Schedule 5(r)

Wireless Communication System (WCS)

California High-Speed Rail Authority

Standard Specifications

TSCC Specifications

SPEC-0022 – Wireless Communication Systems (WCS)

Rev. 1.0

Authored:		12/22/2025
	Nick Ashby, Wireless Systems Lead	Date
Checked:		12/22/2025
	Thomas Newey, Telecoms Lead	Date
Checked:		12/23/2025
	Bruno Comperat, Deputy Director of Rail Engineering	Date
Approved:		12/23/2025
	Ryan Scott, Director of Rail Engineering	Date
Released:		12/23/2025
	Amit Joshi, Configuration Manager	Date

Document Revision History – WCS Specifications

Second Edition

December 2025

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

TABLE OF CONTENT

1 INTRODUCTION

1.1 Scope of the Technical Specification

1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Wireless Communication Systems, hereinafter: WCS.

1.1.2 This Technical Specification is based on the Authority's Design Criteria Manual (DCM) Chapter 12: Communication Systems and Train Control.

1.1.3 The functional architecture of the WCS is presented in Appendix A of this specification.

1.1.4 The requirements are formulated using the following words and their meanings:

- **"Shall":** Indicates mandatory requirement that must be strictly implemented. Any impossibility to fulfil this requirement must be agreed through a derogation case (see change management procedure).
- **"Should":** Indicates preferred course of action, recommendations. No agreement of derogation is necessary, there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course - for example the same goal is reached by other solutions, which are permissible within the binding standards or documents.
- **"Must":** Indicates an obligation or a mandatory requirement.
- **"May":** Indicates a permissible course of action within the limits of the standards, but which is not mandatory to be fulfilled.

2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

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

2.1.2 All generic standards to be used are provided in: Technical Contract Requirements.

2.2 Design Guidelines

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

No	Code	Title
[R2]	DCM_01	Design Criteria Manual Chapter 1: Overview
[R3]	DCM_12	Design Criteria Manual Chapter 12: Communication Systems and Train Control
[R4]	AREMA_17	AREMA Standards Chapter 17 – High-Speed Rail Systems
[R5]	DCM_12	Design Criteria Manual Chapter 26: Roadways and Site Works
[R6]	DCM_2	Design Criteria Manual, Chapter 2: Basis of Design
[R7]	DCM_35	Design Criteria Manual, Chapter 35: Environmental
[R8]	DCM_07	Design Criteria Manual, Chapter 7: Electromagnetic Compatibility

TABLE 66 : DESIGN GUIDELINES AND PROCEDURES.

2.3 Technical Specifications for Interoperability

2.3.1 The applicable Technical Specifications for Interoperability (TSIs) are listed below:

No	TSI	Title
[R9]	CCS TSI	COMMISSION IMPLEMENTING REGULATION (EU) 2023/1695 of 10 August 2023 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union and repealing Regulation (EU) 2016/919

TABLE 67 : LIST OF TSI AND REGULATIONS.

2.4 Standards

2.4.1 The relevant standards to be used for WCS are listed below.

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

No	Standard	Title
[R10]	ADA Section 307	Americans with Disabilities Act (ADA) Standards for Accessible Design, Section 307 – Protruding Objects
[R11]	NFPA 101	National Fire Protection Association (NFPA), 101: Life Safety Code

No	Standard	Title
[R12]	CBC Section 11B-404.2.3	2019 California Building Code (CBC), Chapter 11B, 11B-404.2.3 – Clear Width (Doorways)
[R13]	NFPA 1225	National Fire Protection Association (NFPA), 1225: Standard for Emergency Services Communications
[R14]	CFC S510	California Fire Code Section 510 – Emergency Responder Radio Coverage in Buildings
[R15]	IEC 60529	International Electrotechnical Commission (IEC), 60529: Degrees of protection provided by enclosures (IP Code)
[R16]	IEC 60068	International Electrotechnical Commission (IEC), 60068: Environmental Testing
[R17]	EN 50164-3	European Norm (EN), 50164-3: Lightning Protection Components (LPC) – Part 3: Requirements for Isolating Spark Gaps
[R18]	IEC 61643	International Electrotechnical Commission (IEC), 61643: Low-voltage surge protective devices
[R19]	IEC 60715	International Electrotechnical Commission (IEC), 60715: Dimensions of Low-Voltage Switchgear and Controlgear – Standard Mounting Rails for Mechanical Support of Electrical Devices
[R20]	EN 62305	European Norm (EN), 62305: Protection Against Lightning
[R21]	NFPA 780	National Fire Protection Association (NFPA), 780: Lightning Protection Standard
[R22]	EN 50121-5	European Norm (EN), 50121-5: Railway Applications – Electromagnetic Compatibility – Part 5: Emission and Immunity of Fixed Power Supply Installations
[R23]	EN 55024	European Norm (EN), 55024: Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement
[R24]	EN 300386	European Norm (EN), 300386: Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunications network equipment; Electromagnetic compatibility requirements
[R25]	EN 50122-1	European Norm (EN), 50122-1: Railway Applications – Fixed Installations – Electrical Safety, Earthing and the Return Circuit – Part 1: Protective Provisions against Electric Shock
[R26]	EN 61000-6-2	European Norm (EN), 61000-6-2: Electromagnetic Compatibility (EMC) – Part 6-2: Generic Standards – Immunity for Industrial Environments
[R27]	EN 61000-6-4	European Norm (EN), 61000-6-4: Electromagnetic Compatibility (EMC) – Part 6-4: Emission Standard for Industrial Environments
[R28]	IEC 61000-3-6	International Electrotechnical Commission (IEC), 61000-3-6: Electromagnetic Compatibility (EMC) – Part 3-6: Limitation of Emission of Harmonic Currents in Medium and High Voltage Power Systems
[R29]	IEC 61000-3-7	International Electrotechnical Commission (IEC), 61000-3-7: Electromagnetic Compatibility (EMC) – Part 3-7: Limits – Assessment of Emission Limits for Fluctuating Loads in MV and HV Power Systems

No	Standard	Title
[R30]	IEC 61000-5-2	International Electrotechnical Commission (IEC), 61000-5-2: Electromagnetic Compatibility (EMC) – Part 5-2: Installation and Mitigation Guidelines – Earthing and Cabling
[R31]	EN 50121-3-2	European Norm (EN), 50121-3-2: Railway Applications – Electromagnetic Compatibility – Part 3-2: Rolling Stock – Apparatus
[R32]	EN 50121-4	European Norm (EN), 50121-4: Railway Applications – Electromagnetic Compatibility – Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus
[R33]	EN 1991-1-4	European Norm (EN), 1991-1-4: Eurocode 1 – Actions on Structures – Part 1-4: General Actions – Wind Actions
[R34]	EN 50126	European Norm (EN), 50126: Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
[R35]	EN 50128	European Norm (EN), 50128: Railway Applications – Communication, Signalling and Processing Systems – Software for Railway Control and Protection Systems
[R36]	EN 50129	European Norm (EN), 50129: Railway Applications – Communication, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling
[R37]	3GPP TS 22.179	3rd Generation Project Partnership (3GPP), Technical Specification 22.179: Service Requirements for the Future Railway Mobile Communication System (FRMCS)
[R38]	ETSI TR 103 459	European Telecommunications Standards Institute (ETSI), Technical Reference: 103 459 "System Reference Document - Future Railway Mobile Communication System (FRMCS)
[R39]	ISO/IEC 27001	International Standards Organization (ISO) / International Electrotechnical Commission (IEC), 27001: Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements
[R40]	NIST SP 800-53	National Institute of Standards and Technology (NIST), Special Publication 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations
[R41]	IEC 62443-2-4	International Electrotechnical Commission (IEC), 62443-2-4: Security for Industrial Automation and Control Systems – Part 2-4: Requirements for IACS Solution Suppliers
[R42]	IEC 62351	International Electrotechnical Commission (IEC), 62351: Power Systems Management and Associated Information Exchange – Data and Communications Security
[R43]	EN 50125-3	European Norm (EN), 50125-3: Railway applications - Environmental conditions for equipment - Part 3: Equipment for signaling and telecommunications
[R44]	eCPRI	eCPRI Specification Group, Enhanced Common Public Radio Interface
[R45]	IEEE 1914.3	Institute of Electrical and Electronics Engineers (IEEE) 1914.3: Standard for Radio over Ethernet (RoE) Encapsulations and Mappings
[R46]	EN 50159	European Norm (EN), 50159: Railway Applications – Communication, Signalling and Processing Systems – Safety-related Communication in Transmission Systems

No	Standard	Title
[R47]	3GPP TS 23.379	3rd Generation Project Partnership (3GPP), Technical Specification 23.379: Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2
[R48]	3GPP TS 23.282	3rd Generation Project Partnership (3GPP), Technical Specification 23.282: Functional architecture and information flows to support Mission Critical Data (MCData)
[R49]	3GPP TS 23.281	3rd Generation Project Partnership (3GPP), Technical Specification 23.281: Functional architecture and information flows to support Mission Critical Video (MCVideo)
[R50]	3GPP TS 23.283	3rd Generation Project Partnership (3GPP), Technical Specification 23.283: Mission Critical Communication Interworking with Land Mobile Radio Systems
[R51]	IEC 61508	International Electrotechnical Commission (IEC), 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
[R52]	IEEE 802.11be	Institute of Electrical and Electronics Engineers (IEEE), 802.11be: Extremely High Throughput (aka "Wi-Fi7")
[R53]	3GPP TS 23.228	3rd Generation Project Partnership (3GPP), Technical Specification 23.228: IP Multimedia Subsystem (IMS); Stage 2
[R54]	3GPP TS 24.302	3rd Generation Project Partnership (3GPP), Technical Specification 24.302: Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3
[R55]	3GPP TS 24.229	3rd Generation Project Partnership (3GPP), Technical Specification 24.229: IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
[R56]	3GPP TS 33.402	3rd Generation Project Partnership (3GPP), Technical Specification 33.402: 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses
[R57]	IETF RFC 6442	Internet Engineering Task Force (IETF), Request for Comments (RFC) 6442: Location Configuration Information for GEOPRIV
[R58]	3GPP TS 23.167	3rd Generation Project Partnership (3GPP), Technical Specification 23.167: IP Multimedia Subsystem (IMS) emergency sessions
[R59]	3GPP TS 23.179	3rd Generation Project Partnership (3GPP), Technical Specification 23.179: Functional architecture and information flows to support mission critical communication services; Stage 2
[R60]	3GPP TS 23.203	3rd Generation Project Partnership (3GPP), Technical Specification 23.203: Policy and charging control architecture
[R61]	3GPP TS 22.280	3rd Generation Project Partnership (3GPP), Technical Specification 22.280: Mission Critical Services Common Requirements (MCCoRe); Stage 1
[R62]	3GPP TR 36.942	3rd Generation Project Partnership (3GPP), Technical Report 36.942: Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (RF) system scenarios
[R63]	ITU-R P.1238	International Telecommunication Union Radiocommunication Standardization Sector (ITU-R) P.1238: Propagation data and prediction methods for the planning of indoor

No	Standard	Title
		radiocommunication systems and radio local area networks in the frequency range 300 MHz to 450 GHz
[R64]	ITU-R P.1812	International Telecommunication Union Radiocommunication Standardization Sector (ITU-R) P.1812: A path-specific propagation prediction method for point-to-area terrestrial services in the frequency range 30 MHz to 6 GHz
[R65]	3GPP TS 28.313	3rd Generation Project Partnership (3GPP), Technical Specification 28.313: Management and orchestration; Self-Organizing Networks (SON) for 5G networks
[R66]	NFPA 70	National Fire Protection Association (NFPA), 70: National Electrical Code
[R67]	47 CFR §1.1307	Title 47 of the Code of Federal Regulations (CFR), §1.1307: Environmental Considerations — Actions that May Have a Significant Environmental Effect, for Which Environmental Assessments (EAs) Must Be Prepared
[R68]	47 CFR §1.1310	Title 47 of the Code of Federal Regulations (CFR), §1.1310: Radiofrequency Radiation Exposure Limits
[R69]	ANSI/IEEE C95.1	American National Standards Institute (ANSI) / Institute of Electrical and Electronics Engineers (IEEE), C95.1: Standard for Safety Levels with Respect to Human Exposure to Electric, Magnetic, and Electromagnetic Fields, 0 Hz to 300 GHz
[R70]	IEC 60297	International Electrotechnical Commission (IEC), 60297: Mechanical structures for electronic equipment – Dimensions of mechanical structures of the 482.6 mm (19 in) series.
[R71]	3GPP TS 23.501	3rd Generation Project Partnership (3GPP), Technical Specification 23.501: System architecture for the 5G System (5GS)
[R72]	3GPP TS 23.503	3rd Generation Project Partnership (3GPP), Technical Specification 23.503: Policy and Charging Control Framework
[R73]	3GPP TS 26.114	3rd Generation Project Partnership (3GPP), Technical Specification 26.114: IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction
[R74]	3GPP TS 26.116	3rd Generation Project Partnership (3GPP), Technical Specification 26.116: Speech and audio coding; Performance characterization of speech and audio codecs
[R75]	EN 50701	European Norm (EN), 50701: Railway applications – Cybersecurity.
[R76]	TIA-102	Telecommunications Industry Association (TIA), 102: Project 25 (P25) Land Mobile Radio Communications
[R77]	IEEE 1588	Institute of Electrical and Electronics Engineers (IEEE), 1588: Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
[R78]	EN 14067-4	European Norm (EN), 14067: Railway applications – Aerodynamics, Part 4: Requirements and test procedures for aerodynamics on open track

TABLE 68 : LIST OF APPLICABLE STANDARDS.

2.5 UIC Specifications

No	Version	Title
[R79]	v2.0.0 (Dec-24)	FRMCS Functional Requirements Specification
[R80]	v2.0.0 (Dec-24)	FRMCS System Requirements Specification
[R81]	v2.0.0 (Dec-24)	FRMCS Telecom On-Board Architecture (TOBA) Functional Requirements Specification
[R82]	v2.0.0 (Dec-24)	FRMCS Functional Interface Specification
[R83]	v2.0.0 (Dec-24)	FRMCS Form-Fit-Functional Interface Specification

TABLE 69 : LIST OF APPLICABLE UIC SPECIFICATIONS.

2.6 Other Documents

2.6.1 The following documents shall be referred to:

No	Document	Title
[R84]	Schedule 16	Scope of Work
[R85]	Schedule 5	Digital Communication Network Technical Specification
[R86]	Schedule 5	Medium Voltage and Low Voltage Power Systems Technical Specification
[R87]	Schedule 5	Network Timing System Technical Specification
[R88]	Schedule 5	Cybersecurity Technical Specification
[R89]	Schedule 5	Telephony System Technical Specification
[R90]	Schedule 5	ETCS Technical Specification
[R91]	Schedule 5	CCTV Technical Specification
[R92]	Schedule 5	Electronic Access and Control System Technical Specification
[R93]	Schedule 5	Integrated Control and Supervision System Technical Specification
[R94]	Schedule 5	Public Address and Customer Information System Technical Specification
[R95]	-	*PPDR Rugged Handheld Device for heavy use v1.0 Whitepaper*, NCCOM
[R96]	Schedule 3	Safety, Security and RAM Requirements
[R97]	PLAN-1022 (Rev00, Apr-25)	Interface Management Plan
[R98]	DD-SY-Set	DD-SY-011 TSCC Sites Typical Configuration
[R99]	COPPA	Children's Online Privacy Protection Act (US Federal Act)

No	Document	Title
[R100]	CCPA	California Consumer Privacy Act
[R101]	CalECPA	California Electronic Communications Privacy Act
[R102]	RoHS Directive	Restriction of Hazardous Substances in Electrical and Electronic Equipment

TABLE 70 : OTHER REFERENCE DOCUMENTS.

3 TERMS AND DEFINITIONS

3.1 General

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

4 SYSTEM DESCRIPTION

4.1 Background

***Note to reader**: This Background section provides contextual information to provide clarity when reading this Specification. While this information is documented elsewhere in the train control and telecommunications specifications, it is important to reiterate these principles the WCS are built upon.*

4.1.1 This Technical Specification (*this Specification*) provides the TSCC Contractor with the required information to design and construct the WCS on infrastructure that forms the CHSR System (*the System)*.

4.1.2 The Authority requires WCS to be capable of supporting mission-critical high-speed rail operations, business-critical operational functions, as well as non-critical services for passenger comfort and connectivity.

Criticality Level	Description	Examples	Failure Consequence
Mission-critical	Essential for safe and continuous train operations	Train control radio, SIL4 signaling, interlocking systems	Cessation of network-wide operations. Major passenger disruptions. Immediate reputational and revenue impact. Requires activation of contingency or recovery plans.
Business-critical	Potentially impacts revenue or customer service	Ticketing, CCTV, Passenger Information System	Delays or degradation in service delivery. Major inconvenience to passengers or staff. Timely resolution is required to prevent reputational and revenue impact.
Non-critical	No impact on safety or operations	Passenger Wi-Fi, Infotainment, Digital advertising displays	Minor inconvenience. No impact on train movement or safety.

TABLE 20 : DESCRIPTION AND EXAMPLES OF CRITICALITY LEVELS.

4.1.3 The Authority shall utilize the European Train Control System (ETCS) Level 2 without signals to provide Movement Authority to trainsets on the CHSR right-of-way.

4.1.4 This ETCS system shall utilize FRMCS to provide voice and data communication between trainsets and wayside equipment.

4.1.5 The Authority shall utilize a dedicated telecommunication systems comprising of an IP-based Digital Communications Network (DCN), fiber optic network, wireless communication systems as well as multiple systems used to provide management, oversight and control of the Authority's infrastructure. The systems will be connected via a fiber optic backbone cabling system along the Right-of-Way interconnecting all wayside systems, stations, facilities and the Operational Control center (OCC).

4.1.6 The CHSR OCC will be located at Fresno.

4.2 Purpose of Wireless Communication Systems

4.2.1 The purpose of the WCS is to provide secure voice, data and video communications in a high-speed rail environment:

4.2.2 To and from the following user groups:

- Engineers, Operators, Drivers;
- Conductors;
- Attendants, Crew, Staff;
- Ticket Inspectors / Revenue Protection Officers;
- Transit Security / California Highway Patrol;
- Controllers, Dispatchers, Managers;

- Cleaning & Service Crew;
- Maintenance & Incident Response Crews;
- Emergency Responders, Emergency Response Coordinator;
- Passengers;
- Any other persons authorized to perform work in the CHSR System;
- Other Californian railroad operators;
- Automated wireless and wireline systems.

4.2.3 At or within the following locations:

- Trainsets;
- Station Complexes;
- Control Centers;
- Wayside Shelters / Cabinets;
- Traction Power Facilities;
- Stabling Yards;
- Maintenance Facilities;
- Right-of-Way;
- Designated Emergency Evacuation Areas;
- Any other area where wireless communications can be reasonably expected.

4.2.4 Between fixed and handheld devices, and to access internet, telephony, and corporate and operational networks.

4.2.5 The Authority reserves the right to include additional user groups and locations that can be reasonably expected to be considered part of the CHSR System or required to integrate and/or interoperate with the CHSR System.

