCS solution to facilitate CHSR in-revenue service.

9.2.3 The scope of supply shall include, but not be limited to:

- Wireless access infrastructure, including base stations, access points, antennas, masts, and associated coaxial, optic fiber and power cabling;
- Backhaul and transmission equipment, including switches, routers, and optical or wireless transmission gear;
- Core network components, including network controllers, gateways, and any central management servers;
- User equipment, including handheld terminals, vehicular radios, onboard units, and any mobile communication devices;
- Power supply systems, including UPS, battery backup systems, and power distribution units for WCS equipment;
- Mounting structures, cabinets, shelters, racking, cable trays and enclosures for indoor and outdoor deployments;
- Software, including network management systems (NMS), provisioning tools, configuration management, and cybersecurity features;
- System interfaces, including integration with the Digital Communications Network (DCN), Train Control and Management System (TCMS), and On-board Railway Applications where applicable;
- Test equipment required for installation and commissioning;
- Spare parts, tools, and special test equipment, as per the spares strategy agreed with the Authority;
- Ancillary systems, including lighting, security (e.g., access control), CCTV, environmental conditioning (e.g., heating, ventilation, and air conditioning), and any other supporting infrastructure necessary to ensure safe, secure, ergonomic and reliable operation of WCS equipment installations;
- Documentation, including design documents, installation manuals, test procedures, and as-built records.

9.2.4 The TSCC Contractor shall ensure that all equipment and materials delivered are compliant with relevant standards and project-specific environmental and safety requirements.

9.2.5 The TSCC Contractor shall coordinate all delivery and logistics activities in accordance with the Project Delivery Program and in consultation with the Authority, including any site access restrictions and staging requirements.

9.2.6 The TSCC Contractor shall label and package all equipment and components clearly and securely to facilitate identification, handling, and inventory upon delivery to site.

9.2.7 The TSCC Contractor shall provide a detailed Delivery and Installation Schedule, identifying all major equipment deliveries, installation milestones, and dependencies.

9.2.8 The TSCC Contractor shall provide complete backups of all software and configuration files necessary to restore the system to full operational status in the event of failure or data loss. The TSCC Contractor shall



also supply appropriate and secure storage media or infrastructure for managing, periodically producing and retaining these backups in accordance with the WCS's recovery and cybersecurity requirements.



10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Scope of Work.



11 INSTALLATION AND INTEGRATION

11.1 General Requirements

11.1.1 General installation and integration requirements are defined in the Scope of Work and Schedule 3.



12 TESTING & ACCEPTANCE

12.1 General Requirements

- 12.1.1 General testing and acceptance requirements are defined in the Scope of Work and Schedule 3.
- 12.1.2 All test results and certifications required for the WCS shall be provided by the TSCC Contractor.
- 12.1.3 The following testing requirements are intended to verify compliance with the requirements set out in all preceding sections of this Specification, including but not limited to functional, performance, operational, and interface requirements. Nothing in this section shall be construed as limiting the TSCC Contractor's obligation to meet the full scope of requirements specified elsewhere in this document.
- 12.1.4 The TSCC Contractor shall perform comprehensive redundancy and failover testing across all WCS subsystems, where applicable, including but not limited to the Core Network, Radio Access Network, Transport Network, Network Management Systems, Dispatch Systems, and Power Supplies.
- 12.1.5 The testing shall validate that:
- Redundant components and paths are operational and properly configured to take over in the event of failure;
 - Automatic failover occurs without manual intervention and within system-defined recovery times;
 - No loss of critical communications services (e.g., MCX voice, video, or data) occurs during failover;
 - Stateful recovery is preserved for ongoing MCX sessions, where applicable;
 - Alarm, monitoring, and logging systems accurately detect, report, and log redundancy activation events;
 - Redundancy applies to active-active and active-standby configurations, including:
 - Dual core or distributed User Plane Function/Service Communication Proxy instances;
 - RAN node or sector-level redundancy;
 - Link/path redundancy in the Backbone Transport Network;
 - Redundant power supplies (DC/AC), backup battery systems and generators;
 - Dual NMS/ICSS control interfaces and databases;

Redundancy tests shall simulate single point failures, partial subsystem outages, and complete system switchover scenarios in accordance with the approved test plan and system design. The results shall demonstrate compliance with the specified availability, reliability, and recovery performance targets.

12.2 Specific Requirements for FRMCS

- 12.2.1 All FRMCS-related equipment shall be subjected to functional testing to verify correct installation, configuration, and operation in accordance with the system design and performance requirements.
- 12.2.2 **Radio Access Network Testing**
- 12.2.2.1 Voice and data call tests shall be conducted across representative coverage areas to verify the functionality, reliability, and quality of FRMCS services.
- 12.2.2.2 Antenna installation and alignment shall be verified for compliance with the approved FRMCS radio design, including orientation, height, and tilt parameters.
- 12.2.2.3 The Voltage Standing Wave Ratio (VSWR) and return loss of all coaxial cable installations shall be measured and confirmed to be within acceptable thresholds defined by the manufacturer and design specifications.
- 12.2.2.4 The connectivity between the FRMCS Radio Access Network and the Digital Communications Network (DCN) shall be verified to confirm end-to-end path availability and proper routing.



- 12.2.2.5 The connectivity between the FRMCS BBU and RRH shall be verified to confirm end-to-end path availability and proper routing.
- 12.2.2.6 The interface between the FRMCS RAN, the Network Management System (NMS) and the Integrated Control and Supervisory System (ICSS) shall be tested to ensure successful communication, event reporting, and configuration management.
- 12.2.2.7 Radio network performance shall be validated by measuring key parameters including signal strength (RSRP/RSRQ), throughput, latency, and call success rates in accordance with the FRMCS performance criteria.

12.2.3 Core Network Testing

- 12.2.3.1 Core network testing shall be conducted at both the Operations Control Centre (OCC) and secondary core network at Government Data Center to verify proper deployment and function.
- 12.2.3.2 Core network testing shall include both Site Acceptance Testing (SAT) and System Integration Testing (SIT).
- 12.2.3.3 Site Acceptance Testing (SAT) shall be performed after equipment delivery and installation at the OCC and secondary core network. SAT shall confirm that the installed equipment meets or exceeds the required functional and performance specifications.
- 12.2.3.4 SAT shall be performed individually for each installed core network component, including but not limited to servers, session management functions, gateways, and edge routers.
- 12.2.3.5 System Integration Testing (SIT) shall be conducted to validate the end-to-end functionality of the core network, including integration with the Radio Access Network, DCN, NMS, Dispatch Consoles and external interfaces (e.g., IWF, P25).
- 12.2.3.6 Redundancy and failover testing shall be performed to validate the resilience of the core network. Tests shall simulate failures of critical components and interfaces to confirm continuity of service, including full core failover and isolated element failures.
- 12.2.3.7 Software release and version interoperability testing shall be conducted to assess system behavior following major software upgrades or patch deployments, ensuring continued compliance with functional, security, and interoperability requirements.

12.2.4 Interworking Function (IWF) Testing

- 12.2.4.1 The Interworking Function (IWF) shall be tested to verify voice interoperability between FRMCS/MCX users and external Land Mobile Radio (LMR) systems, including but not limited to P25, TETRA, and analog networks.
- 12.2.4.2 Test scenarios shall include:
 - Group and individual call setup between FRMCS and LMR users;
 - Push-to-Talk (PTT) signaling interoperability;
 - Emergency call bridging;
 - Alias/ID translation and display across systems.
- 12.2.4.3 The IWF shall be subjected to failover testing, including loss of network connectivity or remote radio system availability, to confirm fallback behavior and service recovery.
- 12.2.4.4 Latency, jitter, and audio quality across the IWF interface shall be measured to ensure adherence to 3GPP TS 23.283 [R49] performance guidelines.
- 12.2.4.5 Security testing shall be conducted to verify authentication, access control, and encryption of inter-system communications.

12.2.5 Dispatch Consoles Testing

- 12.2.5.1 The WCS Dispatch Consoles shall undergo functional testing to verify the ability to initiate, manage, and monitor MCX-based communications including voice, video, and data.



Dispatch consoles shall be tested for:

- Push-to-Talk group call control;
- Individual and emergency call initiation;
- Real-time location display and user status indicators;
- Video streaming to/from field units;
- Messaging, alerts, and acknowledgments.

12.2.5.2 Integration with the logging and recording system shall be verified, including synchronized replay of audio, video, and screen actions from the dispatch interface.

12.2.5.3 Dispatch Console performance shall be verified under degraded and high-load conditions, including network congestion and partial subsystem failures.

12.2.5.4 User authentication, access control roles, and profile switching shall be tested against role-based operational scenarios (e.g., OCC controller vs. emergency coordinator).

12.2.6 High-Speed Mobility Testing

12.2.6.1 The FRMCS system shall be tested onboard trains operating at speeds up to 220 mph (354 km/h) to verify service continuity and performance during high-mobility conditions.

Handover testing shall include:

- Inter-gNB handovers under varying signal conditions;
- Seamless call continuity during transitions;
- MCX session continuity and bearer switching;
- Failure scenarios including handover rejections and cell edge dropouts.

12.2.6.2 End-to-end latency, jitter, and throughput shall be measured during train movement, with particular attention to:

- Voice call MOS scores;
- Video streaming stability;
- Packet loss in data sessions.

12.2.6.3 Drive testing shall capture RF metrics (RSRP, SINR, RSRQ), logged GPS data, and session KPIs to validate radio design assumptions.

12.2.6.4 All high-speed testing shall be correlated with Dispatch Console visibility and call control feedback to confirm end-to-end system integrity during mobility scenarios.

12.3 Specific Requirements for ETCS

12.3.1 For the purpose of validating ETCS performance, the TSCC Contractor shall ensure compliance with the minimum requirements specified in the applicable Control-Command and Signaling Technical Specification for Interoperability (CCS TSI), including Commission Implementing Regulation (EU) 2023/1695 and any subsequent versions. These requirements shall include all functionalities required for FRMCS to support a fully operational ETCS Level 2 train control system.

12.4 Specific Requirements for PWS

12.4.1 The TSCC Contractor shall perform comprehensive testing of the Passenger Wi-Fi System (PWS) to validate that all components meet the specified functional, performance, and integration requirements under normal, and peak-load conditions. Testing shall be conducted in accordance with the approved Test and Commissioning Plan and shall include both onboard trainsets and fixed infrastructure (e.g., stations, depots).



12.4.2 Functional Testing

12.4.2.1 Testing shall confirm successful user access to the Wi-Fi network, including:

- Captive portal operation;
- Users shall be able to establish an initial connection and access the internet within 30 seconds of selecting the Wi-Fi network
- Tiered service access (e.g., complimentary and premium);
- Multiple payment and purchase options;
- Authentication and session management, including federated identity.

12.4.2.2 All access control and security features shall be tested, including:

- WPA3 encryption enforcement;
- SSID segmentation between passenger and operational networks;
- Role-based access and traffic isolation.

12.4.2.3 Session continuity shall be tested for roaming users between carriages whilst in motion.

12.4.3 Performance Testing

12.4.3.1 Throughput, latency, and packet loss shall be measured at multiple access points under varying load conditions to verify compliance with the specified performance levels for each service tier.

12.4.3.2 Load testing shall simulate concurrent user access (minimum and maximum expected users per carriage and per station) to assess system scalability and service degradation behavior.

12.4.3.3 QoS enforcement for premium vs. complimentary users shall be validated under network congestion scenarios.

12.4.4 Backhaul and Network Integration Testing

12.4.4.1 The PWS backhaul link (e.g., mmWave, 5G, satellite, or hybrid) shall be tested for:

- Uplink and downlink performance
- Seamless handover between backhaul technologies (if applicable)
- WAN bonding or aggregation behavior (if implemented)

12.4.4.2 The interface between the PWS and the WCS or shared backhaul infrastructure shall be tested to verify traffic segregation, prioritization, and compliance with defined bandwidth allocations.

12.4.4.3 Redundancy and failover scenarios for backhaul links shall be tested to confirm service continuity or graceful degradation.

12.4.5 Access Point and Hardware Validation

12.4.5.1 Access point installation shall be physically inspected and tested for:

- Signal coverage throughout the passenger areas;
- Antenna placement compliance;
- Interference and overlap management.

12.4.5.2 Environmental conditions (e.g., vibration, temperature) shall be validated for compliance with rail-grade hardware standards.

12.4.6 Integration and Monitoring

12.4.6.1 Integration with the Passenger Portal, CRM systems (if applicable), and payment gateway shall be tested, including:



- Session tracking;
- Transaction processing for premium access;
- Usage data collection and reporting.

12.4.7 The TSCC Contractor shall verify end-to-end monitoring of PWS infrastructure, including SNMP polling, alarms, and dashboard visibility through the central Network Management System (NMS) or equivalent platform.



13 SUBMITTALS

13.1 General Requirements

13.1.1 The general submittals required for the system are defined in the Scope of Work.



14 QUALITY MANAGEMENT

14.1 General Requirements

14.1.1 General quality management requirements are defined in the Agreement and associated Schedules.



15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

- 15.1.1 In addition to the mandatory requirements outlined in this specification, the Authority reserves the right to request from the TSCC Contractor and related Suppliers information pertaining to the performance of proposed or supplied elements under similar service conditions, with particular emphasis on railway management aspects which may influence WCS reliability availability maintainability characteristics.



16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.



Schedule 5(s)

Traction Power Supply System (TPSS)

California High-Speed Rail Authority



Standard Specifications

TSCC Specifications

SPEC-0023 – Traction Power Supply System (TPSS)

Rev. 1.0

I. Modak

Authorized:

09/22/2025

Intakhab (Indy) Modak, HV & Traction Power Lead (SME)

Date

A handwritten signature in black ink, appearing to read "Tom Newey", on a light gray rectangular background.

