CONFIDENTIAL

Contract No. 5755

Ottawa Light Rail Transit (OLRT)

Systems Engineering and Assurance Technical Audit (EJV) Report

Document Number	SEMP-PSL-2018-AUD-2001
Version	1.0
Date	29 June 2018

Document Control

		Originated by		Reviewed by	
Original	**Version 1.0**	**Name, Role and Organization**	**Initials**	**Name, Role and Organization**	**Initials**
		F Oshunnyi	FO	Mary McGrath	MMcG
Accepted By		**Name, Role and Organization**	I confirm that I accept the contents of this document and that it can be issued to OLRT.		**Initials**
		Mary McGrath			MMcG
Date	29 June 2018	**Document Status**		Final Released Issue	

Amendment History

Version	Description	Initials	Date
1.0	Final Released Issue to Audit Sponsor	MMcG	29/06/2018

Contents

A. List of tables Contained Within this Report

Table No.1 List of Tables in this Report

1.0 Executive Summary

1.1 Introduction

SEMP Ltd was engaged by Ottawa Light Rail Transit Constructors (OLRT-C) to undertake a Systems Engineering Technical (Intrusive) Audit of EJV Limited, the organisation Designing the infrastructure for the Confederation Line.

The Technical (Intrusive) Audit was conducted between 15 April and 20 April 2018, in line with the Audit Notification Ref: SEMP-PSL-2018-AUD-2001 at OLRT-C Offices – Ottawa. The Audit Sponsor was OLRT-C – Sean Derry – Systems Assurance Manager

1.2 Audit Recommendations

Key Recommendations

The Technical (Intrusive) Audit findings are baselined against the outcome of the Systems Engineering Health Check undertaken in November 2017.

Requirements Management, Verification and Validation and RAM and Safety

1. EJV Project team shall prepare a detailed resource-loaded schedule of activities to address all audit findings/observations (including commitments given to the Auditor during the audit performance). The resource-loaded schedule is to include critical target dates and should be agreed with key stakeholders.

2. EJV Project shall develop and implement an action plan to monitor and demonstrate status reporting of which shall be managed by the Audit Sponsor (OLRT-C System Assurance Manager).

3. The flow of information between the Design Engineering and RAMS teams needs to be improved to minimise the risk of mis-alignment in analyses outcomes, and consequentially result in delays in project delivery.

1.3 Audit Observations

The SEMP Audit Team identified fifty-eight (58) Observations. The classification allocated to each observation (High, Medium, Low) is identified in Section 5.0. The classification rating is described in Table No. 6 section 4.6 of this report.

The EJV Project was not compliant with 15288 or 50126. The audit identified missing key elements of the standards requirements and EJV project needs to achieve a more robust compliancy by addressing the following audit observations.

Requirements, Verification and Validation

Observation No. 1: Requirements Management Plan and Verification and Validation Management Plan (Responsibilities) – Ensure EJV team are aware of the contents and the required application of the Requirements Management Plan (RMP) and Validation and Verification Plan (VVMP).

Observation No. 2: Requirements Management Plan – Document how the requirements process has been tailored for each Primary system. Review and update the RMP.

Observation No. 3: Client requirements – Project Agreement (PA) in DOORS needs to incorporate any agreed changes as defined in (but not limited to) variations, PADI Log, Request for Information (RFIs) documents.

Observation No. 4: Client requirements – Key, high risks, safety critical standards/codes need to be identified and included in the Requirements Management Process.

Observation No. 5: Client requirements – Evidence/assure that all ICDs have been reviewed and accepted by all parties (EJV/Thales/Alstom) – jointly signed records of agreement not evidenced.

Observation No. 6: Stakeholder needs and Requirements Definition – For each Primary System identify a list of the sources of stakeholder requirements that have been used as an input to the Design.

Observation No. 7: System Requirements Definition – Identify any key stakeholder requirements sources that require compliance statements against each clause. The requirements compliance statements need to be clearly identified as part of the Requirements Management Process.

Observation No. 8: Systems Requirements Definition – System requirements assessed as being high risk have not been identified for any of the Primary Systems within the EJV scope. The assessments for high risk need to be completed and developed.

Observation No. 9: Systems Requirements Definition – Requirements derived from Safety and RAM process have not been captured/evidenced.

Observation No. 10: Requirements traceability – Functional analysis outputs (derived requirements) are not currently evidenced in DOORS.

Observation No. 11: Requirements traceability – Procurement specifications do not include traceability back to the Primary System requirements. Procurement specifications need to be imported into DOORS and traced back to Primary System requirements.

Observation No.12 : Requirements Satisfied in Design – No apportionment of Project Agreement (PA) to Primary Systems has occurred – overall statement of compliance is required.

Observation No. 13: Requirements Satisfied in Design – No design evidence was able to be provided to enable design verification (missing information for completion of this element of the audit trail).

Observation No. 14: Requirements Satisfied in Design – No issues management process in place.

Observation No. 15: Requirements Satisfied in Design – Review the design compliance statements for compound clauses to confirm compliance statement is correct.

Observation No. 16: Requirements Satisfied in Design - No evidence was provided of the link between verification and validation events and status. Creation of V&V Matrix in DOORS in accordance with the VVMP providing traceability from tests back to requirements required.

