Schedule 5(d)

Enterprise Asset Management System (EAMS)

California High-Speed Rail Authority

Standard Specifications

TSCC Specifications

SPEC-0008 – Enterprise Asset Management System (EAMS)

Rev. 1.0

Authored:	Vincent Decanter, TCS Engineer	12/22/2025 Date
Checked:	Thomas Newey, Telecom Lead	12/22/2025 Date
Checked:	Bruno Comperat, Deputy Director of Rail Engineering	12/23/2025 Date
Approved:	Ryan Scott, Director of Rail Engineering	12/23/2025 Date
Released:		12/23/2025

Amit Joshi, Configuration Manager Date

Document Revision History – EAMS Specifications

Second Edition

December 2025

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

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Scope of the technical specification

1.1.1 The scope of this Technical Specification is to define The Authority's Requirements for the Enterprise Asset Management System, hereinafter: **EAMS**.

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

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

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

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

2 REFERENCE STANDARDS AND DOCUMENTS

2.1 General

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

2.1.2 All generic standards to be used are provided in: Contract Technical Requirements – Scope of Work.

2.2 Standards

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

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

TABLE 1 - LIST OF APPLICABLE STANDARDS

2.2.2 The EAMS shall support the California HSR program's alignment with ISO 55001 principles and UIC best practices for asset management. These principles include value realization, leadership and accountability, risk-based decision making, and continual improvement across the asset lifecycle. The EAMS shall also support The Authority's strategic asset objectives and enable evidence-based decision making.

2.2.3 In the event of any conflict, inconsistency, or ambiguity between the requirements set out in this specification and those in other applicable documents or standards, the resolution of such conflicts shall be determined by the Authority. The TSCC Contractor shall seek clarification in writing and shall not proceed on assumptions. The Authority's determination shall be final and binding

3 TERMS, DEFINITION, AND ABBREVIATION

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

4 SYSTEM DESCRIPTION

4.1 Purpose of the EAMS

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

4.1.2 The EAMS shall provide mechanisms to measure alignment between asset performance and organizational objectives, enabling data-driven governance and strategic asset planning.

4.2 EAMS Definition

4.2.1 The California High Speed Rail (CHSR) Authority's EAMS shall be a systematic management framework for the governance of the assets value, with the purpose of establishing the asset management plan and asset management objectives.

4.2.2 The EAMS shall apply to both tangible items that have potential or actual value, such as buildings, equipment or human resources, and intangible assets, such as digital twins, configuration baselines, human capital, intellectual property, goodwill, financial assets, or software licenses.

4.2.3 Intangible assets (e.g., configuration baselines, software licenses, digital twins, human capital) shall be modeled as metadata entries or linked data objects, integrated with relevant systems such:

- Building Information Model (BIM)
- Geographic Information System (GIS)
- Electronic Document Management System (EDMS)
- Enterprise Resource Planning (ERP)
- Traffic Management System (TMS)
- Integrated Control and Supervision System (ICSS)
- Power SCADA System
- Monitoring and configuration systems of the various CHSR systems
- Building Management Systems
- HR platforms
- Cybersecurity systems
- Financial systems

4.2.4 The EAMS shall support the setting and monitoring of asset management objectives, risk-based decision support, and continual improvement, as part of the CHSR's broader asset management plan framework.

4.2.5 The internal processes and activities conducted within the EAMS shall be associated with the organizational strategy, relying on the entire organization, regardless of the hierarchy level.

4.2.6 The EAMS shall identify and maintain the relationships between assets and their associated documentation, configurations, version history, and dependency structures, particularly for modular or software-intensive systems.

4.3 EAMS Operational Context

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

4.3.2 EAMS shall provide the ability to manage assets in such a way that they contribute to the successful operation of CHSR, by delivering the expected level of operational performance reliably, efficiently, and sustainably. The main EAMS stakeholders are the operators and maintenance staff.

4.3.3 The EAMS shall support secure, role-based interaction across all relevant stakeholders, including operators, maintenance contractors, the Authority, suppliers, and the wider supply chain.

4.3.4 The EAMS architecture shall be designed with clearly defined functional boundaries and responsibilities for data ownership and exchange with adjacent systems. These definitions shall include documented integration mechanisms, and interface specifications.

4.3.5 The EAMS shall define and document its functional boundaries relative to external systems.

4.3.6 The EAMS shall include multi-role support with configurable user access levels, ensuring that operators, maintenance contractors, and the Authority have appropriate permissions and role-based workflows. Generic or shared user accounts shall not be permitted; each user shall authenticate using unique credentials and be granted the minimum necessary privileges. Access control measures shall be implemented in full compliance with the *TSCC System Technical Specification - Cybersecurity*.

4.4 Design Life

4.4.1 The Design Life requirements of the Asset Management System shall be 15 years, aligned with the lifecycle expectations of California HSR infrastructure systems

4.4.2 The TSCC Contractor shall ensure that the manufacturers shall be able to supply EAMS components with equal or better technical specifications, throughout the required operational lifetime, recognizing the potential for successive generations and evolving sensor technology.

4.4.3 The EAMS design shall include a long-term support and evolution roadmap, demonstrating how hardware and software components will be maintained, upgraded, or replaced over the design life. This shall include:

- Plans for ongoing software and hardware support, data continuity, backward compatibility, and migration paths
- Scheduled refresh strategies and spares management plans for components with shorter inherent lifespans (e.g., field devices, handhelds)
- The ability to integrate any replacement components with equal or better technical specifications elements into the existing EAMS architecture and dependent subsystems without requiring modifications aside from the item being replaced.

4.4.4 The design life shall be supported through a combination of hardware refresh planning, software version upgradeability, vendor support agreements, obsolescence management, and data migration strategies. Static system configurations shall not be assumed beyond five years without formal review and validation by the Authority.

4.4.5 The TSCC Contractor shall ensure that software and data formats remain interoperable with future technologies and shall provide backward compatibility or migration tools as part of system upgrades.

4.4.6 End-of-life planning shall be incorporated into the EAMS architecture, including secure data archiving, handover protocols, and licensing continuity provisions.

5 SYSTEM REQUIREMENT

5.1 General Requirements

5.1.1 The Enterprise Asset Management System shall be designed in accordance with the requirements described in this specification, and other relevant documents listed in Section 2 and the Scope of Work.

5.1.2 The EAMS architecture shall be designed to support maintenance, repair workflows, decision-making, data analysis, system resilience, scalability and to manage costs. The TSCC Contractor shall ensure that the EAMS is properly integrated with all CHSR systems.

5.1.3 The EAMS shall be available in English. Multilingual support, including Spanish, should be considered based on operational and regulatory requirements defined by the Authority.

5.1.4 The EAMS software shall be tailored to workflow specified in *Figure 1*. The process shall be reviewed, developed, and improved to enhance the EAMS performance over time. Workflow configurations shall be customizable, version-controlled, and traceable within the EAMS to support lifecycle assurance, auditability, and maintainability.
Note: Data driven maintenance the EAMS workflow main stages shall be defined and developed as illustrated in *Figure 1*.

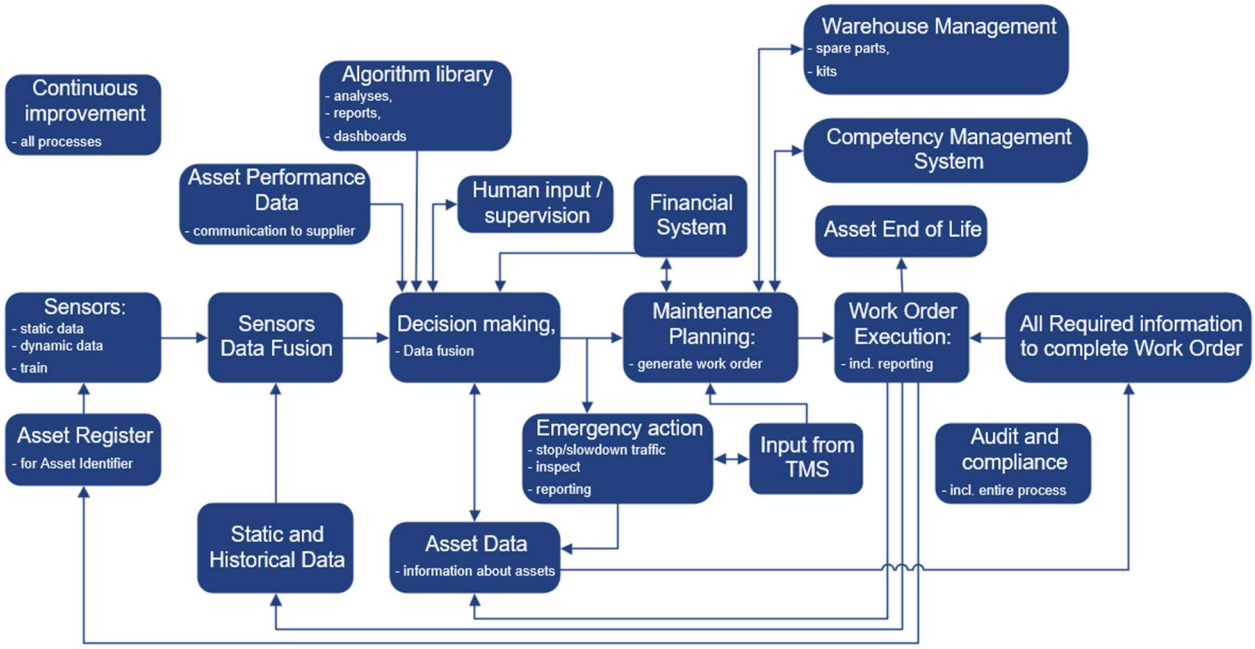

FIGURE 1 - EAMS DATA EXCHANGE WORKFLOW DIAGRAM

5.1.5 **Data Collection:**

5.1.5.1 Sensors shall provide:

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

5.1.6 **Sensors Data Fusion**

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

5.1.7 Decision-Making

5.1.7.1 The EAMS shall support decision-making using:

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

5.1.8 Maintenance Task Planning

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

5.1.9 Work Order Execution and Reporting

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

5.1.10 Asset Register

5.1.10.1 The EAMS shall maintain an authoritative asset identifier register.

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

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

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

5.1.13 Communication Protocols

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

5.1.13.2 The implemented protocols shall include, at a minimum:

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

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

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

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

- OPC Unified Architecture (OPC UA)

- MQTT and MQTT Sparkplug
- EULYNX.