Checked:

10/15/2025

Thomas Newey, Telecoms Lead

Date

A handwritten signature in black ink, appearing to read "Bruno Comperat", on a light gray rectangular background.

Approved:

10/16/2025

Bruno Comperat, Deputy Director of Rail Engineering

Date

A handwritten signature in blue ink, appearing to read "Ryan Scott", on a light gray rectangular background.

Approved:

10/16/2025

Ryan Scott, Director of Rail Engineering

Date

A handwritten signature in blue ink, appearing to read "Amit Joshi", on a light gray rectangular background.

Released:

10/16/2025

Amit Joshi, Configuration Manager

Date



Document Revision History – TPSS Specifications**Second Edition****December 2025**

Revision	Date	Revision Description
0.0	September 22, 2025	First Edition
1.0	December 2025	Second Edition for Addendum 2



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	SCOPE OF THE SYSTEM TECHNICAL SPECIFICATION	5
2	REFERENCE STANDARDS AND DOCUMENTS.....	6
2.1	GENERAL	6
2.2	TSI	6
2.3	STANDARDS	6
2.4	NATIONAL LAWS AND REGULATIONS	11
2.5	UIC RECOMMENDATIONS	12
3	TERMS, DEFINITIONS, AND ABBREVIATIONS	13
4	SYSTEM DESCRIPTION	14
4.1	GENERAL REQUIREMENTS AND SCOPE OF THE TPSS.....	14
4.2	SCALABILITY & PHASING PLAN.....	16
4.3	TPSS CONSUMERS.....	16
4.4	DESIGN LIFE.....	17
5	INTERFACE REQUIREMENTS WITH UPSTREAM POWER SUPPLIER.....	18
5.1	PART 1: PRINCIPAL AGREEMENT AND INTERFACE PROVISIONS	18
5.2	PART 2: ALTERNATIVE EXECUTION AND CONTINGENCY PROVISIONS	20
6	SYSTEM REQUIREMENTS.....	22
6.1	GENERAL REQUIREMENTS.....	22
6.2	ENVIRONMENTAL REQUIREMENTS.....	23
6.3	FUNCTIONAL REQUIREMENTS.....	23
6.4	PERFORMANCE REQUIREMENTS.....	25
6.5	ELECTRICAL PROTECTION REQUIREMENTS.....	27
6.6	EMC/EARTHING & BONDING SYSTEM REQUIREMENTS.....	28
6.7	TPSS SYSTEM INTEGRATION AND INTEROPERABILITY REQUIREMENTS	29
6.8	SECURITY AND CYBERSECURITY REQUIREMENTS.....	30
6.9	CIVIL, STRUCTURAL, BUILDINGS & MEP REQUIREMENTS	30
6.10	RELIABILITY, AVAILABILITY, MAINTAINABILITY, AND SAFETY (RAMS) REQUIREMENTS.....	31
7	ELECTRICAL CALCULATIONS, MODELLING AND STUDIES REQUIREMENTS	33
8	INTERFACES REQUIREMENTS.....	36
8.1	GENERAL REQUIREMENTS.....	36
8.2	THIRD PARTIES INTERFACES.....	36
8.3	EXTERNAL INTERFACES.....	36
8.4	INTERNAL INTERFACES	36
9	MATERIALS, PRODUCT, AND COMPONENTS REQUIREMENTS.....	38
9.1	GENERAL REQUIREMENTS.....	38
9.2	LV DISTRIBUTION	38



1 INTRODUCTION

1.1 Scope of the System Technical Specification

- 1.1.1 The scope of this Technical Specification is to define the California High-Speed Rail Authority's (Authority) Requirements for Traction Power Supply System, hereinafter: TPSS.
- 1.1.2 These requirements shall be implemented and managed in conjunction with all other requirements that together constitute the Agreement.
- 1.1.3 The requirements are formulated using the following words and their meanings:
 - **“Shall”**: Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure);
 - **“Should”**: Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents;
 - **“Must”**: Indicates an obligation or a mandatory requirement; and
 - **“May”**: Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.



2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

2.1.1 The Track and Systems Contractors ("TSCC Contractor") shall apply the then-current standards, guidelines and specifications provided in this chapter for all stages of the design, test, manufacture, supply, delivery, assembly, installation, testing, commissioning and training.

2.2 TSI

2.2.1 The applicable TSIs are listed below:

No	Standard	Title
[R1]	ENE TSI	COMMISSION REGULATION (EU) No 1301/2014 of 18 November 2014 on the technical specifications for interoperability relating to the 'energy' subsystem of the rail system in the Union including the Commission Implementing Regulation (EU) 2018/868 of 13 June 2018, Commission Implementing Regulation (EU) 2019/776 of 16 May 2019 and Commission Implementing Regulation (EU) 2023/1694 of 10 August 2023
[R2]	SRT TSI	COMMISSION REGULATION (EU) No 1303/2014 of 18 November 2014 - concerning the technical specification for interoperability relating to 'safety in railway tunnels' of the rail system of the European Union including commission regulation (EU) 2016/912 of 9 June 2016 L 153 28 10.6.2016 and commission implementing regulation (EU) 2019/776 of 16 May 2019

TABLE 72 LIST OF TSI AND REGULATIONS

2.3 Standards

2.3.1 The relevant standards to be used for TPSS are listed below:

No	Standard	Title
[R3]	BS EN 50163:2004+A3:2022	Railway applications — Supply voltages of traction systems
[R4]	BS EN 50641:2020	Railway applications — Fixed installations – Requirements for the validation of simulation tools used for the design of electric traction power supply systems
[R5]	BS EN 50317:2025	Railway applications — Current collection systems – Requirements for validation of measurements of the dynamic interaction between pantograph and overhead contact line
[R6]	BSEN 50119:2020	Railway applications — Fixed installations – Electric traction overhead contact lines
[R7]	BSEN 50318:2018+A1:2022	Railway applications — Current collection systems – Validation of simulation of the dynamic interaction between pantograph and overhead contact line
[R8]	BS EN 50121 - 1	Railway applications — Fixed installations – Electromagnetic compatibility – Part 1: General



No	Standard	Title
[R9]	BS EN 50121 - 2	Railway applications — Fixed installations – Electromagnetic compatibility – Part 2: Emission of the whole railway system to the outside world
[R10]	BS EN 50121 – 5	Railway applications — Fixed installations – Electromagnetic compatibility – Part 5: Emission and immunity of fixed power supply installations and apparatus
[R11]	EN 50122 – 1:2022+A1:2025	Fixed installations for Railway applications – Electrical safety, earthing and the return circuit – Part 1: Protective provisions against electric shock
[R12]	EN 50122 – 3:2022+A1:2025	Fixed installations for railway applications– Electrical safety, earthing and the return circuit – Part 3: Mutual interaction of AC and DC traction systems
[R13]	EN 50124 - 1	Railway applications — Insulation coordination – Part 1: Basic requirements – clearances and creepage distances for all electrical and electronic requirements
[R14]	EN 50124 – 2:2017	Railway applications. Insulation coordination — Overvoltage and related protection
[R15]	EN 50125 - 2	Railway applications – Environmental conditions for equipment – Part 2: fixed electrical installations
[R16]	EN 50152 – 1:2012+A1:2013	Railway applications — Fixed installations – Particular requirements for alternating current switchgear - Circuit-breakers with nominal voltage above 1kV
[R17]	EN 50152 – 1:2012	Railway applications — Fixed installations – Particular requirements for alternating current switchgear -Disconnectors, earthing switches and switches with nominal voltage above 1kV
[R18]	EN 50388 - 1	Railway applications — Fixed installations and rolling stock – Technical criteria for the coordination between electric traction power supply systems and rolling stock to achieve interoperability - Part 1: General
[R19]	EN 50633:2016	Railway applications. Fixed installations. Protection principles for AC and DC electric traction systems.
[R20]	EN 50126:2017+A1:2024	Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety
[R21]	EN IEC 60146-1-1:2024	Semiconductor converters. General requirements and line commutated converters. Specification of basic requirements.
[R22]	EN 60146 – 1 – 3:1993	Semiconductor convertors. General requirements and line commutated convertors - Transformers and reactors



No	Standard	Title
[R23]	EN 60146 – 2:2000	Semiconductors convertors —General requirements and line commutated convertorsSelf-commutated semiconductor convertors including direct DC convertors
[R24]	EN 50328:2003	Railway applications — Fixed installations – Electronic power convertors for substations
[R25]	EN 50329:2003+A1:2010	Railway applications — Fixed installations – Traction transformers
[R26]	EN 62305-3:2024	Protection against lightning - Physical damage to structures and life hazard
[R27]	EN 60529:1992+A2:2013	Degrees of protection provided by enclosures (IP Code)
[R28]	EN IEC 62305 – 1:2024	Protection against lightning – General Principles
[R29]	EN 62305 – 2:2024	Protection against lightning – Risk management
[R30]	EN 62305 – 4 :2024	Protection against lightning – Electrical and Electronic systems within structures
[R31]	EN 50178:1998	Electronic equipment for use in power installations
[R32]	EN IEC 60068-3-3:2019	Environmental testing – Supporting documentation and guidance. Siesmic test methods for equipment
[R33]	IEC 60050 Series	International Electrotechnical Vocabulary
[R34]	IEC 60255 Series	Measuring relays and protection equipment
[R35]	IEC 60502-1:2021	Power cables with extruded insulation and their accessories for rated voltages from 1 kV (Um = 1,2 kV) up to 30 kV (Um = 36 kV) – All parts
[R36]	IEC 60076 Series	Power transformers
[R37]	IEC 60099 Series	Surge arresters
[R38]	IEC 60146 Series	Semiconductor converters
[R39]	IEC 62271 Series	High-voltage switchgear and control gear – All parts
[R40]	IEC 61000 Series	Electromagnetic compatibility (EMC)
[R41]	IEC 60870 - 5	Telecontrol equipment and systems – Part 5: Transmission protocols



No	Standard	Title
[R42]	IEC 61508 – 1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements
[R43]	IEC 61850:2025	Communication networks and systems for power utility automation
[R44]	IEC 62351:2025	Power systems management and associated information exchange – Data and communications security Network and system security for industrial process measurement and control
[R45]	IEC TS 62443-1-1:2009	Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models
[R46]	IEC 60085:2007	Electrical insulation - Thermal evaluation and designation
[R47]	IEC 60228:2023	Conductors of insulated cables
[R48]	IEC 60332-1-1:2004+AMD1:2015	Tests on electric and optical fiber cables under fire conditions - Part 1-2: Test for vertical flame propagation for a single insulated wire or cable - Procedure for 1 kW pre-mixed flame. Tests on electric and optical fiber cables under fire conditions - Part 3-24: Test for vertical flame spread of vertically-mounted bunched wires or cables.
[R49]	IEC 60364 Series	Low-voltage electrical installations
[R50]	IEC 60479 Series	Effects of current on human beings and livestock, Part 1: General aspects.
[R51]	IEC 60670 Series	Boxes and enclosures for electrical accessories for household and similar fixed electrical installations
[R52]	IEC 60754-1:2011+AMD1:2019	Test on gases evolved during combustion of materials from cables - Part 1: Determination of the halogen acid gas content
[R53]	IEC 60754-2:2011+AMD1:2019	Test on gases evolved during combustion of materials from cables - Part 2: Determination of acidity (by pH measurement) and conductivity.
[R54]	IEC 60811 Series	Electric and optical fiber cables - Test methods for non-metallic materials
[R55]	IEC 60947:2025	Low-voltage switchgear and control-gear – All parts
[R56]	IEEE 80	Guide for Safety in AC Substation Grounding
[R57]	IEEE 142	Recommended Practice for Grounding of Industrial and Commercial Power Systems
[R58]	IEEE 242	Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems



No	Standard	Title
[R59]	IEEE 399	Recommended Practice for Industrial and Commercial Power Systems Analysis
[R60]	IEEE 400 Series	Guide for Field Testing and Evaluation of the Insulation of Shielded Power Cable Systems Rated 5 kV and above
[R61]	IEEE 473	Recommended Practice for an Electromagnetic Site Survey (10 kHz to 10 GHz)
[R62]	IEEE 485	Recommended Practice for Sizing Lead-Acid Batteries for Stationary Applications
[R63]	IEEE 519	Standard for Harmonic Control in Electric Power Systems
[R64]	IEEE 525	Guide for the Design and Installation of Cable Systems in Substations
[R65]	IEEE 551	Recommended Practice for Calculating AC Short-Circuit Currents in Industrial and Commercial Power Systems
[R66]	IEEE 575	Guide for Bonding Shields and Sheaths of Single-Conductor Power Cables Rated 5 kV through 500 kV
[R67]	IEEE 1309	Standard for Calibration of Electromagnetic Field Sensors and Probes (Excluding Antennas) from 9 kHz to 40 GHz
[R68]	IEEE 1159	Recommended Practice for Monitoring Electric Power Quality
[R69]	IEEE 1184	Guide for Batteries for Uninterruptible Power Supply Systems
[R70]	IEEE 1547.2	Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces
[R71]	IEEE 1679.1	Guide for the Characterization and Evaluation of Lithium-Based Batteries in Stationary Applications
[R72]	IEEE 1686	Standard for Intelligent Electronic Devices Cybersecurity Capabilities
[R73]	IEEE 1711	Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links
[R74]	IEEE 1815	Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)
[R75]	IEEE 2030 Series	Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads
[R76]	IEEE 2030.7/2030.8	Standard for the Specification of Microgrid Controllers & Standard for the Testing of Microgrid Controllers
[R77]	IEEE 3002.2	Recommended Practice for Conducting Load-Flow Studies and Analysis of Industrial and Commercial Power Systems