4.3 Definition of Wireless Communication Systems

4.3.1 The WCS shall consist of separate subsystems which provide both common and unique capabilities. The WCS subsystems are:

- Future Radio Mobile Communication System;
- Emergency Responder Communication System;
- Passenger Wi-Fi System.

4.3.2 The TSCC Contractor shall be responsible for all components, systems, interfaces, and activities necessary to fully design, deliver, integrate, test, and operationalize the WCS to the standard required for high-speed rail operations and for CHSR to enter revenue service.

This includes, but is not limited to design, procurement, sourcing, supply, construction, installation, configuration, integration, verification, validation, training, documentation, operations, maintenance and handover of all WCS subsystems, in accordance with the requirements of this and other technical specifications, and subject to acceptance by the Authority.

4.3.3 **Future Radio Mobile Communication System**

4.3.3.1 The Future Radio Mobile Communication System (FRMCS) provides mission-critical voice and data communication between all operational user groups and operational locations across the rail network.

4.3.3.2 The FRMCS ensures that communications essential to the safe and efficient operation of CHSR are maintained under normal, degraded, and emergency conditions, enabling safe train movement, coordination, and response during all possible scenarios, and to mitigate operational disruptions.

4.3.4 **Emergency Responder Communication System**

4.3.4.1 The Emergency Responder Communication System (ERCS) enables OCC personnel to interoperate with Emergency Responders via non-public network communications.

4.3.5 **Passenger Wi-Fi System**

4.3.5.1 The Passenger Wi-Fi System (PWS) is a non-critical subsystem of the WCS that provides a seamless, reliable, secure, high-capacity, and high-speed wireless internet service accessible to passengers via their personal devices.

4.3.5.2 The purpose of the PWS is to allow authorized passengers to access the internet for work and entertainment purposes in a safe and secure manner from personal digital devices with Wi-Fi capabilities during their journey.

4.4 Operational Context

4.4.1 The Wireless Communications Systems (WCS) shall be used operationally by various user groups to support high-speed rail operations, and by passengers during their journey.

4.4.2 The WCS FRMCS shall be able to be utilized from any location within the CHSR System.

4.4.3 All designs shall include provisions for the future expansion of the WCS, beyond the EOS, towards San Francisco, Los Angeles, and Sacramento without substantial re-work and with minimal impact on the operational infrastructure.

4.4.4 The WCS shall be designed and constructed to meet the requirements of the FCS system capacity of 1-2 trains per hour in each direction.

4.4.5 The WCS shall be designed to meet the requirements of the final CHSR service capacity of 12 trains per hour in each direction.

4.4.6 The WCS shall maintain reliable and continuous service performance at train speeds of up to 220mph (354 km/h).

4.4.7 The WCS shall support a diverse set of operational use cases including but not limited to:

- Real-time communication between train crews, station staff and train controllers / dispatchers;
- Emergency response coordination;
- Maintenance coordination;
- Trackside condition monitoring;
- Onboard diagnostics and condition monitoring;
- Passenger entertainment and communication services.

4.4.8 The WCS FRMCS shall provide communication services to mobile users (e.g., train drivers, onboard staff, field maintenance crews), fixed users (e.g., signalers, OCC personnel, security staff), and automated systems. The FRMCS shall ensure consistent coverage, availability, and service quality across the full extent of all the facilities that make up the FCS of the CHSR System (*the System*).

4.4.9 The WCS shall enable seamless interoperability between user groups, and automated systems, supporting the exchange of voice, data, and control signals as required for safe and efficient CHSR operations.

The WCS shall enable the OCC personnel to perform the centralized coordination, supervision, and control of all rail operations across the CHSR System.

4.4.10 To support these functions, the OCC shall utilize WCS Dispatch Consoles, which shall provide authorized personnel with integrated, full featured, real-time access to Mission-Critical, and emergency communications across all WCS subsystems.

4.4.11 The WCS shall support positive CHSR customer satisfaction by enabling the reliable operation of systems that contribute to on-time train performance and functioning passenger facilities. This includes, but is not limited to:

- Providing communication support for systems involved in train control, diagnostics, and fault reporting to minimize service disruptions;
- Ensuring consistent operation of passenger-facing services such as onboard Wi-Fi, information displays, and station connectivity;
- Facilitating timely communication between staff, OCC, and maintenance teams to support proactive issue resolution and service recovery.

4.4.12 The WCS shall enable interoperability between CHSR user groups and third-party user group networks, such as Emergency Responders and other Railroad Operators (e.g., Caltrain, BNSF, Amtrak, LA Metro and Brightline West).

4.4.13 The WCS shall be operated, maintained, and supported in accordance with the operational procedures, rules, and protocols defined by the Authority.

The TSCC Contractor shall ensure that all operational modes, fault management workflows, change control processes, and access protocols for the WCS are fully aligned with the Authority's documented procedures and operational governance framework.

No deviations from these procedures shall be permitted without prior written approval from the Authority.

4.5 Design Life

4.5.1 The Design Life requirements of the WCS shall be 30 years.

4.5.2 The TSCC Contractor shall provide an equipment lifecycle plan demonstrating how all WCS components will be maintained to meet the specified design life.

4.5.3 The TSCC Contractor shall ensure WCS components with shorter design lifespans (e.g., fixed and mobile devices, computing hardware, etc.) shall be managed by scheduled technology refresh strategies and spares management plans.

4.5.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce, supply and support WCS components, or provide replacements with equal or compatible technical specifications, for the entire lifetime required.

5 SYSTEM REQUIREMENTS

5.1 General Requirements

5.1.1 The WCS shall be designed in accordance with the requirements described in this specification, other relevant documents listed in Section 2 of this specification, other CHSR technical specifications and the full CHSR documentation. In the event of any conflict between these documents, the requirements of this specification shall take precedence.

5.1.2 The WCS shall provide secure voice, data and video communication between user groups, locations and network as described in 4.2.1.

WCS Subsystems

5.1.3 The WCS shall comprise multiple subsystems that deliver both shared and subsystem-specific capabilities. These include:

- Future Mobile Radio Communication System (FMRCS);
- Emergency Responder Communication System (ERCS);
- Passenger Wi-Fi System (PWS).

5.1.4 The TSCC Contractor may propose subsystem implementations using separate or combined communication systems, including shared use of wireless technologies (e.g., 4G, 5G, mmWave, Wi-Fi, P25, proprietary) or infrastructure components (e.g., towers, shelters, backhaul, or radio access nodes). The proposal may include alternative delivery or commercial models, such as Public-Private Partnerships or X-as-a-Service, provided all criticality, technical, operational, and compliance requirements are fully satisfied.

5.1.5 Where WCS subsystems are integrated or share infrastructure, the most stringent or mission-critical requirement applicable to any individual subsystem shall govern the combined solution. The TSCC Contractor shall clearly identify shared elements, justify compliance with all relevant subsystem requirements, and demonstrate that no degradation in performance, safety, or reliability will occur.

Note to reader: *The Authority encourages innovative system architectures that minimize physical infrastructure and environmental footprint, provided they maintain the independence, integrity, and availability expected of each WCS subsystem's criticality level.*

Radio Frequency Spectrum

5.1.6 The TSCC Contractor may utilize the Authority's owned 'Upper 700MHz Block A Guard Band' spectrum (757–758 MHz uplink / 787–788 MHz downlink) across the entire geographical area of the Los Angeles to San Francisco CHSR Right-of-Way.

Note to reader: *The Authority acknowledges that this spectrum is not ideally suited to meet the requirements of WCS. The Authority encourages innovative spectrum strategies and active network sharing architectures (e.g., MORAN, MOCN, roaming, MVNO, FirstNet) that minimize the need for exclusive spectrum holdings and reduce overall spectrum use, provided they maintain the independence, integrity, and availability expected of each WCS subsystem in accordance with its criticality level.*

5.1.7 The TSCC Contractor shall be responsible for the identification, acquisition, and ongoing cost of any additional radio frequency spectrum required to satisfy the technical, operational, and regulatory requirements of the WCS subsystems.

5.1.8 All licenses or spectrum usage rights acquired by the TSCC Contractor for the purpose of delivering WCS services shall be transferred or assigned to the Authority upon commissioning, in accordance with applicable regulatory and licensing conditions.

Design, Construct, Operate & Maintain

5.1.9 The design and implementation of the WCS shall incorporate provisions for future expansion to support additional project stages, increased system capacity, and evolving operational requirements. This shall include allowances for physical space, power, network connectivity, core network capacity, software scalability, and licensing. The WCS shall constitute a system that is scalable for future growth and capacity expansion. Software licensing models shall be scalable to accommodate future increases in user numbers, trainset numbers, service frequency, functional modules, and integration with new subsystems, without requiring re-procurement or significant system reconfiguration.

5.1.10 The TSCC Contractor's scope shall include all phases of the WCS including design, source, supply, construct, deploy, install, integrate, test, commission and maintenance to operate a seamless, reliable and secure WCS to support the CHSR System.

Backhaul and Fronthaul

5.1.11 The TSCC Contractor **shall** utilize the optical fiber infrastructure and the associated Digital Communications Network (DCN) for all inter-site connectivity between CHSR locations. Refer to Digital Communications Network Technical Specification.

5.1.12 The use of this existing optic fiber and IP-based DCN shall apply to WCS subsystems requiring backhaul, fronthaul, interconnection, or integration across stations, control centers, equipment shelters, and other designated facilities, unless otherwise approved by the Authority.

5.1.13 The TSCC Contractor shall utilize the existing optical fiber infrastructure where it is possible to provide fronthaul, and where not possible it shall install drop-off (distribution) optic fiber between splice closures and radio transmitters. Splice closures may need to be installed at locations where optic fiber coils have been placed.

5.1.14 Each WCS subsystem backhaul and fronthaul should operate independently but must not interfere with the operation or performance of any other subsystem. Where applicable, shared infrastructure (e.g. antenna systems, cabling) must support multi-service use with defined quality-of-service parameters.

Accessibility

5.1.15 All WCS equipment, enclosures, and associated cabling shall be installed so as not to obstruct pedestrian passageways, emergency egress routes, or required access paths to doors, equipment cabinets, or panels. Equipment shall not protrude into accessible routes in violation of ADA Section 307, and sufficient space shall be maintained to ensure door clearances conform to NFPA 101 (Section 7.2.1.5.3) and CBC Section 11B-404.2.3. All installations shall preserve the clear width and height requirements as defined by NFPA, ADA, and CBC standards for safety and accessibility.

5.1.16 Where additional access roads are required, the TSCC Contractor shall design these access roads to WCS equipment shelters in accordance with the requirements set out in Design Criteria Manual, Chapter 26 Roadways and Site Works. Refer to drawing set DD-SY-Set [R97] for typical site layouts.

Low Voltage Power Supply

5.1.17 All fixed WCS subsystem locations shall be powered by the Low Voltage Power System (LVPS). This requirement applies to all non-trainset and non-OCC WCS infrastructure. Refer to Medium Voltage and Low Voltage Power Supply Technical Specification.

5.1.18 All WCS subsystems installed at the OCC shall be powered from the facility's critical power infrastructure, which shall include uninterruptible power supply (UPS) systems and standby generators, to ensure continuous operation during mains power disruptions. Refer to Medium Voltage and Low Voltage Power Supply Technical Specification.

5.1.19 All WCS core network equipment at the OCC shall use Dual Power Supply Architecture with A-plane and B-plane redundant power supply.

Future Mobile Radio Communication System

5.1.19.1 The Future Mobile Radio Communication System (FRMCS) shall provide mission-critical voice communications primarily between trainset engineers and controllers / dispatchers in the OCC and secondarily be utilized by other operational user groups, as well as mission-critical data communications (e.g., ETCS) between trainset onboard train control equipment and the train control system controlling equipment at the OCC throughout the CHSR System.

5.1.19.2 The FRMCS shall ensure that communications are maintained under normal, degraded, and emergency conditions, enabling safe train movement, coordination, and response during all scenarios.

5.1.19.3 The TSCC Contractor shall design, source, construct, integration test and commissioning, provide training, operate, maintain and warranty all required radio transmission sites to deliver continuous and reliable FRMCS coverage throughout the CHSR System, including stations, tunnels, aerial structures, trenches, at-grade corridors, viaducts and operational facilities, in accordance with the defined coverage and performance requirements.

Note to reader: *The EOS (Merced to Bakersfield) segment does not have any tunnels but does have trenches. It can be assumed that viaducts near residential areas will have noise walls (aka 'sound walls') – The specifics are under development. The contractor must request the latest information from the Authority before starting detailed design. It is the contractor's responsibility to take these items into consideration during radio network planning.*

5.1.19.4 The FRMCS shall be designed for high availability with appropriate redundancy, fault-tolerant components, and self-healing network capabilities to support uninterrupted service delivery, suitable for high-speed rail operations.

5.1.19.5 The TSCC Contractor shall provide a FRMCS compliance report to the Authority that details compliance against Mandatory and Optional requirements from the current version of UIC FRMCS specifications, as per Section 2.5.

5.1.19.6 The TSCC Contractor shall ensure that all components of the FRMCS are upgraded to achieve full compliance with the finalized FRMCS standards within five (5) years of their formal ratification and publication by the UIC and associated 3GPP specifications. The TSCC Contractor shall monitor the development of the FRMCS standards and submit a compliance report, including compliance roadmap, for approval by the Authority within twelve (12) months of FRMCS standards ratification.

5.1.19.7 The TSCC Contractor shall design and supply an FRMCS that is fully software upgradable, such that no hardware replacement will be required to achieve full compliance with the finalized FRMCS standards once they are formally ratified.

5.1.19.8 The TSCC Contractor shall provide a FRMCS that consists of 5G Radio Access Network (RAN), geographically redundant 5G Standalone / FRMCS / MCX Core Network, Inter-Working Function (IWF), Dispatch Consoles, Compact Dispatch Consoles, handheld devices, Network Management System (NMS), NMS workstations, integration with other systems, all required software and licensing.

5.1.19.9 The FRMCS 5G RAN shall include all components required for operational FRMCS service, including but not limited to, such as:

- Equipment shelters, cabinets, and sun shelters for housing RAN infrastructure;
- Equipment accommodation support services such as internal power distribution, climate control, fire protection, lighting, electronic access and physical security provisions;
- Conduit extensions to the accommodation from existing pits, manholes, duct banks, and towers to support fiber, power, and RF cabling;
- Optic fiber extensions, hauling and splicing, to provide backhaul and fronthaul;
- Towers, foundations, cableways, antenna platform, earthing, bonding, antennas, feeders, jumpers, and associated cabling for the deployment of the FRMCS radio equipment;
- All required FRMCS RF equipment, transmission equipment (e.g., switches, routers, multiplexers), and telepower systems including rectifiers, batteries, DC distribution, alarming and power monitoring components;
- Supporting infrastructure like racking and cableways for other TSCC systems required (e.g., FPS, CCTV, EACS, DCN, LVPS, NTS).

5.1.19.10 The FRMCS 5G RAN base stations shall be connected to a 5G Standalone (SA) Core Network infrastructure, which includes all core network functions and IP Multimedia Subsystem, to enable full support for FRMCS-compliant mission-critical features and performance capabilities, as defined by 3GPP and UIC specifications (refer to section 2.5).

5.1.19.11 The FRMCS 5G Standalone (SA) Core Network architecture shall utilize a cloud-native, containerized, and orchestrated Service-Based Architecture, supporting Network Function Virtualization (NFV) principles. The architecture shall support all 5G Core Network Functions and their interactions, including authentication, security, session and mobility management, and service provisioning, in accordance with 3GPP specifications. This architecture will ensure the FRMCS core network is scalable, resilient, portable, and automatable.

5.1.19.12 The FRMCS core infrastructure shall comprise a primary and a secondary 5G Core Network, including FRMCS core network elements, each located at geographically separate sites to provide fault tolerance and service continuity. The system design shall ensure seamless, uninterrupted FRMCS service in the event of a failure or outage at either core location, with no loss of service, session drops, or degradation during automatic core switching. The primary and secondary 5G Core Networks shall be interconnected via standardized 3GPP interfaces.

5.1.19.13 The FRMCS shall be designed with no single point of failure and shall implement an active-active redundancy architecture. All critical network elements - including core functions, transport, and access

components - shall operate in parallel and independent instances capable of load sharing and seamless failover.

5.1.19.14 The FRMCS primary core infrastructure shall be located within the communications room of the OCC.

5.1.19.15 The FRMCS secondary core infrastructure shall be located at a California State Government data center, as approved, or otherwise agreed, by the Authority.

5.1.19.16 The FRMCS may utilize passive and active network sharing arrangements with Mobile Network Operators (Cellular Carriers), including neutral host, MOCN, and MORAN infrastructure sharing.

Note to reader: *The Authority welcomes innovative solutions that leverage existing infrastructure and alternate commercial delivery models (e.g., Public Private Partnerships, X-as-a-Service), while meeting their business requirements for a high availability train control system that is suitable for high-speed rail operations.*

5.1.19.17 The Trainset contractor shall be responsible for the sourcing of trainset radios, but the TSCC Contractor will provide all required information and be jointly responsible for system performance. Refer to Section 6.3 External Interfaces - Trainsets for details of interface and demarcation of responsibilities.

Fixed and Mobile Devices

5.1.19.18 The TSCC Contractor shall provide a range of FRMCS compatible fixed and mobile handheld device options suitable to the operational requirements of the CHSR operational user groups.

5.1.19.19 The TSCC Contractor shall provide FRMCS handheld devices that “PPDR Rugged Handheld Device for heavy use v1.0” NCCOM whitepaper.

5.1.19.20 The TSCC Contractor shall draft and submit a fixed and mobile device catalogue that outlines which devices and accessories are designated for which user groups and user roles for the Authority’s approval. The TSCC Contractor shall provide a ‘demonstration day’ where all catalogue items are able to be tested to assist the Authority to determine which items are best fit for operations.

5.1.19.21 The TSCC Contractor shall provide FRMCS ruggedized handheld devices, with accessories, belt holders, remote speaker microphones, multi-bay chargers, single chargers, spare batteries, etc.

5.1.19.22 The TSCC Contractor shall provide a sample of each type of FRMCS device and accessories to the Authority for testing and approval.

5.1.19.23 The Authority reserves the right to initiate a fixed and mobile device ‘true-up’ process to reconcile proposed device models, configurations, and quantities with evolving operational requirements. This may include substituting device types, adjusting order volumes, or rebalancing allocations between fixed and mobile devices. The TSCC Contractor shall accommodate such changes without delay and shall update pricing, delivery schedules, and inventory records accordingly. Any financial adjustments resulting from the true-up shall be reflected in the subsequent invoicing cycle, subject to mutual agreement.

5.1.19.24 While in-trainset (inside trainset) handheld FRMCS coverage from terrestrial radio sites is excluded from the scope, the business requirement for wireless handheld voice communication between the train driver and onboard crew remains. The TSCC Contractor shall propose and implement a suitable solution to meet this requirement, subject to approval by the Authority (e.g., Wi-Fi, repeater, direct radio-to-radio simplex, etc.).