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

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

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

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

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

5.1.13.9 Open standard shall not include proprietary or undocumented protocol.

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

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

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

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

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

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

5.1.14 **Asset Information**

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

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

5.1.14.2 The EAMS shall provide dashboards and reports on performance metrics such as uptime, response time, integration status, and data freshness, supporting SLA monitoring and operational diagnostics.

5.1.14.3 The EAMS shall provide user-configurable functions to filter, prioritize, and escalate alarms, enabling operators to automatically trigger service requests for specified asset classes or alarm types.

5.1.14.4 The EAMS shall update usage and operational metrics for all relevant assets and subassemblies.

5.1.14.5 The EAMS shall also be capable of transmitting relevant operational status data (e.g., maintenance status, asset availability) to maintain synchronization.

5.2 Environmental Requirements

5.2.1 The EAMS equipment shall meet the environmental requirements defined in Section *7* and any applicable standards listed in Section *2*, including IEC 60068 for environmental testing, and local regulatory requirements applicable to railway infrastructure in California.

5.2.2 The EAMS hardware (including servers, workstations, network devices, and field equipment) shall comply with defined environmental performance parameters including, but not limited to:

- Operating temperature range: –20°C to +55°C (unless otherwise specified by installation location)
- Storage temperature: –40°C to +70°C
- Relative humidity tolerance: 5% to 95% non-condensing
- Vibration resistance compliant with IEC 61373
- Shock resistance and mechanical durability for mobile/portable devices.

5.2.3 All EAMS equipment intended for outdoor or harsh environments shall have a minimum ingress protection rating of IP65 (per IEC 60529), and enclosures shall be resistant to dust, moisture, corrosion, and UV exposure.

5.2.4 EAMS components installed in passenger-accessible or safety-critical areas shall comply with EN 45545-2 fire protection standards, including limits on flammability, smoke emission, and toxicity of fumes.

5.2.5 The TSCC Contractor shall categorize EAMS hardware by installation environment (e.g., OCC, wayside, on-vehicle, depot, mobile/field) and apply environmental requirements accordingly, subject to review and approval by the Authority.

5.2.6 All EAMS devices and infrastructures shall maintain performance during its design life under defined environmental conditions, including resistance to thermal cycling, condensation, and vibration fatigue.

5.2.7 All EAMS hardware and associated components shall comply with environmental sustainability directives, including RoHS (Restriction of Hazardous Substances) and WEEE (Waste Electrical and Electronic Equipment) where applicable.

5.2.8 All EAMS-related equipment, including servers, handheld devices, network hardware, and embedded systems, shall comply with Electromagnetic Compatibility (EMC) requirements and meet the environmental requirements defined in ***Section 5.2***. Compliance shall be demonstrated in accordance with applicable standards, including but not limited to:

- IEC 61000-6-2 (Immunity for industrial environments)
- IEC 61000-6-4 (Emission for industrial environments)
- EN 50121 series (Railway applications – EMC)
- FCC Part 15, Subpart B (for digital devices in the United States).

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

5.2.9 All EAMS hardware components, including third-party integrations, shall conform to both emissions and immunity standards applicable to their installation environment (e.g., OCC, field cabinets, trainsets interfaces).

5.2.10 Where multiple standards apply (e.g., FCC and EN 50121), the more stringent requirement shall prevail unless otherwise agreed with The Authority.

5.2.11 The TSCC Contractor shall provide evidence of EMC compliance via certified lab test reports and declarations of conformity. Testing shall include both conducted and radiated emissions and immunity, verified under representative operating conditions.

5.3 Operational Requirements

5.3.1 The TSCC Contractor shall provide or support a maintenance organization, incorporating all required elements to enable condition-based and predictive maintenance strategies using EAMS data and workflows.

5.3.2 The TSCC Contractor shall determine the required EAMS capacity, **a**nd performance parameters, based on defined maintenance processes and system load expectations (e.g. number of assets, sensor inputs per second, user sessions, storage requirements). These capacity requirements shall be validated against the predictive maintenance strategy and future expansion scenarios**.**

5.3.3 The EAMS shall support continuous 24/7 operation and enable timely execution of all core system functions without degradation.

5.3.4 The TSCC Contractor shall define and implement the necessary redundancy, failover, and disaster recovery (DR) mechanisms—covering Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)—to satisfy these targets.

5.3.5 The EAMS shall minimize manual data entry by integrating data from sensors, Internal Interfaces, External Interfaces, and structured external sources. Where manual input is necessary, field validation and error reduction techniques shall be applied.

5.3.6 The EAMS shall include a monitoring dashboard displaying system status, uptime, data flows, fault conditions, integration status, and performance KPIs. The system shall support automated alerts and logs to assist operators in fault detection and recovery.

5.3.7 The EAMS shall integrate with existing support systems, including the IT Service Desk, and field maintenance teams. A clearly defined incident response and escalation procedure shall be documented for EAMS-related faults or failures.

5.3.8 The TSCC Contractor shall perform usability testing with representative users during HMI development to validate interface design, task efficiency, accessibility, and overall user experience.

5.3.9 The EAMS shall provide role-based HMI views and configurable dashboards tailored to different user profiles (e.g. maintenance engineer, operator, asset manager), with appropriate access controls as per the *TSCC System Technical Specification - Cybersecurity*.

5.3.10 The EAMS user interface (HMI) shall be designed in accordance with ISO 9241-210:2019 Ergonomics of human-system interaction, ensuring usability, efficiency, and accessibility. The interface shall comply with WCAG 2.1 Level AA accessibility standards and adopt best practices from the U.S. Web Design System

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

5.4 Functional Requirements

5.4.1 General Requirements

5.4.1.1 The EAMS shall embed a customizable logic and calculation engine, based on proven solutions from other railway projects. This engine shall support the configuration of user-defined rules, formulas, diagnostic workflows, and asset-specific models, enabling the development of:

- Specialized condition and performance monitoring logic
- Tools aligned with RAM (Reliability, Availability, Maintainability), RCM (Reliability-Centred Maintenance), FRACAS ((Failure Reporting, Analysis, and Corrective Action System), and lifecycle cost models.

5.4.1.2 A web-based HMI solution shall be implemented using scalable, standards-based web technologies (e.g. HTML5, RESTful APIs, JSON). Web servers shall host modular clients optimized for browser compatibility, responsive design, and centralized administration.

5.4.1.3 The EAMS shall support all required protocols for integration with alarm, telemetry, condition monitoring, and operational datasets across CHSR systems and third-party systems. It shall handle both real-time and historical data sources, with built-in support for timestamp validation, schema conformity, buffering, and event prioritization.

5.4.1.4 The EAMS shall allow authorized users to configure, test, and validate logical rules and workflows in a secure sandbox or test environment before production deployment. This environment shall support simulation with sample asset data.

5.4.1.5 All user-defined logic, dashboards, and HMI (Human Machine Interface) configurations shall be version-controlled and include audit logs for changes. Changes shall require approval or validation workflows defined by the Authority.

5.4.1.6 The EAMS HMI shall be accessible on desktops, tablets, and ruggedized field devices, and shall offer configurable role-based views for maintenance personnel, operators, engineers, and administrators.

5.4.1.7 The EAMS shall include Application Programming Interfaces (APIs) and plug-in frameworks to allow future extension of system functions, analytics, and third-party integrations. The API documentation shall be published, version-controlled, and accessible via a developer portal or equivalent interface.

5.4.1.8 The EAMS shall provide detailed system and data ingestion logs, including protocol status, data quality issues, event drops, and latency metrics. These logs shall be available for analysis, alerting, and troubleshooting.

5.4.2 EAMS Data Store

5.4.2.1 The EAMS Data Store shall be an organized, scalable, and secure collection of structured data and documentation for all CHRS assets.

5.4.2.2 The EAMS Data Store shall track, organize, and maintain asset-related information throughout the lifecycle, from acquisition and commissioning to decommissioning and disposal.

5.4.2.3 The EAMS Data Store shall ensure high-quality, highly available Asset Information to support performance, safety, maintenance, and analytical operations across all functional areas of the California High-Speed Rail system.

5.4.2.4 Each asset shall be assigned a unique identifier by the Asset Register. The EAMS shall interface with the Asset Register through a secure and synchronized API or data exchange process, ensuring up-to-date and consistent asset IDs and Asset Information.

5.4.2.5 The EAMS shall incorporate and organize all CHSR assets in a structure identical to the System Breakdown Structure (PBS) and corresponding maintenance plans, from the top system level to individual components.

5.4.2.6 Asset Information data structures and metadata models shall be standardized across asset types to enable consistent reporting, lifecycle analysis, and decision support across all EAMS modules.

5.4.2.7 The EAMS shall support import and export of structured data using formats compatible with commonly used text, presentation, and analytics software (e.g. CSV, XML, JSON, Excel, PDF).

5.4.2.8 The TSCC Contractor shall ensure real-time and batch-mode integration of the EAMS Data Store with CHSR systems, including support for automated data validation and error handling.

5.4.2.9 The EAMS Data Store shall include, but not be limited to, the following content types:

- Spare parts catalogues
- Product acceptance certificates
- As-built drawings and BIM models (linked to GIS)
- Direct linkages to California HSR GIS System
- RAM, RCM and FMEA
- Maintenance and repair history
- Installation and O&M manuals
- System identifiers
- Related documentation required for asset governance, operations, and assurance.

5.4.2.10 The EAMS Data Store shall retain and generate asset-related reports, including automatic and scheduled reports. The system shall support time-based queries and enable users to retrieve historic reports based on asset ID, report type, or time range.

5.4.2.11 All real-time and historical data shall be logically structured by asset and stored in a way that enables analysis at system, subsystem, or component levels. Data ingestion shall be timestamped and source tracked.

5.4.2.12 Information maintained in the EAMS Data Store shall include, but not be limited to:

- Static Asset Information Metadata, such as:
  - Unique asset ID
  - Asset type and classification
  - Asset name and description
  - Manufacturer and model
  - Serial number
  - Technical specifications
  - Acquisition date and cost
  - Warranty or guarantee terms
  - Asset condition/status (e.g., active, under repair, retired)
  - Physical location (coordinates, section ID, facility name)
  - Ownership and custodian information

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

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

5.4.2.13 The EAMS shall utilize a combination of relational, time-series, and unstructured data storage technologies, chosen based on the nature of the data (e.g., operational telemetry, documents, logs, structured records).

