Schedule 5(c)

Electronic Access Control System (EACS)

California High-Speed Rail Authority

Standard Specifications

TSCC Specifications

SPEC-0007 – Electronic Access Control System (EACS)

Rev. 0.0

Authored:	Harshal Jadhav, Telecom System Lead	23 December 2025 Date
Checked:	Thomas Newey, Telecoms Lead	12/23/2025 Date
Checked:	Bruno Comperat, Deputy Director of Rail Engineering	12/123/2025 Date
Approved:	Ryan Scott, Director of Rail Engineering	12/23/2025 Date
Released:	Amit Joshi, Configuration Manager	12/23/2025 Date

Document Revision History – EACS Specifications

Second Edition

December 2025

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

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Scope of the Technical Specification

1.1.1 The scope of this Technical Specification is to define the Authority's Requirements for the Electronic Access Control System (EACS) system, hereinafter: EACS.

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

1.1.3 The functional architecture of the EACS is presented in Appendix A.

- "**Shall**": Indicates a mandatory requirement that must be strictly implemented; a waiver from a mandatory requirement is permissible only with approval of a design variance.
- "**Should**": Indicates a preferred course of action; a design variance is not required if it is not exercised.
- "**Must**": Indicates an obligation or a mandatory requirement.
- "**May**": Indicates a permissible course of action within the limits of the standards; a design variance is not required if it is not exercised.

2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

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

2.2 Design Guidelines

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

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

TABLE 8 DESIGN GUIDELINES

2.3 TSI

2.3.1 Not applicable for the EACS

2.4 Standards

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

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

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

TABLE 9 LIST OF APPLICABLE STANDARDS

2.5 Other Documents

2.5.1 The following other documents shall be referred:

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

TABLE 10 OTHER DOCUMENTS

3 TERMS, DEFINITIONS, AND ABBREVIATIONS

3.1 Terms, Definitions and Abbreviations

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

4 SYSTEM DESCRIPTION

4.1 Purpose of the EACS

4.1.1 The TSCC Contractor shall supply an Electronic Access Control System (EACS) that provides centralized, secure, and auditable control of physical access to all CHSR-managed facilities and assets, supporting NFPA 72 and NFPA 101 life-safety egress requirements during emergency evacuations.

4.1.2 The TSCC Contractor shall supply the EACS to deter and detect unauthorized entry by combining credential-based authentication with intrusion detection and alarm management, in alignment with the CHSR Operational Concept Document.

4.1.3 The TSCC Contractor shall supply the EACS to deliver real-time monitoring and reporting of all access and intrusion events, enabling timely response to security incidents.

4.1.4 The TSCC Contractor shall supply the EACS to support peak-load scenarios—such as simultaneous badge presentations during shift changes—with credential-validation latency and event-throughput performance as defined in Section 5.5 of this document

4.2 EACS System Definition

4.2.1 The EACS is a networked security solution that provides centralized management, monitoring, intrusion detection, and control of physical access to CHSR infrastructure and facilities designated as EACS Protected Areas. The EACS comprises electronic locks, access control devices (e.g. RFID readers, keypads, biometric scanners), control panels, communication interfaces, and a central management platform. It authenticates personnel, logs all access events, generates alarms and integrates with security and operational systems to support asset protection, regulatory compliance, and safe railway operations.

4.2.2 The EACS shall be a state-of-the-art microprocessor-based, software-controlled automatic system with necessary programming functions, annunciation, self-test, and controls.

4.3 EACS System Operational Context

4.3.1 The TSCC Contractor shall supply the EACS to operate continuously, 24 hours per day, 7 days per week, across all CHSR facilities, including stations, depots, shelters, train control rooms, trackside cabinets, and control center—and to integrate with the CHSR Asset Management System for maintenance workflows.

4.3.2 The TSCC Contractor shall supply the EACS to enforce access policies autonomously at field controllers if central communications are interrupted, queuing all events locally for later synchronization.

4.3.3 The TSCC Contractor shall demonstrate the EACS's functionality through the following operational scenarios:

- Routine Access: A valid credential presented at a field reader is authenticated by the local controller (even if offline), the door unlocks, and the event is logged centrally upon reconnection.
- Tailgating Prevention: A second credential presented at a dual-reader portal without a corresponding egress event triggers a local alarm and immediate notification to the Security Operator console.
- Emergency Evacuation: Upon receipt of a verified fire-alarm signal, the EACS automatically releases all egress doors, inhibits entry devices, and logs evacuation-mode activations in accordance with NFPA 101 and NFPA 72.