Observation No. 17: Requirements Satisfied in Implementation - Clarify the division of roles and responsibilities relating to review and acceptance of the product verification and compliance data from suppliers.

Observation No. 18: Requirements Satisfied in Implementation – Clarify the division of roles and responsibilities relating to review and acceptance of the implemented system.

Observation No. 19: Requirements Satisfied in Implementation - Risk-based assessment of assurance is required against the compliance approach detailed in Memo 13 in order to confirm the sufficiency of this approach.

Safety

Observation No. 20: EJV Audit Planning – No evidence of Risk Based intrusion (RBI) Audit programme. No planned audits performed. No Safety (50126) audits performed on the project since inception.

Observation No. 21: EJV Safety Plan - Update Safety Plan to provide/include:

- Detail of the safety certification sign-off for an integrated asset.
- Incorporate the difference in approaches to different primary system designs.
- To address management of lower level suppliers' safety management process(es)
- Safety plan (Safety Argument) needs to state that the Safety report will only be provided for the Design case and excludes the test and commissioning phase. Update Figure No. 4.
- Safety Plan Rev 2.0 does not identify the process on how the management of the supplier for system safety is implemented.

- Safety validation activities- including software - the process of closing out hazards and related derived safety requirements for test and commissioning process needs to be established and detailed into the Safety Plan

Observation No. 22: EJV Safety Plan - The Safety Plan does not differentiate divisions of responsibility and who will be responsible for demonstrating that the safety risk associated with the as-commissioned asset design is ALARP. EJV are only responsible for demonstrating that the safety risks associated with the design of an integrated asset is ALARP (i.e. at (AfC) Approved for Construction drawing). OLRT-C are responsible for the T&C phase of the delivered finalised as-built design by EJV. EJV Safety Plan requires updating to address this observation.

Observation No. 23: **OLRT-C Safety Plan - Safety Planning -** OLRT-C Safety Plan not reviewed nor examined during this audit (not scope in this audit). OLRT-C to follow up and review their Safety Plan, to confirm that the divisions of responsibility are clearly described, who shall be responsible for safety risk associated with the as-commissioned asset design to ALARP. (*NOTE: EJV are only responsible for demonstrating that the safety risk associated with the design of an integrated asset is ALARP (I.e. as AfC approved drawing).*

Observation No. 24: Scope Definition - Hazard Management Matrix to be provided.

Observation No. 25: System Breakdown Structure - Required to be updated to achieve ISO 15288 compliance. The updated document needs to be mapped into the EJV Safety plan after it achieves compliance.

Observation No. 26: EJV Safety Organisation - Competency Training Matrix - to be supplied to Lead Auditor for Safety organisation (which is to match revised Safety Organisation Charts as detailed in the safety plan).

Observation No. 27: EJV Competency Management Regime - Information on competency management of personnel and induction of New Engineers including training requirements to be forwarded to Lead Auditor after audit performance. Response date to be determined by OLRT-C.

Observation No. 28: EJV Track Preliminary Hazard Analysis (PHA) - Track System scope definition requires update. Scope interfaces and interactions to be tabulated. Safety requirements top down and bottom up as well any interface derived requirements need defining. Process for management and transfer of safety risks at the interface level needs clearly defining. Process for the management and acceptance of residual safety risks by RTM and OC-Transpo needs defining.

Observation No. 29: EJV Track Preliminary Hazard Analysis (PHA)– Further development is required. The Track PHA Analysis has been undertaken at high level but is yet to be detailed. Auditor requires the analysis to be developed to incorporate appropriate detail.

Observation No. 30: EJV Track Preliminary Hazard Analysis (PHA) - The Track PHA listed a number of assumptions. However, it was highlighted that these were not assumptions but facts and should be reflected as such in the updated PHA. EJV to update the Assumptions section clearly defining what is in scope and what is out of scope. NOTE: Track PHA is the responsibility OLRT-C.

Observation No. 31: Interface Hazard Management (IHM) – EJV Safety Plan to provide detail on IHM including transfer process.

Observation No. 32: Fire Evacuation – (Shopping Centre) - EJV to provide a single document as evidence on how fire and evacuation risks have been managed in specific stations and in relation to the shopping centre.

Observation No. 33: OSHA – System Safety Plan to be updated with provision of data on how OSHA will be carried out. Responsibilities - OSHA shall be carried out at all levels (i.e. OLRT-C; EJV; Thales; Alstom).

Observation No. 34: PHA - Provision of evidence required that output of the safety analysis has been reviewed by the Engineer of Record.

Observation No. 35: Systems Integration PHAs for Integrated Safety Case - EJV to update the Safety Plan in detail, on the System Integration PHAs that will be carried out to demonstrate completeness of the analysis.

Observation No. 36: Hazard Log Structure - EJV to provide detail on Hazard Log Structure. (Structure to be similar to that of OLRT-C IHL is to be used).

Observation No. 37: Safety requirements - EJV to check and ensure that all safety requirements are identified and mapped to the Requirements V&V process to demonstrate that the safety measures/requirements have been included as part of the design development of systems and equipment in the EJV scope.