5.4.2.14 The EAMS Data Store shall include configurable data retention policies based on asset type, criticality, and regulatory requirements. These policies shall support both short-term operational use and long-term archiving (e.g., 25–30 years for critical infrastructure records).

5.4.2.15 The EAMS Data Store shall implement routine, automated backup and recovery mechanisms, with clearly defined recovery time objectives (RTO) and recovery point objectives (RPO). Backup status shall be monitored, and failures reported to operations teams.

5.4.2.16 The EAMS shall support tamper detection, version control, and cryptographic integrity checks (e.g., checksums, hash validation) for all stored data and documents. All changes shall be audit-logged and traceable.

5.4.2.17 The EAMS shall maintain bi-directional synchronization with external authoritative systems (e.g., GIS, Asset Register, EDMS) and resolve discrepancies using configurable reconciliation rules. Changes shall not result in silent data overwrites.

5.4.2.18 The EAMS Data Store shall be designed for performance at scale, supporting high-volume concurrent queries, indexing, and low-latency access for real-time data ingestion and dashboard displays.

5.4.3 Data Acquisition and Categorization

5.4.3.1 The EAMS shall acquire and integrate structured and unstructured data not only from subsystems but also from all CHSR assets as illustrated in Figure 2. The EAMS shall support multiple ingestion modes including real-time streaming, scheduled batch uploads, and API-based pull mechanisms. Integration security shall comply with the TSCC System Technical Specification - Cybersecurity.

5.4.3.2 The EAMS shall receive structured notifications from connected systems to generate dynamin Asset Information and alerts, with each notification containing, at a minimum:

- A unique registration number generated by EAMS or inherited from the source system
- Status (e.g., created, enriched, closed)
- Identification of the originating system (name or ID)
- A full timestamp (date, hour, minutes, and seconds)

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

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

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

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

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

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

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

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

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

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

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

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

5.4.4 Human Resources System data

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

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

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

5.4.4.2 Integration between the EAMS and HR systems shall use secure, standards-based APIs or data exchange interfaces, and enforce role-based access control to restrict access to sensitive personnel data in accordance with the TSCC System Technical Specification - Cybersecurity and applicable privacy regulations.

5.4.4.3 The EAMS shall incorporate shift calendars, approved leave, overtime limits, and applicable labor or union rules into the scheduling engine to ensure compliance with workplace agreements and personnel availability.

5.4.4.4 All staff assignment and scheduling decisions shall be logged, timestamped, and auditable, including override actions, system-suggested reassignments, and approvals by supervisory personnel.

5.4.4.5 The EAMS shall restrict the assignment of work orders to personnel with expired certifications, pending medical restrictions, or insufficient qualification levels, and alert supervisors to any such conflicts.

5.4.4.6 The EAMS shall support dynamic reassignment of tasks in real-time, enabling planners to respond to unavailability, shift changes, or emergency conditions without compromising compliance rules.

5.4.4.7 The system shall include dashboards and reporting tools to allow resource managers to monitor workload distribution, technician utilization, qualification coverage, and forecasted gaps.

5.4.5 **Mapping and 3D**

5.4.5.1 The EAMS shall integrate geographic and infrastructure data with the CHSR GIS and associated BIM models. This integration shall support visualization of infrastructure geometry, location-based asset data, and the graphical display of asset condition. The EAMS shall link to or embed BIM and GIS layers using open standards such as Industry Foundation Classes (IFC) for BIM and OGC-compliant formats (e.g., WMS, GeoJSON) for GIS.

5.4.5.2 The EAMS shall support interactive 2D/3D map views, including the ability to zoom, pan, filter, and select infrastructure elements or assets from within a GIS or BIM interface embedded in the EAMS HMI.

5.4.5.3 The EAMS shall support live overlay of asset condition data (e.g., alarms, health status, maintenance state) on the GIS/BIM display, using color-coded icons, heatmaps, or similar graphical representations.

5.4.5.4 Users shall be able to search for assets by location, facility, or map zone and filter displayed assets based on status, system, or priority.

5.4.5.5 The GIS and BIM integration shall comply with Schedule 4 – Digital Engineering Requirements and related interface requirements within this document suite.

5.4.5.6 The EAMS shall enforce secure access and user-specific permissions to GIS and BIM data layers in accordance with the TSCC System Technical Specification - Cybersecurity, especially for infrastructure locations that are operationally or security-sensitive.

5.4.6 Electronic Document Management System

5.4.6.1 The EAMS shall integrate an Electronic Document Management System (EDMS) module, either internal or external, to manage all asset-related documents. The EDMS shall support centralized storage, structured access, and lifecycle control for the following document types:

- Maintenance manuals
- Technical manuals
- Training materials
- Procedures and work instructions
- Engineering drawings and schematics
- Spare parts catalogs
- Operational rules and regulatory instructions
- Job aids and task checklists
- Safety instructions and incident response documents
- Regulatory compliance documents
- Work orders and associated reports
- Communication logs related to asset operations
- BIM models and linked GIS documents.

5.4.6.2 The EDMS shall be fully accessible through the EAMS interface and support contextual linking of documents to assets, systems, components, work orders, and maintenance records.

5.4.6.3 The EAMS shall provide configurable dashboards and user-specific views that enable users to retrieve linked documents based on asset, task, or system context. Information security controls, including role-based document access and action auditing, shall be implemented in accordance with the TSCC System Technical Specification - Cybersecurity.

5.4.6.4 The EDMS shall support document lifecycle management, including draft, approval, revision control, archive, and expiration status. Version metadata shall include document owner, version number, status, date modified, and approval history.

5.4.6.5 The EDMS shall enforce role-based access controls (RBAC) and document classification levels (e.g., public, internal, confidential). All document access and edits shall be logged with user ID, timestamp, and action.

5.4.6.6 The EDMS shall support advanced search and retrieval functions, including full-text indexing, filtering by metadata (e.g., asset ID, document type), and real-time query performance suitable for field operations.

5.4.6.7 The EDMS shall integrate with the EAMS Data Store, Asset Register, and BIM/GIS platforms to enable cross-referencing of documents to spatial models and asset hierarchies.

5.4.6.8 The EDMS shall support long-term archiving and retention of documents in accordance with applicable federal and California state regulations (e.g., FRA, CPUC) and shall support open file formats including PDF/A, DOCX, DWG, and IFC.

5.4.6.9 The EDMS shall support optional features including digital watermarking, document expiration dates, read-only distribution, and encryption of sensitive documents, particularly those related to physical security or restricted assets.

5.4.7 Maintenance History and Regulation

5.4.7.1 The EAMS shall record, store, and present the full maintenance history of each asset, including past interventions, planned activities, and ongoing tasks. Maintenance history shall be categorized using configurable parameters such as EAMS asset ID, system type, maintenance type, materials used, and work outcome. Categorization requirements shall be confirmed during implementation workshops.

5.4.7.2 The configuration of maintenance history categories and filters shall be user-driven, based on a library of available metadata fields, and shall not require involvement from the EAMS supplier after commissioning.

5.4.7.3 The EAMS shall maintain a tamper-evident, time-stamped audit trail of all maintenance activities, including system-generated events and user interactions. Audit logs shall be stored in a secure, append-only format and protected in accordance with the TSCC System Technical Specification - Cybersecurity.

5.4.7.4 In the event of an incident, investigation, or insurance claim, authorized personnel shall be able to verify the maintenance status of any asset. All user actions, approvals, and changes related to maintenance activities shall be recorded with timestamps, user ID, and action type to support full traceability.

5.4.7.5 The EAMS shall maintain centralized maintenance history data in a format suitable for regulatory and certification use, including compliance with ISO 55001, ISO 9001, and the standards referenced in Section 2.1. Records shall be readily exportable in support of third-party audits or internal reviews.

5.4.7.6 The EAMS shall link each historical maintenance record to the corresponding work order, technician, asset condition, and applicable maintenance plan, allowing comparison between planned and executed tasks.

5.4.7.7 The EAMS shall support filtering and reporting of maintenance history by asset, location, date range, task type, maintenance outcome, and responsible team or technician.

5.4.7.8 Maintenance history records shall include, where available:

- Fault or failure codes
- Root cause indicators
- Corrective actions taken
- Component(s) replaced
- Downtime and restoration time
- Post-maintenance test results or technician notes.

5.4.7.9 Maintenance history data shall be retained for a period defined by applicable regulatory obligations (e.g., 10 years minimum for general systems; up to 30 years for critical assets) and managed in accordance with the EAMS Data Retention Policy and cybersecurity protocols.

5.4.7.10 Access to maintenance history and audit logs shall be role-restricted, with configurable permission and real-time monitoring of access attempts. Controls shall comply with the TSCC System Technical Specification - Cybersecurity.

5.4.8 Data Corruption

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

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

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

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

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

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

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

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

5.4.9 Evidence and Cause Analysis

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

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

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

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

5.4.9.4 All verified root cause analyses and associated logic, models, or rules shall be added to a version-controlled algorithm library for future reuse and optimization. This library shall be accessible to authorized EAMS users and integrated into broader decision support tools.

5.4.9.5 The EAMS shall trigger RCA automatically based on configurable conditions, such as repeat failures, unplanned downtime events, asset unavailability, or failed maintenance outcomes. RCA initiation criteria shall be defined during system configuration in consultation with the Authority.

5.4.9.6 RCA functionality shall draw from all relevant EAMS modules, including FRACAS records, sensor data, fault codes, maintenance history, operator reports, and inspection logs to form a comprehensive diagnostic base.

5.4.9.7 RCA outputs generated by AI/ML components shall be subject to human validation. The system shall present supporting evidence, reasoning pathways, and confidence indicators. RCA decisions shall include review logs, timestamps, and user approvals.

5.4.9.8 The EAMS shall track the effectiveness of RCA results through closed-loop monitoring, using indicators such as recurrence rate, downtime reduction, or mean time between failures (MTBF) to validate root cause recommendations.

5.4.9.9 RCA modules shall interface with fault management, condition monitoring, and configuration management tools to support holistic asset diagnostics and avoid duplication of analysis functions across systems.

5.4.10 **Maintenance Plan**

5.4.10.1 The EAMS shall support the execution, scheduling, tracking, and completion of all tasks defined in the maintenance plan developed during the design and commissioning phases, in accordance with California HSR maintenance and asset management guidelines. The EAMS shall accommodate various maintenance types, including preventive, corrective, predictive, and condition-based strategies.