No	Standard	Title
[R78]	IEEE C37 Series	Series of standards for power switchgear, including circuit breakers, switchgear assemblies, and related components, used in power systems for protection, control, and interruption of electrical currents
[R79]	IEEE C57 Series	Series comprising technical standards and guides for power, distribution, and regulating transformers, covering general requirements, design, testing, operation, and maintenance, including specifics on loading, insulation, tap changers, and transformer condition monitoring
[R80]	AREMA	Chapter 17 – High-Speed Rail Systems Chapter 33 – Electrical Energy Utilization Chapter 34 – Energy Storage & Alternative Power Supply Chapter 36 – Electric Traction Chapter 37 – Environmental & Sustainability

TABLE 73 LIST OF APPLICABLE STANDARDS

2.4 National Laws and Regulations

2.4.1 The then-current version of the following indicative national laws and regulations shall be applied. The TSCC Contractor is responsible for the compliance with the country's legislation and correct application of regulations also if they are not listed:

No	Standard	Description
[R81]	Code of Federal Regulations (CFR) Title 49	Transportation - Part 229, 236, 238 and 239
[R82]	Code of Federal Regulations (CFR) Title 29	Labor - Part 1910
[R83]	California Public utilities Commission (CPUC)	General Order 95, 128, 176
[R84]	CEQA	California Environmental Quality Act
[R85]	NESC	National Electrical Safety Code
[R86]	NFPA 70	National Electrical Code
[R87]	NFPA 70 E	National Fire Protection Association - Electrical Safety in the Workplace
[R88]	NFPA 72	National Fire Alarm and Signaling Code



No	Standard	Description
[R89]	NFPA 130	National Fire Protection Association - Fixed guideway transit and passenger rail systems

TABLE 23 LIST OF APPLICABLE CALIFORNIAN REGULATIONS

2.5 UIC Recommendations

UIC 552 – Electrical power supply for trains – Standard technical characteristics of the train line



3 TERMS, DEFINITIONS, AND ABBREVIATIONS

3.1.1 All the terms, definitions and abbreviations are provided in: Schedule 5(t) and Schedule 16



4 SYSTEM DESCRIPTION

4.1 General Requirements and Scope of the TPSS

- 4.1.1 The traction power supply system is described in Schedule 16 Scope of Work
- 4.1.2 This System Technical Specification (STS) has been developed on the basis of that description and supplements the traction power section of the SoW.
- 4.1.3 Where any ambiguity or inconsistency exists between the SoW and this Specification, the TSCC Contractor shall seek clarification from the Authority prior to design development.
- 4.1.4 All works, equipment, and systems shall comply with applicable federal, state, and local laws and regulations, including utility interconnection requirements, as well as international and regional standards (e.g. EN, IEC, IEEE, ANSI, etc.) referenced in this Specification. In the event of conflicting requirements between referenced standards or regulations, the following hierarchy shall apply unless otherwise directed by the Authority:
 - 4.1.4.1 Federal, state, and local laws, authority having jurisdiction and regulations (including utility requirements);
 - 4.1.4.2 Contractual requirements defined in this Specification;
 - 4.1.4.3 Applicable international and regional standards (e.g., EN, IEC, IEEE, ANSI, IMC etc.); and
 - 4.1.4.4 Industry best practice where no specific standard applies.
- 4.1.5 Where requirements differ in stringency, the TSCC Contractor shall comply with the most stringent (worst-case) requirement applicable. Any conflicts shall be brought to the attention of the Authority for resolution before proceeding with design or procurement.
- 4.1.6 This STS defines the high-level functional and performance requirements for the TPSS System. It establishes the Authority expectations and requirements, but it is the responsibility of the TSCC Contractor to:
 - 4.1.6.1 Develop detailed designs, construction and manufactures drawings, develop simulation models, calculations and studies for all TPSS systems and equipment; and
 - 4.1.6.2 The TSCC Contractor shall define and provide the detailed technical requirements necessary for Verification and Validation (V&V) of the CHSR project in alignment with the systems requirements specifications. These requirements shall be:
 - 4.1.6.2.1 Derived from the outputs specified in Schedules 1-4 and Schedule 16.
 - 4.1.6.2.2 Incorporated into the project Dynamic Object-Oriented Requirements System (DOORS) database;
 - 4.1.6.2.3 Supported by clearly defined acceptance criteria and tolerances, based on the relevant norms and/or standards;
 - 4.1.6.2.4 Identify the proposed method of V&V (e.g., comprising of the following: Inspection, Demonstration, Test, and Analysis); and
 - 4.1.6.2.5 Each requirement shall include explicitly defined acceptance criteria and tolerances to ensure verifiability.
 - 4.1.6.3 The TSCC Contractor shall prepare and produce Factory Acceptance Test (FAT) procedures, Site Acceptance Test (SAT) procedures, and Static and Dynamic Integrated Test procedures in accordance with EN 50126 to demonstrate compliance with this Specification:



- 4.1.6.3.1 All test procedures shall explicitly reference the detailed requirements and acceptance criteria/tolerances defined in Clause 4.1.6.2;
- 4.1.6.3.2 Pass/fail outcomes shall only be determined on the basis of compliance with these acceptance criteria/tolerances;
- 4.1.6.3.3 All test procedures shall be submitted to the Authority for review and acceptance prior to execution; and
- 4.1.6.3.4 Test results shall include documented evidence demonstrating conformity with the defined criteria/tolerances.
- 4.1.6.4 The TSCC Contractor shall develop an Inspection and Test Plan (ITP) in accordance with its Quality Assurance and Quality Control processes.
- 4.1.6.5 The ITP shall clearly identify all hold points and witness points for the Authority's review and acceptance, and shall demonstrate compliance with the Verification and Validation requirements defined in this document.

The ITP shall:

- 4.1.6.5.1 Identify all hold points and witness points for the Authority's review and acceptance;
- 4.1.6.5.2 Demonstrate how the Verification and Validation requirements defined in Clause 4.1.6.2 will be satisfied, and how the FAT, SAT, and Integrated Test procedures defined in Clause 4.1.6.3 will be implemented;
- 4.1.6.5.3 Be updated throughout the project lifecycle to reflect design, manufacturing, installation, and testing activities; and
- 4.1.6.5.4 The TSCC Contractor shall provide traceability between each requirement, its acceptance criteria/tolerances, and the method of demonstration.
- 4.1.6.6 The TSCC Contractor shall produce vendor level technical specifications for procurement of all TPSS equipment.
- 4.1.6.7 The TSCC Contractor shall ensure all designs, equipment, and tests meet the performance, safety, and interoperability requirements defined herein.
- 4.1.6.8 All detailed design deliverables, studies, models, calculations, procurement specifications, and test plans and procedures shall be submitted to the Authority for review and acceptance prior to procurement, installation, or commissioning.
- 4.1.7 The TPSS shall interface with future Clean Energy Contractor(s), hereinafter referred to as the "Upstream Power Supplier."
- 4.1.7.1 "Clean Energy" shall mean renewable or sustainable energy resources, including but not limited to photovoltaic generation systems with battery energy storage, or such other technologies as the Authority may designate consistent with applicable laws and regulations.
- 4.1.7.2 "Upstream Power Supplier" shall mean the party responsible for developing, owning, operating, or otherwise providing Clean Energy, interconnected with the utility and operating in parallel therewith, for delivery of the power to the TPSS.
- 4.1.7.3 The TPS shall interface with the upstream energy power supplier at the Point of Common Coupling (PCC) nominally 34.5 kV or as confirmed with the utility/clean energy Contractor, but the TSCC Contractor shall verify and confirm the actual service voltage during design development and adjust all related equipment ratings, insulation levels, and interface details accordingly.



- 4.1.8 At the Traction Power Sub-Stations sites as defined in the SoW will facilitate equipment from both the upstream power supplier as well as the TPSS facilities.
- 4.1.9 The upstream energy power supplier will be responsible for providing the switchgear identified as the PCC, with the TSCC Contractor verifying the service voltage and coordinating all interface requirements.
- 4.1.10 All coordination with the upstream energy power supplier shall be captured in an Interface Control Document (ICD) managed by the Authority.
- 4.1.11 The TPSS shall provide a safe, high-quality and reliable power supply for the Rail Systems as defined in clause 4.3.6.
- 4.1.12 The TPSS shall be designed to ensure continuous power is available for traction loads under all operating conditions.
- 4.1.13 The TPSS shall provide reliable and safe traction power under normal, degraded, and emergency operating conditions, supporting staged railway operations from initial service through full build-out.

4.2 Scalability & Phasing Plan

- 4.2.1 The TSCC Contractor shall submit a Scalability & Phasing Plan demonstrating how the traction power system will be delivered and operated across progressive project phases.
- 4.2.2 The Scalability & Phasing Plan shall show required civil footprint, equipment staging, any temporary works, and operational constraints.
- 4.2.3 All TPSS equipment (e.g. SFCs, switchgear, transformers, autotransformers, paralleling posts, switching stations, etc.) shall be modular and capable of being extended in-situ without demolition.
- 4.2.4 The TSCC Contractor shall consider providing spare bays, spare cable ducts, spare cable trays, and space in buildings sized for final equipment.
- 4.2.5 All new permanent works shall be installed to final configuration where practicable to avoid rework.
- 4.2.6 Any temporary equipment shall be removable with minimum disruption to the operational railway.
- 4.2.7 All temporary equipment must meet the same safety, protection and earthing requirements as permanent equipment. Temporary operation shall be fully tested (FAT/SAT) and shall include dynamic tests using representative rolling stock.
- 4.2.8 The TSCC Contractor shall guarantee minimum traction power performance for each phase.
- 4.2.9 The TSCC Contractor shall deliver a modular, phased traction power design enabling staged operations as defined in clause 4.2.1.

4.3 TPSS Consumers

- 4.3.1 The TSCC Contractor shall ensure interoperability of the TPSS with:
 - 4.3.1.1 Upstream power supplier;
 - 4.3.1.2 The Overhead Contact System;
 - 4.3.1.3 Rolling stock;
 - 4.3.1.4 SCADA/Energy Management System;
 - 4.3.1.5 Track and civil structures; and
 - 4.3.1.6 Medium/Low Voltage Non-Traction Power Supplies as applicable.



4.4 Design life

- 4.4.1 The design life of the TPSS equipment shall be in compliance with the requirements of the Authority's Design Criteria Manual, Chapter 2 Basis of Design and Schedule 16 Scope of Works (SoW).



5 INTERFACE REQUIREMENTS WITH UPSTREAM POWER SUPPLIER

5.1 Part 1: Principal Agreement and Interface Provisions

- 5.1.1 The TPSS shall ensure that the upstream power supplier design is fully coordinated and integrated via ICD process to guarantee safe, reliable, and integrated operation.
- 5.1.2 The TSCC Contractor shall not assume fixed upstream power supplier parameters. Instead, the TSCC Contractor shall obtain all necessary interface data as defined in the agreed ICD from the upstream power supplier. Such data shall include, but not be limited to:
 - 5.1.2.1 Energy Management System (EMS), real time data acquisition, control strategies, communication protocols, remote control monitoring, alarm event management and operator actions.
 - 5.1.2.2 Steady state and transient voltage and frequency ranges at PCC;
 - 5.1.2.3 Network impedance and fault level characteristics (positive, negative, and zero sequence);
 - 5.1.2.4 Minimum and maximum short-circuit levels at PCC (3-phase and Single Line Ground (SLD), Root Mean Square (RMS) + DC component) with X/R ratios;
 - 5.1.2.5 Voltage variation and stability characteristics under load and generation changes;
 - 5.1.2.6 Operational configurations for redundancy and degraded modes;
 - 5.1.2.7 Power quality parameters (e.g., harmonics, flicker, unbalance) and distortion limits;
 - 5.1.2.8 Dynamic and transient behavior (e.g., inertia, inverter droop, response times);
 - 5.1.2.9 Steady state & dynamic models for load flow and transient stability studies;
 - 5.1.2.10 Single line and protection schematics for all operating states e.g. normal conditions and conditions without utility, Photovoltaic (PV) Generation/Battery Energy Storage System (BESS);
 - 5.1.2.11 Thevenin equivalents at PCC (magnitude & angle) for each operating state — positive/negative/zero sequences;
 - 5.1.2.12 Impedance vs frequency (0–3 kHz) or equivalent impedance scan to identify any risks to the rail systems and neighbors;
 - 5.1.2.13 Harmonic background (3rd–50th), flicker statistics and predicted harmonic injections from PV/BESS;
 - 5.1.2.14 Control modes of PV/BESS e.g. grid-forming, droop, fault ride-through, reactive power capability;
 - 5.1.2.15 Dynamic models Root Mean Square values & Electromagnetic Transient (EMT) e.g. including inverter control models, PLL/droop settings, Volt/VAR/Volt/Watt controls;
 - 5.1.2.16 BESS State of Charge (SOC) behavior and fault ride-through logic;
 - 5.1.2.17 Expected reclosing/auto-reclose schemes, breaker characteristics, protection clearing times and protection coordination times;
 - 5.1.2.18 Expected operating modes (e.g., normal, degraded, islanded, black start) and transitions;
 - 5.1.2.19 Fire safety report for on-site BESS (if co-located): thermal runaway risk, suppression system specification, and ventilation requirements; and
 - 5.1.2.20 Site access, equipment footprints, cable routing and civil constraints for shared areas. Civil works outside the TSCC Contractor's boundary remain with the upstream power supplier contractor.