4.3.4 The TSCC Contractor shall supply the EACS to support phased roll-out and incremental commissioning, enabling new sites to be commissioned without impacting existing operations.

4.3.5 The TSCC Contractor shall supply integration details for other systems (e.g., Asset Management System, CCTV, Fire Protection) in Section 6 of this document.

4.4 Design Life

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

4.4.2 The design life requirements of the EACS shall allow for the pertinent evolution and technological change of the EACS throughout its life to ensure it remains fit for purpose.

4.4.3 The TSCC Contractor shall ensure EACS components with shorter design lifespans shall be managed by scheduled technology refresh strategies and spares management plans.

4.4.4 The TSCC Contractor shall ensure that the manufacturers will be able to produce EACS system components (with equal or compatible technical specifications) for the entire design life required.

5 SYSTEM REQUIREMENTS

5.1 General Requirements

5.1.1 Scope of Contractor's Responsibility

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

5.1.2 Risk Assessment for Protected Areas

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

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

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

5.1.3 Control & Monitoring Workstations

5.1.3.1 The TSCC Contractor shall use the Integrated Control and Supervision System (ICSS) Workstation as the primary console for all routine EACS control and real-time monitoring functions.

5.1.3.2 The TSCC Contractor shall ensure compatibility and integration of the EACS with the ICSS Workstation to provide the full feature set of control and monitoring functionality.

5.1.3.3 The TSCC Contractor shall supply a dedicated Administrative Workstation—physically and logically separated from ICSS and Security Operator consoles—through which O&M personnel may add, modify, or remove user accounts and credentials following defined, multi-level approval workflows.

5.1.4 **Physical Access Control of Protected Areas**

5.1.4.1 The TSCC Contractor shall lock and control, via the EACS, every access gate along the CHSR right-of-way, including maintenance-and-service personnel (pedestrian) and vehicular gates. The TSCC Contractor's EACS Risk Assessment shall cover all such gates and define appropriate protection levels.

5.1.4.2 The TSCC Contractor shall install the EACS at every designated EACS Protected Area to manage authorized access for routine operations, task-specific activities, and emergency egress.

5.1.4.3 The TSCC Contractor shall protect any system assets located off the right-of-way with EACS, in accordance with the approved risk assessment.

5.1.4.4 The TSCC Contractor shall equip each protected door, window, or opening within EACS Protected Areas with a surface-electromagnetic lock operated by the local EACS control unit.

5.1.4.5 The TSCC Contractor shall ensure all protected doors remain locked when not in use and are monitored by motion-and-request-to-exit sensor circuits that incorporate multiple sensing technologies (not solely passive infrared).

5.1.4.6 The TSCC Contractor shall deploy local EACS control units within each Protected Area, including OCC buildings, stations, depots, maintenance and train-care facilities, traction-power and solar sites, and wayside locations.

5.1.5 **Power and data Resilience**

5.1.5.1 The TSCC Contractor shall support each local EACS control unit with a battery backup sufficient for at least 30 minutes of continuous operation during a power outage and generate alarm notifications to the ICSS Operator when operating on backup.

5.1.5.2 The TSCC Contractor shall provide automatic data-backup functionality so that data and event logs are backed up before being overwritten. Log-file storage capacity shall cover at least one month of events, with a notification issued to the ICSS Operator when storage utilization reaches 90 percent.

5.1.6 **Server Redundancy & Cybersecurity Compliance**

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

5.2 Environmental Conditions Requirements

5.2.1 **Environmental Resilience**

5.2.1.1 The TSCC Contractor shall design and supply the EACS to be resilient to the full range of local environmental and climatic conditions at each installation site, as defined in the CHSR Environmental Specification, including temperature extremes, solar exposure, humidity variations, and salt spray (where applicable).

5.2.1.2 The TSCC Contractor shall ensure all EACS equipment operates satisfactorily under normal usage conditions, including diurnal and seasonal fluctuations.