5.4.10.2 The EAMS architecture shall support the creation, editing, and validation of unscheduled or ad hoc work orders in response to real-time events, sensor alerts, operator requests, or asset failures.

5.4.10.3 The EAMS shall allow a long-term maintenance planning module capable of simulating workload demand, resource utilization, spare parts consumption, and technician availability over multi-year time horizons.

5.4.10.4 Predictive maintenance functionality shall be based on parameters derived from the RAM Analysis Report, including failure rates, meantime between failures (MTBF), and lifecycle cost (LCC) models. These calculations shall be supplemented by Reliability-Centered Maintenance (RCM) logic, data captured in FRACAS, and inputs from the fault management system.

5.4.10.5 The TSCC Contractor, in collaboration with The Authority, shall define and map key diagnostic data points—such as sensor readings, performance thresholds, and fault codes—to equipment-specific diagnostic tables to guide condition-based and reliability-based maintenance interventions.

5.4.10.6 The TSCC Contractor shall evaluate and, where approved by The Authority, implement artificial intelligence (AI) and machine learning (ML) capabilities to support maintenance decision-making. These capabilities shall align with the asset management plan and enhance predictive maintenance, RCM, and CBM functionality. All AI-driven recommendations shall include traceability and human validation before execution.

5.4.10.7 The EAMS shall support version control and approval workflows for maintenance plans. Historical versions shall be retained and auditable to support safety, quality, and regulatory traceability.

5.4.10.8 Maintenance plan execution data—such as early failures, deferrals, and corrective interventions—shall be used to continuously optimize future cycles. The EAMS shall provide a closed-loop feedback mechanism between maintenance outcomes and plan adjustments.

5.4.10.9 The EAMS shall include a visual simulation interface for maintenance forecasting, allowing users to model asset condition projections, workload peaks, technician capacity constraints, and spare part demand.

5.4.10.10 AI/ML models used in predictive maintenance shall be explainable, regularly validated, and monitored for performance drift. Decisions based on AI shall be logged with algorithm version, confidence score, and approval status.

5.4.10.11 This section shall be read in conjunction with the RAM Analysis Report, the RCM/CBM Implementation Plan, and the TSCC System Technical Specification - Cybersecurity where predictive algorithms and sensitive operational data are used.

5.4.11 **Maintenance Analysis Tool**

5.4.11.1 The EAMS shall include a Maintenance Analysis Tool that integrates a diagnostic function defined by the TSCC Contractor and approved by The Authority. The diagnostic function shall include structured tools such as diagnostic tables, fault trees, logic diagrams, and related analysis methods, and shall be aligned with data from FRACAS, condition monitoring, and maintenance history modules.

5.4.11.2 A diagnostic table shall be a structured representation of failure-related information used to assess the health, performance, and operational condition of assets. Diagnostic tables shall be maintained in a centralized and modifiable format.

5.4.11.3 Each diagnostic table shall consolidate relevant parameters, sensor readings, historical events, and calculated thresholds associated with specific asset types or systems.

5.4.11.4 Diagnostic tools shall support operational and maintenance decision-making by generating actionable insights into asset conditions, failure cause, and recommended actions.

5.4.11.5 The EAMS shall include, at a minimum, the following diagnostic and reference tables:

- Symptom/Evidence tables
- Fault tables
- Cause tables
- Remedy tables (including Mean Time to Repair – MTTR)
- Maintenance log tables
- Sensor signal mapping tables
- Diagnostic records (including analysis outcomes and decisions taken).

5.4.11.6 Predefined diagnostic workflows shall be developed to guide maintainers through fault analysis procedures. These workflows shall include decision steps, data checks, recommended actions, and approval logic where required. Workflows shall be user-role-specific, traceable, and linked to associated tables, sensor data, and work order processes.

5.4.11.7 Inspections findings shall be recorded in the EAMS and evaluated against baseline and live asset monitoring data. This may include comparisons of recorded symptoms to sensor values, dynamic thresholds, or failure signatures. Diagnostic logic shall adapt to evolving operational conditions.

5.4.11.8 The TSCC Contractor shall develop and maintain an algorithm library within the EAMS, containing all logic, diagnostic models, and analytical tools used in fault identification and asset condition evaluation.

5.4.11.9 The TSCC Contractor shall develop and maintain an algorithm library within the EAMS, containing all logic, diagnostic models, and analytical tools used in fault identification and asset condition evaluation.

5.4.11.10 The algorithm library shall include metadata such as version number, author, approval status, and model type. Access to the library shall be controlled by user roles and audit logged. The library shall support continuous improvement, subject to validation, review, and approval by The Authority.

5.4.11.11 The Maintenance Analysis Tool shall interface with the FRACAS module, Maintenance History, and Sensor Data Store to correlate events, failure causes, and performance degradation across operational timelines.

5.4.11.12 Diagnostic recommendations and AI-generated outputs shall include supporting rationale, source data references, and confidence scores where applicable. All automated or assisted decisions shall be recorded in a traceable diagnostic log.

5.4.11.13 The EAMS shall support validation and performance testing of diagnostic models (both rule-based and ML-driven) using metrics such as detection accuracy, false positive rate, and time-to-diagnosis.

5.4.11.14 The algorithm library shall include deprecation and rollback controls for outdated or underperforming models. Updates to algorithms shall be logged, versioned, and subject to approval workflows.

5.4.11.15 Access to diagnostic tools and the algorithm library shall comply with the TSCC System Technical Specification - Cybersecurity, including authentication, role-based permissions, and tamper protection of logic and model data.

5.4.12 **Work Orders**

5.4.12.1 The EAMS shall support automatic generation of work orders based on time-based schedules, mileage, usage thresholds, or triggered events from condition monitoring systems. Preventive and predictive maintenance modules shall generate work orders in alignment with defined maintenance plans.

5.4.12.2 The EAMS shall ingest real-time data from connected sensor systems and generate corresponding work orders without delay. Trigger thresholds, escalation conditions, and data mappings shall be configurable by The Authority.

5.4.12.3 The EAMS shall include a comprehensive work order management module with calendar-based visualization and reporting. This module shall interface with other EAMS functions including maintenance planning, documentation, spare parts, tools, human resources, and task libraries defined by The Authority.

5.4.12.4 The work order management module shall support work packaging—organizing and sequencing multiple work orders to minimize downtime, optimize resource allocation, and align with possession windows. The TSCC Contractor shall define detailed packaging procedures for approval by The Authority.

5.4.12.5 The EAMS shall allow authorized users to manually create ad hoc work orders via the EAMS HMI or mobile interface, with appropriate input validation, status tracking, and audit logging.

5.4.12.6 Each work order shall include the required competencies, certifications, and skills for execution, and the EAMS shall validate assigned personnel against these requirements before confirmation.

5.4.12.7 Maintenance personnel shall be required to scan their ID or equivalent credentials (e.g., NFC card, QR code) before accessing trackside areas, restricted zones, or initiating safety-critical work orders.

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

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

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

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

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

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

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

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

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

5.4.12.15 Transitions between statuses shall be governed by configurable workflows, approval conditions, and user roles as defined by The Authority.

5.4.12.16 Work orders exceeding SLA thresholds for response or completion shall trigger automatic alerts, escalation to supervisors, and inclusion in compliance dashboards.

5.4.12.17 Field technicians shall be able to access, update, and close work orders via mobile or tablet devices. Offline functionality shall be supported for remote locations, with data synced when connectivity is restored.

5.4.12.18 The EAMS shall log all actions taken on a work order (e.g., assignment, reassignment, edit, cancellation, closure) along with user ID, timestamp, and device used, in accordance with the TSCC System Technical Specification - Cybersecurity.

5.4.12.19 Completed work orders shall feed directly into maintenance history, FRACAS, and asset condition records. Work order outcomes shall be evaluated against planned scope and used to improve future maintenance planning.

5.4.13 Spare parts management, kits, and tools

5.4.13.1 The EAMS shall include an interface module to integrate with The Authority's supply chain and inventory management systems. This module shall enable seamless coordination between asset management functions and procurement, stock control, and reporting workflows.

5.4.13.2 The EAMS interface module shall provide the following core functions:

- Inventory visibility across all relevant stock locations and storage types
- Distribution, issue, and reclamation of parts for maintenance tasks
- Repair management workflows for tools and equipment across storage areas, depots, and mobile units
- Supplier management and linking of spare parts to approved vendors
- Inventory cost tracking, including acquisition, restocking, mobilization, and demobilization costs.

5.4.13.3 The EAMS shall support identification and labeling of packaged maintenance kits, including contents, part numbers, quantities, shelf-life (if applicable), and linked asset types. AutoID technologies (e.g., RFID, barcode) shall be used where practicable.

5.4.13.4 Spare parts modelling within the EAMS shall support the following attributes, at a minimum:

- Number in stock (initial and max holding quantity)
- Mobilization time (time from withdrawal to usage)
- Restocking thresholds and reorder points
- Restocking time (lead time to replenish)
- California refurbishment time (turnaround time for reusable items)
- Cost data (unit cost, overhead, and logistical costs)

5.4.13.5 The EAMS shall process all types of labeling used in California HSR using AutoID principles where feasible. Manual override methods shall be allowed only in defined exception cases and tracked by user ID and timestamp.

5.4.13.6 The EAMS shall support creation, assignment, and tracking of maintenance kits and tools within work orders. Kits may be predefined or assembled dynamically based on asset type, fault, or required maintenance action.

5.4.13.7 The EAMS shall manage tool inventory by tracking tool type, location, availability, calibration status, maintenance records, costs, responsible users, check-out/check-in events, and condition.

5.4.13.8 The EAMS shall support tool auditing and reporting functions to support forecasting, procurement decisions, and tool utilization analysis. Safety-critical tools shall include tamper alerts, loss prevention features, and usage thresholds.

5.4.13.9 The EAMS shall automate the ordering, restocking, quality assurance, issue, and return processes for spare parts and consumables. Minimum stock thresholds and alert levels shall be configurable by The Authority.

5.4.13.10 The EAMS shall integrate with software inventory and license management systems for tools and equipment with embedded firmware or software. Version control, patch history, and access to associated configuration files shall be supported.