- 5.1.3 The TSCC Contractor shall not be responsible for generating or guaranteeing the accuracy of the upstream data as defined in Clause 5.1.2. Responsibility for provision of this data rests with the upstream power supplier.
- 5.1.4 However, the TSCC Contractor shall incorporate all upstream-power-supplier parameters defined in Clause 5.1.2 into its design and shall perform modelling, studies, and calculations covering the full electrical system downstream of the PCC at the utility service voltage (medium voltage, nominally 34.5 kV or as confirmed with the serving utility). The studies shall address the following:
 - 5.1.4.1 The Traction feeders to the SFCs;
 - 5.1.4.2 Non traction feeders to technical buildings via RMUs and step-down transformers; and
 - 5.1.4.3 Downstream electrical loads supplied by those feeders (e.g., traction, auxiliary systems, signaling, communications, and building systems) to the extent necessary to demonstrate system compliance, power quality, voltage stability, and fault levels.
- 5.1.5 The TSCC Contractor shall demonstrate that the overall integrated design is fully compliant with:
 - 5.1.5.1 The Rail Systems requirements of this Specification;
 - 5.1.5.2 Applicable Utility Grid Codes and Standards;
 - 5.1.5.3 TSCC Contractor studies/designs must be accepted by the utility via an ICD and authority before energization; and
 - 5.1.5.4 Any gaps, inconsistencies, or missing data as defined in clause 5.1.2 in the ICD shall be promptly identified and reported to the Authority for resolution with the upstream power supplier contractor.
- 5.1.6 The TSCC Contractor shall incorporate the upstream power supplier inverter control characteristics, as defined in Clauses 5.1.2.14 to 5.1.2.18, into its modelling and studies to demonstrate that power flow, voltage stability, and protection coordination within the traction and non-traction networks remain compliant with this Specification and the applicable Grid Codes.
- 5.1.7 The TSCC Contractor shall coordinate with the Authority and the upstream power supplier contractor to confirm equipment footprints, access routes, and construction and testing/commissioning sequencing to avoid schedule conflicts and ensure safe energization.
- 5.1.8 The TPSS shall ensure a minimum separation distance is maintained between TPSS equipment and upstream power supplier equipment, in accordance with IEC/IEEE insulation coordination requirements and NFPA fire separation codes.
- 5.1.9 Shared use of duct banks is permitted only where agreed in writing, with physical or metallic barriers to prevent induced voltages and electromagnetic coupling.
- 5.1.10 The TSCC Contractor shall ensure a temporary power supply, if necessary, for construction, installation, testing, and commissioning works.
- 5.1.11 The TSCC Contractor shall coordinate with the upstream power supplier via the ICD to ensure a single integrated earthing system is implemented, demonstrated, and documented across the site to avoid hazardous potential differences between TPSS and upstream power supply equipment.
- 5.1.12 The integrated earthing system shall comply with IEEE 80 and EN 50522 series and shall be validated through step-and-touch voltage studies and confirmed by on-site test results.
- 5.1.13 The TSCC Contractor shall provide all traction-side grounding, bonding, and equipotential connections up to a defined interface bar, where the upstream power supplier shall connect their system.



- 5.1.14 The TSCC Contractor shall coordinate with the upstream power supplier to ensure that BESS earthing practices (e.g., DC grounding) do not compromise the railway return current system.
- 5.1.15 The TSCC Contractor shall clearly define the protection zones of TPSS equipment versus upstream-side equipment.
- 5.1.16 Fault contribution and minimum/maximum fault current levels shall be declared by the upstream power supplier contractor. The TSCC Contractor shall design protection selectivity, accordingly, as defined in Clauses 4.1.12 to 4.1.14.
- 5.1.17 The TSCC Contractor shall ensure that traction-side protection (SFCs, feeders, OCS) remains selective and coordinated under all shared substation operating modes.
- 5.1.18 Control of upstream power supplier assets shall remain with the upstream operator. The TSCC Contractor shall provide, via an agreed ICD, the required interface relays, interoperability protocols, and signal exchange list to enable control, monitoring, safe isolation and interlocking with the operation control room operator.
- 5.1.19 The TSCC Contractor shall provide communication, emergency procedures, developed jointly with the upstream power supplier through the ICD, and validated during integrated testing and commissioning.

5.2 Part 2: Alternative Execution and Contingency Provisions

The provisions of this Part 2 are included to ensure continuity of the project in the event that the upstream power supplier works are deferred. The TSCC Contractor shall therefore ensure TPSS reliability with utility only supplies while incorporating provisions for seamless future integration of clean energy sources.

In the event of a deferral of the clean energy scope, and for the avoidance of doubt, the final service voltage at the Point of Common Coupling (PCC) shall be determined during design development in coordination with the serving utility. All references to 34.5 kV within this specification shall be understood as indicative only. The Designer shall verify and confirm the actual service voltage and shall adjust all associated system architecture, equipment ratings, insulation levels, and interface details accordingly.

- 5.2.1 The TSCC Contractor shall design the TPSS to operate reliably with power supply from the utility grid alone, in the event that the upstream power supplier energy sources are not yet commissioned as defined in clause 5.1.
- 5.2.2 The PCC medium-voltage switchgear (nominally 34.5 kV or as confirmed with the serving utility) shall normally be provided by the upstream energy supplier. In the event that the upstream energy supplier does not proceed, the TSCC Contractor shall design, provide, install, and commission the PCC medium-voltage switchgear, including all associated protection, control, auxiliaries, and interfaces compatible with the confirmed utility service voltage and step-down transformer.
- 5.2.3 The TSCC Contractor shall be responsible for coordinating and agreeing all necessary design, protection, and operational parameters with the utility provider, in accordance with the Interface Control Document (ICD), to ensure reliable and secure TPSS operation under the utility only scenarios.
- 5.2.4 The TSCC Contractor shall incorporate provisions to facilitate the later integration of additional upstream clean energy sources without requiring major redesign of the TPSS. These provisions shall include, as a minimum:



- 5.2.4.1 Interface capacity and protection settings at the PCC (utility service voltage) to accommodate future multi-source operation;
- 5.2.4.2 Space allocation and design allowances for future control, protection, and communication interfaces to integrate clean energy controls with TPSS SCADA and protection systems;
- 5.2.4.3 Selectivity, inverter control and protection logic designed such that future additional fault current contributions from the clean energy can be accommodated through parameter adjustment, without replacing TPSS equipment;
- 5.2.4.4 Earthing and bonding system design compatible with both utility only operation and later clean energy integration; and
- 5.2.4.5 SCADA and control system interface protocols designed to allow seamless extension for clean energy monitoring and control, consistent with this specification.
- 5.2.5 The TSCC Contractor shall demonstrate, through the studies and deliverables defined in Clause 5.1.4, that the overall interconnected traction power system, including the upstream power supplier, is stable, secure and compliant with all specified requirements.
- 5.2.6 These studies shall be performed irrespective of whether the clean energy facilities are commissioned concurrently with the traction power system or deferred to a later stage.
- 5.2.7 The TSCC Contractor shall ensure that control and protection coordination of the traction power system is compatible with both conventional utility supply and inverter-based clean energy supply, including:
 - 5.2.7.1 Fault ride-through and dynamic response to regenerative braking conditions;
 - 5.2.7.2 Management of fault contributions and protection selectivity during abnormal events; and
 - 5.2.7.3 Stability under both upstream and downstream (traction network/trains) disturbances.
- 5.2.8 These requirements shall be incorporated into the system design, regardless of whether renewable clean energy facilities are commissioned at the same time as the traction power system or at a later date to be integrated into the system.



6 SYSTEM REQUIREMENTS

6.1 General Requirements

- 6.1.1 The TSCC Contractor shall provide Traction Power Supply Systems at Authority's provided land parcels.
- 6.1.2 The TPSS system shall be future-proof, based on the most up-to-date and proven technology, if any unproven technology is to be used, this shall be submitted for approval by the Authority before design begins.
- 6.1.3 Proven technology means that the TPSS system shall be based on components that have been proven in similar service and configured in an arrangement that has been demonstrated in a report to provide the required performance.
- 6.1.4 The TSCC Contractor shall provide as a minimum, but not limited to, the following parts of the TPSS systems;
 - 6.1.4.1 Medium-voltage outgoing feeder cables from the PCC to the Static Frequency Converters (SFC), nominally 34.5 kV or as confirmed with the serving utility;
 - 6.1.4.2 Static Frequency Converters, including power conversion, transformers, filters, control, protection, and redundant cooling systems;
 - 6.1.4.3 2x25 kV outgoing feeders from the SFC to the switchgear;
 - 6.1.4.4 2x25 kV outgoing feeders for the connections to the OCS track side switches;
 - 6.1.4.5 Interconnection power, control and communication cables;
 - 6.1.4.6 Autotransformers;
 - 6.1.4.7 Switchgear, circuit breakers, isolators, disconnectors, ground switches;
 - 6.1.4.8 Surge arresters;
 - 6.1.4.9 Return cables;
 - 6.1.4.10 Interlocking;
 - 6.1.4.11 Traction Power Supply Facility, Switching Station and Paralleling Stations;
 - 6.1.4.12 Grounding and bonding systems, for Traction Power Supply Facilities, Switching Station and Paralleling Stations for earthing grids;
 - 6.1.4.13 Bonding of rails and metallic structures;
 - 6.1.4.14 Lightning protection systems;
 - 6.1.4.15 Civil, Structural and MEP works for Traction Power Supply Facilities, Switching Station and Paralleling Stations, including duct banks, trenches, HVAC, fire protection, lighting, outdoor lighting, small power and auxiliary AC/DC supplies;
 - 6.1.4.16 Protection systems;
 - 6.1.4.17 SCADA systems, integrated into the Railway Operation Control Room with IEC 61850/IEC 60870 protocols; and
 - 6.1.4.18 Local and remote control, monitoring and system integration.



6.2 Environmental Requirements

- 6.2.1 The TSCC Contractor shall ensure that all traction power supply system (TPSS) equipment complies with the environmental conditions defined in EN 50125-2 “Railway applications — Environmental conditions for equipment — Part 2: Fixed electrical installations”, unless otherwise specified.
 - 6.2.1.1 Equipment shall be suitable for operation under the site-specific environmental conditions as defined in the Design Criteria Manual chapter 35 for each TPSS location.
 - 6.2.1.2 Where the Design Criteria Manual Chapter 35 does not define certain environmental parameters, the TSCC Contractor shall apply the relevant Environmental Class (e.g., Class TX) as defined in EN 50125-2 for outdoor equipment.
 - 6.2.1.3 The TSCC Contractor shall confirm site specific environmental limits such as ambient temperature, humidity, altitude, and solar radiation with the Engineer before finalizing equipment design and testing documentation.
 - 6.2.1.4 All design, selection, and testing of TPSS equipment shall demonstrate compliance with the applicable environmental conditions referenced above.
- 6.2.2 The TPSS equipment shall be designed to operate satisfactorily under all variations of load, pressure, and temperature that may occur under normal and abnormal operating conditions.
- 6.2.3 The ingress protection (IP) rating, in accordance with EN 60529, shall be at least IP41 for indoor TPSS equipment and at least IP65 for outdoor TPSS equipment.
- 6.2.4 The TPSS equipment shall be protected against pests and local fauna.
- 6.2.5 The TPSS shall be designed to minimize electrical energy losses and to remain suitable for the local environmental and site-specific conditions.

6.3 Functional Requirements

- 6.3.1 The TSCC Contractor shall implement energy efficiency optimization solutions with the support of intelligent metering function and plant automation.
- 6.3.2 The TPSS shall be designed for continuous duty operation under the railway’s specified service patterns, including sustained high-speed operation and regenerative braking.
- 6.3.3 The TPSS equipment shall be designed to withstand short-term overloads and regenerative surges without damage or unsafe operation.
- 6.3.4 The system shall remain stable under dynamic operating conditions, including:
 - 6.3.4.1 Rapid train acceleration and braking;
 - 6.3.4.2 Simultaneous demand from multiple trains; and
 - 6.3.4.3 Transitions between normal and degraded modes of supply.
- 6.3.5 The TPSS protection systems shall maintain selectivity and discrimination under all operating conditions, including minimum and maximum short-circuit levels.
- 6.3.6 The TSCC Contractor shall support and act on study outputs as defined in Section 5 and provide mitigation proposals where instability or unacceptable system behavior is identified.
- 6.3.7 The TSCC Contractor must ensure that the TPSS design is fully coordinated with the upstream power supplier architecture to guarantee safe, reliable, and interoperable operation.



- 6.3.8 The TSCC Contractor shall demonstrate, through modelling, calculations and studies, that the traction power system (from Point of Common Coupling to pantograph & return system) remains compliant under the full range of upstream operating conditions.
- 6.3.9 TSCC Contractor must ensure all simulations shall be carried out using approved validated and certified software according to EN 50641 to model the upstream network, medium voltage network, static frequency converter (SFC), traction system, protection schemes, EMC, grounding and return/bonding systems.
- 6.3.10 The SFCs shall be capable of stable parallel operation in a closed synchronous mesh configuration with other substations.
- 6.3.11 The SFC shall be capable of bidirectional power flow, including regenerative braking absorption.
- 6.3.12 The TPSS shall ensure the fault current contribution is sufficient for downstream protection selectivity, based on declared PCC minimum fault levels.
- 6.3.13 Harmonic emissions shall comply with IEC 61000-3-6/IEEE 519 at PCC, with filters provided where required.
- 6.3.14 The TSCC Contractor shall ensure that electromagnetic compatibility (EMC), earthing, bonding, and return current designs are verified for the integrated system, including interface with neighbors, rolling stock, signaling, telecoms and civil assets.
- 6.3.15 The TSCC Contractor shall provide a fully integrated earthing and bonding system to ensure personnel safety, equipment protection, and system stability.
- 6.3.16 The TSCC Contractor shall ensure the return current system shall be designed in accordance with EN 50122 and IEEE 80, ensuring safe management of return currents and limiting step and touch potentials.
- 6.3.17 The TPSS shall comply with EMC requirements in accordance with EN 50121-5, EN 50388, and applicable parts of the IEC/EN 61000 series (including IEC 61000-3-6 and IEC 61000-4), IEEE 519 and CPUC Rule 21.
- 6.3.18 TSCC Contractor shall ensure the earthing and bonding design shall account for co-location with upstream power supply equipment (e.g. BESS, filters, PCC switchgear) to avoid hazardous potential differences.
- 6.3.19 The TSCC Contractor shall develop simulation models, using approved validated and certified software according to EN 50641 & calculations and studies of the traction system and the overall power system including the Medium Voltage supply to the Power Supplies for:
- 6.3.19.1 Steady-state load flow & traction modelling;
 - 6.3.19.2 AC & DC Short-circuit studies;
 - 6.3.19.3 Protection coordination & selectivity studies;
 - 6.3.19.4 Arc Flash rating of equipment;
 - 6.3.19.5 Insulation coordination;
 - 6.3.19.6 Lightning protection;
 - 6.3.19.7 Dynamic and transient performances;
 - 6.3.19.8 Harmonic and power quality behavior;
 - 6.3.19.9 Earthing & Bonding, EMC and return current distribution; and



6.3.19.10 Interlocking & operational concept.

6.3.20 The TSCC Contractor shall develop and submit from the simulation models and studies as defined in 6.3.21 & Section 7 the following deliverables but not limited to. In order to ensure a fully compliant integrated rail systems power supply design as stipulated in this document.