Observation No. 38: Allocation & Apportionment of Safety requirements including interfaces - EJV to provide detail on how they will demonstrate compliance to SIL 2 functionality against EN 50128 "Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems." This includes EN50128 requirement to have an independent reviewer within the EJV organisation (separate from the project and design organisation).

Observation No. 39: Use Cases - The Track PHA document identified a number of generic safety risks associated with the track design (e.g. broken rail). However, there was no traceability of how these safety risks have been managed in design and development of the track design including S&C.

Observation No. 40: Safety – EJV Configuration and Change Control - EJV need to ensure that all parties work to the most up to date Safety Plan Version.

Observation No. 41: Safety – Design Engineering Changes – No evidence could be cited where any changes that may have had a bearing of system safety was reviewed by a System safety and RAM Professional. Further, it could not be demonstrated that the Safety and RAM Analysis was reflective of the As-Built Design. NOTE: : OLRT-C Configuration and Management Plan that is currently under production calls for safety assessments to be carried out on potential major design change that may arise from the T&C Phase.

Observation No. 42: Safety – Test results from Test and Commissioning activities meeting safety requirements – EJV Safety function is not being made aware of the test results in order to check these are meeting the safety requirements. Greater collaboration required between EJV Design Engineering and Safety & RAM Teams, particularly in relation to requirements management and final design/build configuration.

Safety Case

Observation No. 43: System Safety - Safety Case – EJV to provide detail on the safety argument for the Integrated Station asset.

Observation No. 44: Safety Argument for All Primary Systems – Suppliers of sub-systems need to provide safety case documentation to substantiate the safety claims and arguments and these must be captured by the EJV Hazard Log , PHA and final safety report. Safety plan needs to be updated **– also See Observation No.21**.

Observation No. 45: Safety reports – Each Station Type – Safety report shall be produced for each type of Station which shall include the Civil, Architectural, Mechanical, Electrical and Public Health as well as communications systems – key risks to be demonstrated for the functionality for each station which must include Fire and Evacuation risks.

Observation No. 46: Safety Validation Activities (including software) – EJV to provide detail of their responsibilities for hazard resolution for the detailed design phase. (NOTE: OLRT-C have the responsibility to provide Test and commissioning evidence to support closure of hazards and its related derived safety requirements). EJV to clearly define this responsibility in the next System Safety plan revision (uplift of document).

Observation No. 47: OLRT-C and EJV - Integrated safety argument – A joint OLRT-C/EJV activity to be instigated – agreement to be reached on who will provide the integrated safety argument for the integrated Asset. Key example: Station, TVS etc.

Observation No. 48: SIL 2 – Software requirements - The next revision of Software Development Plan needs to demonstrate how the software development process will demonstrate compliance against SIL 2 EN 50128 (PA Requirements).

RAM

Observation No. 49: RAM Planning – EJV RAM Plan – Updated RAM Plan required the observations raised on the EJV Safety Plan relating to scope, system boundaries and definitions, division of responsibility between IFC design and test and commissioning shall be applied to the revised next revision of the EJV RAM plan update.

Observation No. 50: RAM Organisation – Insufficient EJV resource for the RAM activity. OLRT-C to review their Safety and RAM resource profile to ensure that they, themselves as receivers of assurance documentation can carry out a thorough review and acceptance of the cascade of documentation that will be submitted in the coming months. Go to Section 1.2 Audit Recommendation - Key recommendation No.1 and Key Recommendation No.3.above.

Observation No. 51: RAM Analysis – EJV RAM Analysis yet to commence. The audit concentrated on RAM Planning as there were no RAMS Analysis to sample. See Observation No.52 below.

Observation No. 52: RAM Methodology for calculations and FMECA Template – Methodology for calculating reliability and maintainability of primary systems needs to be agreed with OLRT-C prior to initiating any RAM calculations. FMECA template requires acceptance by OLRT-C prior to initiating any FMECA work.

Observation No. 53: RAM Maintenance Task Analysis – EJV to ensure that RTM are to be a stakeholder in the maintenance task analysis output.

Observation No. 54: RAM Requirements / Apportionment of RAM Requirements / RAM Validation activities – Planning - EJV to comprehensively address the issue of RAM requirements in order to support adequate planning, activities and demonstration against requirements.

Observation No. 55: RAM Requirements - RAM Targets / Apportionment of RAM Requirements, RAM Validation activities – EJV to seek clarification from Client with regards to specific RAM targets.

Observation No. 56: **Safety and RAM Validation Plans –** EJV needs to clearly document the relevant systems engineering approach in line with PA requirements.

Observation No. 57: RAM Demonstration (Collaborative working groups) – Resource - Design engineering need to provide the necessary technical evidence for the safety team(s) to deliver the necessary safety approvals for all Primary Systems and the final integrated solution. EJV could not provide any detail on what requirements are for the EJV Scope of delivery for Reliability Demonstration.

Observation No. 58: RAM Plan does not include a section on Reliability Demonstration. EJV to add section to cover this element.

Assurance and Competency

Processes

Observation No. 2: Validation and Verification Plan (VVMP) – Document how the requirements process has been tailored for each system. Review and update the VVMP.

Observation No. 4: Client requirements – Key, high risks, safety critical standards/codes need to be identified and included into the Requirements Management Process.

