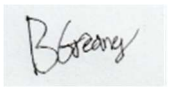
Schedule 5(a)

Cybersecurity

California High-Speed Rail Authority

Standard Specifications
TSCC Specifications
SPEC-0005 – Cybersecurity
Rev. 0.0

Authored:		10/15/2025
	Ben Greaney, Senior Cybersecurity Specialist	Date
Checked:		10/15/2025
	Thomas Newey, Telecoms Lead	Date
Checked:		10/16/2025
	Bruno Comperat, Deputy Director of Rail Engineering	Date
Approved:		10/16/2025
	Ryan Scott, Director of Rail Engineering	Date
Released:		10/16/2025
	Amit Joshi, Configuration Manager	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

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, configurating 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 of 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 on-boarding 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 on-boarding 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 of 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.