6.4 Performance Requirements

6.4.1 The TPSS shall be designed to meet the following performance requirements:

6.4.2 The maximum line speed design in accordance with EN 50163 and EN 50388.

6.4.2.1 The TPSS sizing shall be in accordance with the peak & prolonged frequency of the planned train services.

6.4.2.2 The Traction Power System shall be designed with full redundancy to ensure continuous operation under the following single electrical contingency conditions (failures/planned outages):

6.4.2.2.1 Loss of any one incoming sources;

6.4.2.2.2 Loss of any one static frequency converter;

6.4.2.2.3 Loss of any outgoing distribution equipment/feeder;

6.4.2.2.4 Loss of any one autotransformer paralleling/switching station; and

6.4.2.2.5 Loss of any negative feeder.

6.4.3 Degradation of train performance may be accepted in case of double electrical contingency conditions (simultaneous occurrence of more than 1 single electrical contingency condition in any electrical section). The degradation shall be defined by traffic operation study.

6.4.4 The TSCC Contractor shall design for overload capacity, short-term peak load during train acceleration, and safe handling of regenerative braking without instability.

6.4.5 The TPSS Contractor shall ensure that the voltage at the train pantograph under normal and disturbed operating conditions remains within the limits specified in EN 50163 and EN 50388:

6.4.5.1 This includes maintaining acceptable voltage drops under maximum traction load, limiting voltage dips and flicker caused by load changes or regenerative braking;

6.4.5.2 Ensuring compatibility with all rolling stock types; and

6.4.5.3 Compliance shall be demonstrated through design calculations, validated simulation models, and, where applicable, testing with prototype or reference rolling stock.

6.4.6 The TPSS shall allow seamless integration with the utility upstream power supplier to maintain voltage and frequency at the overhead contact system within specified limits (per EN 50163/EN 50388 or equivalent), under normal, peak and degraded load conditions.

6.4.7 The TPSS shall manage power flow between the utility upstream power supplier and regenerative braking from traction loads to optimize energy efficiency, minimize losses, and maintain supply availability.

6.4.8 The TPSS shall be protected against electrical faults through appropriately rated protection devices and fault detection/isolation mechanisms, ensuring minimum disruption to operations in accordance with applicable standards.



- 6.4.9 The TSCC Contractor shall make provisions for automatically switching between power sources to maintain supply availability.
- 6.4.10 The TSCC Contractor should incorporate power factor correction equipment if required to improve the system's efficiency and minimize losses, when integrating renewable clean energy sources or during low-load conditions.
- 6.4.11 The TPSS shall ensure that all control, monitoring and protection devices are connected to a centralized SCADA system with real-time monitoring capabilities for system operators.
- 6.4.12 The TPSS shall ensure interoperability by defining and implementing necessary communication standards (e.g. SCADA protocols, IEC 61850, IEC 60870-5-104) for seamless operation, monitoring, and control.
- 6.4.13 The TSCC Contractor shall provide reliable and secure communication and data transfer from the TPSS field devices to the centralized SCADA system in accordance with defined protocols and cybersecurity requirements.
- 6.4.14 Each traction substation facility, switching station, and paralleling post shall be equipped with auxiliary power systems to support protection, control, SCADA, communications, lighting, outdoor lighting, HVAC, fire detection/suppression, and security systems.
- 6.4.15 Auxiliary LV Supply shall normally be derived from a dedicated auxiliary transformer connected to the medium-voltage bus (nominally 34.5 kV or as confirmed with the serving utility) or local utility service, with redundancy or backup supply as per the Authority requirements.
- 6.4.16 DC Systems and Batteries shall provide uninterrupted supply to:
 - 6.4.16.1 Protection relays and interlocking devices;
 - 6.4.16.2 Control and SCADA systems;
 - 6.4.16.3 Telecoms and security devices; and
 - 6.4.16.4 Emergency lighting, alarms, and essential auxiliaries.
- 6.4.17 Batteries shall be sized for a minimum 6 hours autonomy (or Authority-specified requirement) under full critical load.
- 6.4.18 Battery Chargers shall be provided with alarm & monitoring and shall all be integrated into the SCADA system.
- 6.4.19 UPS Systems shall be online double-conversion type, configured with redundancy (N+1), and sized to carry all critical loads during switchover to DC systems or auxiliary transformer supply.
- 6.4.20 LV distribution shall include protection, discrimination, and monitoring, with design documentation (SLDs, load schedules, sizing calculations) submitted for review.
- 6.4.21 All auxiliary systems shall be designed for maintainability, with clear access, hot-swappable components where practicable, and health monitoring integrated into SCADA.
- 6.4.22 The TPSS shall provide a dedicated Traction Power SCADA system integrated with the Authority's OCC (Operations Control Centre).
- 6.4.23 The TPS shall provide HMI displays at substations, OCC, and remote operator workstations.
- 6.4.24 Provide alarms, events, sequence of events recording, trending, and power quality monitoring.



- 6.4.25 Substation Automation shall be based on IEC 61850 architecture, with IEDs and protection relays supporting GOOSE messaging for fast peer-to-peer communication.
- 6.4.26 SCADA Communication Protocols: IEC 60870-5-104 or DNP3 shall be used for remote communication between substations and OCC (Authority preference to be confirmed).
- 6.4.27 Gateways shall be provided where protocol conversion is required.
- 6.4.28 The TPSS shall provide alarms, events, sequence of events recording, trending, and power quality monitoring.
- 6.4.29 The TPSS shall provide remote monitoring and control of but not limited to:
 - 6.4.29.1.1 SFCs and transformers;
 - 6.4.29.1.2 Switchgear, circuit breakers, and disconnect/isolators switches;
 - 6.4.29.1.3 Traction Power Supply Facilities, Switching Stations and Paralleling Posts;
 - 6.4.29.1.4 Auxiliary and protection systems; and
 - 6.4.29.1.5 Fire, HVAC, security alarms (as required).
- 6.4.30 The TSCC Contractor shall develop and submit for Authority's acceptance the HMI to be implemented for the TPSS in the Sub-Station and the OCC for control and monitoring.
- 6.4.31 The TPSS shall coordinate with the upstream power supplier's SCADA for exchange of operational signals, breaker status, fault alarms, load flow, power quality, and renewable integration status.
- 6.4.32 The TPSS Contractor shall provide a complete Interface Signal Exchange List (ISEL) defining all alarms, events, analog/digital measurements, and control signals exchanged between traction power SCADA, upstream power supplier SCADA, and OCC.
- 6.4.33 All signals shall include time stamping with millisecond accuracy; time synchronization shall be achieved via GPS or NTP/PTP across all devices.
- 6.4.34 TPSS shall provide redundancy and availability for dual redundant fiber optic communication paths between traction substations, switching stations, paralleling post and OCC.
- 6.4.35 TPSS shall ensure the network architecture shall eliminate single point of failure and provide automatic change over.
- 6.4.36 The TSCC Contractor shall provide as-built drawings, certificates, test logs, commissioning records, and software/hardware configuration details at final handover.
- 6.4.37 The TSCC Contractor shall provide spare parts list, maintenance tools and training.

6.5 Electrical Protection Requirements

- 6.5.1 The TPSS shall clearly define the protection zones of traction-side equipment versus upstream-side equipment.
- 6.5.2 The TSCC Contractor shall design protection selectivity accordingly taking into consideration fault contribution and minimum/maximum fault current levels from upstream power supply and regenerative braking.
- 6.5.3 The TPSS shall ensure that traction-side protection (SFCs, feeders, OCS) remains selective and coordinated under all shared substation operating modes.



- 6.5.4 The OCS circuit breakers shall be provided with intelligent electronic microprocessor-based protective relays and devices to protect against short-circuits and conductor overloading conditions.
- 6.5.5 The TPSS protection design shall take into account the limited short circuit current capability of the SFC systems.
- 6.5.6 The protection system shall be able to distinguish between short circuits fault and overloading conditions.
- 6.5.7 Each circuit breaker shall be equipped with a primary and backup protection.
- 6.5.8 The TPSS shall consider double end feeding.
- 6.5.9 The TPSS shall consider automatic reclosing protection to be implemented all sequences shall be described.

6.6 EMC/Earthing & Bonding System Requirements

- 6.6.1 The TSCC Contractor shall ensure that EMC/earthing and bonding of the TPSS system are designed and implemented to prevent or minimizing risks such as:
 - 6.6.1.1 Electric shock hazards to personnel and equipment;
 - 6.6.1.2 Ground potential differences; and
 - 6.6.1.3 Electromagnetic interference (EMI) affecting system operation and external equipment.
- 6.6.2 The TSCC Contractor shall demonstrate compliance with EMC/earthing and bonding requirements through design calculations, grounding studies, and field testing. The verification shall include:
 - 6.6.2.1 Emissions and immunity testing;
 - 6.6.2.2 Measurements of ground resistance;
 - 6.6.2.3 Touch, step & transferred voltages; and
 - 6.6.2.4 Assessment of potential gradients and EMI mitigation.
- 6.6.3 All designs and tests shall comply with relevant standards, including:
 - 6.6.3.1 EN 50122-1, EN 50388, EN 50121-5, IEC 61000 series as applicable to traction power systems, to demonstrate compliance with EMC limits;
 - 6.6.3.2 IEEE Std 80 (Guide for Safety in AC Substation Grounding);
 - 6.6.3.3 IEEE Std 142 (Green Book – Grounding of Industrial and Commercial Power Systems); and
 - 6.6.3.4 IEEE Std 81 (Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials).
- 6.6.4 The TPSS shall develop a detailed design for the earthing and bonding system, ensuring:
 - 6.6.4.1 Correct grounding of all metallic parts, electrical installations, and structural components;
 - 6.6.4.2 Electrical continuity between all conductive parts to prevent any floating potentials;
 - 6.6.4.3 Adequate separation of functional and protective earth connections;
 - 6.6.4.4 Suitable earthing electrodes (e.g., earth rods, earthing plates, or grids) to meet the system's current and fault requirements; and



- 6.6.4.5 Earth resistance is within permissible limits for safe operation.
- 6.6.5 The TPSS System shall be connected to the running rails by at least 2 return cables. Each return cable shall be of sufficient size to carry the maximum load current, thereby allowing for the failure of 1 return cable.
- 6.6.6 In direct proximity to operational DC railway, earthing and bonding solutions of all metallic structures shall be compatible with the requirements of EN 50122-3.
- 6.6.7 The TSCC Contractor shall ensure the earthing system, its components and bonding conductors shall be capable of distributing and discharging the fault current without exceeding thermal and mechanical design limits based on backup protection operating time.
- 6.6.8 TSCC Contractor shall make provisions for all the sub-system of the earthing & bonding to be tested.
- 6.6.9 The TSCC Contractor shall ensure that the earthing system shall maintain its integrity for the expected installation lifetime with due allowance for corrosion and mechanical constraints.
- 6.6.10 Minimum cross-sections shall be calculated taken into account mechanical strength, stability against corrosion and thermal strength.
- 6.6.11 Earthing system performance shall avoid damage to equipment due to excessive potential rise, potential differences within the earthing system and due to excessive currents flowing in auxiliary paths not intended for carrying parts of the fault current.
- 6.6.12 The TSCC Contractor's system shall identify sources of electromagnetic emissions and highlight potential sources of interference and their interactions within the TPSS and its sub-systems.
- 6.6.13 The TPSS shall develop and implement design solutions to mitigate EMC risks, including but not limited to:
 - 6.6.13.1 Ensuring appropriate shielding for sensitive components and wiring;
 - 6.6.13.2 Implement effective grounding techniques to reduce electromagnetic interference;
 - 6.6.13.3 Install filters to limit conducted emissions and improve immunity; and
 - 6.6.13.4 Optimize component and wiring layout to mitigate any coupling and interference.
- 6.6.14 The TSCC Contractor shall perform electromagnetic modelling and simulation to predict the system's performance in terms of emissions and immunity.
- 6.6.15 The TSCC Contractor shall develop a detailed test plan procedure for the planning and execution of testing of earthing/bonding, and emissions and immunity, as defined in clause 6.6.2. The test plan shall include all relevant standards and verification methods as defined in clause 4.1.6.3 and shall be submitted to the Authority for review and approval.
- 6.6.16 The TSCC Contractor shall use simulation tools to test different scenarios and verify the effectiveness of EMC mitigation techniques before procurement and construction.
- 6.6.17 The TSCC Contractor shall maintain a thorough audit trail of all TPSS EMC-related activities, including risk assessments, design decisions, tests, and modifications. Ensuring that all EMC-related documentation is easily accessible for review by internal or external auditors.