Network Planning

5.1.19.25 The TSCC Contractor shall perform FRMCS radio network planning, including propagation modelling and candidate site evaluation, to determine optimal locations for radio sites along the CHSR Right-of-Way.

5.1.19.26 As part of the radio network planning exercise, the TSCC Contractor shall include ETCS RBC boundary limit analysis. The TSCC Contractor shall demonstrate how the radio site locations have

been selected to avoid FRMCS radio handover in the ETCS RBC/RBC boundary areas along the CHSR Right-of-Way.

5.1.19.27 The TSCC Contractor's design shall detail the site evaluation and selection process used to determine optimal locations for radio sites.

5.1.19.28 FRMCS radio sites shall be located within the CHSR Right-of-Way by default but can be within the CHSR System.

Note to Reader: *Radio site locations shall be prioritized, with stations being the first preference, then signaling equipment rooms, Traction Power locations, BBU Hotel locations, before/after viaducts/trenches, etc. It is intended that radio sites be placed at the end of station platforms, but there may be instances where other locations could be considered (e.g., car parks).*

5.1.19.29 The final number, location, and configuration of FRMCS radio sites shall be determined through the TSCC Contractor's detailed radio propagation study. This study shall account for local topography, land use, coverage, and factors like accessibility, power and backhaul, structural suitability, safety and compliance, environmental factors, security, hazards, co-location and interference, future expandability, and total cost of ownership.

5.1.19.30 The TSCC Contractor shall draft and submit FRMCS Concept Design and Coverage Study to the Authority for review and approval prior to detailed design and deployment. The Coverage Design shall demonstrate how the operational and performance requirements are met.

Note to reader: *The network design should demonstrate the CHSR operational and performance requirements can be met by the FRMCS network designs. E.g., Appropriate network architecture for the railway traffic control communication and ETCS needs along the track.*

5.1.20 **Dispatch Consoles**

5.1.20.1 The WCS Dispatch Consoles shall support the operational needs of OCC personnel, managers, supervisors, dispatchers and train controllers responsible for the safe and efficient management of train operations, and coordination and control of train movements across the CHSR System.

5.1.20.2 The WCS shall support, and the TSCC Contractor shall provide, two types of dispatch consoles to meet the differing operational needs across the rail network:

- Dispatch Console: The Dispatch Console shall be a full-feature, fixed-location dispatch console intended for use within the OCC. It shall support the complete range of WCS functionality, including voice group management, priority call handling, call recording, incident coordination, and integration with other operational systems.
- Compact Dispatch Console (CDC): The CDC shall be a lightweight, cost-effective, and portable console designed for use by field personnel or secondary user groups such as maintenance teams, emergency coordinators, or station supervisors. It shall provide essential dispatch functionality with support for FRMCS connectivity, group voice communication, user presence/status monitoring, and basic call management. The CDC may be implemented as a tablet-based or compact form-factor solution with a simplified user interface suitable for mobile and semi-fixed deployment in non-OCC facilities.

5.1.20.3 The WCS Dispatch Consoles and Compact Dispatch Console shall be COTS hardware and shall have touch-screen operation. WCS Dispatch Console workstation layout, including hardware and accessories, will be codeveloped with the Authority to meet the OCC operational requirements.

5.1.20.4 The WCS Dispatch Consoles shall be integrated directly into the FRMCS core network and can be considered FRMCS Dispatch Consoles, and part of the FRMCS system for the purposes of this Specification. The two terms may be used interchangeably within this Specification.

5.1.20.5 The WCS Compact Dispatch Consoles shall either wirelessly connect to the FRMCS or Wi-Fi via VPN, or hardwired via the DCN. The Compact Dispatch Console will have the same operational, functional and performance requirements as FRMCS mobile devices and thus can be considered as FRMCS mobile devices for the purposes of this specification.

5.1.20.6 The WCS Dispatch Consoles should be implemented as 'Universal Consoles' that provide the required OCC workstation services and capabilities of all the train control and telecommunications sub-systems from one workstation, specifically the Integrated Control and Supervision System (ICSS) workstation/console. The intent is to minimize physical hardware and desk space requirements by consolidating functionality into shared, integrated workstations. There is no requirement for WCS Dispatch Consoles to be deployed on dedicated or physically separate hardware from other systems, provided operational performance, security, and availability requirements are maintained.

5.1.20.7 The TSCC Contractor shall provide Dispatch Consoles with accessories and all required hardware and software to function as per requirements.

5.1.20.8 The TSCC Contractor shall provide Compact Dispatch Consoles with accessories and all required hardware and software to function as per requirements.

5.1.20.9 The WCS Dispatch Console functions shall align with the defined roles and responsibilities of OCC personnel as documented in the Authority's operational procedures and manuals, and be compliant with the Controller Equipment requirements of the UIC FRMCS specifications (refer to section 2.5).

5.1.20.10 The TSCC Contractor shall design, source, provide, install, test, commission, operate, and maintain WCS Dispatch Consoles that enable OCC personnel to initiate and manage voice and data communications in accordance with their operational roles and system integration requirements.

5.1.20.11 The TSCC Contractor shall engage in a co-design process with the Authority's OCC personnel to ensure that the WCS Dispatch Consoles meet operational workflows, Human Factors principles, and ergonomic best practices. The TSCC Contractor shall incorporate user feedback throughout the design lifecycle and shall provide early and ongoing access to functional console environments to support user training, familiarization, and operational readiness.

5.1.21 **Emergency Responder Communication System**

5.1.21.1 The Emergency Responder Communications System (ERCS) is exempt from the duplicate core infrastructure requirement.

5.1.21.2 The ERCS shall enable secure, direct, and interoperable communication between OCC personnel and Emergency Responders using non-public networks, such as P25 and FirstNet.

5.1.21.3 The ERCS shall be integrated into the WCS Dispatch Consoles to allow OCC personnel to communicate with Emergency Responders and Dispatchers.

5.1.21.4 The ERCS shall include all equipment required to interconnect the WCS with external Emergency Responder radio communication networks like P25 and FirstNet.

5.1.21.5 The ERCS shall be designed in compliance with applicable public safety communications codes, including:

- NFPA 1225 – Standard for Emergency Services Communications;
- California Fire Code Section 510 – Emergency Responder Radio Coverage in Buildings;
- Any additional requirements mandated by the Authority Having Jurisdiction (AHJ).

5.1.22 **Passenger Wi-Fi System**

5.1.22.1 The PWS shall provide a non-critical seamless, reliable, secure, high-capacity and high-speed Wi-Fi service that is easily accessible to passengers via their personal devices throughout their train journey.

5.1.22.2 The PWS shall utilize mmWave (60GHz unlicensed band) Trainset-to-Trackside (mmWave TtT) architecture to provide the highest possible bandwidth and data rates, and to align with similar solutions provided by other comparable Railroad Operators (e.g., Caltrain).

5.1.22.3 The TSCC Contractor shall design, construct, commission, operate and maintain all required radio transmission sites to deliver continuous and reliable PWS mmWave Trainset-to-Trackside (mmWave TtT) coverage throughout the CHSR Right-of-Way, including tunnels, aerial structures, trenches, at-grade corridors, viaducts where passenger in-revenue services traverse, in accordance with the defined coverage and performance requirements.

5.1.22.4 PWS mmWave transmitters shall be installed on Overhead Contact System (OCS) masts. No requirement for dedicated PWS radio towers.

5.1.22.5 The PWS mmWave TtT transmitters shall be parented back to dedicated PWS edge switches, prior to interfacing with DCN, at FRMCS BBU Hotel locations via fronthaul optic fiber.

5.1.22.6 The PWS shall be designed to minimize the required number of optic fibers required to interconnect mmWave TtT transmitters.

5.1.22.7 The PWS core infrastructure shall be located within the communications room of the OCC.

Network Planning

5.1.22.8 The TSCC Contractor shall perform PWS radio network planning, including propagation modelling and site evaluation, to determine optimal locations for PWS transmitters along the CHSR Right-of-Way.

5.1.22.9 The final number, location, and configuration of PWS mmWave TtT transmitters shall be determined through the TSCC Contractor's detailed radio propagation study. This study shall account for local topography, land use, coverage, and factors like accessibility, power and backhaul, structural suitability, safety and compliance, environmental factors, security, hazards, co-location and interference, future expandability, and total cost of ownership.

5.1.22.10 The TSCC Contractor shall perform PWS in-train Wi-Fi coverage planning, including propagation modelling and antenna location evaluation, to determine optimal locations for PWS antennas within trainsets to ensure highest levels of Wi-Fi coverage are available to passengers.

5.1.22.11 The TSCC Contractor shall submit PWS Concept Design and Coverage Study, both TtT transmitters and in-train Wi-Fi, to the Authority for review and approval prior to detailed design and deployment. The Coverage Design shall demonstrate the operational and performance requirements are met.

5.2 Environmental Requirements

5.2.1 The WCS shall be designed in accordance with the Design Criteria Manual, Chapter 2: Basis of Design, section 2.2.10 Environmental, and Chapter 35: Environmental.

5.2.2 The WCS shall be designed in accordance with the requirements described in EN50125-3 Railway applications - Environmental Conditions for Equipment - Part 3: Equipment for Signaling and Telecommunications, Section 4: Environmental Conditions.

5.2.3 The WCS shall be designed in accordance with the Design Criteria Manual, Chapter 7: Electromagnetic Compatibility, section 7.1.2 Regulations, Codes, Standards, and Guidelines.

5.2.4 The WCS design should minimize the environmental impact of the WCS and of the entire CHSR operations during O&M phase.

5.2.5 All WCS designs for equipment in the Right-of-Way shall be suitable for electrified territory operations with appropriate mitigations in place to negate the possible safety and WCS performance risks.

5.2.6 The WCS equipment shall be designed and constructed to withstand the environmental conditions applicable to its installed location for the WCS design life. The level of protection shall comply with the

following Location Specific Requirements. The design shall demonstrate suitability of the selected equipment location categories.

5.2.7 The TSCC Contractor shall ensure that all electrical and electronic equipment supplied and installed complies with the requirements of the RoHS Directive (2011/65/EU as amended by 2015/863/EU) on the Restriction of Hazardous Substances in Electrical and Electronic Equipment [R101]. The TSCC Contractor shall retain records demonstrating RoHS compliance for all applicable equipment and components and make them available for inspection upon request.

Location Specific Requirements

5.2.8 WCS equipment locations shall be defined as:

- Indoor: A fully enclosed, climate-controlled environment protected from external weather conditions. Examples include control rooms, equipment rooms, trackside equipment shelters and occupied buildings.
- Outdoor Sheltered: A non-climate-controlled environment that provides partial protection from direct exposure to weather. Examples include covered platforms, tunnels, and ventilated enclosures.
- Outdoor Fully Exposed: An environment with no protection from external elements, subject to full weather exposure. Examples include trackside areas, open rooftops, and freestanding equipment.

5.2.9 The Indoor WCS equipment shall be compliant with the following environmental requirements:

- Data Center equipment Ingress Protection: IP 30 minimum (IEC 60529 [R14]);
- Temperature range: 0 to 40 °C (IEEE 60068-2-1 [R15]);
- Relative Humidity: 5%-95% Non-Condensing (IEEE 60068-2-30/78 [R15]);

5.2.10 The Outdoor Sheltered WCS equipment shall be compliant with the following environmental requirements:

- Ingress Protection: IP 54 minimum (IEC 60529 [R14]);
- Temperature Range: -20 °C to +50 °C (without direct solar load);
- Relative Humidity: 5%-95% Non-Condensing (IEEE 60068-2-30/78 [R15]);
- Wind Load: Sustained wind speed: 20 m/s; gusts: 30 m/s;
- Rain Exposure: Drip and splash protection only (equipment must not be directly exposed to rainfall);
- Seismic Considerations: Equipment and mounting structures shall meet applicable seismic anchorage and structural requirements of the California Building Code (CBC);
- Vibration & Shocks: IEC 60068-2-27 (Shocks), IEC 60068-2-6 (Vibration) [R15];

5.2.11 The Outdoor Fully Exposed WCS equipment shall be compliant with the following environmental requirements:

- Ingress Protection: IP 67 minimum (IEC 60529 [R14]);
- Temperature Range: -35 °C to +50 °C (without solar load; must tolerate California desert extremes), to +70 °C (with solar load);
- Relative Humidity: 5%-95% Non-Condensing (IEEE 60068-2-30/78 [R15]);
- Wind Load: Sustained wind: 24 m/s (approx. 54 mph); gusts: 40 m/s (approx. 89 mph) per CBC wind loading provisions;
- Rain Intensity: Minimum 50 mm/hour (per Caltrans design storm assumptions);
- Ice and Sleet: 12.5 mm (for northern and mountainous California regions);
- Seismic Considerations: Equipment and mounting structures shall meet applicable seismic anchorage and structural requirements of the California Building Code (CBC);
- Vibration & Shocks: IEC 60068-2-27 (Shocks), IEC 60068-2-6 (Vibration);
-

5.2.12 All WCS equipment locations shall be compliant with:

- Lightning Protection: EN 50164-3, IEC 61643, EN 60715, EN 62305, NFPA 780 (installed in accordance with the California Fire Code and local AHJ requirements);
- EMC: EN 50121-5, EN 55024, EN 300386, EN 50122-1, EN 61000-6-2, EN 61000-6-4, IEC 61000-3-6, IEC 61000-3-7, IEC 61000-5-2, EN 50121-3-2, EN 50121-4.

5.2.13 All Outdoor Fully Exposed WCS equipment cabinets that are exposed to direct sunlight shall be fitted with sun shelters or protective overhead covers designed to shield the cabinets from direct solar radiation. The sun shelter shall be engineered to reduce the impact of solar heat gain and assist in maintaining internal cabinet temperatures within the equipment's specified operating range.

Sun shelters shall:

- Extend beyond all sides of the cabinet by a minimum of 300 mm;
- Be constructed from UV-resistant, non-combustible, and weather-resistant materials;
- Be structurally rated for local environmental conditions including:
  - Sustained wind speeds up to 24 m/s and gusts up to 40 m/s (per general design standards);
  - Aerodynamic pressure and suction forces generated by passing high-speed trains operating at speeds up to 220mph (354 km/h), including transient crosswinds and turbulence;
  - Train-induced pressure loads of at least 1.5 kPa, based on dynamic pressure from high-speed train passage in close proximity, consistent with railway aerodynamic standards such as EN 14067-4 or equivalent;
  - Comply with applicable wind load factors for railway proximity as specified in the California Building Code (CBC) and relevant railway design standards (e.g. EN 1991-1-4 where applicable);
- Not obstruct ventilation, access, or maintenance activities;
- Be integrated into the overall equipment grounding, bonding and lightning protection scheme, where applicable;
- Be designed and constructed to achieve a design life of 30 years with appropriate corrosion and UV resistance, subject to appropriate maintenance.

5.3 Operational Requirements

5.3.1 The TSCC Contractor shall be responsible for the configuration, management, provisioning, maintenance and planning of all operational aspects of the WCS, including but not limited to coverage, capacity, performance, periodic reporting, user roles, prioritization and communication talkgroup matrix (Fleetmap) structures. All proposed configurations shall be documented and submitted to the Authority for review and approval prior to implementation.

5.3.2 **Future Mobile Radio Communication System**

5.3.2.1 The FRMCS shall function as the communications system of last resort for safety-related and time-critical operational communications. In the event of a partial or complete failure of other communications subsystems, the FRMCS shall remain operational and capable of supporting essential voice and data communication between train drivers and OCC personnel, and other user groups such as maintenance personnel. The FRMCS shall support the coordination of activities required to restore degraded or failed systems, ensuring safe and continuous CHSR operations under abnormal or emergency conditions.

Note to reader: *The FRMCS voice communications will be required by crews to restore other failed systems and/or rescue passengers during an outage. Hence, the FRMCS system needs to be operational during all possible outage scenarios.*

5.3.2.2 The FRMCS shall allow all train drivers and the OCC to maintain communications while the trainset is in operation throughout the complete CHSR Right-of-Way, including stabling yards and maintenance facilities.

5.3.2.3 The FRMCS shall allow all CHSR operational personnel to communicate from all locations throughout the full CHSR System, including indoor locations where coverage is not meeting performance criteria and enhancement is required. Preference will be given to terrestrial FRMCS radio sites to address inbuilding coverage where possible.

5.3.2.4 In indoor areas where outdoor radio coverage does not meet the required performance levels for the FRMCS, the TSCC Contractor shall provide dedicated indoor radio coverage solutions. Indoor coverage shall be delivered using appropriate technologies such as Distributed Antenna Systems (DAS), small cells, or other solutions suitable for the specific building type, usage, and radio environment. The indoor coverage design shall ensure seamless connectivity and service continuity for CHSR operational personnel in accordance with the overall system performance requirements.

5.3.2.5 The FRMCS shall incorporate sufficient redundancy, independence, and coverage to remain operational during communications outages, including support for maintenance teams accessing infrastructure or trainsets during fault rectification and service recovery.

5.3.2.6 The FRMCS shall support the operation of ETCS Level 2, including integration with safety-critical functions rated to SIL 4 in accordance with relevant CENELEC standards (EN 50126, EN 50128, and EN 50129). The implementation shall comply with the applicable requirements of the European Union Agency for Railways Control Command and Signaling TSI (CCS TSI), particularly those relating to the interoperability of FRMCS and ETCS systems. Refer to ETCS Technical Specification.

5.3.2.7 The FRMCS shall maintain continuous service availability in the event of hardware, software, link or power failure, consistent with high-availability targets suitable to support SIL 4 compliant systems.

5.3.2.8 The FRMCS design shall support operational functionality in accordance with the service requirements specified in 3GPP TS 22.179 “Service Requirements for the Future Railway Mobile Communication System (FRMCS)” and ETSI TR 103 459 “System Reference Document - Future Railway Mobile Communication System (FRMCS)”. The design shall ensure that all operational communications align with the functional and performance expectations outlined in these specifications.

5.3.2.9 The FRMCS shall enable OCC personnel and authorized operational staff to transmit operational data and service updates to trainset systems including, but not limited to, the Public Address and Customer Information System (PACIS), and train crew devices and terminals. This capability shall support:

- Real-time service announcements (e.g. delays, disruptions, platform changes);
- Scheduled or dynamic passenger information updates (e.g. next stop, arrival times, transfer connections);
- Remote coordination with train crew and conductors for service instructions and incident management.

5.3.2.10 Refer to Public Address and Customer Information System Technical Specification for further details.

5.3.2.11 The FRMCS shall support continuous voice talkgroup communication between Train Drivers and Train Dispatchers as trainsets cross Dispatch Area boundaries. Dispatch Area’s are also known as Target Areas or Areas of Responsibility.

5.3.2.12 The FRMCS shall ensure that trainset voice talkgroup communication with the correct Train Dispatcher is maintained, based upon location, without requiring driver intervention during transitions between Dispatch Areas.