5.2.2 **Ingress protection**

5.2.2.1 The TSCC Contractor shall supply outdoor EACS enclosures with a minimum ingress-protection rating of IP66.

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

5.2.3 **Mechanical Durability**

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

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

5.3 Operational Requirements for EACS

5.3.1 Operational Compliance

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

5.3.2 Operational Modes and Availability

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

- Normal
- Off-Hours
- Lockdown
- Maintenance.

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

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

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

5.3.3 Remote Monitoring and Control

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

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

5.3.4 Maintenance Access Support

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

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

5.3.5 Security Continuity and Failover

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

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

5.4 Functional Requirements for EACS

5.4.1 General System Functions

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

5.4.1.2 The TSCC Contractor shall supply the EACS to detect and report the status (open/closed) of every protected door.

5.4.1.3 The TSCC Contractor shall supply the EACS to uniquely address and identify every sensor and device.

5.4.1.4 The TSCC Contractor shall supply the EACS to provide comprehensive reporting in multiple formats (Word, Excel, PDF) with user-defined filters. Example reports shall include, but not be limited to:

- **Daily Access Summary:** Total number of granted and denied entries per door, per credential type, and per user group.
- **Unauthorized Access Log:** Detailed list of all access-denied events, forced-door activations, tailgating incidents, and tamper alarms.
- **User Activity Report:** Individual credential usage history over a specified period, showing access times, locations, and authentication devices.
- **Blacklist Report:** Current list of revoked, expired, or stolen credentials, including revocation timestamps and responsible administrator.
- **Maintenance Mode Audit:** Record of all Maintenance Mode activations, including user identity, start/end times, and affected areas.
- **Alarm Trend Analysis:** Aggregated alarm counts by severity and type, with time-series charts to identify hotspots and peak periods.
- **User Provisioning & Deprovisioning Audit:** Monthly tally of user adds, moves, and drops, including special-role assignments (admins, emergency responders), to verify adherence to least-privilege principles.
- **Credential Lifecycle Report:** Summary of credential enrolments, expirations, revocations, and role-based assignments over the past month, highlighting any abnormal spikes (e.g. mass expirations).
- **Incident Response Activity Report:** Details of all security incidents simulated or real (e.g., tailgating events, forced-door alarms), response times, actions taken, and closure status.
- **Configuration Change Log:** Chronological record of all approved configuration changes (who changed what, when, and why), tied back to the Change Request IDs and approval signatures.

5.4.1.5 The TSCC Contractor shall supply the EACS to notify the ICSS Operator of any loss or recovery of communications between local control units and the ICSS (including control-unit failures).

5.4.1.6 The TSCC Contractor shall supply the EACS so that, when in local maintenance mode, all other system functions remain fully operational.

5.4.1.7 The TSCC Contractor shall supply the EACS to provide comprehensive reporting—Access, Event, Activity, and Blacklist Reports—in multiple formats (Word, Excel, PDF) with user-defined filters.

5.4.1.8 The TSCC Contractor shall supply the EACS with an optional time-attendance module for selected doors, subject to the Authority's approval.

5.4.1.9 The TSCC Contractor shall supply central servers with fully redundant master/secondary configurations, ensuring automatic failover of the secondary server upon primary-server malfunction.

5.4.2 **Access Control Functions**

5.4.2.1 The TSCC Contractor shall supply the EACS to grant access to EACS Protected Areas only to authorized personnel.

5.4.2.2 The TSCC Contractor shall supply the EACS to restrict and deny access to unauthorized personnel.

5.4.2.3 The TSCC Contractor shall supply the EACS to monitor in real time all access attempts—both authorized and unauthorized—to EACS Protected Areas.

5.4.2.4 The TSCC Contractor shall supply the EACS to generate alarms for any unauthorized access attempts.

5.4.2.5 The TSCC Contractor shall supply the EACS to detect and report fraudulent access events, including forced-door openings, held-open doors, tampering, and credential-denied presentations.

5.4.2.6 The TSCC Contractor shall ensure each access-control event or alarm record includes:

- Date and time of the event
- Event type
- Event location
- Credential or user reference
- Authentication device used
- Authorization result (and cause if denied)
- Failure type (if applicable)
- Alarm severity
- Acknowledgement state.