Observation No. 7: System Requirements Definition – Identify any key stakeholder requirements sources that shall require compliance statements against each clause. The requirements compliance statements need to be clearly identified as part of the Requirements Management Process.

Observation No. 14: Requirements satisfied in Design – No issues management process in place.

Risk Management

Observation No. 20: EJV Risk Based intrusion Audit Programme - No Risk Based intrusion (RBI) audit programme. No audits performed on the project concerning 15288, 50126 standards scope and the PA.

Competency

Observation No. 26: EJV Safety Organisation - Competency Training Matrix - To be supplied to Lead Auditor for Safety organisation (which is to match revised Safety Organisation Charts as detailed in the safety plan).

Observation No. 27: EJV Competency Management Regime - Information on competency management of personnel and induction of New Engineers including training requirements to be forwarded to lead Auditor after audit performance.

Audit Outcome Conclusion
Poorly Controlled

2.0 Introduction and Background

2.1 Introduction

In November 2017 SEMP Ltd were engaged by OLRT-C to provide a Systems Engineering Health Check for the Confederation Line project as requested by the City of Ottawa (the Client, the Railway Owner, the Railway Operator and the Railway Regulator) appointed Safety Auditor (SA), TUV. The City's SA had been requested to provide an interim assessment of OLRT-C progress in light of the OLRT-C 180-day Notice of Revenue Service Availability.

2.2 Background

The intent of the Systems Engineering Health Check was to provide a level of confidence that OLRT-C is on track to deliver an integrated, safe, operational railway system in time for the planned start of revenue service. The broad findings from the Health Check are illustrated in Figure 1.

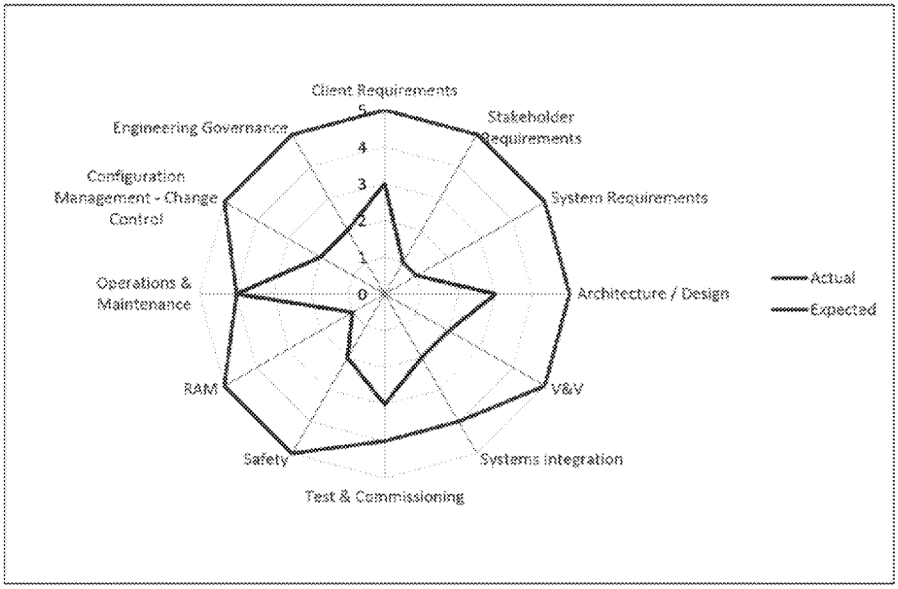

Figure No 1. SEMP Health Check Illustration

As a follow on from the Systems Engineering Health Check, OLRT-C System Assurance Manager (Audit Sponsor) of Ottawa Light Rail Transit Constructors (OLRT-C) commissioned a further suite of audits of all participating "Primary System Suppliers" to occur in sequence.

2.3 Purpose of Audit

Evaluation of Systems Engineering Process

Systems Engineering Process covering Safety and RAM(s), together with evidenced Assurance outputs to verify compliance against the Project Agreement (PA) contract clauses, engineering requirements and standards.

2.4 Scope of Audit

Primary Systems Level - Requirements, Validation and Verification, Systems Assurance and Systems Engineering Process, Safety, RAM(S), Assurance documentation (outputs)

Primary (Rail) Systems to be Examined / Sampled

Tunnel Ventilation System (TVS) including interface to signalling and comms;

Traction Power (including HV AC Switchgear),

Transformer Rectifier, 1500Vdc switchgear,

Disconnect and Transfer switch,

Rail Grounding Switch,

Stray current, emergency trip;

Track Work – Switch Machines only;

Communications and Control (including SCADA);

TSCC (Transit System Control Centre);

Underground and Elevated Station

2.5 Audit Criteria

Safety Standards - BS EN50126, BS EN 50128 (IEC 62279), BS EN 50129, IEC 61508, ISO/ IEEE 15288, DOT-FTA-MA-26-5005-00-01 (Hazard Analysis Guidelines for Transit Projects, U.S. Department of Transportation, Federal Transit Administration (January 2000)

RAMS Standards – IEEE 497, ISO 14224, CAN/CSA – 0632-90 – Reliability and Maintainability Management Guidelines, CAN/CSA-0396 – Software Quality Assurance Standards

Project Agreement - Schedule 15-2, Part 1, Schedule 15-2, Part 1, Article 9 & 10

Competency - Canadian Professional Engineers Act (PEO)

2.6 Audit Objectives

REQUIREMENTS, VALIDATION AND CERIFICATION

2.6.1 Objective No 1: REQUIREMENTS

a. To confirm that a requirements management process is fully evidenced and implemented.

b. To confirm that a complete, correct and validated requirements set exists including Client requirements, stakeholder requirements and derived requirements (from specialist disciplines such as safety / RAM).

c. To confirm that requirements are traced – where the requirements came from and where they are satisfied.