5.3.2.13 The FRMCS shall dynamically reassign talkgroups as trainsets cross Dispatch Area boundaries based upon requests from other TSCC subsystems, such as the Traffic Management System.

5.3.2.14 The FRMCS shall enable authorized operational user groups to access core system functionality, such as Asset Management Systems (AMS) and corporate information, through mobile applications or web-based interfaces on FRMCS devices. This capability will provide efficiencies for mobile user groups.

E.g., Train crew and station personnel could have tablets with range of applications to support their operational duties.

5.3.2.15 The TSCC Contractor shall develop a comprehensive fleetmapping plan (configuration and talkgroup matrix) to define the logical organization of users and communication groups within the WCS that meets the Authority's operating requirements. The fleetmap shall address user role definitions, talkgroup structures, call priority levels, communication access rules, and device provisioning requirements. The plan shall support operational scenarios and role-based communications and shall be submitted to the Authority for review and approval prior to implementation.

5.3.2.16 The FRMCS should include a Test Network that duplicates all elements of the FRMCS production network that can be utilized for pre-deployment testing of proposed software, hardware and configuration changes prior to implementation on the FRMCS production network.

5.3.2.17 The FRMCS shall support all the required WCS Dispatching Consoles functionality.

5.3.3 **Dispatch Consoles**

5.3.3.1 The WCS Dispatch Consoles shall allow OCC train controllers / dispatchers to interoperate with other Railroad Operator train controllers / dispatchers for the purposes of traffic coordination and emergency scenarios (e.g., Caltrain, BNSF, Amtrak, LA Metro and Brightline West).

5.3.3.2 The WCS Dispatch Consoles shall allow OCC personnel to coordinate mission-critical and emergency communications with all relevant CHSR user groups, including train drivers, train crew, maintenance crews, station staff, and emergency responders.

5.3.3.3 OCC personnel shall be able to automatically configure all WCS Dispatch Consoles based on a preconfigured user profiles and dispatcher 'areas of responsibility' activated in TMS (as well automatically adjust the Location Dependent Addressing area in the Dispatch Console according to the changed dispatcher are of responsibility in TMS).

5.3.3.4 The WCS Dispatch Consoles shall remain fully operational under normal, degraded, and emergency conditions, with automatic failover to redundant paths, dual UPS power and standby generating plant mains power in the event of any primary system failure.

5.3.3.5 For the purposes of OCC business continuity - In the event of degraded operating scenarios, WCS Dispatch Consoles shall retain operational capability by being able to connect into the core network over the internet via a secure Virtual Private Network (VPN).

5.3.3.6 The FRMCS Test Network should replicate the WCS Dispatch Console capabilities to provide training functions for OCC dispatchers and train controllers.

5.3.4 **Emergency Responder Communication System**

5.3.4.1 The ERCS shall remain operational under normal, degraded, and emergency operating conditions, including infrastructure power loss, partial communications failures, or disaster scenarios.

5.3.4.2 The ERCS shall allow OCC personnel to initiate and maintain voice and data communications with public safety agencies during emergency incidents.

5.3.4.3 The ERCS shall allow OCC personnel to interconnect (aka 'patch' or 'bridge') ERCS and FRMCS talkgroups calls, to facilitate emergency responder communications with any FRMCS end user.

5.3.4.4 The ERCS shall support integration into the incident command structure managed by the Authority Having Jurisdiction (AHJ) during response efforts.

5.3.4.5 The ERCS shall allow OCC operators to monitor, communicate, and exchange information with multiple responder units simultaneously. The ERCS shall interoperate with:

- Emergency Responder Control Centers;
- Portable responder radios;
- Mobile units;
- Incident command vehicles;

- Regional PSAPs;
- Inter-agency gateways and mutual aid radio systems.

5.3.5 **Passenger Wi-Fi System**

5.3.5.1 The Passenger Wi-Fi System (PWS) shall provide continuous coverage and consistent passenger user experience inside trainsets while stationary and in motion, including tunnels, cuttings and trenches.

5.3.5.2 The PWS shall allow passengers to maintain digital connectivity to the internet via their personal devices throughout their train journey from within the trainsets.

5.4 Functional Requirements

Network Timing Synchronization

5.4.1 The WCS shall utilize the Network Timing Systems to provide accurate and consistent time synchronization across all WCS fixed and onboard subsystems. Refer to Network Timing System Technical Specification for further details.

Network Monitoring System

5.4.2 The TSCC Contractor shall deliver a Network Management System (NMS) that provides a centralized, secure, and standards-aligned network monitoring and management system, including OCC workstations, for all WCS subsystems, including the FRMCS, ERCS, PWS and WCS Dispatch Consoles, excluding Compact Dispatch Consoles.

5.4.3 This NMS shall provide the following features:

- Network element access – The NMS shall provide connectivity to all core network elements and RAN elements in the WCS;
- User management – The NMS shall control user access and distinguish user roles;
- Alarm management – The NMS shall enable users to configure, capture, log and report alarms through a centralized user interface;
- Performance management – The NMS shall enable users to view real-time, periodic, and historical data of network element performance for troubleshooting and optimization, including field-based analysis tools or probes;
- Configuration management – The NMS shall enable users to automatically manage system backup configurations, track configuration changes to network elements, and enable mass updates of configuration settings;
- License management – The NMS shall enable users to update operating licenses that govern core and field network elements;
- Inventory management – The NMS shall enable users to explicitly know and understand each element of the WCS to track individual components and parts, including software and firmware identification;
- Storage capability – The NMS shall capture the configuration and performance data with adequate storage for backup configuration checks;
- Provisioning – The NMS shall enable users to commission, upgrade, or decommission network elements;
- Service provisioning – The NMS shall support service provisioning workflows, including the configuration of subscriber profiles, QoS policies, network slice assignments, and policy rules by interfacing with 5GC functions such as UDM, PCF, SMF, and NSSF;
- SIM/eSIM provisioning – The NMS shall interface with the operator's or Authority's SIM provisioning platform to enable the secure download, activation, and lifecycle management of eSIM profiles in accordance with GSMA Remote SIM Provisioning architecture (e.g., SM-DP+, SM-SR);
- Cybersecurity – The NMS shall include robust cyber security measures that meet the recommendations of the Cybersecurity Technical Specification.

5.4.4 To manage all these different elements, the NMS will provide a Graphical User Interface (GUI) with three independent windows: a network topology status and health map, a performance dashboard and an alarm dashboard.

5.4.5 The NMS shall provide a real-time network statistics dashboard that presents key operational and performance indicators across all WCS subsystems, including but not limited to core network elements, RAN nodes, transmission systems, and service endpoints. The dashboard shall support customizable views and user-defined thresholds to highlight system health, alarms, and usage patterns.

5.4.6 The NMS shall support both automated and ad hoc reporting capabilities, including:

- Real-time metrics such as traffic volume, session status, user load, latency, jitter, packet loss, and resource utilization;
- Periodic performance reports (e.g., hourly, daily, weekly, monthly) with trend analysis, peak usage statistics, and Service Level Agreement compliance indicators;
- Usage reports per subsystem, network slice, user category, radio site or location;
- Export of reports in common formats such as PDF, CSV, and XML for integration with external systems.

5.4.7 The TSCC Contractor shall ensure that reports and dashboards are accessible via a secure web-based interface, support role-based access controls, and retain historical data in accordance with the Authority's data retention policy.

5.4.8 The NMS shall support secure remote interrogation capabilities to enable authorized support personnel, including escalated third-level or vendor support teams, to access diagnostic tools and system telemetry for fault isolation and performance analysis.

Remote access shall be provided exclusively via a secured Virtual Private Network (VPN) connection that meets the Authority's cybersecurity requirements, as per Cybersecurity Technical Specification. All remote sessions shall enforce multi-factor authentication (MFA/2FA).

5.4.9 The NMS shall ensure that:

- Remote interrogation access is restricted to defined user roles and scoped permissions;
- All access attempts, successful logins, commands executed, and session durations are logged and auditable;
- Remote access can be revoked in real-time by the Authority if required;
- All remote data exchanges are end-to-end encrypted and comply with relevant cybersecurity standards (e.g., ISO/IEC 27001, NIST 800-53, or local equivalents).

5.4.10 The NMS alarm, performance and status monitoring capabilities shall be integrated into the Integrated Control and Supervision System (ICSS). The ICSS performs the 'manager of managers' function, so only high level and high priority information is required to be passed between subsystems. The ICSS can obtain data directly from the WCS subsystems, rather than via the NMS if this is more practical.

5.4.11 **Performance Reporting**

5.4.12 The TSCC Contractor shall deliver monthly WCS subsystem performance and maintenance reports, aligned with system assurance and cybersecurity standards. Reports shall include:

- Usage statistics, including:
  - Passenger Wi-Fi sessions service use;
  - Operational subsystem traffic volumes (e.g. FRMCS & Dispatch Console voice/data loads);
- Performance metrics, including:
  - Throughput, latency, jitter, packet loss, and session duration;
  - Radio coverage gaps and signal strength trends;

- Availability and reliability reporting aligned with RAMS metrics from EN 50126 / EN 50129, including Mean Time Between Failures (MTBF) and incident frequency;
- Service Level Agreement (SLA) and Key Performance Indicators (KPIs) tracking, including compliance summaries and trend analysis;
- Security and access audit summaries, as required under IEC 62443-2-4 and IEC 62351, including:
  - Configuration changes;
  - Intrusion detection alerts;
  - Access violations;
- Documentation of:
  - Preventive maintenance activities and results;
  - Firmware/software patch deployments;
  - Hardware lifecycle events (e.g. replacements, EOL notices).

5.4.13 **Equipment Racking**

5.4.14 Where required, the TSCC Contractor shall provide equipment racks to house all WCS equipment in accordance with applicable standards. Equipment racks shall comply with IEC 60297 for mechanical dimensions and mounting, and shall be suitable for the environmental conditions defined in EN 50125-3 where applicable (e.g. trackside shelters, equipment rooms).

5.4.15 Each rack shall be supported by a dedicated power circuit, with circuit breakers installed in a clearly labeled and readily accessible local distribution panel within the same equipment room or enclosure. All power cabling shall be hardwired and comply with the National Electrical Code (NEC) and other applicable electrical codes.

5.4.16 Where required, the TSCC Contractor shall provide outdoor-rated telecommunications cabinets to house all required network, power, and support equipment in external environments, including along the railway Right-of-Way, at stations, and at other operational facilities. Outdoor cabinets shall be designed to meet the environmental, electrical, and mechanical protection requirements appropriate for their deployment conditions and shall comply with EN 50125-3 and the applicable Location Specific Requirements (5.2.8).

5.4.17 Future Mobile Radio Communication System

5.4.17.1 All functional requirements defined in the latest version of the Future Railway Mobile Communication System (FRMCS) Functional Requirements Specification (FRS), as published by the UIC FRMCS Functional Working Group (FWG), shall be implemented by the TSCC Contractor.

5.4.17.2 The TSCC Contractor shall submit a detailed compliance statement mapping the FRMCS design to the FRMCS FRS requirements, identifying any deviations, partial implementations, or non-compliant items, for review and approval by the Authority.

5.4.17.3 The FRMCS shall be capable of supporting FRMCS-compliant mission-critical voice, data, and video services (MCX), and shall enable future integration with FRMCS-based infrastructure and equipment, including support for standardized interfaces, functional architecture, and radio access technologies as specified in 3GPP Release 17 or later and UIC FRMCS specifications.

5.4.17.4 The FRMCS design shall comply with all system requirements defined in the latest version of the FRMCS System Requirements Specification (SRS) published by the UIC, ensuring alignment with international railway communication standards and future interoperability.

5.4.17.5 The FRMCS shall provide the full voice, data and video feature set, including Railway Emergency Communication (Emergency Duress), as detailed in the 3GPP MCX and UIC FRMCS specifications. The TSCC Contractor shall highlight any non-compliance or missing features.

Radio Access Network Architecture

5.4.17.6 The FRMCS shall implement a Centralized Radio Access Network (C-RAN) architecture, whereby Baseband Unit (BBU) processing is consolidated at a central facility ("BBU Hotel"), and Remote Radio Heads (RRHs) are installed at the top of radio towers. The RRHs shall connect to the centralized BBUs via high-speed fronthaul links to enable enhanced coordination, cost efficiency, and optimized resource utilization. Refer to *Figure 25*.

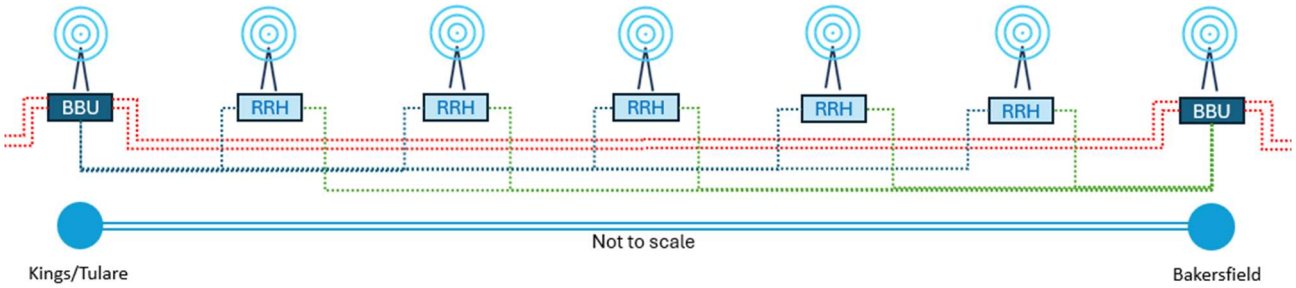

Figure 25 : Example of Centralized Radio Access Network (C-RAN) architecture, with a flat DCN ring (red) providing backhaul connectivity to BBU Hotel sites and with redundant fronthaul fiber from BBU to RRH sites (blue/green). If the fronthaul connectivity or the BBU fails, the RRH radio sites utilize the secondary BBU to maintain operations. NB: The BBU Hotels also have RRH for the tower collocated. In this example, all fiber is within the same cable run, providing a single point of failure.

5.4.17.7 This architecture shall be employed to minimize the physical footprint, and power requirements of radio sites along the CHSR Right-of-Way, reduce environmental impact, and support centralized resource pooling, simplified maintenance, and improved network scalability and resiliency.

5.4.17.8 The TSCC Contractor shall ensure the use of standards-based fronthaul interfaces (e.g., eCPRI or IEEE 1914.3) to interconnect RRHs and BBUs, and shall provide suitable protection, synchronization, and transport performance to support all FRMCS requirements.

5.4.17.9 The TSCC Contractor shall deploy BBUs at centralized, secure locations referred to as "BBU Hotels", where multiple Remote Radio Head (RRH) sites along the Right-of-Way are logically and physically parented to shared redundant BBUs.

5.4.17.10 BBU Hotels may be notionally located at locations designated as "Communication Site" on the CHSR "Schematic Track Layout and System Sites" **.** documentation. These sites have been prepared with space, power, and civil infrastructure suitable to accommodate towers, equipment shelters and related telecommunications facilities.

5.4.17.11 The TSCC Contractor shall dual parent (or dual-homed) RRH's to BBU Hotel locations to provide redundancy to address BBU equipment or fronthaul failure risk.

5.4.17.12 The BBU Hotels shall be designed to support:

- Fronthaul connectivity to all associated RRHs using high-capacity, low-latency links;
- Redundancy and survivability consistent with subsystem criticality;
- Future traffic growth.

5.4.17.13 The TSCC Contractor shall submit a BBU Hotel deployment plan identifying all parent-child RRH relationships, fronthaul link specifications, site readiness conditions, degraded operation scenarios and proposed system integration, subject to Authority review and approval.

5.4.17.14 The FRMCS shall utilize a redundant Radio Access Network architecture providing either:

- Double Coverage, where every operational zone is served by at least two overlapping base stations within the same FRMCS network. Refer to Figure 26; or
- Duplicated Coverage, where two logically and functionally independent FRMCS radio access systems provide overlapping coverage using separate radio, transmission, and DC power system

(including batteries), while allowing shared use of non-electronic physical assets such as towers, shelters, conduits, optic fiber cables and utility power supply. Refer to Figure 27.

The FRMCS design shall ensure that the failure of any individual radio site, equipment node, or backhaul path does not result in service interruption for safety-critical voice or data.

Note to reader: *Double coverage results in no loss of coverage during a single site outage due to completely overlapping coverage from adjacent site. Duplicated coverage results in no loss of coverage during equipment failure. Duplicated coverage does not provide the same level of availability but can provide near the same level and reduce the number of radio sites required.*

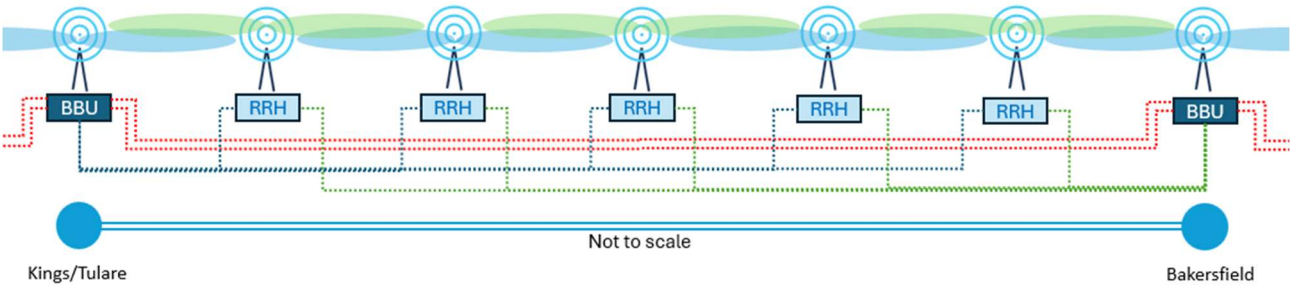

Figure 31 : Example of Centralized Radio Access Network (C-RAN) architecture, with 'Double Coverage'. Each adjacent radio site provides completely overlapping coverage. If any radio site fails, there is no loss of coverage.

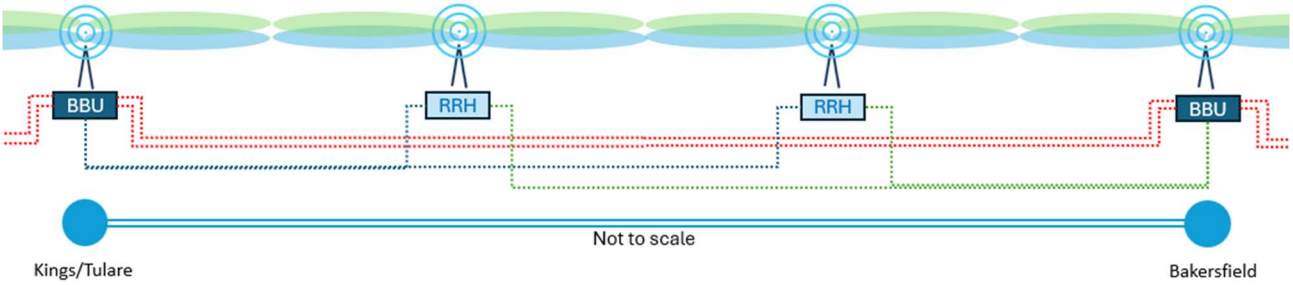

Figure 27 : Example of Centralized Radio Access Network (C-RAN) architecture, with 'Duplicated Coverage'. Each radio site has duplicated equipment, effectively two radio sites at one location. If any radio component fails, there is no loss of coverage, and there is battery backup and deployable generators to address loss of power.