5.4.13.11 Files such as configuration settings, digital certificates, and calibration files shall not be stored within the EAMS itself but may be referenced by link. The EAMS shall maintain metadata and provide secure version-controlled access to these external files.

5.4.13.12 The EAMS shall support classification of stock by criticality, type (e.g., serialized, consumable, refurbished), and location (e.g., central warehouse, depot, mobile unit), enabling precise inventory control and safety stock planning.

5.4.13.13 The EAMS shall track the lifecycle of spare parts and tools, including shelf life, expiration, warranty, and obsolescence. Alerts shall be generated for items nearing end-of-life, expiring calibration, or superseded part status.

5.4.13.14 Calibration tracking shall include calibration intervals, due dates, traceability to standards, and certification storage. Non-compliant tools shall trigger hold status and alert the responsible team.

5.4.13.15 The EAMS shall support predictive inventory forecasting based on historical usage trends, maintenance schedules, and seasonal demand patterns. Forecast data shall be used to support budgeting and supply chain planning.

5.4.13.16 Spare parts shall be linked to asset-specific Bills of Materials (BOMs), including compatible and alternative parts. The EAMS shall support automated part suggestions based on fault type and asset configuration.

5.4.13.17 All spare parts, tools, and consumables associated with critical assets shall comply with access control, audit logging, and integrity monitoring requirements as defined in the TSCC System Technical Specification - Cybersecurity.

5.4.14 **FRACAS**

5.4.14.1 The EAMS shall include an integrated FRACAS (Failure Reporting, Analysis and Corrective Action System) module to track, analyze, and close out asset failures, incidents, and corrective actions.

5.4.14.2 The FRACAS module shall enhance The Authority's ability to manage asset reliability, minimize downtime, and improve operational performance. By systematically tracking and analyzing failures, the FRACAS shall support optimization of maintenance strategies, resource planning, and long-term asset lifecycle decisions.

5.4.14.3 FRACAS module shall reference asset hierarchies and physical locations within the EAMS to accurately log failures and incidents and link them to individual assets or systems.

5.4.14.4 The work order module shall be integrated with the FRACAS module so that all incidents can be linked to the associated maintenance tasks and executed actions.

5.4.14.5 The FRACAS module shall be configured to capture detailed contextual information to support root cause analysis (RCA), including environmental conditions, operating parameters, maintenance history, inspection reports, and user comments.

5.4.14.6 The FRACAS module shall enable lifecycle tracking and performance measurement of affected assets using dashboards, KPIs, and start centers linked to work orders. Key indicators such as MTBF, MTTR, failure rate, and incident recurrence shall be supported.

5.4.14.7 Each failure or incident shall follow a defined lifecycle within the FRACAS module, including status stages such as Reported, Under Review, RCA Complete, Corrective Action Assigned, Verified, and Closed. Status changes shall be workflow-driven, timestamped, and role-governed.

5.4.14.8 The maintenance data associated with FRACAS records shall include, at a minimum:

- Work order ID
- Maintenance task ID and procedure reference
- Affected asset ID
- Task interval (scheduled frequency)
- Due date and actual completion date
- Total downtime and labor hours
- Parts and materials used
- Inspection and test results
- Description of discovered faults
- Summary of corrective actions taken.

5.4.14.9 FRACAS reports shall be used to identify opportunities for maintenance strategy optimization, risk reduction, and service performance improvements, while preserving safety and compliance objectives.

5.4.14.10 The EAMS shall support extraction and export of FRACAS records and reports for analysis by maintenance engineers, safety personnel, and asset managers.

5.4.14.11 The EAMS shall be capable of generating FRACAS records automatically when defined fault codes, alerts, or failure criteria are detected by the system.

5.4.14.12 The FRACAS module shall include incident classification features to assign severity levels, impact types (e.g., safety, reliability, operational), and root cause categories. These classifications shall be used for triage, prioritization, and escalation workflows.

5.4.14.13 The FRACAS module shall support continuous improvement processes by enabling tracking of recurring failures, monitoring of action effectiveness, and generation of feedback into preventive maintenance plans and decision support tools.

5.4.14.14 The FRACAS module shall integrate with the Evidence and Cause Analysis tools (see Section 5.4.8), allowing incident records to be linked to root cause trees, diagnostic outputs, and algorithm library references.

5.4.14.15 The FRACAS module shall include configurable alerting for overdue corrective actions, incomplete RCA tasks, or repeated incidents on the same asset.

5.4.14.16 All FRACAS actions, decisions, and edits shall be logged and traceable to the initiating user, with timestamped records and role-based access controls as defined in the TSCC System Technical Specification - Cybersecurity.

5.4.14.17 The FRACAS module shall provide a closed-loop feedback mechanism to the EAMS maintenance planning module, allowing confirmed root causes and repeated incident data to influence task intervals, procedures, or asset replacement strategies.

5.4.14.18 The FRACAS module shall support periodic safety and compliance reviews, and provide configurable reports for regulatory submissions, insurance claims, and internal audits.

5.4.14.19 The FRACAS module shall support the classification and tracking of **defects** as a specific failure event type. Defects may include installation errors, manufacturing non-conformances, punch list items, or anomalies detected during inspection, commissioning, or handover. Each defect shall be linked to the affected asset, severity level, and related warranty, quality, or supplier documentation where applicable.

5.4.15 Asset Management Plan

5.4.15.1 The TSCC Contractor, in agreement with the Authority, shall develop an Asset Management Plan that provides sufficient information to support lifecycle investment decisions. The plan shall guide decisions relating to:

- Trade-off analysis for ageing assets
- Optimization of maintenance strategies
- Replacement or investment in new equipment scenarios

5.4.15.2 The Asset Management Plan shall be structured and categorized according to major asset groups, including at minimum: track systems, civil works, and major electromechanical systems (e.g., power, signaling, ventilation, control systems).

5.4.15.3 The TSCC Contractor shall provide periodic forecast reports identifying planned obsolescence and decommissioning of parts, subassemblies, or complete subsystems. These forecasts shall support proactive investment planning and maintenance schedule adjustments.

5.4.15.4 The Asset Management Plan shall be driven by Reliability-Centered Maintenance (RCM) and/or Condition-Based Maintenance (CBM) principles, with a focus on minimizing lifecycle cost, unplanned outages, and safety risks.

5.4.15.5 The TSCC Contractor shall prepare and submit the Asset Management Plan to The Authority for review and approval prior to implementation.

5.4.15.6 The Asset Management Plan shall be evidence-based, using best practices and supporting models to justify recommendations. These models shall include reliability analysis, FRACAS trends, lifecycle cost (LCC) analysis, and relevant performance indicators.

5.4.15.7 The Asset Management Plan shall align with the principles of ISO 55001 (Asset Management – Management Systems – Requirements) or equivalent industry-standard frameworks to ensure traceability, risk-based planning, and value optimization across the asset lifecycle.

5.4.15.8 The Asset Management Plan shall define governance roles and responsibilities, including designation of a plan owner, revision approver, and implementation oversight by The Authority.

5.4.15.9 The plan shall be reviewed and updated at least once every year, or following any significant change to asset class performance, maintenance strategy, or service level requirements.

5.4.15.10 The plan shall be traceable to EAMS modules including the asset register, maintenance planning, FRACAS, and predictive analytics. Changes in asset condition or failure rates shall be reflected in its planning assumptions and recommendations.

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

5.4.16 **Asset Condition Survey and Monitoring**

5.4.16.1 The TSCC Contractor shall establish periodic asset condition surveys and audits to assess asset degradation and deterioration using industry best practices. The proposed methodology and frequency shall be submitted to The Authority for approval.

5.4.16.2 Condition audits shall support the projection of asset degradation, identification of failure trends, and modeling of remaining useful life in short-, medium-, and long-term horizons to inform investment planning and replacement strategies.

5.4.16.3 The TSCC Contractor shall prepare and submit an Asset Condition Survey Management Plan that outlines the methodology for collecting, assessing, and reporting on asset conditions. The plan shall present a structured, data-driven approach to maximize asset life while maintaining required levels of availability, performance, and safety.

5.4.16.4 The EAMS shall support condition assessments through the analysis of available data sets, including inspection data, sensor readings, historical work orders, and operational performance metrics. Condition audits may be initiated manually or triggered automatically based on threshold values.

5.4.16.5 The TSCC Contractor shall propose an audit frequency for each major asset class, based on criticality, risk, and degradation profiles. This shall be reviewed and approved by The Authority.

5.4.16.6 The EAMS shall host all asset-related data necessary for maintenance contractor operations, including condition records, inspection logs, usage data, and access to the current Asset Register and maintenance history.

5.4.16.7 If maintenance contractors maintain separate data systems, the transfer of operational and condition data into the EAMS shall be mandatory. The EAMS shall serve as the authoritative master system and the single source of truth for all operational data, asset condition, competencies, required equipment, and maintenance activities across the California High-Speed Rail program.

5.4.16.8 The EAMS shall maintain the master copy of all condition monitoring and inspection data. TSCC Contractor internal systems may only serve as temporary or read-only repositories and must synchronize with the EAMS per defined data transfer protocols.

5.4.16.9 The EAMS shall support periodic reporting of asset condition to original equipment manufacturers (OEMs), suppliers, or The Authority. Reports shall be auto generated or scheduled based on configured time intervals or events.

5.4.16.10 The Asset Condition Survey Management Plan shall define the types of condition evaluation used (e.g., visual inspection, structural assessment, sensor-derived metrics), condition scoring scales (e.g., 1–5 or health index), and asset-specific thresholds for concern or replacement.

5.4.16.11 The EAMS shall support geospatial tagging and photographic or video evidence collection during surveys. Condition data shall be linked to the GIS/BIM representation of each asset.

5.4.16.12 Condition data collected from maintenance contractors shall be subject to validation rules, version control, and audit logging. Only verified data shall influence planning, reporting, or investment recommendations.

5.4.16.13 The EAMS shall differentiate between condition surveys (manual, planned evaluations), monitoring (continuous, sensor-based tracking), and inspections (event- or schedule-based assessments) for traceability and reporting clarity.

5.4.16.14 All condition data shall comply with the TSCC System Technical Specification - Cybersecurity, including data integrity validation, encryption in transit/storage, and user-based access controls.

5.4.16.15 Outputs of the asset condition survey shall feed directly into the Asset Management Plan (see Section 5.4.15), maintenance strategy optimization, and capital investment prioritization modules.