5.4.2.7 The TSCC Contractor shall supply the EACS to log all personnel access to Protected Areas, including:

- Identity of the individual(s) gaining access
- Relationship of the individual(s) to the equipment accessed
- Identity of any person granting or escorting access, including third-party contractors

5.4.2.8 The TSCC Contractor shall supply the EACS so that, once authenticated, personnel must pass through the protected door within a configurable timeout; otherwise, the door shall re-lock.

5.4.2.9 The TSCC Contractor shall supply the EACS to provide manual override, lock, and unlock capabilities for protected doors, including scheduled override times.

5.4.2.10 The TSCC Contractor shall supply the EACS to continuously supervise lock and reader health and report any device failures.

5.4.2.11 The TSCC Contractor shall supply the EACS so that, in the event of a local control-unit failure:

- No new authentications are accepted
- Controlled doors remain locked.

5.4.2.12 The TSCC Contractor shall supply the EACS so that, in the event of a power outage, local control units continue operating on battery backup for at least 30 minutes.

5.4.2.13 The TSCC Contractor shall supply the EACS so that, in the event of communications loss between readers and the local control unit, no new authentications are accepted.

5.4.2.14 The TSCC Contractor shall supply the EACS so that, in the event of a reader failure:

- Controlled doors remain locked
- Other readers and functions are unaffected

5.4.2.15 The TSCC Contractor shall supply the EACS so that local control units automatically reconnect and upload locally logged events once normal communications resume.

5.4.2.16 The TSCC Contractor shall supply the EACS readers to automatically reconnect and forward buffered logs when communications are restored.

5.4.2.17 The TSCC Contractor shall supply each protected door with an emergency-door-release mechanism (inside the Protected Area) to manually unlock the door in case of emergency.

5.4.2.18 The TSCC Contractor shall supply each local control unit with sufficient I/O and reader ports to manage all protected doors within its Protected Area.

5.4.3 **Intrusion Detection Functions**

5.4.3.1 The TSCC Contractor shall supply the EACS to monitor intrusion sensors within each Protected Area.

5.4.3.2 The TSCC Contractor shall supply the EACS to report any intrusion alarms in real time.

5.4.3.3 The TSCC Contractor shall supply the EACS to detect and alert on unauthorized attempts to breach doors, windows, fences, or interior motion—bookmarking events for OCC staff.

5.4.3.4 The TSCC Contractor shall ensure each intrusion event or alarm record includes:

- Date and time of the event
- Event type
- Event location
- Sensor reference
- Failure type (if applicable)
- Alarm severity
- Acknowledgement state

5.4.3.5 The TSCC Contractor shall supply the EACS so that intrusion-sensor inputs to local control units use dry contacts or I/O relays.

5.5 Performance Requirements for EACS

5.5.1 General Performance Requirements

5.5.1.1 The TSCC Contractor shall supply local EACS control units sized to manage the number of intrusion and access points determined by the approved EACS Risk Assessment for each facility type (OCC buildings, stations, depots, maintenance and train-care facilities, traction-power facilities and solar sites, wayside facilities, and related fenced areas).

5.5.1.2 The TSCC Contractor shall assess the proposed subsystem architecture and define a local-archiving retention period that meets the Authority's audit and operational needs and shall configure each local control unit to archive the requisite volume of events without data loss.

5.5.1.3 The TSCC Contractor shall supply credential-reader hardware and firmware such that the access-card response time does not exceed 300 ms, measured from card presentation in the reader field to the grant/deny indication.

5.5.1.4 The TSCC Contractor shall install and configure credential readers to reliably detect cards placed no more than 50 mm from the reader surface. The magnetic or mechanical door sensors shall operate correctly with an actual door-gap of 5 mm ± 2 mm.

5.5.1.5 The electromagnetic locks and strike plates shall be installed with an alignment tolerance of ± 2 mm in two axes to maintain proper holding force.

5.5.2 Peak Concurrency

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

5.5.3 Event-Processing Throughput

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

5.5.4 Local-Archive Capacity & RTO/RPO

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

5.5.5 System-Health Monitoring Under Load

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

5.5.6 **Failover & Recovery Drills**

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

5.5.7 **Safety Requirements**

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

5.5.8 **RAM Requirements**

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

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

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

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

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

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

5.6 Cybersecurity and Security Requirements

5.6.1 **General Requirement**

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

5.6.2 **EACS- Specific Security Controls**

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

5.6.3 **Encrypted Reader–Panel Communications:**

5.6.3.1 All reader–controller links shall use a supervised protocol (e.g., OSDP Secure Channel v2 or equivalent), with session keys rotated at least daily.