6.7 TPSS System Integration and Interoperability Requirements

- 6.7.1 The TPSS shall model the complete power system, as defined in clause 6.3.19 & Section 7.



- 6.7.2 The TPSS shall demonstrate full interoperability compliance as defined in clause 6.7.1 of all assets under the following conditions:
- 6.7.2.1 Normal and degraded operation;
 - 6.7.2.2 Light & Full Load;
 - 6.7.2.3 Engineering hours;
 - 6.7.2.4 Regenerative braking with multiple trains under both light & full loads; and
 - 6.7.2.5 Different operational configurations (single-source operation) to simulate disturbance modes for instance loss of utility or clean energy as defined in clause 6.7.2.
- 6.7.3 The TPSS Contractor shall ensure compliance with EN 50388 (traction power supply and rolling stock interface).
- 6.7.4 The TPSS shall ensure compliance with the utility grid codes.

6.8 Security and Cybersecurity Requirements

- 6.8.1 The TPSS shall be fully compliant with the Authority's cybersecurity policies.
- 6.8.2 All traction SCADA and communication systems shall comply with IEC 62443 for industrial cybersecurity, including applicable system and component level requirements.
- 6.8.3 Segregation between traction power SCADA, signaling, and telecom networks shall be implemented, either physically or logically, to prevent unauthorized access and interference.
- 6.8.4 Secure remote access for diagnostic or maintenance purposes shall be provided using strong authentication and encrypted communication, with full logging and audit trails of all access and actions.

6.9 Civil, Structural, Buildings & MEP Requirements

- 6.9.1 The TSCC Contractor shall design and construct buildings for the traction substations facility, switching stations, and paralleling posts.
- 6.9.2 Facilities for housing electrical equipment shall comply with this Specification and shall also be designed and constructed in accordance with Schedule 16 Section 4 Civil Works as defined in the SoW.
- 6.9.3 Facilities for housing electrical equipment, whether provided as permanent buildings or modular housings, shall include, but not be limited to, the following:
- 6.9.3.1 HVAC systems to maintain equipment environmental conditions;
 - 6.9.3.2 Fire detection and suppression systems (FM-200, inert gas, or sprinklers as appropriate);
 - 6.9.3.3 Emergency lighting, small power, and auxiliary supply systems;
 - 6.9.3.4 Civil foundations, plinths, hard standing access roads, turning space for maintenance vehicles;
 - 6.9.3.5 Anti trespass fencing, controlled access gates, CCTV, and outdoor lighting;
 - 6.9.3.6 All appropriate operational signage (e.g. warning, danger signs, location, mileage emergency contacts etc.);
 - 6.9.3.7 Drainage, bunding, and environmental protection measures;
 - 6.9.3.8 Noise mitigation and seismic design;
 - 6.9.3.9 Fire safety and emergency response provisions; and



- 6.9.3.10 Spare ducts and space for future expansion.
- 6.9.4 The TSCC Contractor shall deliver site layout drawings and civil design packs including all calculations related to civil works, building structures, HVAC and MEP works.
- 6.9.5 Buildings shall meet applicable fire, seismic, and occupational safety codes.
- 6.9.6 The TSCC Contractor shall design substation civil works to allow independent secure access for TPSS staff and upstream supplier staff.
- 6.9.7 Shared areas (roads, parking, emergency exits) shall be coordinated in the site layout plan.

6.10 Reliability, Availability, Maintainability, and Safety (RAMS) Requirements

- 6.10.1 The TPSS shall comply with the safety requirements defined in the TSCC Contractor's Safety Analysis Report.
- 6.10.2 The TSCC Contractor shall prepare a Safety Case for the TPSS, in accordance with:
 - 6.10.2.1 EN 50126 (RAMS);
 - 6.10.2.2 EN 50128 (software systems, if applicable); and
 - 6.10.2.3 EN 50129 (safety-related electronic systems).
- 6.10.3 The Safety Case shall include hazard identification, risk assessment, and mitigation strategies for traction power equipment and interfaces.
- 6.10.4 The TSCC Contractor shall treat TPSS safety as an integral part of the design, commencing at project initiation, to ensure potential hazards are identified, assessed and resolved with minimal impact on schedule and cost.
- 6.10.5 The TPSS design and operational procedures shall incorporate fail-safe principles such that failures shall not disable the system, cause human injury, damage equipment, or result in inadvertent operation of critical equipment.
- 6.10.6 TPSS equipment shall be located and arranged so that access for operation, maintenance, or repair does not require personnel to be exposed to hazards such as entrapment, chemical burns, electric shock, sharp edges, or toxic atmospheres.
- 6.10.7 TPSS design and operational procedures shall include suitable warning and caution notes in operational, assembly, maintenance and repair documentation, and shall provide distinctive markings on hazardous components, equipment, or facilities for personnel protection.
- 6.10.8 Energy equipment shall be located so as not to infringe on required personnel protection.
- 6.10.9 Emergency stop/isolation buttons shall be provided in TSCC Contractor's technical rooms to enable rapid disconnection of electrical supply in case of fire or other emergencies.
- 6.10.10 The TSCC Contractor shall prepare and maintain a RAMS program for the TPSS addressing:
 - 6.10.10.1 Reliability: component failure rates, redundancy provisions;
 - 6.10.10.2 Availability: minimum service continuity levels during failures;
 - 6.10.10.3 Maintainability: access, spares, diagnostics, and modular replacement; and
 - 6.10.10.4 Safety: compliance with SIL requirements for protection and control systems.
- 6.10.11 The RAMS program shall also ensure that:



- 6.10.11.1 The system continues to operate safely at reduced capacity during degraded operation or equipment failure.
- 6.10.11.2 Power supply interlocking maintains minimum protection against unsafe operations.
- 6.10.11.3 Degraded modes and equipment failures are monitored and logged for RAM reporting.
- 6.10.11.4 Subsystem RAM requirements are specified where FMECA identifies failure modes affecting maintenance, operations, or safety, using a risk-based approach.
- 6.10.11.5 Trial operation tests shall include staff readiness for degraded modes and emergency conditions, following operator and maintainer procedures.
- 6.10.12 The RAMS targets shall align with overall railway system performance requirements as defined by the Authority.
- 6.10.13 Through design, installation, and testing & commissioning, the TSCC Contractor shall ensure that TPSS equipment and subsystems can be safely energized, with all associated risks controlled, documented, and verified.
- 6.10.14 The TSCC Contractor shall maintain an auditable record of safety analyses, hazard logs, risk assessments, test results, and energization authorizations to demonstrate compliance with RAMS obligations and to satisfy oversight by the FRA or other regulatory authorities.
- 6.10.15 The RAMS program shall address interfaces between TPSS, upstream power suppliers, auxiliary systems, and protection/control systems, ensuring hazards are managed across system boundaries.
- 6.10.16 Testing and commissioning of TPSS equipment and subsystems shall be carried out in accordance with the procedures and Inspection Test Plans defined in Clauses 4.1.6.3 and 4.1.6.4. The results shall form part of the evidence base for the Safety Case and RAMS Program.
- 6.10.17 Safety and RAMS requirements defined in Clauses 6.10.13 through 6.10.16 shall be treated as derived safety and RAMS requirements. These requirements shall be inserted into the Project Requirements Management System (e.g., DOORS) in accordance with Clause 4.1.6.2, with full traceability to higher-level safety requirements and RAMS program deliverables, and maintained as auditable evidence throughout the project lifecycle.



7 ELECTRICAL CALCULATIONS, MODELLING AND STUDIES REQUIREMENTS

- 7.1.1 The TSCC Contractor shall update models at each project phase and provide them to the Authority for system level integration.
- 7.1.2 The studies shall demonstrate safe and stable operation as defined in 6.7.
- 7.1.3 The TSCC Contractor shall deliver EMC & earthing and bonding design reports.
- 7.1.4 The TSCC Contractor shall deliver protection coordination studies and relay settings from the upstream energy power supply to downstream final loads.
- 7.1.5 The TSCC Contractor shall provide a grid connection study verifying compliance with utility interconnection requirements.
- 7.1.6 The TSCC Contractor shall provide a dynamic stability study assessing voltage and frequency stability under various conditions.
- 7.1.7 The TSCC Contractor shall submit a harmonic distortion analysis report ensuring compliance with IEEE 519 limits for voltage and current harmonic content.
- 7.1.8 The TSCC Contractor shall submit an insulation coordination study, defining the required insulation levels for the TPSS & components.
- 7.1.9 The TSCC Contractor shall provide energy losses evaluation report for the whole traction power system.
- 7.1.10 The TSCC Contractor shall provide protection study for DC faults from the PV generation and Battery Energy Storage System to ensure safety, reliability, and protection of the traction power system.
- 7.1.11 The TSCC Contractor shall provide a lightning protection study, including direct strike shielding and surge arresters to protect the TPSS Systems.
- 7.1.12 The TSCC Contractor shall provide an arc flash study to ascertain the minimum PPE requirements for the maintenance operator.
- 7.1.13 The TSCC Contractor shall submit an electromagnetic interference (EMI) and transient overvoltage study, addressing switching transients, harmonics, and electromagnetic disturbances.
- 7.1.14 The TSCC Contractor shall provide a voltage profile analysis at key system nodes in the rail systems, including the 34.5 kV bus bar (nominally 34.5 kV or as confirmed with the utility/clean energy contractor), SFC outputs 2X25 kV, OCS, and non-traction buildings, ensuring voltage remains within allowable limits under all operating conditions.
- 7.1.15 The TSCC Contractor shall demonstrate the voltage (V) current (A) active (P) and reactive (Q) power across all the traction power system elements, including utility, PV/BESS, traction loads, and non-traction loads.
- 7.1.16 The TSCC Contractor shall demonstrate the power factor, ensuring overall power factor compliance at the point of common coupling (PCC) and across the traction power system.
- 7.1.17 The TSCC Contractor shall demonstrate the loading analysis for the traction power system, ensuring loading remains within thermal and electrical design limits under steady-state and transient conditions.



-
- 7.1.18 The TSCC Contractor shall provide a consolidated power quality report, evaluating flicker, transients, and voltage unbalance under normal and worst-case conditions.
 - 7.1.19 The TSCC Contractor shall develop a phase imbalance and neutral current study, ensuring balanced power distribution across phases to minimize system inefficiencies.
 - 7.1.20 The TSCC Contractor shall submit a ferro resonance study, evaluating potential issues from switching effects.
 - 7.1.21 The TSCC Contractor shall provide a Ferranti effect analysis, modelling voltage rise in lightly loaded long transmission/distribution cables.
 - 7.1.22 The TSCC Contractor shall develop a controlled switching strategy to minimize transient effects from breaker operations.
 - 7.1.23 The TSCC Contractor shall submit a voltage stability study ensuring voltage levels are maintained under various operating conditions in particular reference to the upstream power supply network.
 - 7.1.24 The TSCC Contractor shall demonstrate simulation studies modelling train movement, acceleration, coasting, braking, and regenerative power.
 - 7.1.25 The TSCC Contractor shall demonstrate simulation studies to determine thermal limits for the Overhead Contact & Return System.
 - 7.1.26 The TSCC Contractor shall submit a voltage drop analysis along the Overhead Contact System modelling expected voltage variations from the substation to the trains under peak, non-peak and contingency conditions.
 - 7.1.27 The TSCC Contractor shall submit a train voltage profile study, ensuring voltage at the pantograph remains within operational limits under all operating conditions.
 - 7.1.28 The TSCC Contractor shall submit a traction return path and grounding study, analyzing return current distribution back to the source.
 - 7.1.29 The TSCC Contractor shall provide an earthing and bonding study to prevent injury, corrosion and unintended current paths.
 - 7.1.30 The TSCC Contractor shall submit a regenerative braking power flow analysis, evaluating how regenerated energy is distributed to the OCS, non-traction loads, and BESS.
 - 7.1.31 The TSCC Contractor shall provide cable sizing calculations for all outgoing feeders, considering voltage drop, thermal limits, and fault current withstand capability as per the installation methods.
 - 7.1.32 The TSCC Contractor shall submit a SFC performance study, including power conversion efficiency, voltage control, and response to regenerative braking.
 - 7.1.33 The TSCC Contractor shall provide a protection and fault clearance strategy for the 2x25 kV traction supply.
 - 7.1.34 The TSCC Contractor shall submit cable screen and bonding requirements, ensuring conformance of the shielding and grounding of HV, LV & control/communication cables.
 - 7.1.35 The TSCC Contractor shall provide the EMC separation requirements, defining minimum clearances and segregation for high-voltage, low-voltage, and control/communication circuits.
 - 7.1.36 The TSCC Contractor shall provide cable routing and cable tray design, ensuring compliance with fire safety and mechanical protection requirements.
-



- 7.1.37 The TSCC Contractor shall develop a Safety Compliance Plan, covering PPE, arc flash mitigation, and personnel training.
- 7.1.38 The TSCC Contractor shall provide the operational philosophy including the interlocking methods.
- 7.1.39 The TSCC Contractor shall provide the operational diagrams (e.g. isolation/single line diagrams etc.) and the O&M manuals for the systems.



8 INTERFACES REQUIREMENTS

8.1 General Requirements

8.1.1 Interfaces are classified as below:

- 8.1.1.1 Third Party interfaces: interfaces between TSCC Contractor systems and systems provided by Third Party (excluding Authority's contractors);
- 8.1.1.2 External interfaces: interface between TSCC Contractor systems and systems provided by the Authority's contractors (Civils Packages, Stations contractor, Facilities contractor, Solar PV and BESS contractors); and
- 8.1.1.3 Interfaces between systems within the TSCC Contractor's scope.

8.1.2 The TSCC Contractor shall develop design considering the identified Third Parties, External and Internal interfaces to ensure the required functionalities and performance described in this specification.