FRMCS Feature Set

5.4.17.15 The FRMCS shall align with UIC FRMCS Functional Use Cases, 3GPP MCX redundancy principles, and safety-critical system design practices under EN 50159.

5.4.17.16 The FRMCS shall provide mission-critical Push-to-Talk (MCPTT) voice communication, as per 3GPP Mission-Critical Services: MCPTT (TS 23.379) and including:

- Individual and talkgroup calling;
- Emergency call initiation with pre-emption and override;
- Call priority management and call queuing;
- Support for late join and ambient listening (subject to policy).

5.4.17.17 The FRMCS shall enable Mission-Critical Data (MCData) communication, as per 3GPP Mission-Critical Services: MCData (TS 23.282) and including:

- Reception and acknowledgement of control instructions and timetables;
- Transmission of diagnostic and fault data from onboard systems to the OCC;
- Support for Cab Display Systems receiving text messages from OCC personnel.

5.4.17.18 The FRMCS should provide Mission-Critical Video (MCVideo) capability, as per 3GPP Mission-Critical Services: MCVideo (TS 23.281), to support:

- On-demand video transmission from the train cab to the OCC;
- Streaming of predefined onboard CCTV or event camera feeds during incidents.

Note to reader: *The Authority acknowledges that the Authority's spectrum limitations (5.1.6), the Authority requires streaming CCTV capability from trainsets. This alternatively could be provided by the PWS. The Authority encourages innovative alternative proposals to be submitted that meet the underlying business requirement to provide the streaming CCTV capability.*

5.4.17.19 The FRMCS shall support Dynamic Group Management, enabling OCC personnel, via Dispatch Consoles and other TSCC subsystems, to:

- Create, modify, and dissolve mission-critical voice talkgroups in real time;
- Assign drivers/trainsets, maintenance teams, and field staff to specific talkgroups as required for operations or emergencies.

5.4.17.20 The Dynamic Group Management capability shall allow OCC personnel to interconnect (aka 'patch' or 'bridge') other systems that have been integrated into the WCS Dispatch Consoles.

5.4.17.21 The FRMCS shall support dynamic talkgroup reassignment requests, and confirm completion of reassignment, from WCS Dispatch Consoles and other TSCC subsystems.

5.4.17.22 The FRMCS shall support user configurable rules-based reassignment of trainset talkgroups based on location, train ID, or section transitions (i.e., As trainsets crosses a Dispatcher's Area of Responsibility boundaries).

5.4.17.23 The FRMCS shall maintain support for emergency override calls that can reach multiple Dispatcher Areas regardless of dynamic talkgroup affiliation.

5.4.17.24 The FRMCS shall support end-to-end prioritization of all mission-critical communications, ensuring that safety-critical data (e.g. ETCS messages) and emergency voice calls are assigned the highest levels of QoS and priority across all network domains, including RAN, Core Network, and Transport Network. The system shall also support the configuration and enforcement of differentiated priority levels for other voice, data services (e.g. operational voice, maintenance data), in accordance with 3GPP QoS Class Identifiers (QCIs or 5QI), pre-emption capabilities, and local operational policies.

5.4.17.25 The FRMCS shall have the capability to store location data from FRMCS handheld devices. This data shall be able to be retrieved by the WCS Dispatch Consoles.

5.4.17.26 **Interoperability**

5.4.17.27 The TSCC Contractor shall provide an Interworking Function (IWF) to enable interoperability between the FRMCS-based communications system and existing or third-party Land Mobile Radio (LMR) systems, including but not limited to P25, TETRA, and analog conventional radio networks.

5.4.17.28 The IWF shall support voice interoperability to allow Operations Control Centre (OCC) dispatchers to:

- Initiate and receive group and individual voice calls between FRMCS and LMR users
- Participate in emergency calls initiated from LMR or FRMCS terminals
- Maintain Push-to-Talk (PTT) control behavior across systems
- View the caller identity and source system for all interworked calls
- Monitor, record, and replay interworked communications via the telephony logging system

5.4.17.29 The IWF shall support signaling and media translation in accordance with 3GPP TS 23.283 and applicable FRMCS and MCX specifications. The solution shall ensure interoperability without compromising the call priority, preemption, or quality-of-service mechanisms defined for FRMCS.

5.4.17.30 The TSCC Contractor shall provide interoperability between the FRMCS-based communications system and the FirstNet public safety broadband network (FirstNet), allowing authorized users, including OCC dispatchers, to communicate with FirstNet users via standards-based Mission Critical Services (MCX).

The interoperability solution shall support:

- Group and individual voice calls between FRMCS and FirstNet users using MCPTT (Mission Critical Push-to-Talk);
- Emergency call support across both networks, including priority and preemption;
- Location transparency, allowing OCC dispatchers to view the identity and affiliation (FRMCS or FirstNet) of the user;
- SIP/IMS-based interconnection and service-level interoperability in accordance with 3GPP TS 23.283 (LMR Interworking) and TS 23.379;
- End-to-end QoS control, ensuring MCX bearer traffic maintains service integrity and priority when traversing between the FRMCS and FirstNet environments.

5.4.17.31 The TSCC Contractor shall ensure that any interconnection with FirstNet complies with applicable cybersecurity, authentication, and identity federation policies as mandated by the Authority and by the FirstNet Authority.

5.4.17.32 Public Help Points shall provide two-way voice communication between the public and authorized railway personnel. Where required, Public Help Points shall be capable of operating over the FRMCS, utilizing its voice transport and call routing capabilities to establish reliable, prioritized connections with station staff, OCC personnel, or emergency responders. The system shall support integration with the Telephony System logging environment, including caller identification, location tagging, and call recording and logging. Refer to Telephony System Technical Specification.

Handheld Devices

5.4.17.33 FRMCS handheld devices shall support location reporting using multiple Global Navigation Satellite Systems (GNSS), including but not limited to GPS, Galileo, GLONASS, and BeiDou. Devices shall allow for programmable location reporting intervals (cadence) to suit operational requirements. All reported location data shall be transmitted to and captured by a centralized location server for real-time monitoring and historical tracking.

5.4.17.34 FRMCS handheld devices **should** support man down detection, lone worker monitoring, and ambient listening capabilities to enhance the safety of operational personnel. These features shall integrate with Mission Critical Push-to-Talk (MCPTT) emergency procedures as defined in 3GPP standards, enabling automatic emergency alerts, location update, and remote microphone activation under defined conditions. These capabilities are defined as:

- Man Down: An automatic emergency alert triggered by device sensors detecting that the user is motionless or in an abnormal posture (e.g., horizontal position) for a defined period;
- Lone Worker: A safety feature that monitors user activity and requires periodic check-ins, by pushing the PTT button in response to an alert. Failure to respond within a set timeframe triggers an emergency alert;
- Ambient Listening: The remote activation of a device's microphone, typically during an emergency call, to allow dispatchers or supervisors to hear the surrounding environment without user intervention.

FRMCS Recording and Logging

5.4.17.35 All FRMCS voice, data and metadata shall be recorded and logged for a minimum of 90 days. Refer to Telephony System Technical Specification for further information about logging requirements.

5.4.18 **Dispatch Consoles**

5.4.18.1 WCS Dispatch Consoles and Compact Dispatch Consoles shall provide authorized users with the full 3GP MCX and FRMCS feature set, such as, but not limited to:

- One to many push-to-talk (PTT) voice talkgroup communications;
- Simultaneous talkgroup communications;
- Broadcast talkgroup communications;
- Private / General call communications;
- Prioritized talkgroup and individual calling;
- Emergency Duress (Railway Emergency Call) functionality;
- Messaging, alerts, and acknowledgments;
- Interoperability between subsystems;
- Location-based user identification (FRMCS handheld devices);
- Patching within and between subsystems.

5.4.18.2 WCS Dispatch Consoles shall support user authentication, dynamic and multi-role assignment, and customizable UI profiles based on the assigned role of the operator (e.g., Train Dispatcher, Emergency Coordinator). That is, upon authenticating users shall be presented with the console configuration based upon their profile and role. Supervisors / managers shall be able to dynamically change the roles of users.

5.4.18.3 The WCS Dispatch Consoles shall display a real-time list of all active trainsets (identified by running train numbers) currently located within the Dispatch Area (Area of Responsibility) of the assigned dispatcher/operator. The console shall support direct voice communication with a specific trainset by allowing the dispatcher to initiate a call through a simple touch selection of the train number on the touch screen interface. As each Dispatch Area is associated with a dedicated talkgroup, and trainsets are dynamically reassigned to the appropriate talkgroup based on their location, the console shall ensure the dispatcher has visibility and calling capability for all trainsets currently affiliated with their designated Dispatch Area talkgroup.

5.4.18.4 WCS Dispatch Consoles and / or the dispatch workstation shall be integrated with other train control and telecommunications sub-systems, such as the Telephony System.

5.4.18.5 WCS Dispatch Consoles shall be designed to support integration with the FRMCS, which supports the ETCS SIL 4 subsystem. The WCS Dispatch Consoles components and their associated interfaces shall be developed, verified, and maintained in accordance with the safety requirements necessary to support a SIL 4 environment, in alignment with IEC 61508 and applicable railway safety standards.

5.4.19 **Interoperability between WCS subsystems**

5.4.19.1 The WCS shall support interoperable voice and data communication between FRMCS, PWS and Dispatch Console subsystems and Authority's corporate IT network (where required).

5.4.19.2 This WCS interoperability shall ensure that:

- Authorized users across different subsystems can exchange critical voice, data, and control messages securely and without degradation;
- Interfaces between subsystems comply with relevant open standards (e.g., 3GPP, IEEE, IETF) to enable seamless integration and future extensibility;
- Data can be accessed between WCS subsystems and Authority's corporate IT network (e.g., via DCN Firewall);

- Where subsystems operate on separate logical or physical infrastructure, appropriate interworking gateways, Inter-Working Functions, APIs, or middleware shall be implemented to maintain functionality and service continuity.

5.4.19.3 The TSCC Contractor shall demonstrate interoperability through system integration testing and provide documentation showing interface compatibility and user-level communication flows between subsystems, and demonstrate that this interoperability facilitates CHSR operations.

5.4.20 **ETCS Support**

5.4.20.1 The FRMCS shall provide the radio access bearer services for ERTMS/ETCS ensuring the overall safety of the end-to-end transmission between trainset and trackside ERTMS/ETCS applications. Refer to ETCS Technical Specification [R89] for further information.

5.4.20.2 The FRMCS shall ensure that ETCS safety-critical data is assigned the highest end-to-end priority level across all network segments, including the RAN, Core Network, and Transport Network. The system shall guarantee low latency, high reliability, and zero tolerance for pre-emption of ETCS traffic, using dedicated QoS parameters aligned with 3GPP-defined 5QI 75 or equivalent, and shall implement appropriate traffic marking, bearer selection, and resource reservation to support continuous and uninterrupted ETCS operation.

5.4.21 **Emergency Responder Communication System**

5.4.21.1 The ERCS shall be integrated into the WCS Dispatch Consoles system.

5.4.21.2 The ERCS shall support the following communication capabilities from WCS Dispatch Consoles:

- P25 radio voice interoperability with local, regional, and state responders;
- FirstNet LTE/5G data access (e.g., for video streaming, file sharing);
- Push-to-Talk (PTT) integration between OCC and responder teams;
- Support for unit ID, talkgroup assignment, and incident-specific channels.

5.4.21.3 The TSCC Contractor may utilize the FRMCS IWF to integrate ERCS with external Emergency Responder systems.

5.4.21.4 The specific agencies, channels and talkgroups will be determined in consultation with the Authority and each of the Authority Having Jurisdiction (AHJ) for emergency response within the CHSR System.

5.4.22 **Passenger Wi-Fi System**

5.4.22.1 The Passenger Wi-Fi System (PWS) shall provide a reliable, secure data communication between passenger devices and the internet, and operational personnel devices.

5.4.22.2 Profiling of network traffic shall be developed in detail for proper network dimensioning.

5.4.22.3 The PWS shall support uninterrupted session handover (unnoticeable to end users) between station and train W-Fi networks to preserve user sessions during boarding and alighting.

Note to reader: *At the time of drafting is it unknown if passenger wi-fi service will be provided at stations.*

5.4.22.4 If no station wi-fi service is initially implemented, the TSCC Contractor shall produce guidance for future reference on how to support uninterrupted session handover to mitigate the scenario where station Wi-Fi is introduced in future.

PWS User Experience and Accessibility

5.4.22.5 The PWS shall use a unified web browser-based authentication portal across stations and trains, offering:

- Fast user onboarding via captive portal, QR scan, and CHSR mobile app;
- Onboarding portal will be plain, simple, intuitive, free of advertising and branded as specified by the Authority;

- New users shall be able to establish an initial connection and access the internet within 30 seconds of selecting the Wi-Fi network, under normal network conditions;
- Authentication shall support federated identity and third-party sign-on using widely adopted providers such as Google, Apple ID, and Facebook;
- Accepted authentication protocols include OAuth 2.0, OpenID Connect, and SAML 2.0;
- Tiered access options (e.g., free basic, paid premium) with session persistence;
- Accessibility-compliant design (WCAG 2.1 AA or higher);
- Recognizing returning users and automatically re-establishing sessions to minimize reconnection time and improve user experience;
- Privacy policy and Fair Use policy confirmation during onboarding.

5.4.22.6 The PWS shall include a tiered passenger access model comprising:

- A **complimentary Wi-Fi** service access will be included with the passenger's train ticket, offering basic connectivity with configurable speed and daily data restrictions (specific volume to be defined during implementation planning). This basic tier shall support general web browsing, messaging, and email.
- A **premium Wi-Fi** service will be available for purchase, designed to support high-bandwidth applications including HD video streaming, cloud collaboration tools, and real-time video communications, including priority over 'basic tier' users.

5.4.22.7 The PWS tiering scheme may be changed by the Authority prior to or following the commencement of revenue service. The PWS shall support changing the number, naming, branding, pricing, access rights, data limits, quality-of-service levels, and feature sets of passenger Wi-Fi service tiers, including additional tiers, through a configurable management interface, without requiring hardware modifications or service disruption.

5.4.22.8 The PWS shall provide an integrated and secure digital payment gateway to enable access to the premium Wi-Fi service. The gateway shall support multiple forms of secure digital payment, including but not limited to:

- Credit/debit card payments (e.g., Visa, Mastercard, Amex);
- Mobile wallets (e.g., Apple Pay, Google Pay);
- QR code-based payments and carrier billing (where available);
- Integration with existing rail ticketing applications or passenger account systems.

5.4.22.9 All transactions shall be processed in compliance with the Payment Card Industry Data Security Standard (PCI DSS) and applicable consumer protection regulations.

5.4.22.10 The PWS premium service shall be able to be purchased as an additional service during CHSR ticket purchasing via all the CHSR ticket purchasing mechanisms. Activation of PWS service will be by the authentication portal.

5.4.22.11 The PWS shall allow users to seamlessly upgrade from the basic service to the premium Wi-Fi service during the journey without requiring session termination or loss of connectivity.

PWS Network Architecture and Technology

5.4.22.12 The PWS proposed architecture shall utilize high-bandwidth, low-latency backhaul technologies, with a strong preference for mmWave-based Train-to-Trackside (TtT) communications as the primary backhaul solution, particularly leveraging the unlicensed 60 GHz band for fixed wireless access at stations and along the rail corridor.

To augment coverage, availability, or performance, the solution may also incorporate or be supported by:

- 5G NR, including network slicing to optimize the passenger experience;
- Trackside wireless, hybrid satellite-mmWave solutions, or equivalent technologies for onboard connectivity;
- WAN bonding or aggregation techniques to increase backhaul capacity and resilience;
- An access point antenna architecture appropriate for the physical train environment and concurrent user demand.

All proposed technologies shall be interoperable, scalable, and optimized for the railway operational and passenger environment.

5.4.22.13 The PWS shall feature:

- Wi-Fi 7 (IEEE 802.11be) access points and backward compatibility with Wi-Fi 6/6E/5;
- Intelligent session management and aggregation of available backhaul technologies as defined in 5.4.22.12;
- Seamless user roaming and load balancing across station and train networks.

5.4.22.14 The PWS RF components must be optimized for rail environments and shall not interfere with critical operational systems (e.g., TPS, FRMCS, ETCS).

5.4.22.15 The PWS shall implement full network traffic segregation between:

- Passenger traffic (public internet access);
- Backhaul, Network Management Systems and other control plane systems.

5.4.22.16 This segregation shall be enforced through VLANs, firewalls, and access control lists (ACLs) to prevent unauthorized lateral movement or eavesdropping between networks.

Voice-over-Wi-Fi (VoWiFi) Support

5.4.22.17 The PWS shall support Voice over Wi-Fi (VoWiFi) services in accordance with 3GPP TS 23.228 (IP Multimedia Subsystem - IMS), 3GPP TS 24.302 (IMS registration over untrusted non-3GPP access), and 3GPP TS 24.229 (IMS core network signaling) [R54].

5.4.22.18 The PWS shall enable seamless access to VoWiFi for passenger devices registered with major U.S. carriers, including at least AT&T, Verizon, T-Mobile, and UScellular, without any user device configuration changes. The system shall also support VoWiFi access for international roaming subscribers whose home operators support IMS-based Wi-Fi calling.

5.4.22.19 The PWS shall:

- Provide IPv4 and IPv6 support for IMS signaling and media traffic;
- Support IPsec encapsulation and tunneling of IMS traffic in accordance with 3GPP TS 33.402 [R55] for non-3GPP access security;
- Enable Quality of Service (QoS) classification and marking for IMS signaling and RTP media (e.g., via DSCP);
- Prioritize VoWiFi bearer traffic to maintain acceptable Mean Opinion Score (MOS) and minimize latency, jitter, and packet loss.

5.4.22.20 The PWS shall support Network Address Translation (NAT) traversal and appropriate firewall configurations to ensure VoWiFi signaling and media flows are not blocked or degraded.

5.4.22.21 The PWS shall support emergency VoWiFi calls (e.g., E911) by:

- Allowing device-originated emergency SIP calls to reach the mobile operator’s IMS core;
- Supporting Location Information Server (LIS) interaction and/or enabling the device to transmit location metadata over Wi-Fi (e.g., via IETF RFC 6442 or 3GPP TS 23.167);

- Not impeding compliance with operator obligations to provide emergency services via VoWiFi.

PWS Usage Restrictions and Content Protection

5.4.22.22 The PWS shall implement content filtering mechanisms to restrict access to websites and online services that fall under any of the following categories:

- Malicious or phishing domains;
- Known sources of malware, spyware, or ransomware;
- Illicit content (e.g., child exploitation, illegal drug sales, human trafficking);
- Violent or extremist material;
- Gambling and explicit adult content;
- Parental controls will be enabled.