5.6.4 **Network Encryption**

5.6.4.1 All IP-based traffic (controllers↔servers, workstations↔servers, mobile-credential interfaces) shall employ TLS 1.3, with certificates issued and managed by the CHSR OT PKI in accordance with FIPS 140-2/ISO 27001.

5.6.5 **Credential Lifecycle Audit**

5.6.5.1 All credential operations (enrollment, renewal, suspension, revocation) shall be logged in real time and forwarded in a standardized format (CEF or JSON) to the OT SIEM.

5.6.6 **Firmware Integrity**

5.6.6.1 All firmware images for controllers, readers, and sensors shall be digitally signed; the system shall verify each signature before installation.

5.6.7 **Key Management**

5.6.7.1 All cryptographic keys shall be generated, stored, and used within a FIPS 140-2 Level 2+ HSM (or equivalent), with at least annual key rotation and formal emergency-revocation procedures.

5.6.8 **Automated Isolation**

5.6.8.1 Upon detection of a high-severity security event (e.g., panel compromise, credential theft), the EACS shall automatically isolate affected field controllers through configurable OT-zone firewall rules.

5.6.9 **Extended Log Retention**

5.6.9.1 Audit-log retention shall meet or exceed the Cybersecurity Technical Specification, with access-control and intrusion logs retained for a minimum of three years per The Authority's Records Management Plan.

5.6.10 **Reporting and Assurance**

5.6.10.1 The TSCC Contractor shall submit quarterly Security Assurance Reports for the EACS, detailing patch status, vulnerability-scan results, key-rotation logs, and incident metrics.

5.6.10.2 The TSCC Contractor shall arrange an annual independent security audit—addressing encrypted channels, HSM usage, log integrity, and credential workflows—with findings and corrective-action plans delivered to the Authority.

5.6.11 **Integration with OT Cybersecurity Platform**

5.6.11.1 The EACS shall forward all security events, system-health alarms, and audit logs to the CHSR OT cybersecurity platform over encrypted channels for correlation, alerting, and long-term archival.

5.6.11.2 The EACS shall consume threat-intelligence feeds (e.g., blacklisted credential IDs, revoked certificates) via secure REST APIs and automatically quarantine or revoke affected credentials or panels.

6 INTERFACES REQUIREMENTS

6.1 General Requirements

6.1.1 Interfaces are classified as below:

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

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

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

6.2 External Interface – stations contractors

6.2.1 **TSCC EACS equipment integration in stations**

6.2.1.1 The TSCC Contractor shall provide to the station contractors:

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

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

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

6.2.2 **External Interface – facilities FPS system**

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

6.3 External Interface – facilities contractors

6.3.1 **EACS equipment integration in facilities**

6.3.1.1 The TSCC Contractor shall provide to the facilities contractor:

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

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

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

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

6.3.2 **External Interface – facilities FPS system**

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

6.4 Internal Interface

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

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

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

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

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

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

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

6.4.4 **Interface with CCTV System**

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

6.4.5 **Interface with traction substations and shelters**

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

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

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

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

6.4.7 **Interface with Low Voltage Power System**

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

7 MATERIALS, PRODUCT AND COMPONENTS REQUIREMENTS

7.1 General Requirements

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

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

7.1.3 The TSCC Contractor shall supply all power- and signal-distribution cabling as low-toxicity, low-smoke, zero-halogen, fire-retardant construction.

7.1.4 The EACS shall be complete with all equipment, supporting structures, hardware, licenses, software, cabling, and ancillary services which are useful for efficient operation of the EACS components. Such accessories and materials shall be deemed to be within the scope of this specification, whether specifically mentioned or not.

7.1.5 All special tools and test equipment intended for configuration of the EACS shall be deemed to be within the scope of this specification, whether specifically mentioned or not.

7.2 SW and HW Requirements

7.2.1 **Hardware requirements**

7.2.1.1 All cables shall be fire and flame retardant, halogen-free, non-corrosive, etc., in accordance with local applicable Laws.