8.1.3 The TSCC Contractor shall, if necessary, propose any additional interfaces required to ensure the functionalities and performance described in this specification.

8.2 Third Parties Interfaces

8.2.1 Federal Railroad Administration.

8.2.2 Utility Provider.

8.2.3 Upstream Power Supplier

8.3 External Interfaces

8.3.1 The TSCC Contractor shall manage the electrical interfaces for the connection at the PCC with the upstream power supplier contractor.

8.3.2 The TPSS interface to the upstream power supplier will be at the cable terminations within the 34.5 kV outgoing feeders switchgear at the PCC (nominally 34.5 kV or as confirmed with the utility/clean energy contractor).

8.3.3 The TSCC Contractor shall coordinate with the Federal Railroad Administration to meet their requirements for the energization of the power supply.

8.4 Internal Interfaces

8.4.1 The TSCC Contractor shall ensure all necessary load profiles, connected equipment data, and electrical parameters of the non-traction systems connected to 34.5kV Medium Voltage Network (nominally 34.5 kV or as confirmed with the utility/clean energy contractor), is considered for the detailed system modelling, calculations, studies, to perform the overall integrated power supply design as defined in clause 6.3.19.

8.4.2 The interface point shall be the secondary side terminals of the auxiliary transformer for the non-traction systems.

8.4.3 The TSCC Contractor shall provide LV Power Supply to the following TPSS Systems;

- 8.4.3.1 Traction Power Supply Facility;
- 8.4.3.2 Switching Station; and
- 8.4.3.3 Paralleling Station.



- 8.4.4 As defined in the Standard Specifications STS Medium Voltage & Low Voltage Power Supply TSCC Contractor Specifications.
- 8.4.5 TPSS interface to the OCS will be at the track side switch.
- 8.4.6 The TPSS will not be responsible for the design, procurement and installation of the track side switch. This shall be provided by the OCS contractor.
- 8.4.7 The connection between the Traction Power Supply Facility, Switching Station and Paralleling Station for the 2X25 kV feeders to the OCS track side switch should be designed and installed by the TSCC Contractor.
- 8.4.8 TPSS will supply the LV power and control/communication cables to the track side switch located outside the Traction Power Supply Facility, Switching Station and Paralleling Station.
- 8.4.9 In the instance where the track side switch is not located in the vicinity as defined in clause 8.4.5. The LV power and control/communication cable shall be supplied by the nearest non traction system building.
- 8.4.10 The connection between the return circuit and the running rails at the Traction Power Supply Facility, Switching Station and Paralleling Station shall be designed and installed by the TSCC Contractor.



9 MATERIALS, PRODUCT, AND COMPONENTS REQUIREMENTS

9.1 General Requirements

- 9.1.1 All materials supplied shall conform to the requirements and test methods of the relevant standards and regulations.
- 9.1.2 All materials supplied shall be of sufficient grade and quality to meet the designed life requirements.
- 9.1.3 Electrical equipment and cables shall be de-rated according to the method of installation, manufacturer's recommendations or applicable codes and standards, for the design conditions.
- 9.1.4 The TPSS equipment shall be complete with all parts and accessories or material which are useful for efficient operation of the TPSS system components. Such accessories and materials shall be deemed to be within the scope of this specification whether specifically mentioned or not.
- 9.1.5 The supply shall include all supporting structures, embedded parts, auxiliary equipment, mechanical linkages, auxiliary circuits wiring, interlocking devices necessary for their efficient operation. All such parts and accessories shall be deemed to be within the scope of this specification whether specifically mentioned or not.
- 9.1.6 TSCC Contractor power equipment shall be designed ensuring adequate protection from rodent action. Additionally, the TSCC Contractor shall implement any measures ensuring rodent eradication.
- 9.1.7 The supply of material products and components shall include where appropriate UV protection is.

9.2 LV Distribution

- 9.2.1 Refer to Standard Specifications STS Medium Voltage & Low Voltage Power Supply TSCC Contractor Specifications.



Schedule 5(t)

Glossary of Terms, Abbreviations, and Definitions

California High-Speed Rail Authority



Standard Specifications

TSCC Specification

SPEC-0024 – Glossary of Terms, Abbreviations, and Definitions

Rev. 0.0

Authored:

A handwritten signature in blue ink, appearing to read "Francois Pignard".

Francois Pignard, Engineer

10/15/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Thomas Newey".

Thomas Newey Telecoms Lead

10/15/2025

Date

Checked:

A handwritten signature in black ink, appearing to read "Bruno Comperat".

Bruno Comperat, Deputy Director of Rail Engineering

10/16/2025

Date

Approved:

A handwritten signature in blue ink, appearing to read "Ryan Scott".

Ryan Scott, Director of Rail Engineering

10/16/2025

Date

Released:

A handwritten signature in blue ink, appearing to read "Amit Joshi".

Amit Joshi, Configuration Manager

10/16/2025

Date



Document Revision History – Glossary of Terms, Abbreviations, and Definitions**First Edition****September 2025**

Revision	Date	Revision Description
0.0	September 2025	First edition



TABLE OF CONTENTS

1 ACRONYMS AND ABBREVIATIONS 4

2 DEFINITIONS 11



1 ACRONYMS AND ABBREVIATIONS

Abbreviation	Description
2	
2FA	Two Factor Authentication
3	
3GPP	3 rd Generation Project Partnership
A	
ADA	Americans with Disabilities Act
ADAAG	ADA Accessibility Guidelines
AFILS	Audio-Frequency Induction Loops
ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
ASP	Axle Load speed Profile
ATAF	Automatic Track Ahead Free
ATO	Automatic Train Operation
ATR	Automatic Train Reporting
ARS	Automatic Route Setting
B	
BBU	Baseband Unit
BG	Balise Group
BMCA	Best Master Clock Algorithm
BRDS	Broken Rail Detection System
C	
CA	Certificate Authority
CALEA	Communications Assistance for Law Enforcement Act
CBC	California Building Code
CBI	Computer-Based Interlocking
CBM	Condition-Based Monitoring
CCPA	California Consumer Privacy Act
CCS	Control-Command and Signaling
CCTV	Closed Circuit Television
CDR	Call Detail Records
CES	Conditional Emergency Stop
CHSR	California High Speed Rail
CIDs	Customer Information Displays
CIS	Customer Information System
CLI	Command Line Interface
C-RAN	Centralized Radio Access Network
COPPA	Children's Online Privacy Protection Act
COTS	Commercial Off The Shelf (hardware and software)
COS	Class of Services



Abbreviation	Description
CPR	Coupled Power Ratio
CSOC	Cybersecurity Operations Center
CWDM	Coarse Wavelength Division Multiplexing
D	
DANS	Dynamic Ambient Noise Sensors
DAS	Distributed Antenna System
DC	Direct Current
DCM	Design Criteria Manual
DCN	Digital Communications Network
DDS	Derailment Detection System
DMI	Driver Machine Interface
DMZ	Demilitarized Zone
DSCP	Differentiated Services Code Point
DWDM	Dense Wavelength Division Multiplexing
E	
E911	Enhanced 911
EACS	Electronic Access and Control System
EAMS	Electronic Asset Management System
ECCS	Energy Control and Command System
eCPRI	Enhanced Common Public Radio Interface
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EN	European Norm
EoA	End of Authority
EoL	End of Life
EOS	Early Operating Segment
EoS	End of Support
ERA	European Union Agency for Railways
ERCS	Emergency Responder Communication System
ERTMS	European Railway Traffic Management System
ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
EU	European Union
EUG	ERTMTS Users Group
EULYNX	European initiative to standardize interfaces for digital railway control and signaling systems.
EVACS	Emergency Voice/Alarm Communication Systems
EVPN	Ethernet Virtual Private Network
F	
FAC	Local facility / Facility
FAR	First Article Demonstration Review (System Development Life Cycle Milestone)
FAT	Factory Acceptance Testing
FCC	Federal Communications Commission
FCS	First Construction Section
FDR	Final Design Review (System Development Life Cycle Milestone)
FIPS	Federal Information Processing Standards
FIM	Free Issue Material



Abbreviation	Description
FO	Fiber Optic
FPS	Fire Protection System
FRMCS	Future Railway Mobile Communication System
FS	Full Supervision (ETCS mode)
FTR	Field Testing Review (System Development Life Cycle Milestone)
G	
GD NTC	
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GTFS	General Transit Feed Specification
GUI	Graphical User Interface
H	
HABDS	Hot-Axle Box Detection System
HDEWS	Hazard Detection and Early Warning System
HMF	Heavy Maintenance Facility
HMI	Human Machine Interface
HST	High Speed Train
HV	High Voltage
I	
ICD	Interface Control Document
ICMP	Internet Control Message Protocol
ICSS	Integrated Control and Supervisory System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IERS	International Earth Rotation and Reference Systems Service
IFRA	
IM	Infrastructure Manager
IMF	Infrastructure Maintenance Facility
IMS	IP Multimedia Subsystem
IP	Internet Protocol OR Ingress Protection
IPVPN	Internet Protocol Virtual Private Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information and Telecom
IWF	Inter Working Function
IXL	Interlocking
J	
JRU	Juridical Recording Unit



L	
L2	ETCS Level 2
LCC	Life Cycle Cost
LF	Local Facility
LMF	Light Maintenance Facility
LMR	Land Mobile Radio
LT	ETCS level transition
LV	Low Voltage
LVPS	Low Voltage Power System
M	
MA	Movement Authority
MB	Marker Board
MCData	Mission-Critical Data
MCPTT	Mission-Critical Push-to-Talk
MCDS	Meteorological Condition Detection System (wind, rain, flood, earthquake)
MCVideo	Mission-Critical Video
MCX	Mission-Critical Services
MDM	Maintenance & Data Management
MEWP	Mobile Elevating Work Platform
MFA	Multi-Factor Authentication
MIB	Management Information Base
MM	Multi Mode (Optical Fiber)
MOCN	Multi-Operator Core Network
MORAN	Multi-Operator Radio Access Network
MOS	Mean Opinion Score
MOWF	Maintenance Of Way Facility
MOWS	Maintenance Of Way Siding
MPE	Maximum Permissible Exposure
MV	Medium Voltage
N	
N32	Network Interface 32
NEC	National Electrical Code
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NMS	Network Management System
NTP	Notice to Proceed
NTPS	Non-traction power supply
NTS	Network Timing System
NVR	Network Video Recorder
O	
O&M	Operations and Maintenance
OAuth	Open Authorization
OB	On-Board
OBU	ETCS On-Board Unit
OCC	Operation Control Centre
OCS	Overhead Contact System
ODF	Optical Distribution Frame
ONVIF	Open Network Video Interface Forum



OS	On-Sight (ETCS mode)
OC	Object Controller
OT	Operational Technology
OTDR	Optical Time Domain Reflectometer
P	
P25	Project 25
PABX	Private Automatic Branch Exchange
PAS	Public Address System
PACIS	Public Address and Customer Information System
PBD	Permitted Braking Distance
PCI DSS	Payment Card Industry Data Security Standard
PDT	Pacific Daylight Time
PG	Platform Gate System
PHP	Passenger Help Point
PIR	Project Initiation Review (System Development Life Cycle Milestone)
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PoE	Power over Ethernet
PSP	Power Supply Point
PST	Pacific Standard Time
PSTN	Public Switched Telephone Network
PTP	Precision Time Protocol
PTT	Push-to-Talk
PWS	Passenger Wi-Fi System
Q	
QoS	Quality of Service
R	
RAM	Reliability, Availability, Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RAN	Radio Access Network
RaSTA	Rail Safe Transport Application protocol
RBAC	Role-Based Access Control
RBC	Radio Block Centre
RCM	Reliability Centred Maintenance
RF	Radio Frequency
RFI	Radio Frequency Interference
RFID	Radio Frequency Identification
ROW	Right-of-Way
RRH	Remote Radio Head
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RT	Reverberation Time
RTMS	Rail Temperature Monitoring System
RVDS	Road Vehicle Detection System (vehicle, rock, landslide)
S	
SAML	Security Assertion Markup Language
SAT	Site Acceptance Testing
SCADA	Supervisory Control and Data Acquisition
SCI	Standard Communication Interface



SCP	Session Control Protocol
SDR	System Definition Review (System Development Life Cycle Milestone)
SEP	
SIEM	Security Information and Event Management
SIG	Signaling
SIL	Safety Integrity Level
SINR	Signal-to-Interference-plus-Noise Ratio
SIP	Session Initiation Protocol
SIT	System Integration Testing
SH	Shunting (ETCS mode)
SL	Sleeping (ETCS mode)
SL-A	Security Level Achieved
SL-C	Security Level Capability
SL-T	Security Level Target
SNMP	Simple Network Management Protocol
SM	Single Mode (Optical Fiber)
SoM	Start of Mission
SPD	Surge Protection Device
SPL	Sound Pressure Level
SR	Staff Responsible (ETCS mode)
SSP	Static Speed Profile
STI	Speech Transmission Index
SuC	System under Consideration
T	
TAP	Telematic Applications Program for Passenger services
TCEH	Train Control Equipment Housing
TCF	Train Certification Facility
TCR	Technical Contract Requirements
TCS	Train Control System
TD	Train Describer
TDS	Train Display System
TDG	Time-Distance Graph
TEL	Telephony System
TETRA	Terrestrial Trunked Radio
TLS	Transport Layer Security
TMS	Traffic Management System
TOD	Time-of-Day
TS	Track Side
TSA	Temporary Shunting Area
TSCC	Track and Systems Construction Contract
TSF	Training and Simulation Facility
TSI	Technical Specifications for Interoperability
TSR	Temporary Speed Restriction
TTM	Timetable Management
TTS	Text-to-Speech
TVP	Track Vacancy Proving
U	
UES	Unconditional Emergency Stop
UIC	International Union of Railways