5.4.17 **Obsolescence Management**

5.4.17.1 The TSCC Contractor shall develop and maintain an Obsolescence Management Plan (OMP), to be approved by the Authority and integrated into the EAMS as a functional module with associated reporting and data tracking capabilities.

5.4.17.2 The Obsolescence Management Plan shall describe processes and strategies to manage and mitigate obsolescence risk to preserve operational performance, safety, and maintainability. It shall include, at a minimum:

- Guidelines for identifying and replacing obsolete components and equipment, with specific focus on electronic and software-dependent systems.
- Replacement strategies based on modular and open architectures to support partial upgrades. Any deviations from modular/open architecture shall require prior written approval by The Authority.
- Software update strategies to address compatibility, patching, and end-of-support risks, with preference for modular and decoupled implementations.
- Inventory plans for strategic and non-strategic spare parts.
- Management of tool obsolescence, including identification of new tool requirements and secure disposal of outdated equipment.
- Processes to proactively monitor vulnerable components and subsystems using EAMS analytics and supplier lifecycle data.

5.4.17.3 The EAMS shall provide functionality to monitor component development roadmaps, supply chain availability, and commercial lifecycle status of all software and hardware components. Alerts shall be generated for components approaching end-of-life.

5.4.17.4 Maintenance engineering staff shall ensure that all spare parts contracts include up-to-date obsolescence condition information for critical components, including manufacturer support status, last-time-buy notifications, and replacement part references.

5.4.17.5 Upon identifying an obsolete component, the TSCC Contractor shall initiate actions to identify, evaluate, test, and gain all required internal and external approvals for replacement, refurbishment, or adaptation of equivalent components.

5.4.17.6 For each obsolete component replaced, the TSCC Contractor shall provide full documentation covering testing, installation procedures, operational validation, and configuration control for hardware and/or software.

5.4.17.7 Obsolescence shall be considered during the equipment specification and design phase. Systems shall prioritize the use of open, modular architectures to facilitate partial redesigns, interface updates, and integration of new technologies.

5.4.17.8 Selected architectures shall conform to recognized or emerging market standards (e.g., software languages, interface protocols). Any deviation shall be justified and is subject to written approval by The Authority.

5.4.17.9 The TSCC Contractor shall provide a list of anticipated obsolete equipment on an annual basis and upon request via the EAMS. This list shall project the upcoming period and support advanced scheduling of replacement or mitigation actions.

5.4.17.10 At contract close-out and during the maintenance handover process, the TSCC Contractor shall demonstrate that no critical system or component will become obsolete for a minimum period after handover to be approved by The Authority.

5.4.17.11 If the TSCC Contractor is unable to demonstrate continued operability of the system due to foreseeable obsolescence, they shall remain liable for renewal, reengineering, or replacement costs required to sustain asset functionality.

5.4.17.12 The Obsolescence Management Plan shall be aligned with the principles of IEC 62402 – Obsolescence Management – Application Guide or equivalent international standards. The plan shall include structured risk assessment, monitoring, mitigation, and resolution processes.

5.4.17.13 Obsolescence risk shall be assessed using a criticality-based scoring model considering component impact, system function, vendor dependency, and lifecycle support. High-risk items shall be prioritized in the OMP with defined mitigation strategies.

5.4.17.14 The EAMS shall integrate obsolescence tracking with the Asset Register, Maintenance Planning, Spare Parts Inventory, and FRACAS modules to ensure full traceability and proactive planning.

5.4.17.15 Supplier monitoring shall be included in the obsolescence strategy, including tracking of OEM lifecycle notifications, end-of-sale/end-of-support announcements, and coordinated last-time-buy actions.

5.4.17.16 The TSCC System Technical Specification - Cybersecurity shall be applied to all software and firmware obsolescence cases. Unsupported software versions shall be risk assessed, patched, or replaced as part of the security maintenance lifecycle.

5.4.17.17 The TSCC Contractor shall define an obsolescence change control workflow, including review, validation, and approval stages involving engineering, cybersecurity, and system safety representatives.

5.4.18 **Lifecycle Management**

5.4.18.1 The EAMS shall include a Lifecycle Management Tool that supports data-driven decision-making throughout the asset lifecycle. This tool shall be used to assess the total cost of ownership, performance, and timing of asset renewal or refurbishment.

5.4.18.2 The EAMS shall calculate the Lifecycle Cost (LCC) for each individual asset registered in the EAMS at intervals defined by The Authority, and upon key trigger events such as major repair, cost deviation, or condition change.

5.4.18.3 The EAMS shall calculate the mean LCC by asset class or equipment type, using aggregated operational and maintenance data stored in the EAMS. These calculations shall be performed at intervals defined by The Authority or as required for planning and investment analysis.

5.4.18.4 LCC analysis results shall be stored in a structured format within the EAMS and used as input to other EAMS modules, including:

- Asset Management Plan (AMP)
- Obsolescence Management
- Maintenance Strategy Optimization
- Capital Investment Forecasting.

5.4.18.5 Common LCC models and reference analyses for California HSR assets shall be developed by the TSCC Contractor and stored in a reusable library within the EAMS. The models shall be version-controlled and subject to review and approval by The Authority.

5.4.18.6 All LCC analyses shall follow a recognized international standard such as ISO 15686-5, EN 60300-3-3, or an equivalent framework approved by The Authority. The selected methodology shall ensure repeatability, transparency, and defensibility of results.

5.4.18.7 The EAMS shall require LCC models to incorporate, at a minimum: initial capital cost, installation, preventive and corrective maintenance, energy consumption, downtime cost, obsolescence, and end-of-life decommissioning.

5.4.18.8 LCC calculation logic shall be fully integrated with EAMS modules including Work Orders, FRACAS, Spare Parts Inventory, Asset Condition, and Obsolescence data to maintain accuracy and real-time cost reflection.

5.4.18.9 The Lifecycle Management Tool shall support scenario-based and sensitivity analysis, allowing The Authority to evaluate cost and risk across multiple operational or funding assumptions (e.g., varying failure rates, inflation, discount rates).

5.4.18.10 LCC outputs shall be used as input into decision support tools for asset renewal planning, budgeting, risk-based prioritization, and maintenance strategy justification.

5.4.19 Building Information Modelling and Digital Twins

5.4.19.1 The EAMS shall be fully compatible with Building Information Modeling (BIM) data structures and Digital Twin applications, and shall implement integration protocols that allow seamless communication, synchronization, and management of asset lifecycle information. The EAMS shall be designed to integrate with BIM and Digital Twins in a way that is compatible with BIM's representation of assets and information contained within BIM models and the California HSR GIS geodatabase.

5.4.19.2 The EAMS shall enable two-way integration with Digital Twins, allowing asset performance data, condition monitoring, and maintenance status to be visualized and analyzed in real time within the digital twin environment.

5.4.19.3 Digital Twin shall support functions such as real-time simulation, predictive diagnostics, spatial analytics, and 3D visualization of asset condition and interventions. Integration with FRACAS, LCC, and Asset Condition modules shall be supported.

5.4.19.4 The EAMS shall track BIM model versions, distinguish between "as-designed," "as-built," and "as-maintained" states, and store update history in compliance with the system's configuration management plan.

5.4.19.5 Access to BIM and Digital Twin data shall be governed by role-based permissions and logged for audit purposes. Integration shall align with the TSCC System Technical Specification - Cybersecurity, and data exchanges shall be encrypted and validated.

5.4.20 Reporting, Analysis and auditing

5.4.20.1 The EAMS shall generate reports across all relevant maintenance and asset management categories to support operational decision-making and performance analysis. At a minimum, the reporting functionality shall cover:

- Asset availability and downtime tracking
- Materials usage and consumption trends
- Labor and material cost reporting, including cost per task and per asset

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

5.4.20.2 Reports shall support business intelligence functions, be visualized via dashboards, and provide insights to optimize maintenance planning and investment decisions.

5.4.20.3 The EAMS system shall support seamless scalability, enabling integration of new equipment, subsystems, or modules without the need for architectural redesign or server infrastructure overhaul. Reporting functionality shall accommodate new data streams and equipment classes dynamically.

5.4.20.4 The EAMS shall provide a fully documented and license-free interface (e.g., REST API, ODBC/JDBC) to support the integration of third-party analytics, visualization, and reporting tools. The interface shall allow read/write access to defined datasets, including historical logs, real-time data, and master records, as approved by The Authority.

5.4.20.5 The EAMS reporting engine shall support full lifecycle coverage, from asset acquisition through retirement. Reports shall include inputs/outputs from integrated systems, compliance with audit requirements, configuration change logs, and lifecycle-based risk assessments. All reporting functions shall align with The Authority's cybersecurity and auditability requirements.

5.4.20.6 The EAMS shall support export of reports in multiple standard formats (e.g., CSV, PDF, XLSX, JSON, XML), and allow automated report scheduling, email delivery, and user-defined distribution lists.

5.4.20.7 The EAMS shall support configurable role-based access to reports, dashboards, and analytics modules. Users shall only view and access information within their assigned scope of responsibility.

5.4.20.8 The EAMS shall include time-series analytics tools for evaluating trends over configurable historical ranges (e.g., 7-day, 30-day, 12-month). These tools shall support anomaly detection, forecasting, and seasonal comparison of asset behavior.

5.4.20.9 The EAMS shall maintain an immutable audit log of all system activity, including user actions, data imports/exports, asset configuration changes, and system access events. Audit logs shall be exportable, queryable, and retained in accordance with the TSCC System Technical Specification - Cybersecurity.

5.4.20.10 The EAMS shall support the definition and tracking of custom KPIs and performance indicators. Users shall be able to configure KPIs using system data fields, define thresholds, and visualize them within dashboards or reports.

5.4.20.11 The EAMS shall generate cybersecurity-related operational reports, including access violation summaries, failed login attempts, system event logs, and patch status compliance, to support CSOC and regulatory reporting.

5.4.21 Mobile EAMS Devices

5.4.21.1 The EAMS-FRMCS integration shall support communication with handheld mobile devices (e.g., Android, iOS, rugged tablets) for:

- Viewing and updating work orders:
- Logging faults, alarms, or asset condition data
- Uploading photos, audio notes, and GPS location

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

5.4.21.2 All handheld devices accessing the EAMS via FRMCS shall:

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

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

5.4.21.4 The EAMS shall provide:

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

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

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

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

5.5 Performance Requirements for EAMS

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

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

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

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

5.5.3 The EAMS shall integrate a performance monitoring module to track and report on system quality metrics, including at minimum:

- System availability and uptime
- Scheduled vs. unscheduled downtime
- Service and data accuracy levels
- User experience (latency, failed interactions, responsiveness)
- Integration latency with connected systems
- These KPIs shall be presented via configurable dashboards and exported for SLA and compliance tracking.