2.6.2 Objective No 2: VALIDATION AND VERIFICATION

a. To confirm that a Verification and Validation management process is fully evidenced and implemented.

b. To confirm that the requirements have been satisfied in preliminary design, that they are also satisfied in final (detailed) design, and, satisfied in the construction / installation, integration, and trial commissioning stages.

SYSTEMS ENGINEERING – SAFETY (RAMS)

2.6.3 Objective No 3: SAFETY ORGANISATION AND PLANNING

a. Examine and review the Safety Case, Strategy and Approval Process

b. Determine / Identify Safety and safety related documentation and its management

c. Review Safety Assessment including Independent Safety Assessment (ISA), where applicable

2.6.4 Objective No 4: HAZARD LOGS AND SAFETY REQUIREMENTS

Perform a targeted sample compliance inspection of the Hazard Log(s) and Safety Requirements

d. Identify the RAM Organisation and Planning responsibilities (competencies)

e. Examine Hazard Log Management - Safety Analysis – Hazard Identification, Hazard Analysis, Interface Hazard Analysis, Risk Assessment, Change Safety Analysis – (process, controls and management)

f. Sample and pull for evidence RAM Analysis – Modelling, Apportionment of targets and requirements,

g. Check Failure mode analysis and management (e.g. failure mode and effects analysis)

h. Check and determine maturity and completeness of the Reporting and Corrective Action System trackers and action plans.

2.6.5 Objective No 5: ASSURANCE & COMPETENCY

a. Check for Organisation charts (Organograms) – Design and Assurance
b. Quality (Design) Assurance Management Plans – Check management controls, distribution and periodic review cycles
c. Check Design and Assurance RFI, TQ, NCRs tracker logs and their management (pertinent to the Packages identified in this audit scope);
d. Sampling and Cross checks to the Delegated Authorities Listing (Competency Plan Signatories) on the selected random samples - assurance sign off.

3.0 Audit Information

3.1 Audit Notification

The audit notification was prepared by the SEMP Audit Team on 30th March 2018 and released for issue to EJV through OLRT-C offices on 4TH April 2018. OLRT-C were tasked (in the capacity of the Audit Sponsor role) to manage the collection, collation and issue of key documentation in response to SEMP requests. See Attachment No.1 to this report.

There was no EJV documentation or data(Plans) received by the SEMP Audit team from OLRT-C for the preparation and review for the audit from the Audit Sponsor.

Therefore, in the absence of any EJV documentation or data having not been received from OLRT-C - the OLRT-C Systems Assurance Management Plan (SAMP) – a document produced by SEMP - was used as the baseline for the preparation for the audit examination.

3.2 Audit Timetable

Item	Scheduled Activity Date	Week No / Year 2018
Preparation and planning		
Authority to Proceed from Audit Sponsor	Week commencing 3rd March 2018	Week No 10 Year 2018
Audit notification scoping and preparation Issue Audit Notification to audit sponsor	30th March 2018 ~~4th April 2018 Initial issue~~ 5th April 2018 Final issue	Week No 14 Year 2018 Week No 14 Year 2018 Week No 14 Year 2018
Audit Performance DESKTOP OFFSITE		
Desktop review examination of objective evidence OFF SITE	Early April 2018	Week No 14/15 Year 2018
Audit Performance ON SITE		
Opening Meeting	16th April 2018 MORNING	Week No 16 Year 2018
Start of Site Fieldwork	16th April 2018 AFTERNOON	Week No 16 Year 2018
End of Site Fieldwork	19th April 2018	Week No 16 Year 2018
Closing meeting (Wash Up)	20th April 2018 AFTERNOON	Week No 16 Year 2018
Audit Reporting OFFSITE		
Commence and Prepare draft audit report on field work findings	24th April 2018	Week No 17 Year 2018
Target Issue date of completed report	25th May 2018	Week No 21 Year 2018
Final Audit Report target Issue date Final Report Issue date	25th May 2018 21th June 2018	Week No 21 Year 2018 Week No 25 2018
Follow Up & Close Out of Audit Findings	NONE by SEMP – Follow up and close out of Audit Findings and Issues to be by OLRT-C	OLRT-C to manage