5.4.22.23 The content filtering solution shall use a regularly updated threat intelligence feed and shall be configurable to comply with jurisdictional requirements, including those of schools or family-focused services.

5.4.22.24 The TSCC Contractor shall ensure compliance with applicable regulations concerning the protection of minors online, including COPPA (Children's Online Privacy Protection Act) and equivalent state legislation where applicable.

5.4.22.25 Attempts to access restricted content shall be intercepted with a branded informational page that clearly states the reason for the restriction.

5.4.22.26 The system shall log access attempts to restricted content for security auditing purposes, while ensuring compliance with privacy legislation (e.g., CCPA).

PWS Data Logging and Retention

5.4.22.27 The PWS shall log user traffic metadata for all active sessions. This includes, but is not limited to:

- Timestamp of session start and end;
- Source and destination IP addresses;
- MAC address of the connecting device;
- Access point and train/station identifier;
- Protocol type (e.g., HTTP, HTTPS, DNS);
- Volume of data transmitted and received.

5.4.22.28 Logged metadata shall be logically associated with the authenticated user account, session token, or device identifier (e.g., MAC address) for traceability and auditing purposes.

5.4.22.29 Full packet inspection or payload capture shall not be performed, except for network diagnostics or legal interception purposes, and only under strict access control and authorization.

5.4.22.30 All logged data shall be retained securely for a period of 6 months, where the retention period shall be defined in accordance with applicable legal, regulatory, and operational requirements (e.g., CALEA compliance, internal security policies).

5.4.22.31 Access to log data shall be restricted to authorized personnel and protected through:

- Role-based access control (RBAC);
- Audit trails of access and retrieval;
- Multi-factor authentication for privileged users.

5.4.22.32 All retained data shall be stored in encrypted form (at rest and in transit) and in compliance with data protection laws including the California Consumer Privacy Act (CCPA) [R99], the California Electronic Communications Privacy Act (CalECPA) [R100], and any applicable federal regulations.

5.4.22.33 Upon expiry of the retention period, logs shall be securely deleted or anonymized in accordance with documented data disposal procedures.

5.4.22.34 Users shall be notified via the Wi-Fi login portal or privacy policy that metadata logging is performed and retained, along with a summary of their data rights under CCPA [R99].

5.5 Performance Requirements

5.5.1 The WCS FRMCS and PWS shall support all required voice, data, and control communications with no degradation in quality, latency, or handover performance at train speeds up to 220 mph (354 km/h) and dynamic integration testing at 242 mph. The system shall ensure uninterrupted connectivity for mobile users and onboard systems during all high-speed operations, while meeting performance targets.

5.5.2 All WCS coverage requirements shall be evaluated under peak revenue service conditions, including during passenger peak hour periods. Coverage verification assessments shall account for body absorption and crowd density effects, ensuring that signal strength and quality meet specified performance thresholds in fully occupied environments. The TSCC Contractor shall prepare and submit a detailed coverage verification report to the Authority, including methodology, measurement results, analysis, and any identified non-compliances or remedial actions.

5.5.3 The WCS shall comply with the RAM requirements defined in Schedule 1 – Safety, Security and RAM Requirements.

5.5.4 **Future Mobile Radio Communication System**

5.5.4.1 All FRMCS voice, data, and video shall meet the 3GPP MCX performance targets, as per TS 22.179:

- MCPTT call setup time ≤ 300 ms (95% of attempts);
- MCPTT end-to-end voice latency ≤ 300 ms;
- MCPTT speech intelligibility: Maintain intelligible voice under packet loss up to 5% and variable bitrates;
- MCPTT Mean Opinion Score (MOS): ≥ 4.0 under nominal network conditions using POLQA for AMR-WB or EVS codecs;
- MCPTT Codec Support: System shall support AMR-WB and optionally EVS, with forward error correction as per 3GPP TS 26.114 and TS 26.116 MCData transfer latency ≤ 1 second for 1 kB control message;
- MCVideo start-up time ≤ 1 second, with video latency ≤ 500 ms;
- Guaranteed QoS class identifiers (QCI) per 3GPP TS 23.203 or 5QI per TS 23.501.

Performance shall be validated through objective testing (e.g., POLQA, E-model, or equivalent) and documented in the TSCC Contractor's System Test and Verification Plan which will be submitted to the Authority for approval.

5.5.4.2 The FRMCS shall provide seamless radio coverage for MCX services (voice, video, and data) in all areas where trainset movement, operational control, and maintenance activities take place, in accordance with the coverage expectations outlined in 3GPP TS 22.179, TS 23.179, and TS 22.280.

5.5.4.3 The FRMCS shall ensure, under normal, degraded, and emergency operating conditions:

- 100% geographical FRMCS coverage across the EOS CHSR System;
- Signal strength of -95 dBm or better RSRP (for 5G) with a coverage probability of 95% at the antenna input of end-user devices in all operational areas;

- Coverage design shall assume an antenna height of 4 meters above rail level for train-mounted rooftop antennas operating within the railway Right-of-Way, and 1 meter above ground level for handheld radio devices used in stations, yards, maintenance facilities, and operational areas;
- Indoor FRMCS coverage (if required) in OCC and stations via DAS, repeaters, or base station coverage;
- Signal availability shall be maintained during typical propagation impairments, including body blockage, high-speed movement up to 220 mph (354 km/h), and multipath fading.

5.5.4.4 FRMCS coverage performance shall be validated via drive testing, walk testing, or trainset testing consistent with 3GPP TR 36.942, ITU-R P.1238, and P.1812.

5.5.4.5 The FRMCS shall be dimensioned to support peak concurrent usage of mission-critical services, including MCPTT, MCVideo, and MCData, during normal operations, planned events, and emergency scenarios. The system shall support the maximum operational train frequency without degradation in service performance. Performance shall align with 3GPP-defined KPIs for latency, availability, and call setup times as specified in TS 22.179, TS 23.179, and TS 28.313, and shall support simultaneous talkgroup communications, emergency call handling, and dynamic resource allocation under congested or degraded conditions.

5.5.4.6 The TSCC Contractor shall determine the minimum effective per-user downlink and uplink throughput required to support the full suite of services, including MCX and ETCS, at maximum train frequency. The FRMCS shall be designed to meet or exceed these throughput levels across the entire alignment, including in tunnels, trenches, cuttings, and viaducts, under both normal and degraded network conditions.

5.5.4.7 The FRMCS network shall also be dimensioned to support all operational and safety-critical communications across the CHSR System. OCC traffic controllers shall be able to maintain uninterrupted communication with all trainsets in their jurisdiction at all times. Baseline capacity shall include reasonable headroom for future extensions or reconfigurations, without requiring major capital investment.

5.5.4.8 All capacity planning assumptions, service profiles, and dimensioning models shall be documented in the TSCC Contractor's System Design and Performance Plan. Compliance with capacity and throughput requirements shall be validated during Factory and Site Acceptance Testing under simulated peak-load conditions.

5.5.4.9 The FRMCS shall be designed and optimized to achieve a handover success rate of at least 99.5% under normal operational conditions. Handover procedures shall maintain active sessions for all mission-critical services, including voice, video, and data, without perceptible service degradation or dropouts.

5.5.4.10 The FRMCS shall be configured to avoid unnecessary handovers and cell reselections, including so-called "ping-pong" effects, through appropriate parameter tuning (e.g., hysteresis, time-to-trigger). Cell mobility behaviors shall be optimized for high-speed train movements, including in coverage overlap areas, tunnels, and viaduct transitions.

5.5.4.11 The FRMCS shall support configurable prioritization of voice, data, and video communications in accordance with the operational requirements defined by the Authority. The system shall:

- Enable assignment and enforcement of QoS, Priority, and Pre-emption parameters on a per-service and per-user basis;
- Support dynamic configuration and policy control using mechanisms defined in 3GPP TS 23.501 and TS 23.503;
- Ensure that Mission-Critical services such as MCPTT, MCData, and MCVideo are mapped to appropriate 5QI (5G QoS Identifier) values, with support for guaranteed bit rate (GBR) and non-GBR flows as required;
- Allow the Authority to define priority levels for specific user roles (e.g., drivers, controllers, maintenance staff) and use cases (e.g., emergency, routine, background);

- Ensure that all prioritization policies are enforced consistently across the 5G/FRMCS Core, RAN, and DCN segments;
- Provide the Authority with the capability to update prioritization policies through a secure configuration management interface.

5.5.4.12 If 3rd party infrastructure sharing is utilized (e.g. 5G Slicing), the FRMCS shall provide call prioritization, preemption, and quality-of-service control to maintain communication integrity during congestion under normal, degraded, and emergency conditions.

5.5.4.13 If Time Division Duplexing (TDD) is used within the FRMCS, all base stations shall maintain an absolute time alignment with a common time reference, with a maximum network-wide time deviation not exceeding 1.5 microseconds. This synchronization requirement ensures proper frame alignment and mitigates inter-cell interference in TDD-based deployments.

Backup Power

5.5.4.14 FRMCS BBU Hotel locations shall be equipped with standby generators capable of supporting full system load for a minimum of 24 hours. Fuel storage and refueling provisions shall be sufficient to maintain continuous operation for the specified duration under normal and emergency conditions. The BBU hotel locations will have sufficient battery backup for the standby generator to operate efficiently.

5.5.4.15 FRMCS RRH locations shall be equipped with rectifiers and battery backup systems capable of sustaining operations for a minimum of 12 hours in the event of Medium/Low Voltage Power System (LVPS) failure. The battery systems shall be appropriately rated, monitored, and maintained to ensure reliable performance under all environmental conditions. The batteries shall be dimensioned for 12 hours autonomy at the end of their serviceable lifetime.

5.5.4.16 All FRMCS locations shall be provided with an external connection point for a backup generator to enable temporary power supply during outages of the LVPS, including BBU Hotel in case of on-site standby generator failure or maintenance. This provision shall ensure uninterrupted operation of all critical WCS functions during LVPS failures, planned maintenance, or emergency situations. At shared locations, like Traction Power or Signaling, standby generators can be shared.

5.5.4.17 All FRMCS backup power systems will have alarming and monitoring integrated into either the WCS NMS and/or the Integrated Control and Supervisory System (ICSS), to ensure power, generator and battery status and optimal performance can be monitored at all times. Refer to Integrated Control and Supervision System Technical Specification.

5.5.5 Dispatch Consoles

5.5.5.1 WCS Dispatch Consoles in the OCC shall be designed to maintain 99.999% availability (five-nines) and be connected via redundant paths to the WCS core infrastructure.

5.5.6 Emergency Responder Communication System

5.5.6.1 The ERCS shall maintain:

- Voice communication latency ≤ 300 milliseconds round-trip;
- System availability ≥ 99.99% annually in all emergency-critical locations;
- Uptime during grid outages through backup power (minimum 2 hours per code).

5.5.7 Passenger Wi-Fi System

5.5.7.1 The Passenger Wi-Fi System (PWS) shall be designed, delivered, and operated with the objective of achieving high levels of customer satisfaction and becoming a valued service offering of the train operator. To this end:

- The TSCC Contractor shall implement all reasonable measures to ensure the service is perceived as fast, reliable, and easy to use by the majority of passengers;

- The TSCC Contractor shall maintain a minimum Passenger Satisfaction Rating of 85% (as measured through periodic user surveys or feedback mechanisms approved by the Authority) and shall demonstrate continuous improvement in response to passenger feedback;
- Failure to maintain this satisfaction threshold over two consecutive reporting periods may trigger remedial action, including the submission of a formal Service Improvement Plan, subject to Authority approval.

5.5.7.2 At a minimum, the end user experience of PWS performance (in terms of reliability, speed, ease of access, and media streaming capability) shall be comparable to that provided on leading commuter and intercity rail services such as Caltrain, Amtrak, Brightline West or equivalent high-speed rail international benchmarks. Submissions should clearly outline how proposed solutions meet or exceed and ability to maintain these benchmarks.

5.5.7.3 The end-to-end network should support a minimum aggregate backhaul capacity of 2 Gbps per trainset with higher performance solutions preferred.

5.5.7.4 Each active passenger device shall experience:

- Sustained minimum download speed of 20 Mbps;
- Latency less than 50 milliseconds to common public internet endpoints;
- Jitter less than 20 milliseconds when using common public internet services;
- Ability to stream HD video (Netflix/YouTube), use real-time communication (VoIP/video calls/messaging services), and cloud-based applications (Microsoft Teams/Slack/Webex).

5.5.7.5 The PWS shall support a minimum of 450 concurrent users per trainset. Two trainsets may be coupled together for service. A double-traction train will carry a minimum of 900 passengers.

5.5.7.6 The PWS shall provide 99.5% monthly uptime per trainset.

5.5.7.7 There are no additional backup power requirements for PWS.

5.6 Security and Cybersecurity Requirements

5.6.1 All WCS equipment locations shall have CCTV coverage to mitigate the risk of theft of copper, batteries, generators, and other critical infrastructure. This includes installing CCTV on radio towers to provide additional coverage. CCTV systems shall be designed and installed in accordance with the CCTV Technical Specification [R90]. CCTV footage from these locations shall be transmitted to the OCC in real-time for monitoring, recording, and incident response purposes.

5.6.2 The WCS system shall nominate a System Owner that is accountable for cybersecurity risk ownership and mitigation.

5.6.3 All WCS equipment locations shall utilize the Electronic Access and Control System. Refer to Electronic Access and Control System Technical Specification.

5.6.4 The design of the security systems for the WCS radio sites shall be compliant with the CCTV System and Electronic Access and Control System Technical Specifications .

5.6.5 The WCS design shall be in full compliance with the Authority's cybersecurity policies specified in Cybersecurity Technical Specification.

5.6.6 The WCS security requirements shall mature over time based upon national and international standards and guidelines. Submissions should clearly outline how proposed solutions meet or exceed and the ability to maintain best industry practice security compliance.

Network Management System

5.6.7 The WCS Network Management System (NMS) shall enforce strict access control measures. All user access shall require individual credentials and be authenticated via role-based access control (RBAC) mechanisms. Administrator access shall require multifactor authentication (MFA). Default credentials must be changed prior to commissioning. Authentication, authorization, and access control requirements

shall be compliant with the Cybersecurity Technical Specification, specifically the least-privilege design principle and access review requirements.

5.6.8 The NMS shall generate and securely retain audit logs of all user activity, configuration changes, login attempts, and system events. Logs shall include timestamps, user IDs, IP addresses, and event types. Logs shall be protected against tampering and accessible only by authorized personnel.

5.6.9 All management communications between the NMS and network elements shall be encrypted using TLS 1.3. Remote access to the NMS shall be centrally managed and must be compliant with the remote access requirements defined in the Cybersecurity Technical Specification.

5.6.10 The NMS operating environment shall be hardened in accordance with vendor or industry security guidelines / best practices. All unnecessary services and ports shall be disabled. The operating system and application software shall be regularly updated with security patches. Patching shall be completed in accordance with change management processes and vulnerability and patch management requirements outlined in the Cybersecurity Technical Specification.

5.6.11 The NMS shall enforce session timeouts and automatic logoff for inactive sessions. Concurrent sessions shall be logged and optionally restricted by policy. Session Management, including session timeouts, shall be implemented and configured in compliance with the Cybersecurity Technical Specification , including remote access or local access to NMS systems.

5.6.12 The NMS shall support integration with external Security Information and Event Management (SIEM) systems via syslog or equivalent protocols that are supported by the target SIEM. The NMS TSCC Contractor shall be responsible for coordinating with the SIEM configuration team to ensure that adequate and relevant security event information is correctly formatted and ingested. The system shall support anomaly detection and alerting for suspicious behavior. Refer to Cybersecurity Technical Specification.

5.6.13 The NMS platform shall include or support the integration of endpoint protection tools. The system shall be regularly scanned for known threats, and alerts shall be generated for any detected issues.

5.6.14 Configuration data and logs from the NMS shall be regularly backed up to a secure, access-controlled storage location. Backup integrity shall be tested periodically, and recovery procedures shall be defined and documented. Backup and restoration technology, processes, and procedures shall align with the backup and restoration requirements defined in the Cybersecurity Technical Specification.

5.6.15 The TSCC Contractor shall implement a documented process for assessing, testing, and applying security patches to the NMS software and operating system, in line with a defined patching schedule and risk profile.

5.6.16 The NMS cybersecurity controls shall comply with applicable standards, including ISO/IEC 27001, NIST SP 800-53, and relevant rail cybersecurity guidance (e.g., EN 50701 where adopted). The TSCC Contractor shall provide evidence of security compliance during system design review and acceptance testing.

5.6.17 The NMS shall be configured to support the network security and network segmentation design as defined in the Cybersecurity Technical Specification by monitoring and verifying network configurations and producing alerts where non-compliance or anomalies are detected.

5.6.18 **Future Mobile Radio Communication System**

5.6.18.1 The FRMCS shall implement end-to-end encryption, mutual authentication, and user role verification as defined in 3GPP mission-critical service specifications and UIC FRMCS security guidance. Refer to Cybersecurity Technical Specification for further details on access controls, encryption, and mutual authentication.

5.6.18.2 Access to FRMCS devices, WCS Dispatch Consoles, and network interfaces shall require user and device authentication, with support for Role-Based Access Control (RBAC) and audit logging.

5.6.18.3 The FRMCS shall be implemented with Control Plane and User Plane network segmentation, firewall protection, and intrusion detection mechanisms to isolate operational communications from non-critical services.

5.6.18.4 All ingress and egress traffic between the FRMCS network and any external or interconnected networks (including but not limited to the NMS/ICSS, SIEM, TMS, etc.) shall be explicitly controlled through stateful firewalls. The default policy for all firewall rules shall follow a deny-by-default approach, permitting only traffic that is explicitly defined and authorized in accordance with the Cybersecurity Technical Specification.

5.6.18.5 Each interconnection point between the FRMCS network and external networks shall be protected by a firewall or security gateway that supports granular packet filtering, deep packet inspection, logging, and intrusion detection/prevention capabilities. These firewalls shall be configured to restrict traffic to the minimum set of required ports, protocols, and IP addresses necessary for each interface's operational function.

5.6.18.6 An Intrusion Detection System (IDS) shall be deployed at key points within the FRMCS architecture to monitor network traffic for signs of malicious activity or policy violations. The IDS shall be integrated with the Security Operations Centre (SOC) and Security Information and Event Management (SIEM) platform to enable real-time alerting, forensic analysis, and correlation with other network events. At a minimum, IDS sensors shall be placed at:

- The boundary between the FRMCS core network and external systems;
- Within the FRMCS core network to monitor control and user plane traffic;
- At network aggregation points where traffic from the Radio Access Network enters the transport/core network.

5.6.18.7 The design and configuration of the IDS shall follow the segmentation, zoning, and threat detection principles defined in the Cybersecurity Technical Specification.