7.2.1.2 Detailed cable routing and labelling plans shall be delivered by the TSCC Contractor.

7.2.1.3 The TSCC Contractor's design for all central servers shall be on-premises, either physical, virtualized, or cloud-based, to facilitate system evolution and comply with cybersecurity requirements.

7.2.1.4 Hardware, software, firmware, or data changes required to support future extensions or expansions on-line shall be accomplished without performance or functionality degradation or availability to the operational systems.

7.2.1.5 The structured cabling shall be certified according to the latest applicable standards in this regard.

7.2.1.6 The structured cabling cables shall be compliant with (not limited to):

- CAT6A cables shall comply with IEC 61156-5 CAT6A.
- CAT7A cables shall comply with IEC 61156-5 CAT7A.
- Cables' flame retardancy shall comply with IEC 60332-1. Indoor cables shall withstand 120 minutes.
- Cables shall be halogen-free (HFFR) and shall comply with IEC 60754-2.
- Cables evaporated smoke density under burning conditions shall comply with IEC 61034.
- CAT6A/CAT7A patch cords shall be shielded.
- CAT6A/CAT7A patch cords shall be earthed and bonded.
- RJ45 molded connectors shall comply with IEC 11801.

7.2.1.7 Regarding the terminating and interconnecting equipment of the structured cabling it shall include (not limited to):

- termination protection devices
- distribution cabinets
- cross-connects
- cable trays and hangers
- CAT6A/CAT7A patch cords

7.2.1.8 Equipment Interfaces shall operate under IP with Ethernet RJ-45 and fiber connections.

7.2.1.9 LV electrical cables, control and communication cables for EACS shall be fire-rated.

7.2.1.10 The EACS equipment provided shall be expandable without requiring the replacement of existing equipment.

7.2.1.11 Hot-swappable elements, such as fans and power supplies, should be swappable without tools.

7.2.2 **Software Requirements**

7.2.2.1 The Operating of all the EACS devices shall be provided with the latest stable release.

7.2.2.2 All application software shall be upgraded to the latest stable release and shall support all the requirements specified. All software licenses shall be provided.

7.2.2.3 The EACS shall have an interface with the ICSS system (Integrated Control and Supervision System) for the functions dedicated to the control and monitoring of the EACS, i.e., Intrusion Detection, Access Control, and Archiving.

7.2.2.4 The TSCC Contractor shall provide the EACS software, which shall be a full-featured Security Management System software package.

7.2.2.5 The EACS software shall provide the administration function of the software, i.e., the creation, deletion, and configuration of accounts, sites, and Operators.

7.2.2.6 The EACS software configuration features shall gather all the functions dedicated to the creation and the configuration of the items related to the EACS: accounts, sites, schedules, readers, sensors, events archiving, dashboards, etc.

7.2.2.7 The EACS software shall provide an administration function for database management, including synchronization with local EACS control units and other functions such as edit, add, delete, search, sort, and print for EACS records and reports.

7.2.2.8 The EACS software shall be provided for the user administration responsible to ensure functionality related the user and user groups (for example, safety and security operator, head of security, IT administrator, users administrator, users, etc.) administration and management including levels of access rights by access location, time (day, time), user enrolment, user credentials (access cards, code keys, biometrics) management, i.e. their creation, configuration (including their credentials) or suspension; card personalization, etc.

7.2.2.9 User creation/suspension /deletion, modification of user credentials, activation/suspension /deactivation of the identification means associated with a user, and user profile assignment shall be performed at a central level.

7.2.2.10 EACS statuses (alarms and events) and modes of the EACS equipment shall be transmitted to the EACS software.

7.2.2.11 The EACS software shall display alarms and events in a list format and a graphical user interface (GUI), with the ability to export in multiple file types.

7.2.2.12 Control and monitoring of the EACS devices shall be provided (opening of EACS protected doors, arming or disarming an area, etc...) from the EACS software.

7.2.2.13 Control of the EACS device mode (operational, inhibition and maintenance) shall be provided from the EACS software.

7.2.2.14 Display of the operational status of any EACS device (in maintenance, inhibited, operational, out of service, etc.) shall be provided by the EACS software.

7.2.2.15 Display of the technical status of any EACS device (in service, isolated, in failure...) shall be provided by the EACS software.