TABLE No. 2 Audit Timetable

3.3 Audit Itinerary (Confirmed)

Date / Time	Duration	Topic Element	Cognisant Personnel
16th April 2018 - Mon Day 1 9.00am – 12.30pm INTRODUCTIONS	0.5 day	Opening Meeting **Sign the Audit Attendance Signatory Log** **Setting the scene – Introductions** **Scope and Purpose of Audit Explained** **Agreeing (this) Proposed Audit Itinerary**	ALL Lead Auditor SEMP Audit team ALL
		LUNCH	
1.30pm – 5.00pm	0.5 day	Requirements, Validation & Verification + Design Primary System Track	**S Gilbey / S Leonard + D Ellis**
	0.5 day	Safety and RAM (RAMS) + Assurance Primary System Track	**J Ahmed / M McGrath/ F Oshunniyi+ D Ellis Team**
17th April 2018 - Tues Day 2 9.00am – 12.30pm	0.5 day	Requirements, Validation & Verification + Design Primary System Stations	**S Gilbey / S Leonard + D Ellis Team**
	0.5 day	Safety and RAM (RAMS) + Assurance Primary System Stations	**J Ahmed / M McGrath/ F Oshunniyi + D Ellis Team**
		LUNCH	
1.30pm – 5.00pm	0.5 day	Requirements, Validation & Verification + Assurance Primary System Traction Power	**S Gilbey / S Leonard + D Ellis Team**
	0.5 day	Safety and RAM (RAMS) + Assurance Primary System Traction Power + Integration	**J Ahmed / M McGrath/ F Oshunniyi + D Ellis Team**
18th April 2018 – Wed Day 3 9.00am – 12.30pm	0.5 day	Requirements, Validation & Verification + Design Primary System Traction Power	**S Gilbey / S Leonard + D Ellis Team**
	0.5 day	Safety and RAM (RAMS) + Assurance Primary System Traction Power & Distribution (Up to OC) incl integration	**J Ahmed / M McGrath/ F Oshunniyi + D Ellis Team**
		LUNCH	
1.30pm – 5.00pm	0.5 day	Requirements, Validation & Verification + Design Primary System TVS	**S Gilbey / S Leonard + D Ellis Team**
	0.5 day	Safety and RAM (RAMS) + Assurance Primary System TVS	**J Ahmed / M McGrath/ F Oshunniyi + D Ellis Team**
19th April 2018 – Thurs Day 4 9.00am – 12.30pm	0.5 day	Requirements, Validation & Verification + Design Primary System Comms	**J Ahmed / M McGrath/ F Oshunniyi + D Ellis Team**

	0.5 day	Safety and RAM (RAMS) + Assurance Primary System Comms	**J Ahmed / M McGrath/ F Oshunniyi + D Ellis Team**
		LUNCH	
1.30pm – 5.00pm AUDIT performance END	0.5 day	Requirements, Validation & Verification + Design Primary System Comms	**J Ahmed / M McGrath/ F Oshunniyi + D Ellis Team**
	0.5 day	Safety and RAM (RAMS) + Assurance Primary System Comms	**J Ahmed / M McGrath/ F Oshunniyi + D Ellis Team**
20th April 2018 – Fri Day 5 9.00am – 1.00pm AUDIT FINDINGS REVIEW	0.5 day	SEMP Audit Team Caucus – findings review	SEMP AUDIT TEAM ONLY
2.00pm – 3.30pm	1.5 hrs	Closing Meeting Sign the Audit Signatory Attendance Log **Wash up & feedback (*Summarising the audit findings – high level- initial report)*** **Timetable for audit report delivery** **Required** response(s) timetable **- close out dates for audit findings**	ALL SEMP Audit team Audit Sponsor Auditees to agree with OLRT-C

Table No. 3 Audit Itinerary (Confirmed)

3.4 Audit team

SEMP Audit Team

- SEMP - Lead Auditor – M McGrath Email: mary.mcgrath@sempltd.com
- SEMP Requirements, Verification and Validation Auditor – S.Gilbey & S.Leonard
- SEMP - Systems Engineering, Integration and System Architecture – D Wynne
- SEMP - RAM and Safety Auditors – Dr. J Ahmed and F Oshunniyi

3.5 Auditee Details and Location

EJV

EJV Audit Host: David Ellis – Senior Designer Manager

Email: David.Ellis@snclavalin.com

1.3.5 Auditee Participants

The audit was conducted over a series of interviews to assess the EJV team's compliance with the Audit objectives and reference documents (outlined in the Audit Notification Ref: SEMP-PSL-2018-AUD-2001). There was a core team of auditees, which was then supported by other organisation members to respond to specific queries or contribute to lines of enquiry.

EJV representation, at varying times during the audit, included (but not limited to):

- EJV – Design Manager
- EJV - Safety team
- SNC-L – Director – Safety and System Assurance
- SNC – RAM Engineer
- EJV – Quality Manager
- EJV (WSP) Project Co-ordinator
- OLRT-C – Systems Engineering
- EJV – Communication(s) Systems Engineer
- EJV – Electrical Facilities

1.3.6 Audit Observers

There were some 20+ Observers in attendance during the audit performance. The Observers (representative sample below) were (but not limited to):

- OLRT-C Safety representative
- Ottawa City Representatives (including Safety Auditor)
- OLRT-C – V&V Lead
- OLRT-C – V&V Engineer
- OLRT-C – Safety Assurance Engineer
- OLRT-C – RAM Specialist
- RTM – Maintenance Director
- EJV – Commercial management
- OLRT-C – Technical, Design, Integration
- OLRT-C - Systems Assurance Engineer
- OC Transpo – CSO & Transit Operations