5.6.19 **Dispatching Consoles**

5.6.19.1 WCS Dispatch Consoles shall enforce role-based access control, session timeout, and two-factor authentication for all OCC users accessing WCS systems. Shared or generic user accounts shall not be able to be utilized.

5.6.19.2 The WCS Dispatch Consoles shall support federated identity authentication and single sign-on (SSO) in accordance with industry-standard protocols such as SAML 2.0, OAuth 2.0, or OpenID Connect (OIDC). The system shall enable dispatch personnel to authenticate using credentials from CHSR Authority corporate accounts, and shall allow seamless access to all authorized FRMCS functions and integrated applications without requiring repeated logins.

5.6.19.3 All communications between dispatch consoles and WCS infrastructure shall be encrypted using FIPS 140-2 compliant cryptographic algorithms, with audit logging enabled for all access, configuration changes, and communication events.

5.6.20 **Emergency Responder Communication System**

5.6.20.1 The ERCS shall use secure, encrypted communication protocols conforming to public safety standards:

- AES-256 encryption for P25 and FirstNet services;
- Compliance with NIST 800-53 and FirstNet security frameworks.
- **Passenger Wi-Fi System**
- The PWS shall implement:
- WPA3 encryption or higher on all access points;
- TLS-based secure authentication and data encryption;
- Logical and physical network segmentation between passenger and operational systems, including the use of distinct SSIDs for each network to ensure isolation of traffic, enforce access control policies, and prevent cross-network interference or compromise.

5.6.20.2 The PWS must comply with:

- Local data protection laws (e.g., California Consumer Privacy Act (CCPA));
- FCC radio frequency licensing and telecommunications regulations.

6 INTERFACE REQUIREMENTS

6.1 General Requirements

6.1.1 Interfaces are classified as below:

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

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

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

6.1.4 The identified WCS Third Party, External and Internal interfaces are represented in Figure 28~~Figure 28~~ below.

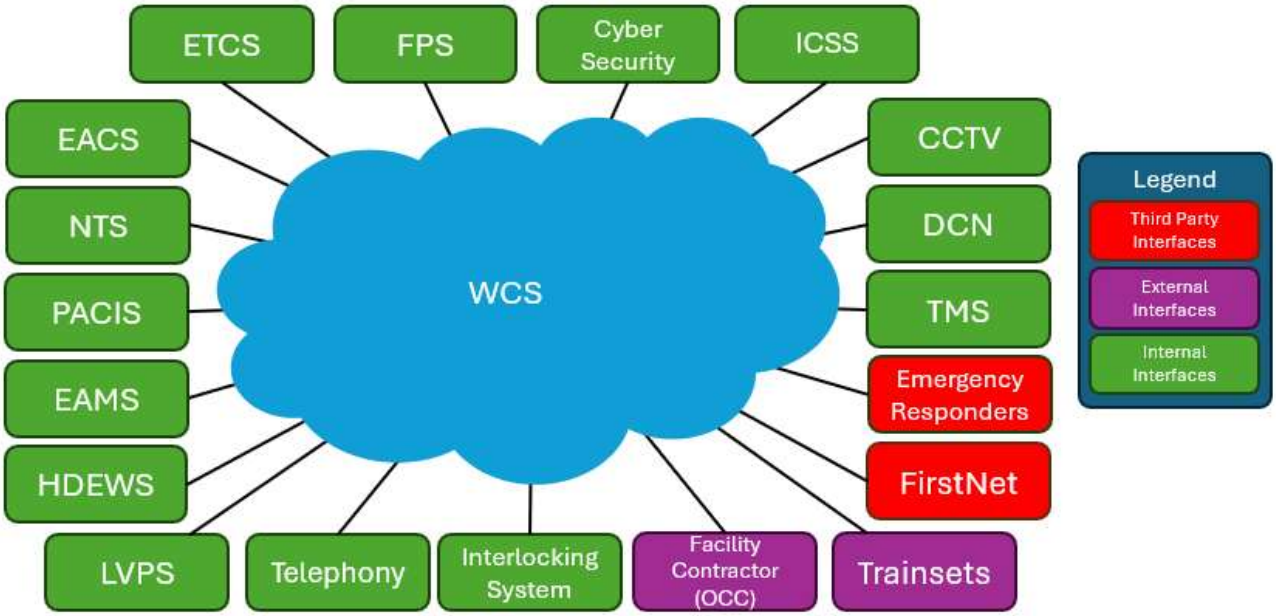

FIGURE 28: WCS THIRD PARTY, EXTERNAL AND INTERNAL INTERFACES.

6.2 Third Party Interfaces

The following section provides requirements associated with the Third Party interfaces between WCS and other systems.

6.2.1 With regard the Third Party interface, the TSCC Contractor shall follow the process defined in the Authority Interface Management Plan and shall support the Authority in developing the requirements and a scope split with related stakeholders. The TSCC Contractor shall execute the Third Party interfaces based on defined requirements and scope split.

6.2.2 The TSCC Contractor shall implement an external interface to enable interoperability between the FRMCS/MCX system and external Project 25 (P25) Land Mobile Radio (LMR) networks used by Emergency Responders during normal and emergency operations via the IWF.

6.2.3 The interface shall:

- Connect to external P25 systems via standardized interfaces, including but not limited to the Inter-RF Subsystem Interface (ISSI) and/or Console Subsystem Interface (CSSI) as defined in TIA-102;
- Support exchange of group and individual voice calls between FRMCS/MCX users (e.g., train drivers, OCC dispatchers) and P25 radio users, with transparent PTT behavior and call continuity;
- Enable emergency call bridging and participation in inter-agency talkgroups, including dynamically assigned talkgroups during coordinated incident response;
- Apply appropriate identity mapping and alias translation, ensuring P25 user identifiers are visible and meaningful to FRMCS/MCX users and vice versa;
- Maintain QoS, call priority, and preemption behavior across the interface in accordance with the priority schemes used in both systems;
- Include all necessary physical, protocol, and security configurations to support the interface, including encryption handling, firewall rules, IP routing, and port configurations.

6.2.4 The TSCC Contractor shall work collaboratively with the Authority and relevant Emergency Responders to define interface parameters, talkgroup mappings, testing protocols, and failover behavior during the integration planning phase.

6.2.5 The TSCC Contractor shall provide an external interface between the FRMCS and FirstNet, to support interoperable mission-critical communications between railway operational users and external emergency responders.

6.2.6 The interface shall support the following capabilities:

- Mission-Critical Services interworking, including MCPTT, MCVideo, and MCData, in accordance with 3GPP TS 23.283 (LMR/MCX interworking) and TS 23.379 (inter-PLMN MCX service interworking);
- Use of a Security Edge Protection Proxy to enable secure inter-PLMN signaling exchange over the N32 interface, with end-to-end integrity, encryption, and topology hiding;
- User authentication, identity federation, and QoS coordination, allowing authorized FirstNet users to participate in railway-specific talkgroups or receive real-time incident communications during joint operations;
- Support for dynamic group creation, inter-agency call patching, and roaming or guest access subject to policy-based control by the Authority;
- Compliance with all applicable cybersecurity, privacy, and interoperability requirements, including adherence to PCI DSS, FIPS 140-2, and relevant federal or jurisdictional public safety interconnection standards.

6.2.7 The TSCC Contractor shall work with the Authority, FirstNet Authority and FirstNet operator to define interconnection parameters, network trust models, and service-level expectations prior to deployment.

6.2.8 The TSCC Contractor shall co-ordinate with the other D&B contractors to include but not limited to planning approvals.

6.2.9 The WCS shall interface with the on-board system of trains (scope of trainset contractor, to enable voice / data traffic, emergency calls, selected on board alarm/status information and on-board public address announcements.

6.2.10 The WCS core networks and Dispatch Consoles shall be located at the OCC. The TSCC Contractor shall liaise with the OCC TSCC Contractor to ensure that the OCC meets the WCS requirements.

6.2.11 The TSCC Contractor shall ensure that the WCS integrates, where required, with the Asset Management System being provided under a different CHSR contract.

6.2.12 The WCS, PWS and FRMCS (5G Core) shall interface with the internet firewalls/gateway at the OCC via the DCN.

6.3 External Interfaces - Trainsets

The following section provides requirements associated with the External Interface between the TSCC Contractor and Trainset contractor to deliver the onboard WCS components.

6.3.1 The TSCC Contractor shall be responsible for providing the Trainset contractor, in a timely manner and in alignment with the approved project schedule, all high-level designs, interface designs, technical specifications, and technical documentation necessary to support the integration of onboard WCS subsystems. This shall include, but not be limited to:

- Equipment specifications;
- Physical and electrical interface specifications;
- Equipment power requirements;
- Space and mounting requirements;
- Environmental and cooling requirements;
- Antenna placement guidelines and RF cable routing information;
- Data connectivity and signal interface details;
- Installation and commissioning procedures.

6.3.2 All documentation shall be sufficiently detailed to enable the Trainset Contractor to proceed with detailed design, procurement, and installation activities without delay.

6.3.3 The Trainset Contractor shall be responsible for the installation design, procurement and supply of onboard WCS equipment (as specified by the TSCC Contractor), provision of power and cabling, mounting provisions, installation, and integration with other trainset systems. The Trainset Contractor shall also perform onboard commissioning and testing in accordance with the interface documentation and requirements provided by the TSCC Contractor.

6.3.4 The TSCC Contractor shall provide comprehensive support for the integration and commissioning of the onboard WCS subsystems. This includes:

- Bench and factory testing of WCS equipment;
- Supervision and technical support during installation;
- Integration and configuration of systems onboard;
- Functional verification and interoperability testing;
- Coordination with the Trainset Contractor to ensure compliance with the Technical Specifications and interface requirements.

6.3.5 Support shall be provided both remotely and onsite as requested by the Trainset Contractor and/or the Authority to ensure successful system integration.

6.3.6 The TSCC Contractor and Trainset Contractor shall share joint responsibility for verifying the correct operation of the onboard WCS subsystems during dynamic testing, including full end-to-end system functionality. Any non-conformances or integration issues identified during testing shall be investigated and resolved collaboratively, in accordance with the project's integration, test, and defect resolution procedures. Final handover shall not proceed until both parties have confirmed resolution of all critical issues affecting system performance or compliance.

6.4 External Interfaces – stations contractor

6.4.1 The TSCC Contractor shall ensure that the PWS core network shall allow the integration of station contractor's Wi-Fi access network.

6.4.2 The TSCC Contractor shall provide all required information to station contractor to facilitate the design and integration.

6.5 External Interfaces – facilities contractor

6.5.1 The TSCC Contractor shall install all WCS core network equipment in the OCC being provided by the facilities contractor.

6.5.2 The TSCC Contractor shall provide to the facilities contractor:

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

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

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

6.6 Internal Interfaces

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

6.6.1.1 The FRMCS core network infrastructure shall have redundant interface with the DCN to ensure secure and reliable transport of FRMCS data and to provide resilient interconnection between all FRMCS BBU Hotel and RRH sites and the core network infrastructure.

6.6.1.2 The FRMCS and DCN shall be integrated in a manner that enables FRMCS fixed and handheld devices to securely and reliably access data and services provided by other systems connected to the DCN.

6.6.1.3 The FRMCS DCN backhaul transmission shall be implemented with a ring-based architecture to enable automatic rerouting of communications to the core network in the event of a DCN transmission link or node failure. This design shall ensure continuity of service by utilizing redundant DCN transmission paths between FRMCS radio sites, specifically BBU Hotels, and between FRMCS and the DCN, maintaining full network connectivity and resilience along the CHSR Right-of-Way.

6.6.1.4 The FRMCS core network shall have redundant interface with the DCN Firewall and/or Broadband Network Gateway.

6.6.1.5 The PWS trackside transmitters shall interface with the DCN switches at trackside equipment shelters via dark fiber, and the PWS core network infrastructure shall interface with the DCN at the OCC, via dedicated VLAN.

6.6.1.6 The PWS shall interface with the DCN management VLANs to support remote monitoring, configuration, and performance logging of PWS components.

6.6.1.7 The PWS core network shall interface with the DCN firewall to manage secure access to internet-hosted services, including cloud-based content filtering and system updates.

6.6.1.8 The PWS transmitters shall connect to the DCN via managed trackside Ethernet switches capable of supporting VLAN segmentation and Quality of Service (QoS) for PWS traffic.

6.6.2 Interface with European Train Control System (ETCS)

6.6.2.1 The onboard FRMCS radios shall interface with the onboard ETCS system to enable the exchange of safety-critical signaling data, including the transmission of train position reports from the ETCS to the RBC and the reception of Movement Authority messages from the RBC via FRMCS. This interface shall support the establishment and maintenance of a dedicated and secure communication session between the train and the trackside ETCS infrastructure.

6.6.2.2 The interface between the FRMCS and ETCS systems, both onboard and core network, shall meet Safety Integrity Level 4 (SIL 4) as defined in EN 50126, EN 50128, and EN 50129, to ensure the safe transmission and reception of signaling information critical to train operation. Compliance shall be demonstrated through appropriate safety case documentation and certification.

6.6.2.3 The FRMCS shall have redundant interface with the ETCS Radio Block Center (RBC) system for enabling exchange of signaling information (Movement Authority). The RBC receives the train position from the onboard ETCS via FRMCS and sends the authorization for the train to continue running. The authorization is sent to the train through a dedicated and safe communication session.

6.6.3 Interface with Telephony System

6.6.3.1 The FRMCS shall have a redundant interface with the Telephony System, which acts as the central switching system for phone calls. The telephony system handles internal traffic between stations and acts as the gatekeeper to the outside world.

6.6.3.2 The Dispatch Consoles shall be integrated with the Telephony System, which acts as the central recording and logging system for all Dispatch Consoles and FRMCS voice, data and metadata.

6.6.3.3 The Telephony System shall provide the voice, data and metadata recording and logging capabilities of the FRMCS.

6.6.4 Interface with Network Timing System (NTS)

6.6.4.1 The FRMCS shall have redundant interface with the NTS for accurate current time display and for precise calculations required for time estimation.

6.6.4.2 The NTS shall integrate with the FRMCS BBU Hotels to provide precise time and frequency synchronization using IEEE 1588v2 Precision Time Protocol and/or Synchronous Ethernet, ensuring coordination of time-sensitive functions such as radio resource management, handover, and TDD frame alignment across the FRMCS Radio Access Network.

6.6.4.3 The PWS core system shall interface with the NTS provided by the DCN to ensure time synchronization across all PWS components for logging, monitoring, and coordination purposes.

6.6.5 Interface with Integrated Control and Supervisory System (ICSS)

6.6.5.1 The WCS NMS shall integrate with the ICSS to enable end-to-end monitoring, fault management, and performance reporting of the WCS infrastructure. This integration shall support standard interfaces and protocols to ensure compatibility with ICSS subsystems, and allow for centralized visibility and control within the broader operational management environment.

6.6.6 Interface with Train Management System (TMS)

6.6.6.1 The FRMCS shall accept MCX Application Server API calls, such as Dynamic Talkgroup Reassignment, from the Train Management System and other TSCC subsystems interconnected via the DCN.

6.6.7 Interface with Medium/Low Voltage Power System

6.6.7.1 All FRMCS RAN infrastructure, BBU Hotel and RRH cabinet locations, shall be powered by the MV+LV Power System.

6.6.7.2 All PWS trackside transmitters shall be powered by the MV+LV Power System.

6.6.7.3 All WCS core network equipment at the OCC shall be powered by the MV+LV Power System.

6.6.8 **Interface with Passenger Announcement and Customer Information System (PACIS)**

6.6.8.1 The FRMCS shall integrate with the PACIS at the core network and on the trainset, to allow Passenger Announcements to be made in the OCC and broadcast in the trainset, and for Customer Information System onboard the trainset to be updated from the OCC.

6.6.9 **Interface with Cybersecurity**

6.6.9.1 The FRMCS shall integrate with all Cybersecurity infrastructure and follow all implementation guidance as specified in the Cybersecurity Technical Specification

6.6.10 **Interface with Fire Protection System (FPS)**

6.6.10.1 All WCS equipment shelters shall be protected by the FPS.

6.6.11 **Interface with Electronic and Access Control System (EACS)**

6.6.11.1 All WCS equipment locations, apart from trackside cabinets and transmitters, shall have access controls provided by the EACS.

6.6.12 **Interface with Interlocking System (IXL)**

6.6.12.1 The FRMCS shall provide wireless communication between Trackside Worker Protection Devices, that are in a handheld ruggedized tablet form factor, and the Interlocking System. The FRMCS shall provide high priority for mission-critical (safety-critical) communications.

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

6.6.13.1 The FRMCS shall provide wireless communication between official handheld devices and the Enterprise Asset Management Systems to allow CHSR personnel to access core system functionality through mobile or web browser-based applications.

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

6.6.14 **Interface with other TSCC Sub-systems (TSCC's)**

6.6.14.1 The FRMCS core network shall be integrated with other TSCC's via the DCN, to support secure connectivity between fixed and mobile FRMCS devices and other TSCC's. This capability shall enable authorized users to access core system functionality through mobile applications or web-based interfaces on FRMCS devices. This capability shall also enable automated systems to access core system functionality, such as Hazard Detection and Early Warning System.

6.6.15 **Interface with other WCS Sub-systems**

6.6.15.1 The FRMCS Core Network, specifically the Inter-Working Function, shall integrate into the ERCS to facilitate the interface between the WCS Dispatch Consoles and external Emergency Responder systems.

6.6.15.2 The WCS NMS shall integrate with and monitor the WCS subsystems.

7 MATERIAL, PRODUCT AND COMPONENT REQUIREMENTS

7.1 General Requirements

7.1.1 All materials supplied by the TSCC Contractor shall conform to the requirements and test methods of the relevant EN standards or other applicable recognized standards. Refer to 2.4.

7.1.2 All materials supplied shall be of sufficient grade and quality to meet the design lifetime requirements.

7.2 Software and Hardware Requirements

7.2.1 The FRMCS and ERCS design shall be based on COTS, open architecture, and modular system architecture, with standard 3GPP non-proprietary interfaces.

7.2.2 The PWS design shall be based on COTS, open architecture, and modular system architecture, with standard non-proprietary interfaces for the subcomponents that are supported by standardized interfaces (e.g., Wi-Fi7, IP, etc.). It is acknowledged that mmWave trainset to track solutions are not standardized.

7.2.3 The FRMCS servers shall have redundant architecture including hardware, power supply, cabling and software so that FRMCS functionality remains available during any one failure of hardware, power supply, cabling and software.

7.2.4 All WCS cabling shall be designed, supplied, and installed and commissioned by TSCC Contractor.

7.2.5 All WCS cabling shall operate in the temperature range from -35 °C to 85 °C and comply with section 5.2 Environmental Requirements.

7.2.6 All WCS cabling shall comply with applicable U.S. standards and codes, including the National Electrical Code (NEC), NFPA 70, and relevant UL or ASTM standards for fire resistance, smoke propagation, and installation in commercial and transportation environments. Cabling shall be listed or certified by a Nationally Recognized Testing Laboratory.

7.2.7 The coaxial cables connecting the RRH to the antennas shall be dimensioned to guarantee the maximum transfer of power to the antennas.