5.5.4 The EAMS system shall support full customization and shall be based on a modular architecture to ensure separation of services, flexibility in future development, and the ability to isolate system components for independent scaling and maintenance.

5.5.5 The failure of any single EAMS node, hardware component, or service endpoint shall not disrupt overall EAMS operations. Redundant system elements shall take over seamlessly to maintain availability.

5.5.6 In the event of a communications failure between peripheral equipment and the systems in the OCC, BOCC, or Local Control Rooms, the EAMS and peripheral equipment shall continue operating in a standalone, degraded-but-safe mode until communications are restored.

5.5.7 The EAMS shall comply with all safety-related performance and fail-safety requirements as defined in the Contract including any Safety Integrity Level (SIL) classifications applicable to EAMS-controlled functions.

5.5.8 The EAMS shall meet the RAM targets defined in Schedule 1 – Safey, Security and RAM Requirements, including specified targets for MTBF (Mean Time Between Failures), MTTR (Mean Time to Repair), and system availability. These metrics shall be validated during system performance testing and monitored continuously in operation.

5.5.9 The EAMS shall implement system-wide load balancing and horizontal scaling mechanisms to optimize performance under peak conditions. Clustering of application services and failover configurations shall be tested during system acceptance.

5.5.10 The performance of security controls (e.g., encryption, multifactor authentication, intrusion detection) shall be validated to ensure no degradation of user experience or system responsiveness.

5.5.11 All EAMS performance data, including response times and user load metrics, shall be captured and stored for analysis and compliance verification for a minimum period (e.g., at least 24 months), agreed with The Authority.

5.5.12 EAMS modules related to safety, security, or system integrity shall include built-in performance self-checks and watchdog mechanisms that trigger alerts on delay thresholds or degraded processing speed.

5.5.13 The EAMS shall provide a continuous performance dashboard accessible by The Authority, with color-coded SLA compliance indicators, trend analysis, and custom threshold alerts.

5.6 Cybersecurity and Security Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.6.13 EAMS components shall be hardened in accordance with applicable industry standards and the *CHSR Cybersecurity Technical Specification*. Any deviation shall require written approval from the Cybersecurity Lead and other appropriate senior stakeholders.

5.6.14 The EAMS shall support automated security health checks, with alerts generated for misconfiguration, outdated software components, or integrity check failures.

5.6.15 The EAMS shall have a nominated System Owner who shall be accountable for cybersecurity risk ownership and mitigation.

5.6.16 The EAMS System Owner shall be responsible for ensuring that appropriate resources are present at cybersecurity threat modelling and risk assessment activities.

6 INTERFACE REQUIREMENTS

6.1 General Requirements

6.1.1 Interfaces are classified as below:

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

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

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

6.1.4 All EAMS interfaces shall support structured, standards-based data formats such as JSON, XML, OPC UA, or CSV, and comply with any semantic or schema constraints.

6.1.5 All EAMS interfaces shall be protected by cybersecurity controls including encryption (e.g., TLS 1.3), message authentication, endpoint validation, and compliance with the *TSCC System Technical Specification - Cybersecurity*.

6.1.6 Interfaces that support high-frequency data exchanges (e.g., condition monitoring, telemetry) shall meet the defined performance requirements for message latency, throughput, and system responsiveness.

6.1.7 All interfaces that exchange sensitive or operational data (e.g., financial, TPS, security telemetry) shall implement secure communication protocols such as TLS 1.3, mutual certificate authentication, and VPN tunneling where required.

6.1.8 Each interface shall include fault handling logic, including:

- Retry strategies
- Alert generation on failed communication
- Data integrity checks
- Logging of malformed or incomplete messages.

6.1.9 All active interfaces shall be monitored for status, latency, error rates, and availability. EAMS shall present this information in a health dashboard and expose logs to the r central monitoring system.

6.1.10 All interfaces shall comply with the *TSCC System Technical Specification - Cybersecurity*, including:

- Access control enforcement
- Endpoint authentication
- Encrypted communication
- Logging of interface activity and failures.

6.1.11 All raw data received by the EAMS shall be mapped to a normalized internal data model defined in an EAMS Data Dictionary. Inconsistent or unstructured input formats shall be rejected or quarantined for validation.

6.1.12 Monitoring interfaces shall use open and widely adopted protocols such as OPC UA, MQTT, or RESTful APIs. Data payloads shall be structured using standard formats (e.g., JSON, XML) and comply with an EAMS schema registry.

6.1.13 The EAMS shall provide a feedback mechanism to source systems indicating data reception status, validation success/failure, and any generated events or anomalies triggered by the received data.

6.1.14 All monitoring data interfaces shall include:

- Endpoint authentication
- Data integrity checks (e.g., checksums or digital signatures)
- Encryption during transit (e.g., TLS 1.3)
- Role-based access restrictions
  in accordance with the TSCC System Technical Specification - Cybersecurity.

6.1.15 Monitoring data shall be processed and stored within the EAMS to support:

- Trend analysis and dashboards
- Predictive maintenance (via ML/AI modules)
- FRACAS root cause analysis
- Lifecycle cost modeling (LCC)
- Condition-based maintenance (CBM) routines.

6.1.16 Additional metering and telemetry data may be transmitted to the EAMS from subsystems, including but not limited to energy consumption, voltage/current fluctuations, pressure, temperature, and vibration metrics. The TSCC Contractor shall identify the relevant data sources and ensure the EAMS can ingest and process these values at the required frequency.

6.1.17 The EAMS shall interface with existing subsystems to automatically gather available operational data including, but not limited to:

- Time-of-use data (e.g., ON/OFF sequences, cycle counts, power-up frequency) for each device and sub-component
- Non-emergency fault or warning events
- Alarms and condition-based alerts with associated metadata (e.g., location, priority, asset ID).

6.1.18 Security appliances and platforms (e.g., intrusion detection, endpoint protection) shall be integrated with the EAMS for telemetry, configuration monitoring, and operational coordination, subject to approval and alignment with the *TSCC System Technical Specification - Cybersecurity*.

6.2 Third Parties Interfaces

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

6.3 External Interfaces

6.3.1 Interfaces with operator systems

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

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

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

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

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

6.3.2 **Interfaces with stations contractors**

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

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

6.3.3 **Interfaces with facilities contractors**

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

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

6.3.4 **Interfaces with civil contractors**

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

- Civil structures: bridges, viaducts, tunnels

6.3.5 Interfaces with trainsets contractor

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

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

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

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

- Solar PV production
- Battery Electrical Storage System

6.4 Internal interfaces

6.4.1 TSCC Subsystems static and dynamic Asset Information

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

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

6.4.2 Interface with Network Timing System (NTS)

6.4.2.1 The EAMS shall interface with NTS systems to integrate static Asset Information data and exchange real-time, near-real-time, and historical data of NTS as described in the NTS Technical Specification.

6.4.2.2 The EAMS shall interface with the Network Timing System to synchronize the timestamps across all EAMS components and subsystems.

6.4.2.3 Time synchronization shall include fallback mechanisms and periodic drift detection. All logs and transactions within the EAMS shall include synchronized timestamps for traceability and event reconstruction.

6.4.3 Interface with Traffic Management System (TMS)

6.4.3.1 The EAMS shall interface with the TMS to receive structured data regarding the status of engineering possessions, including start/end times, affected sections, and operational constraints. This data shall be used to suppress or adjust maintenance scheduling during affected periods.

6.4.3.2 The EAMS shall receive incident and delay information from TMS, including root cause classification, location, impacted assets, and timestamp. This information shall be used to generate corrective maintenance work orders, flag affected assets for condition reassessment and correlate with FRACAS records.

6.4.4 Interface with Integrated Control and Supervision Systems (ICSS)

6.4.4.1 Where overlaps exist between ICSS and other CHSR subsystems, a single, normalized data structure and processing logic shall be applied to avoid duplication and maintain consistency in alarm and event processing.

6.4.5 Interface with Digital Communication Network (DCN)

6.4.5.1 The EAMS equipment shall be connected to the DNC via a dual-redundant physical and logical path to ensure continuous availability.

6.4.5.2 The TSCC Contractor shall ensure that all data transmitted between the EAMS and the DCN is protected using secure communication protocols, including encryption (e.g., TLS 1.3, IPSec, or MACsec), mutual authentication, and integrity validation. All network transmission security shall comply with the *TSCC System Technical Specification - Cybersecurity*.

6.4.5.3 The EAMS shall operate within the DCN delivered network infrastructure using a defined subnet or VLAN segment. The network configuration shall support logical separation of services, role-based access controls, and zoning for IT/OT isolation as required by the California HSR Network Architecture Guidelines and *TSCC System Technical Specification - Cybersecurity*.

6.4.5.4 All EAMS communication over the Digital Communication Network shall use encrypted transport protocols (TLS 1.3, MACsec, or equivalent) and enforce endpoint authentication. Credentials and keys used shall be rotated in accordance with the Public Key Infrastructure (PKI) requirements of the *TSCC System Technical Specification - Cybersecurity*.

6.4.5.5 EAMS network interfaces shall be logically segmented using VLANs or software-defined networking (SDN) constructs to separate functional domains (e.g., asset telemetry, maintenance data, admin access). Segmentation shall align with security zones defined in the *TSCC System Technical Specification - Cybersecurity*.

6.4.5.6 The EAMS shall continuously monitor the health of its connection to the DCN.

6.4.6 **Internal with Wireless Communication Systems (WCS)**

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

6.4.7 Interfaces with Medium and Low Voltage Power System

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

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

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

6.4.7.3 The EAMS shall monitor UPS and battery systems for:

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

6.4.8 Interface with Cybersecurity

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

6.4.8.2 The EAMS shall integrate with the following cybersecurity systems:

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

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

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

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

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

7 MATERIALS, PRODUCTS AND COMPONENTS REQUIREMENTS

7.1 General Requirements

7.1.1 All materials supplied by the TSCC Contractor shall comply with applicable United States standards (e.g., ASTM, ANSI, IEEE, NFPA). Where no equivalent U.S. standard exists, relevant EN, ISO, or other internationally recognized standards may be used, as approved by The Authority and defined in *Section2.2*.