(For a detailed listing of all attendees – see Attachment No. 2)

3.6 Reference documents

ISO 9001:2008 / 2015 Quality Management Systems – Requirements

BS ISO 10018:2012 Quality Management - Guidelines on People Involvement and competence

ISO 19011:2015 Guidelines for auditing management systems

Document number awaited from OLRT-C (SEMP produced) Systems Assurance Management Plan (SAMP) – *review by Safety Auditor – Pending*

OLRT-C AAPP WBS & Schedule - Latest issue

3.7 Glossary (Terms, Abbreviations and Definitions)

Term	Definition	Source
Activity	Smallest identified object of work in a project	ISO 9000:2015
Audit	Systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.	ISO 9000:2015
Audit Client (Sponsor)	Organisation or person requesting an audit	ISO 9000:2015
Audit Conclusion	Outcome of an audit provided by the auditor / audit team after consideration of the audit objectives and all audit findings	ISO 9000:2015
Audit criteria	Set of Policies, procedures or requirements used as a reference against which objective evidence is compared	ISO 9000:2015
Auditee	Organisation being audited	ISO 9000:2015
Audit Evidence	Records, statements of fact or other information, which are relevant to the audit criteria and verifiable	ISO 9000:2015
Audit Findings (Issues)	Results of the evaluation of the collected audit evidence against audit criteria	ISO 9000:2015
Auditor	Persons who conducts the audit	ISO 9000:2015
Audit Plan / Audit Itinerary	Description of the activities and arrangement for an Audit	ISO 9000:2015
Audit programme	Set of one or more audits planned for a specific time frame and directed towards a specific purpose	ISO 9000:2015
Audit Scope	Extent and boundaries of an audit	ISO 9000:2015

Term	Definition	Source
Capability	Ability of an object to realise an output that will fulfil the requirements for that output	ISO 9000:2015
Characteristic	Distinguishing feature	ISO 9000:2015
Competence	Demonstrated ability to apply knowledge and skills to achieve intended results	ISO 9000:2015
Concession	Permission to use or release a product that does not conform to specified requirements	ISO 9000:2015
Conformity	Fulfilment of requirement	ISO 9000:2015
Continual improvement	Recurring activity to enhance performance	ISO 9000:2015
Contract	Binding agreement design and development set of processes that transform requirements for an object into more detailed requirements for that object	ISO 9000:2015
Correction	Action to eliminate a detected conformity	ISO 9000:2015
Corrective Action	Action to eliminate the cause of a non-conformity and to prevent re-occurrence	ISO 9000:2015
Corrective Action Request (CAR)	A form used during audit performance / reporting to request that action be taken to correct a non-conformance identified during an audit	ISO 9000:2015
First Party Audit	Also called an Internal Audit. An audit conducted by SEMP on itself, for management review and other internal purposes (e.g. to confirm the effectiveness of the management system or to obtain information for the improvement of the management system). Internal audits can form the basis for self-declaration of conformity.	ISO 19011:2011

Term	Definition	Source
Second Party Audit – EXTERNAL AUDIT	Supplier Audit.	ISO 19011:2011
Third Party (Certification) Audit	Audit carried out by an auditing organisation independent of the Client and the user, for certifying Client Management system. (E.g. BSI; LRQA; BVQI; SGS, other)	ISO/IEC ISO 17021:2011
Guide	Person appointed by the auditee to assist the audit team	ISO 9000:2015
NDA	Non-Disclosure Agreement	Commercial requirement contract
Non-Conformity	Non-fulfilment of a requirement	ISO 9000:2015
Observation	Applicable Audit Methods – Table B1.	ISO 19011:2011 Annex B
Objective Evidence	Data supporting the existence or verity of something	ISO 9000:2015
Recommendation	Points specified by the audit plan – good practice and opportunities for improvement	ISO 19011:2011 Clause 6.4.7
Output	Result of a process	ISO 9000:2015
SMART	Specific, Measurable, Achievable, Relevant/Realistic and Timebound	Quality
EOC	Engineer of Record	Canadian Professional Engineers Act (PEO)
PHA	Preliminary Hazard Analysis	50126

Term	Definition	Source
RAM	Reliability, Availability and Maintainability	50126
RMP	Requirements Management Plan	51288
RFI	Request for information	RECORD
VVMP	Validation and Verification Plan	51288

Table No. 4 Glossary (Terms, Abbreviations and Definitions)

4.0 Audit Protocols

4.1 Opening Meeting

4.1.1 Setting the scene for the Audit

The Lead Auditor introduced the Audit (Examination) Team, explained the purpose of the audit and its objectives.

The Proposed Audit itinerary was discussed, and the Confirmed Itinerary agreed. It was further explained that there would be zero Corrective Actions Requests (Non-Conformances, Deficiency report(s) raised by SEMP Audit team during the performance of this audit.

It was explained that the audit progress would be recorded by the Lead Auditor and any observations would be allocated a finding classification (See Paragraph 4.9 below for Audit Classifications).