7.2.2.16 Events archiving and reports yielding shall be provided by the EACS software.

7.2.2.17 Searching of the events or alarms history shall be ensured at least according to the following criteria:

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

7.2.2.18 The Operator shall be able to release an EACS protected door (temporary/permanently) from the EACS software.

7.2.2.19 The Operator shall be able to lock an EACS protected door (temporarily/permanently) from the EACS software.

7.2.2.20 The Operator shall be able to visualize the technical status of the EACS equipment from the EACS software.

7.2.2.21 The Operator shall be able to visualize and change the operational mode of the EACS equipment from the EACS software.

7.2.2.22 The Operator shall be able to visualize and acknowledge EACS alarms from the EACS software.

7.2.2.23 The Operator shall be able to visualize the EACS Protected Area layout in at least four levels: room, floor, perimeter, and railroad section.

7.2.2.24 The Operator shall be able to remotely arm/disarm an EACS Protected Area (or group of Protected Areas) from the EACS software.

7.2.2.25 The Operator shall receive an alarm when the emergency door release mechanism, if any, has been used (emergency exit is activated) on the EACS software.

7.2.2.26 The Operator shall be able to re-arm the emergency door release mechanism, if any, to reactivate the door lock.

7.2.2.27 The quantity of users allowed by the EACS software shall be agreed with the Authority.

7.3 EMC Requirements

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

7.3.2 The TSCC Contractor shall mitigate emissions and susceptibility through appropriate shielding, filtering, and grounding.

8 TOLERANCES

Not applicable to EACS.

9 SCOPE OF SUPPLY AND DELIVERY

9.1 General Requirements

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

9.2 Specific Requirements

9.2.1 The TSCC Contractor shall supply, deliver, and install all hardware, software, firmware, and ancillary items necessary to implement the complete EACS solution in accordance with this specification.

9.2.2 All supplied items shall be factory-new (unless otherwise agreed), fully compatible, factory-configured for plug-and-play deployment, and delivered with required licenses, certificates, and documentation.

9.2.3 The TSCC Contractor shall submit a detailed Bill of Materials for Authority review, covering quantities, part numbers, revisions, and supplier information, and shall update it to reflect any approved changes.

9.2.4 The EACS scope of supply and delivery shall include (not limited to):

- Central server(s) with database
- Local EACS control units.
- Software.
- Smart cards.
- Card reader
- Combined authentication devices (biometric + card + code key).
- Intrusion detection sensors (passive infrared, glass-break, vibration, door-position).
- Request-to-exit push buttons.
- Electromagnetic locks, strike plates.
- Emergency Door Release mechanisms
- Cabling and connectors.
- Racks.
- Full-featured Security Management System software suite, including Administration, Monitoring, Reporting, and Archiving modules
- Software architecture documentation, including a full definition of protocols used.
- Software licenses.
- Auxiliary elements, supporting structures, special tools and test equipment.
- Spare parts.
- Maintenance laptops.
- Dedicated Administrative workstation for user/credential management.

10 MANUFACTURING

10.1 General Requirements

10.1.1 General manufacturing requirements are defined in the Contract.

11 INSTALLATION AND INTEGRATION

11.1 General Requirements

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

11.2 System Integration Requirements

11.2.1 The TSCC Contractor shall integrate local controllers, central servers, and workstations into the CHSR OT network, enforcing VLAN segmentation, mutual-TLS, and OSDP Secure Channel.

11.2.2 The TSCC Contractor shall configure time synchronization (NTP/PTP) so that all EACS devices maintain clock drift within ±1 ms per 24 hours.

11.2.3 The TSCC Contractor shall import credential and user-group data via the Administrative Workstation, verify replication to all controllers within 5 minutes, and test login/logout workflows.

11.2.4 The TSCC Contractor shall integrate intrusion and access-control events with the ICSS Workstation, CCTV, Fire Protection, and OT SIEM, executing positive and negative test cases.

11.2.5 The TSCC Contractor shall implement tamper-detection and chain-of-custody procedures for cryptographic keys and HSM modules during installation, in line with the Cybersecurity Technical Specification.

12 TESTING & ACCEPTANCE

12.1 General Requirements

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

12.2 Specific Requirements

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

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

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

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

13 SUBMITTALS

13.1 General Requirements

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

14 QUALITY MANAGEMENT

14.1 General Requirements

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

15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

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

16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.