7.2.8 All WCS antennas shall be designed, supplied, and installed and commissioned by TSCC Contractor. FRMCS antenna pans and tilts shall be validated post construction to ensure optimal operation.

7.2.9 All antennas for FRMCS shall support electronic tilt.

7.2.10 All RRH for FRMCS shall operate in the temperature range from -35 °C to +70 °C and shall have a minimum IP67 design, and comply with section 5.2 Environmental Requirements.

7.2.11 All WCS core network infrastructure for shall be designed, supplied, and installed and commissioned by TSCC Contractor.

7.2.12 All WCS core network infrastructure shall be dimensioned and licensed to guarantee the performance of the services needed for the complete functioning of the WCS.

7.2.13 The TSCC Contractor shall supply all necessary software licenses required for the operation, management, and maintenance of the WCS. All licenses shall include sufficient headroom to accommodate expected future capacity growth, as defined by the Authority's forecasted system expansion, without requiring additional procurement or renegotiation within the initial operational period.

7.3 Radio Site Preparation Requirements

7.3.1 All the requirements concerning the site preparation, e.g., civil works, fencing, access and technical buildings are described in the Scope of Work.

7.3.2 The FRMCS radio sites shall be designed, constructed, operated and maintained as per the requirements in section 5.1.22.7 Environmental Requirements.

7.3.3 FRMCS radio site locations shall be selected and designed to ensure safe, secure, and practical operation and maintenance. Site selection shall avoid hazard areas like flood-prone areas and vehicular crash risk

zones. Adequate provisions shall be made for access by maintenance vehicles, including space for crane or Mobile Elevating Work Platform operations, as well as parking. Each site shall be designed to include appropriate fencing, access control, and physical security measures in accordance with applicable standards and operational requirements.

7.4 Radio Tower Requirements

7.4.1 The FRMCS radio towers shall be a self-standing monopole structure made from concrete and/or metal and shall have the less environmental impact and require the minimum footprint as possible.

7.4.2 The FRMCS radios towers height shall be 100 foot / 30.48 meters from top of the running rails. No antennas shall be higher than this height limit.

7.4.3 The TSCC Contractor shall supply and install all foundations, lightning protection, earthing, and bonding systems required for masts and towers at standalone radio sites.

7.4.4 At sites co-located with traction power facilities, tower/mast foundations, earthing, and bonding systems shall be provided by Traction Power Contractors. The TSCC Contractor shall define and communicate all relevant technical and interface requirements to the Traction Power Contractors to ensure compliance with WCS system needs.

7.4.5 All equipment installed on radio towers shall incorporate appropriate bird-proofing measures tailored to local wildlife conditions, to prevent damage, maintain operational reliability, and ensure compliance with environmental protection requirements.

7.4.6 The TSCC Contractor shall design each radio tower to support the installation of multiple cellular carrier antennas, including provision for mounting infrastructure such as an antenna platform or equivalent structure. The design shall allow for sufficient structural capacity, antenna separation, cabling pathways, and access to accommodate current and future multi-operator deployments in accordance with relevant structural and safety standards.

7.4.7 At station locations or other high-demand sites, the TSCC Contractor shall design the radio tower compound with adequate space, access, and utility provisions to accommodate additional equipment huts or shelters for third-party Mobile Network Operators (e.g., Verizon, AT&T, T-Mobile). The design shall include appropriate foundations, power supply, cabling pathways, and physical security measures to enable future co-location of carrier equipment without requiring significant civil modifications or service disruption.

7.4.8 The TSCC Contractor shall ensure that all radio tower designs, equipment, and installations comply with all applicable local, state, and national codes, regulations, and standards. The TSCC Contractor shall provide evidence of such compliance, including but not limited to certifications, test reports, and design documentation, as required by the Authority or relevant regulatory bodies.

7.4.9 The FRMCS radio towers shall be designed, constructed, and maintained to exceed its minimum design life, ensuring continued structural integrity, operational reliability, and compliance with applicable standards throughout its lifecycle. The TSCC Contractor shall implement maintenance and inspection regimes, aligned with relevant codes and manufacturer recommendations, to proactively manage degradation and extend service life beyond the nominal design period.

7.5 RF Exposure Requirements

7.5.1 The WCS, including all transmitting infrastructure such as cellular, Wi-Fi, and radio antennas, shall be designed, installed, and operated in full compliance with Federal Communications Commission (FCC) regulations governing human exposure to radiofrequency (RF) electromagnetic fields.

7.5.2 All WCS antenna installations shall:

- Comply with RF Exposure limits as specified in 47 CFR §1.1307, §1.1310, and related FCC guidance (e.g., OET Bulletin 65).
- Be evaluated for Maximum Permissible Exposure compliance, accounting for both occupational and general population exposure zones.

- Implement appropriate signage, physical barriers, and administrative controls where exposure may exceed general population Maximum Permissible Exposure thresholds.
- Ensure that co-located transmitters are considered in cumulative exposure assessments.
- Provide site-specific RF exposure compliance documentation prior to system activation or commissioning.

RF Exposure evaluations shall follow procedures outlined by the FCC Office of Engineering and Technology, and where applicable, adhere to exposure limits defined in ANSI/IEEE C95.1. The TSCC Contractor shall coordinate with facility owners and safety personnel to ensure proper RF safety training and signage in accordance with FCC regulations.

7.5.3 The TSCC Contractor shall provide a complete RF Exposure Compliance Package demonstrating that all WCS transmitting infrastructure complies with FCC regulations (47 CFR §1.1307 and §1.1310) and ANSI/IEEE C95.1 exposure limits.

The package shall include:

- Site-specific RF exposure evaluation reports, including Maximum Permissible Exposure calculations and RF hazard contour diagrams;
- Antenna inventory with transmit power, frequency, gain, and FCC certifications;
- Evidence of RF safety signage and physical barrier implementation;
- Photographic evidence and annotated as-built drawings;
- Confirmation of RF safety training for relevant personnel;
- A signed compliance statement confirming adherence to FCC and industry standards.

The documentation shall be submitted and accepted prior to commissioning.

8 TOLERANCES

Not applicable to Wireless Communications Systems.

9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

9.1.1 General requirements are described in the Scope of Work document.

9.2 Specific Requirements

9.2.1 The TSCC Contractor shall supply, deliver, install, test, and commission all components necessary for a fully functional WCS, as specified in this Technical Specification.

9.2.2 The TSCC Contractor shall be responsible for the design, manufacture, factory acceptance testing (FAT), delivery, site installation, integration, site acceptance testing (SAT), and commissioning of the WCS solution to facilitate CHSR in-revenue service.

9.2.3 The scope of supply shall include, but not be limited to:

- Wireless access infrastructure, including base stations, access points, antennas, masts, and associated coaxial, optic fiber and power cabling;
- Backhaul and transmission equipment, including switches, routers, and optical or wireless transmission gear;
- Core network components, including network controllers, gateways, and any central management servers;
- User equipment, including handheld terminals, vehicular radios, onboard units, and any mobile communication devices;
- Power supply systems, including UPS, battery backup systems, and power distribution units for WCS equipment;
- Mounting structures, cabinets, shelters, racking, cable trays and enclosures for indoor and outdoor deployments;
- Software, including network management systems (NMS), provisioning tools, configuration management, and cybersecurity features;
- System interfaces, including integration with the Digital Communications Network (DCN), Train Control and Management System (TCMS), and On-board Railway Applications where applicable;
- Test equipment required for installation and commissioning;
- Spare parts, tools, and special test equipment, as per the spares strategy agreed with the Authority;
- Ancillary systems, including lighting, security (e.g., access control), CCTV, environmental conditioning (e.g., heating, ventilation, and air conditioning), and any other supporting infrastructure necessary to ensure safe, secure, ergonomic and reliable operation of WCS equipment installations;
- Documentation, including design documents, installation manuals, test procedures, and as-built records.

9.2.4 The TSCC Contractor shall ensure that all equipment and materials delivered are compliant with relevant standards and project-specific environmental and safety requirements.

9.2.5 The TSCC Contractor shall coordinate all delivery and logistics activities in accordance with the Project Delivery Program and in consultation with the Authority, including any site access restrictions and staging requirements.

9.2.6 The TSCC Contractor shall label and package all equipment and components clearly and securely to facilitate identification, handling, and inventory upon delivery to site.

9.2.7 The TSCC Contractor shall provide a detailed Delivery and Installation Schedule, identifying all major equipment deliveries, installation milestones, and dependencies.

9.2.8 The TSCC Contractor shall provide complete backups of all software and configuration files necessary to restore the system to full operational status in the event of failure or data loss. The TSCC Contractor shall

also supply appropriate and secure storage media or infrastructure for managing, periodically producing and retaining these backups in accordance with the WCS's recovery and cybersecurity requirements.

10 MANUFACTURING

10.1 General Requirements

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

11 INSTALLATION AND INTEGRATION

11.1 General Requirements

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

12 TESTING & ACCEPTANCE

12.1 General Requirements

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

12.1.2 All test results and certifications required for the WCS shall be provided by the TSCC Contractor.

12.1.3 The following testing requirements are intended to verify compliance with the requirements set out in all preceding sections of this Specification, including but not limited to functional, performance, operational, and interface requirements. Nothing in this section shall be construed as limiting the TSCC Contractor's obligation to meet the full scope of requirements specified elsewhere in this document.

12.1.4 The TSCC Contractor shall perform comprehensive redundancy and failover testing across all WCS subsystems, where applicable, including but not limited to the Core Network, Radio Access Network, Transport Network, Network Management Systems, Dispatch Systems, and Power Supplies.

12.1.5 The testing shall validate that:

- Redundant components and paths are operational and properly configured to take over in the event of failure;
- Automatic failover occurs without manual intervention and within system-defined recovery times;
- No loss of critical communications services (e.g., MCX voice, video, or data) occurs during failover;
- Stateful recovery is preserved for ongoing MCX sessions, where applicable;
- Alarm, monitoring, and logging systems accurately detect, report, and log redundancy activation events;
- Redundancy applies to active-active and active-standby configurations, including:
- Dual core or distributed User Plane Function/Service Communication Proxy instances;
- RAN node or sector-level redundancy;
- Link/path redundancy in the Backbone Transport Network;
- Redundant power supplies (DC/AC), backup battery systems and generators;
- Dual NMS/ICSS control interfaces and databases;

Redundancy tests shall simulate single point failures, partial subsystem outages, and complete system switchover scenarios in accordance with the approved test plan and system design. The results shall demonstrate compliance with the specified availability, reliability, and recovery performance targets.

12.2 Specific Requirements for FRMCS

12.2.1 All FRMCS-related equipment shall be subjected to functional testing to verify correct installation, configuration, and operation in accordance with the system design and performance requirements.

12.2.2 **Radio Access Network Testing**

12.2.2.1 Voice and data call tests shall be conducted across representative coverage areas to verify the functionality, reliability, and quality of FRMCS services.

12.2.2.2 Antenna installation and alignment shall be verified for compliance with the approved FRMCS radio design, including orientation, height, and tilt parameters.

12.2.2.3 The Voltage Standing Wave Ratio (VSWR) and return loss of all coaxial cable installations shall be measured and confirmed to be within acceptable thresholds defined by the manufacturer and design specifications.

12.2.2.4 The connectivity between the FRMCS Radio Access Network and the Digital Communications Network (DCN) shall be verified to confirm end-to-end path availability and proper routing.

12.2.2.5 The connectivity between the FRMCS BBU and RRH shall be verified to confirm end-to-end path availability and proper routing.

12.2.2.6 The interface between the FRMCS RAN, the Network Management System (NMS) and the Integrated Control and Supervisory System (ICSS) shall be tested to ensure successful communication, event reporting, and configuration management.

12.2.2.7 Radio network performance shall be validated by measuring key parameters including signal strength (RSRP/RSRQ), throughput, latency, and call success rates in accordance with the FRMCS performance criteria.

12.2.3 **Core Network Testing**

12.2.3.1 Core network testing shall be conducted at both the Operations Control Centre (OCC) and secondary core network at Government Data Center to verify proper deployment and function.

12.2.3.2 Core network testing shall include both Site Acceptance Testing (SAT) and System Integration Testing (SIT).

12.2.3.3 Site Acceptance Testing (SAT) shall be performed after equipment delivery and installation at the OCC and secondary core network. SAT shall confirm that the installed equipment meets or exceeds the required functional and performance specifications.

12.2.3.4 SAT shall be performed individually for each installed core network component, including but not limited to servers, session management functions, gateways, and edge routers.

12.2.3.5 System Integration Testing (SIT) shall be conducted to validate the end-to-end functionality of the core network, including integration with the Radio Access Network, DCN, NMS, Dispatch Consoles and external interfaces (e.g., IWF, P25).

12.2.3.6 Redundancy and failover testing shall be performed to validate the resilience of the core network. Tests shall simulate failures of critical components and interfaces to confirm continuity of service, including full core failover and isolated element failures.

12.2.3.7 Software release and version interoperability testing shall be conducted to assess system behavior following major software upgrades or patch deployments, ensuring continued compliance with functional, security, and interoperability requirements.

12.2.4 **Interworking Function (IWF) Testing**

12.2.4.1 The Interworking Function (IWF) shall be tested to verify voice interoperability between FRMCS/MCX users and external Land Mobile Radio (LMR) systems, including but not limited to P25, TETRA, and analog networks.

12.2.4.2 Test scenarios shall include:

- Group and individual call setup between FRMCS and LMR users;
- Push-to-Talk (PTT) signaling interoperability;
- Emergency call bridging;
- Alias/ID translation and display across systems.

12.2.4.3 The IWF shall be subjected to failover testing, including loss of network connectivity or remote radio system availability, to confirm fallback behavior and service recovery.

12.2.4.4 Latency, jitter, and audio quality across the IWF interface shall be measured to ensure adherence to 3GPP TS 23.283 [R49] performance guidelines.

12.2.4.5 Security testing shall be conducted to verify authentication, access control, and encryption of inter-system communications.

12.2.5 **Dispatch Consoles Testing**

12.2.5.1 The WCS Dispatch Consoles shall undergo functional testing to verify the ability to initiate, manage, and monitor MCX-based communications including voice, video, and data.

Dispatch consoles shall be tested for:

- Push-to-Talk group call control;
- Individual and emergency call initiation;
- Real-time location display and user status indicators;
- Video streaming to/from field units;
- Messaging, alerts, and acknowledgments.

12.2.5.2 Integration with the logging and recording system shall be verified, including synchronized replay of audio, video, and screen actions from the dispatch interface.

12.2.5.3 Dispatch Console performance shall be verified under degraded and high-load conditions, including network congestion and partial subsystem failures.

12.2.5.4 User authentication, access control roles, and profile switching shall be tested against role-based operational scenarios (e.g., OCC controller vs. emergency coordinator).

12.2.6 **High-Speed Mobility Testing**

12.2.6.1 The FRMCS system shall be tested onboard trains operating at speeds up to 220 mph (354 km/h) to verify service continuity and performance during high-mobility conditions.

Handover testing shall include:

- Inter-gNB handovers under varying signal conditions;
- Seamless call continuity during transitions;
- MCX session continuity and bearer switching;
- Failure scenarios including handover rejections and cell edge dropouts.

12.2.6.2 End-to-end latency, jitter, and throughput shall be measured during train movement, with particular attention to:

- Voice call MOS scores;
- Video streaming stability;
- Packet loss in data sessions.

12.2.6.3 Drive testing shall capture RF metrics (RSRP, SINR, RSRQ), logged GPS data, and session KPIs to validate radio design assumptions.

12.2.6.4 All high-speed testing shall be correlated with Dispatch Console visibility and call control feedback to confirm end-to-end system integrity during mobility scenarios.

12.3 Specific Requirements for ETCS

12.3.1 For the purpose of validating ETCS performance, the TSCC Contractor shall ensure compliance with the minimum requirements specified in the applicable Control-Command and Signaling Technical Specification for Interoperability (CCS TSI), including Commission Implementing Regulation (EU) 2023/1695 and any subsequent versions. These requirements shall include all functionalities required for FRMCS to support a fully operational ETCS Level 2 train control system.

12.4 Specific Requirements for PWS

12.4.1 The TSCC Contractor shall perform comprehensive testing of the Passenger Wi-Fi System (PWS) to validate that all components meet the specified functional, performance, and integration requirements under normal, and peak-load conditions. Testing shall be conducted in accordance with the approved Test and Commissioning Plan and shall include both onboard trainsets and fixed infrastructure (e.g., stations, depots).

12.4.2 **Functional Testing**

12.4.2.1 Testing shall confirm successful user access to the Wi-Fi network, including:

- Captive portal operation;
- Users shall be able to establish an initial connection and access the internet within 30 seconds of selecting the Wi-Fi network
- Tiered service access (e.g., complimentary and premium);
- Multiple payment and purchase options;
- Authentication and session management, including federated identity.

12.4.2.2 All access control and security features shall be tested, including:

- WPA3 encryption enforcement;
- SSID segmentation between passenger and operational networks;
- Role-based access and traffic isolation.

12.4.2.3 Session continuity shall be tested for roaming users between carriages whilst in motion.

12.4.3 **Performance Testing**

12.4.3.1 Throughput, latency, and packet loss shall be measured at multiple access points under varying load conditions to verify compliance with the specified performance levels for each service tier.

12.4.3.2 Load testing shall simulate concurrent user access (minimum and maximum expected users per carriage and per station) to assess system scalability and service degradation behavior.

12.4.3.3 QoS enforcement for premium vs. complimentary users shall be validated under network congestion scenarios.

12.4.4 **Backhaul and Network Integration Testing**

12.4.4.1 The PWS backhaul link (e.g., mmWave, 5G, satellite, or hybrid) shall be tested for:

- Uplink and downlink performance
- Seamless handover between backhaul technologies (if applicable)
- WAN bonding or aggregation behavior (if implemented)

12.4.4.2 The interface between the PWS and the WCS or shared backhaul infrastructure shall be tested to verify traffic segregation, prioritization, and compliance with defined bandwidth allocations.

12.4.4.3 Redundancy and failover scenarios for backhaul links shall be tested to confirm service continuity or graceful degradation.

12.4.5 **Access Point and Hardware Validation**

12.4.5.1 Access point installation shall be physically inspected and tested for:

- Signal coverage throughout the passenger areas;
- Antenna placement compliance;
- Interference and overlap management.

12.4.5.2 Environmental conditions (e.g., vibration, temperature) shall be validated for compliance with rail-grade hardware standards.

12.4.6 **Integration and Monitoring**

12.4.6.1 Integration with the Passenger Portal, CRM systems (if applicable), and payment gateway shall be tested, including:

- Session tracking;
- Transaction processing for premium access;
- Usage data collection and reporting.

12.4.7 The TSCC Contractor shall verify end-to-end monitoring of PWS infrastructure, including SNMP polling, alarms, and dashboard visibility through the central Network Management System (NMS) or equivalent platform.

13 SUBMITTALS

13.1 General Requirements

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

14 QUALITY MANAGEMENT

14.1 General Requirements

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

15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

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

16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.