UL	Underwriters Laboratories
UM	User Management
UPF	User Plane Function
UPS	Uninterruptable Power Supply
UTC	Coordinated Universal Time
V	
V&V	Verification and Validation
VAS	Video Analytics System
VLAN	Virtual Local Area Network
VMS	Video Management System
VoWi-Fi	Voice over Wi-Fi
VPN	Virtual Private Network
VRS	Voice Recording System
VWD	Video Wall Display
VXLAN	Virtual Extensible Local Area Network
W	
WCS	Wireless Communication Systems
WDM	Wavelength Division Multiplexing
WS	Workstation



2 DEFINITIONS

Terms	Description
As Low As Reasonably Practicable (ALARP)	It means the risk management principle whereby the degree of risk in a particular situation can be balanced against the time, trouble, cost and physical difficulty of taking measures to avoid the risk.
Asset Information	Means the combined set of static data (asset identification, description, specification, serial number, drawings, manuals, plans, certificates, etc.) dynamic data (condition, status, faults, event, alarms, cycles, meters, etc.) required to support the management of assets through the Enterprise Asset Management System.
Authority	California High Speed Rail Authority
Backhaul	The connection between the cell site (BBU/RRH) and the core network (e.g. the internet or operator's central systems). It carries user data and signaling to and from the wider network.
Business-critical	A label for a type of service. Potentially impacts revenue or customer service. It causes disruption but does not stop services.
Call-on route	Certain locations are permitted to allow more than one train into a single section, e.g. to join trains or enable two trains to use one platform. The movement of the second train into an occupied section is authorized by setting a "call-on" route.
CCS TSI	CCS TSI stands for the Technical Specification for Interoperability for "Control-Command and Signaling". The TSI aims to facilitate the development and deployment of the European Rail Traffic Management System (ERTMS) by setting common standards and requirements for the relevant subsystems.
Certificate Authority	A trusted entity that issues, validates, and manages digital certificates used for authentication and encrypted communication.
Computer Based Interlocking (CBI)	Safety equipment that contains the interlocking logic which processes the route setting activity based on the TMS commands, and the control of the wayside objects. The CBI is usually composed of several racks centrally located in the OCC buildings:



Terms	Description
Conditional Emergency Stop (CES)	In ETCS, a message from the Radio Block Centre (RBC) to the trainset on-board equipment, initiating a forced brake application unless the system acknowledges and revokes the emergency stop message before passing a defined point.
TSCC Contractor	Company, or entity engaged by the Authority to deliver the works as described in the TSCC Contract documents.
Danger Point (ETCS)	In ETCS, refers to the location beyond the End Of Authority that can be reached by the front of the train without creating a hazardous situation.
Debris Class A	A type of ETCS Eurobalises specified in CCS TSI SUBSET-036.
Degraded Operation	Means the state of continuing operations with significant unplanned failures.
Demilitarized Zone	A network segment that sits between either internal and external systems (IT Environments) or between IT and OT systems (OT Environments). The purpose is to add a controlled buffer where traffic can be controlled and filtered, usually with multiple firewalls. Supporting services and security services (such as authentication servers and anti-malware servers) are hosted in the DMZ.
Design Life	The expected operational lifespan of the system.
Digital Communications Network (DCN)	The optical fiber infrastructure and associated network equipment used for all inter-site connectivity between CHSR locations, based upon IP/MPLS.
Earthing and Bonding System	The arrangement of earth conductors and bonding conductors, typically including an earth grid, earth electrodes, overhead earth wires, cable sheaths, equipotential bonding cables, earth continuity conductors and parallel earthing conductors.
Electromagnetic Compatibility (EMC)	The ability of a piece of equipment or system to function satisfactorily in its electromagnetic environment without introducing electromagnetic disturbances to anything in that environment.



Terms	Description
Electronic Access Control System (EACS)	A networked security solution that provides centralized management, monitoring, intrusion detection, and control of physical access to CHSR infrastructure and facilities designated as EACS Protected Areas. The EACS comprises electronic locks, access control devices (e.g. RFID readers, keypads, biometric scanners), control panels, communication interfaces, and a central management platform.
Emergency Responder Communication System (ERCS)	A subsystem of WCS that enables OCC personnel to interoperate with Emergency Responders via non-public network communications.
Enterprise Asset Management System (EAMS)	A subsystem composed of tools, software and hardware to manage CHSR assets across their entire life.
EULYNX	European initiative to standardize interfaces for digital railway control and signaling systems.
Eurobalises	Passive, trackside transponders used in the ETCS to transmit information to Trainsets.
European Train Control System (ETCS)	Standardized European train control system defined in the CCS TSI. ETCS consists of 2 major parts: • Trackside equipment, in TSCC scope of work • On-board (on trainsets) equipment in Trainset contractor scope of work
External Interface	Interface between TSCC systems and systems provided by other CHSR contractors (civils packages, stations contractor, facilities contractor, Solar PV and BESS contractors);
Facilities	In the context of California High Speed Rail, Facilities refers to: • Operation Control Center (OCC) • Heavy Maintenance Facility (HMF) • Maintenance Of Way Facilities (MOWF) • Light Maintenance Facility (LMF) • Train Certification Facility (TCF)



Terms	Description
Factory Acceptance Test (FAT)	Test or series of Tests undertaken on equipment and systems to ensure all design and manufacturing problems for both hardware and software are resolved before full manufacturing begins.
Failover	The capability to switch to a redundant or standby system upon the failure of the currently active system.
Free Issue Material	Free Issue Material (FIM) refers to materials or equipment supplied by the client (e.g. CHSR Authority) to a contractor or supplier free of charge, for use in executing a project or contract.
Fronthaul	The high-speed connection between the Baseband Unit (BBU) and the Remote Radio Head (RRH) at the cell site. It carries the raw radio signals for processing and needs very low delay.
Future Radio Mobile Communication System (FRMCS)	A subsystem of WCS that provides mission-critical voice and data communication between all operational user groups and locations across the rail network. FRMCS is an international wireless communications standard for railway communication and applications specified in CCS TSI.
Handing Over RBC	Refers to an RBC/RBC Handover process within the ETCS, where communication and control responsibility for a train are transferred from one RBC to an adjacent RBC.
Handover	The process of transferring an ongoing call or data session from one channel connected to the core network to another.
Hazard Detection and Early Warning System (HDEWS)	A collection of integrated technologies and sensors designed to oversee and manage various auxiliary components of the trainsets and wayside infrastructure to monitor and control the trainset health, broken rail or falling vehicles detection, among others.
Headway	The interval of time between Trains moving in the same direction on the same route.
Human Factors	The discipline that applies knowledge of human capabilities and limitations to the design, operation and maintenance of technological systems



Terms	Description
Information Technology	Systems, hardware, and software used to create, process, or store information, information is data that is used for business or project purposes.
Integrated Control and Supervision System	The control systems used to control and monitor the operation in a safe, reliable, and accurate manner, including: • Digital Communication Network • Wireless Communication System • Electronic Access Control System • Network Timing System • Closed Circuit Television System • Public Address and Customer Information System • Network Timing System • Hazard Detection and Early Warning System • Enterprise Asset Management System • LV Power Supply System • Fire Protection System • Building Management System (Lighting, Elevators, Escalators, HVAC)
Interlocking (IXL)	The TSCC system is to ensure protection against the following hazardous situations: • Collision of trains; • Train derailment; • Operation mishandling by the Dispatcher The Interlocking system is composed of: • Computer Based Interlocking (CBI) • Object Controllers (OC) • Wayside Objects • Interlocking Maintenance and Diagnostic Terminal (MDT)
Internal Interface	Means interface between two systems within the TSCC Contractor's own scope of work.
Interoperability	The ability of different systems, devices, or organizations to work together. Can be used to describe technology interoperating and user groups or organizations interoperating.



Terms	Description
Low Voltage Power System (LVPS)	As defined in the STS Medium Voltage and Low Voltage Power Systems
Markers Boards	Visible, colored, and retroreflective panels placed trackside to convey specific information to the train driver during degraded modes of operation of ETCS.
Medium Voltage Power System (MVPS)	As defined in the STS Medium Voltage and Low Voltage Power Systems
Mission-critical	A label for a type of service. Essential for safe and continuous train operations. Failure causes immediate operational impact.
Mission-Critical Push-to-Talk (MCPTT)	A feature of FRMCS that supports individual and one to many talk group calling, emergency call initiation, call priority management, and other critical communication functions
Movement Authority	In ETCS, a Movement Authority (MA) is a digital permission that allows a train to proceed into a specific track section, specifying the permitted speed, braking curves for safe stopping, and the authorized distance (End of Authority).
Non-critical	A label for a type of service. Has no direct impact on safety, operations, or customer service. Failure causes minimal or no disruption.
Operational Technology	Refers to the hardware and software systems that facilitate the operation of the CHSR, used to distinguish assets from IT assets.
Operations Control Center (OCC)	The central facility where the coordination, supervision, and control of all rail operations across the CHSR System takes place.
Overhead Contact System (OCS)	The overhead contact system used to transmit electrical energy to Trainsets.
Passenger Information Display (PIDS)	The digital signage system and devices used to show real-time service, operation and navigation information to passengers.



Terms	Description
Passenger Wi-Fi System (PWS)	A non-critical subsystem of WCS that provides a seamless, reliable, secure, high-capacity, and high-speed wireless internet service accessible to passengers.
Power SCADA System	The control systems used to control and monitor the operation in a safe, reliable, and accurate manner, including: • Traction Power Systems • Medium Voltage Power Systems • Photovoltaic (PV) farms and Battery Electrical Storage System (BESS)
Protected Areas	Intrusion detection, and control of physical access to CHSR infrastructure and facilities by EACS system.
Radio Access Network (RAN)	The Radio Access Network (RAN) is the part of a FRMCS/5G network that connects user devices (like phones or trainset radios) to the core network.
Radio Block Center	Device used at ETCS Level 2 acting as a centralized safety unit. Using radio connection, it receives train position information and sends Movement Authority and further information required by the train for its movement.
Redundancy	Is defined for a system as 'N-x', where: • "N" is the number of items, components or sub-systems required to be operational to ensure all operations activities can be undertaken; and • "x" is the minimum number of items, components or sub-systems that may 'fail' or be removed from service without affecting or reducing the operations activities,
Safety Integrity Level (SIL)	Means the relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction based on the CENELEC standards EN 50126, EN50128 and EN5012
Security Levels	A defined level of cybersecurity robustness required for a system or zone based on threat, risk, and consequence, based on the IEC62443 standard.



Terms	Description
Shelters	Housing and protection for TSCC equipment located on wayside ensuring safety, security, and operational reliability from environmental elements and hazards.
Site Acceptance Tests (SAT)	Tests that are carried out on all installed Assets, or groupings thereof to ensure that the installation has been correctly completed and meet the design requirements
Static Speed Profile (SSP)	In ETCS, the description of the fixed speed restrictions of a given line. The speed restrictions can be related to such items as maximum line speed, curves, points, tunnel profiles, bridges.
System Breakdown Structure (SBS)	Means a hierarchical decomposition of the entire system into its constituent subsystems, and components.
System Owner	Entity accountable for mitigating cybersecurity risk, nominated for each system, as defined in the cybersecurity standard.
System under Consideration	The complete set of infrastructure, devices, endpoints, components, personnel, processes, and supporting technologies that contribute to the operation and security of the assets identified for cybersecurity consideration.
Telecommunication Systems	In CHSR project context, Telecommunication Systems refers to the following systems: • CCTV System • Electronic Access Control System (EACS) • Enterprise Asset Management System (EAMS) • Hazard Detection and Early Warning Systems (HDEWS) • Integrated Control and Supervision Systems (ICSS) • Public Address and Customer Information System (PACIS) • Telephony System • Wireless Communication Systems (WCS)
Third Party Interface	Means interface between a system within the TSCC Contractor's scope of work and a system within a Third-Party scope of work.



Terms	Description
Traction Power System	A power delivery system containing electro-mechanical components used to transfer power from the traction power supply system to the pantograph of electric Trainsets.
Train Control System	In CHSR project context, Train Control Systems refers to the following systems: • European Train Control System • Interlocking • Traffic Management System
Unconditional Emergency Stop (UES)	In the ETCS, a command that causes the train's brakes to apply immediately and unconditionally, without driver override, when the system detects a dangerous situation such as exceeding a Movement Authority.
UNISIG	The technical body responsible for the development, maintenance and updating of the CCS/TMS technical specifications which include ETCS and ATO.
Validation	Means confirmation that the final system fulfills its intended use, meets The Authority needs, and supports the Concept of Operations.
Verification	Means confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
Verification and Validation (V&V)	Means both Verification and Validation.
Verification Cross Reference Matrix	Means a matrix of Verification activities details appended to requirements.
Verification Evidence	Means the documented information that proves a requirement has been successfully verified according to the specified verification method.
Verification Method	Means the specific approach or technique used to determine whether a requirement has been fulfilled: Test, Demonstration, Inspection, Analysis, and Review.



Terms	Description
Verification Procedure	Means the detailed step-by-step process that defines how a verification method will be applied to confirm that a requirement is met.
Wayside Objects (Interlocking)	The equipment controlled and monitored by the Interlocking System shall be capable of controlling and monitoring at least the following wayside objects and monitoring their status: • Switch Machines • Derailers • Signals • Axle counters • Staff Protection System
Wireless Communication Systems (WCS)	The systems are designed to provide secure voice, data, and video communications in a high-speed rail environment. Includes passenger wi-fi.
Zone and Conduit	Zone and Conduits are defined in the IEC62443 and CENELEC TS 50701. They are cybersecurity groupings of assets into “zones” based on several factors (see cybersecurity standard) with controlled and security connectivity between zones, known as “conduits”.