7.1.2 All materials supplied shall be of sufficient quality to meet the designed service life requirements defined in the California HSR RAM and LCC strategies, and shall be verified through applicable certification, documentation, and testing protocols.

7.1.3 All materials shall be supported by certificates of compliance (e.g., mill test certificates, manufacturer declarations) indicating conformity with applicable standards. Where third-party certifications are required (e.g., UL, FM, NSF), copies shall be provided prior to installation.

7.1.4 A hierarchy of applicable standards shall be followed in this order of preference:

- California HSR-specific standards
- U.S. national standards (e.g., ASTM, ANSI, AASHTO, IEEE)
- ISO/IEC or other international standards
- EN standards (when justified and accepted by The Authority).
- All materials shall be selected with consideration for:
- Long-term availability and resistance to obsolescence
- Use of environmentally sustainable or recyclable materials
- Avoidance of restricted substances (e.g., per REACH, RoHS).

7.1.5 For materials or components with embedded software (e.g., smart sensors), the following shall apply:

- Firmware version shall be documented and tracked
- Components shall be assessed for known vulnerabilities (e.g., CVEs)
- Software updates shall follow secure patch management
- Unauthorized remote access features shall be prohibited.

7.2 Software and Hardware specific requirements

7.2.1 The EAMS design shall be based on Commercial Off-The-Shelf (COTS) components, open architecture, and modular system architecture, using industry-standard, non-proprietary interfaces.

7.2.2 The TSCC Contractor's design for all central servers shall be on-premises, either physical, virtualized, or cloud-based, to support storage and data exchange. All solutions shall comply with the *TSCC System Technical Specification - Cybersecurity*. Containerized infrastructure may also be considered, provided it meets operational and security requirements.

7.2.3 The EAMS handheld devices shall be fanless and ergonomically designed to improve user comfort in field conditions.

7.2.4 EAMS handheld devices shall demonstrate optimal performance and scalability to support growing data volumes and concurrent users. Devices shall maintain responsive performance under varying load conditions and be compatible with future EAMS database and feature expansions.

7.2.5 EAMS handheld devices shall support at least a minimum period of active use (e.g., 12 hours), agreed with The Authority, with the EAMS application and shall feature rapid charging capabilities.

7.2.6 The EAMS system shall include redundant power supply to prevent single points of failure.

7.2.7 EAMS devices shall be connected to the Uninterruptible Power Supply (UPS) infrastructure of the OCC or other critical facilities where installed.

7.2.8 The EAMS shall support future scalability and modular expansion while meeting or exceeding its REAMS targets, including support for degraded modes and failover conditions.

7.2.9 The TSCC Contractor shall provide EAMS workstations at each maintenance facility and within the OCC.

7.2.10 EAMS shall be provided with all required software licenses to support full lifecycle use.

7.2.11 License utilization shall be analyzed by the TSCC Contractor, and the most cost-effective solution proposed (e.g., subscription-based or perpetual), with the number of licenses minimized to meet operational needs.

7.2.12 The EAMS shall support the use of handheld or portable smart devices by field engineers and technicians for maintenance and inventory purposes, including wireless EAMS access and automatic asset identification using embedded tags (e.g., RFID or NFC).

7.2.13 The EAMS shall maintain and update all records in real time. Its architecture shall prevent data loss from single points of failure and shall include automated failure detection with corresponding alarms.

7.2.14 The EAMS system shall include:

- Servers located at the OCC
- Operating system platforms based on modern, industry-standard technologies (e.g., Linux or Windows)
- Local storage and analysis infrastructure, including container-based applications, where applicable.

7.2.15 The EAMS software shall be fully web-architected using modern development frameworks and technologies.

7.2.16 The EAMS shall support integration with Common Data Environment (CDE) servers and related services.

7.2.17 EAMS software shall be accessible to mobile maintenance staff via handheld terminals. Offline mode support shall be provided, allowing access to essential functions when network connectivity is unavailable.

7.2.18 All general-purpose software (e.g., operating systems, data stores, process control, networking, telecoms, and cloud infrastructure) shall be proven industrial-grade solutions widely used in commercial and critical infrastructure applications.

7.2.19 The EAMS interface shall be responsive and optimized for multiple user roles (e.g., operators, engineers, managers), and adaptable to devices such as PCs, tablets, and smartphones. AR/VR technologies may be used to support asset data visualization during maintenance activities.

7.2.20 The TSCC Contractor shall define, in conjunction with The Authority, the data-driven maintenance strategy and required EAMS modules to optimize asset performance.

7.2.21 Access to EAMS archives shall be controlled via strong authentication mechanisms. Access to sensitive repositories shall be restricted, logged, and protected with password policies that align with the *TSCC System Technical Specification - Cybersecurity*.

7.2.22 The EAMS server operating environment shall support lightweight client HMI architecture and multi-session support. Cybersecurity requirements for deployment shall be confirmed and integrated through formal workshops with The Authority.

7.2.23 The TSCC Contractor shall specify a web-based EAMS HMI using modern server and webserver architectures, including virtual machine and container support for scalability and simplified administration.

7.2.24 The TSCC Contractor shall provide a dedicated handheld application for field maintenance staff.

7.2.25 The processing capabilities of EAMS servers, workstations, and peripherals shall be sufficient to handle all operational events and include automatic backup and restoration functions for software and data.

7.2.26 The EAMS hardware and software components shall be optimized to support fast data visualization, minimal latency, and high-resolution display quality under all system loads.

7.2.27 Hardware scaling for the EAMS system shall primarily support horizontal expansion by adding servers and modular computers or storage elements.

7.2.28 The TSCC Contractor shall provide full version control records for all EAMS firmware, software, and handheld applications. Updates shall follow patch management and vulnerability scanning procedures defined in the *TSCC System Technical Specification - Cybersecurity*.

7.2.29 All operating systems and third-party software shall be hardened in accordance with CIS Benchmarks or equivalent standards.

7.2.30 All EAMS handheld devices shall be ruggedized and managed through Mobile Device Management (MDM). Devices shall support remote wipe, full disk encryption, and secure login methods.

7.2.31 The TSCC Contractor shall demonstrate that EAMS hardware and software will remain serviceable for a minimum of 15 years. Upgrade paths, component interchangeability, and modularity shall be documented and maintained.

7.2.32 All EAMS hardware and software components shall undergo Factory and Site Acceptance Testing, including:

- Performance under full system load
- Failure/recovery validation
- Backup and restoration functionality.

7.2.33 The TSCC Contractor shall deliver full installation, configuration, operation, and maintenance manuals for all software and hardware components, including interface specifications.

8 TOLERANCES

Not applicable to EAMS

9 SCOPE OF SUPPLY AND DELIVERY

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

9.2 Specific Requirements

9.2.1 Hardware and Infrastructure

9.2.1.1 The TSCC Contractor shall supply all central, backup, redundant, and edge servers necessary to support the EAMS architecture.

9.2.1.2 The TSCC Contractor shall supply and install EAMS operator workstations and Human-Machine Interfaces (HMIs) at the Operations Control Center (OCC), Backup OCC (BOCC), and Infrastructure Maintenance Facilities.

9.2.1.3 All EAMS hardware components shall support horizontal and modular scalability and include redundant power supplies, local storage, and UPS integration.

9.2.2 Software and Licenses

9.2.2.1 The TSCC Contractor shall provide and install all required EAMS software, including database engines, analytics modules, handheld apps, mobile interfaces, and web-based HMI platforms.

9.2.2.2 The EAMS software architecture shall include full documentation of the system structure, communication protocols, interfaces, API definitions, and integration points with other systems.

9.2.2.3 The TSCC Contractor shall supply all required software licenses and subscriptions for the full lifecycle of the EAMS. Licenses must be transferrable to The Authority at the time of handover and shall not impose vendor lock-in.

9.2.2.4 A license register shall be maintained by the TSCC Contractor and delivered to The Authority, including type, scope, expiry dates, renewal conditions, and terms of use.

9.2.3 Tools, Spares and Auxiliary Equipment

9.2.3.1 The TSCC Contractor shall deliver all specialized test tools and diagnostic equipment necessary to validate, operate, and maintain the EAMS.

9.2.3.2 An initial set of spare parts for critical EAMS components shall be provided and documented in the asset register, including part numbers, expected replacement intervals, and storage requirements.

9.2.3.3 The TSCC Contractor shall supply all auxiliary equipment required for installation and protection of EAMS assets, including but not limited to mounting brackets, cases, cable bindings, and field accessories for handheld devices.

9.2.4 Training and Knowledge Transfer

9.2.4.1 The TSCC Contractor shall deliver training to OCC operators, field technicians, cybersecurity personnel, and maintenance planners. Training shall be delivered in both classroom and hands-on formats.

9.2.4.2 Training materials, including user guides, quick reference sheets, and safety instructions, shall be included as part of the documentation deliverables.

9.2.5 Support and Handover

9.2.5.1 The TSCC Contractor shall provide post-delivery support, including patches, software updates, and maintenance for the full design life of the EAMS, in accordance with REAMS and cybersecurity requirements.

9.2.5.2 At the time of project handover, the TSCC Contractor shall deliver a final transfer package including:

- Final system configuration
- Complete and validated backups
- Password vault or credential record
- Software license keys and certificates
- Confirmation of transfer of ownership and IP rights where applicable.

10 MANUFACTURING

10.1 General Requirements

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

11 INSTALLATION AND INTEGRATION

11.1 General Requirements

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

12 TESTING, VALIDATION AND ACCEPTANCE

12.1 General Requirements

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

12.2 Specific Requirements Factory Acceptance Testing (FAT)

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

12.2.2 FAT shall include functional testing of:

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

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

12.3 Specific Requirements Site Acceptance Testing (SAT)

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

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

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

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

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

12.4 Specific Requirements Performance Benchmark Testing

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

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

12.5 Specific Requirements Cybersecurity

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

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

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

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

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

13 SUBMITTALS

13.1 General Requirements

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

14 QUALITY MANAGEMENT

14.1 General Requirements

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

15 ADDITIONAL INFORMATION REQUESTED

15.1 General Requirements

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

16 LOGISTICS

16.1 General Requirements

16.1.1 General logistics requirements are defined in the Agreement.