It was further explained that OLRT-C would be managing the audit report findings and their subsequent or required close out. The SEMP Audit Team were solely engaged to Prepare and Perform the audit and that the SEMP Audit Team remit finished with the delivery of the Audit Report (This document).

4.1.2 Non-Disclosure Agreement (NDA)

There was no NDA required or signed up to facilitate the performance of this audit.

4.2 Introductions and Attendance Signatory Logs

Attendance Logs were signed each person in attendance whom also introduced themselves for the record. See Attachment No. 2 appended to this to this report for all attendance signatory logs. Prior to the audit performance commencement, the participating auditees were identified for participation in the audit examination.

Note 1: At commencement of each day or at every new section (element) of the audit performance, attendance signatory logs were completed. These signatory logs identify all those whom participated / or who were observers during the audit performance.

4.2.2 Observers of Audit (Assurance Partners)

Note 1: Observers (Assurance Partners) remained during the audit activity (performance) either for the whole of the audit (as identified in the audit itinerary and as detailed in the signatory attendance logs) or for part of the audit.

Note 2: Observers present during the audit performance were informed by the Lead Auditor at the opening meeting, that they cannot influence the audit trail, or the recording of objective evidence being delivered but can make suggestions for the Lead Auditor to consider for use, or not, for input into the Audit report.

4.3 Audit Process

During the Audit opening Meeting the protocol for the audit performance was explained the Lead Auditor, these were as follows:

4.4 Revisions to Audit Scope

The Lead Auditor (Audit Team) undertakes documentation review, audit discussions with the auditees and observations together the necessary evidence. Any revisions to the audit scope required during the audit performance must be agreed with the Audit Sponsor, Assurance Partner and Principal Auditees.

4.5 Key issues Identified

Key issues identified during the audit performance must be raised with the auditee as soon as they arise. The Lead Auditor keeps the Assurance Partners and the Principal Auditees informed of the assignment progress, emerging findings and any agreed actions.

4.6 Significant Issues

Significant issues that indicate a Poorly Controlled conclusion (see section 4.7 below) must be brought to the attention of the Audit Sponsor, Assurance Partners and Principal Auditees at the earliest opportunity. Any conditions or practices that are legislative or system engineering non-compliances or present a risk to health and safety of others must be reported immediately to the manager responsible as well as the Principal Auditees and Assurance Partners.

4.7 Audit Conclusion Categories

The significance of the issues identified is used to determine the overall conclusion of the audit as follows:

Audit Conclusion	Audit Description
Well controlled	Only to be given in circumstances where there are no issues to report, and the Lead auditor feels it appropriate, a conclusion of well controlled may be achieved.
Adequately controlled	Generally, there are no Priority 1 high risk issues, some Priority 2 medium risk issues and / or any number of Priority 3 Low risk issues. Control systems are effective but some opportunities to strengthen the control environment have been identified. Circumstances may arise where although there is a Priority 1 issue the overall conclusion is adequately controlled.
Requires improvement	One or more Priority 1 High risk issues, together with any number or Priority 2 Medium risk and/or Priority 3 Low risk issues. In this situation, the control environment is generally not effective, although there has not been a widespread breakdown in controls. Circumstances may arise where there are no Priority 1 High risk issues, but the volume of Priority 2 Medium risk or Priority 3 Low risk issues warrants an overall conclusion of requires improvement.
Poorly controlled	One or more Priority 1 High risk issues, together with any number or Priority 2 Medium risk issues, and/or Priority 3 Low risk issues. Issues are of a nature that indicates widespread weakness in control or a basic lack of control in the area under review.

Table No. 5 Audit Conclusion Categories

4.8 Audit Findings Classifications

During the performance of the audit the Auditors and the Principal Auditees agreed the categorisation of findings (Red, Amber, Green). These classifications are evidenced in Section 5.0 Detailed Report.

See table below for categorisation definitions.

Level	Description
Priority 1 – HIGH RISK	Significant weakness(es) in the control environment which, if not addressed, have the potential to undermine the achievement of key corporate and / or business area objectives.
Priority 2 – MEDIUM RISK	Oher control weaknesses that are less significant, but nonetheless have the potential to threaten achievement of corporate and or/business area objectives.
Priority 3 – LOW RISK	Whilst not necessarily a control weakness there is a potential for process improvement by, for example, ensuring compliance with good practice, increasing process efficiency, identifying area of 'over control'; or strengthening the overall control environment by building upon the existing controls.
Good Practice	Controls, practices, processes etc. judged to be above what is normally expected

Table No. 6 Audit Findings Classifications

4.9 Recording of Findings during Audit Performance

During the Audit Performance the discussions, questions and answer examination scenarios were recorded by the Lead Auditor to facilitate the production of this audit report. Any deficiencies or adverse finds were agreed with the auditee as the audit progresses. The audit findings classifications were applied as jointly agreed.

4.10 Closing Meeting

The Closing Meeting was attended by EJV, OLRT-C, City and Safety Auditor representatives and the SEMP Audit Team. The Attendance signatory log was signed for Closing meeting. SEMP Audit team gave a presentation in the form of an initial report of the audit findings and outline recommendations. See Attachment No. 3

5.0 Detailed Report

5.1 Requirements and Verification and Validation

ISO/IEC/IEEE 15288 Basis

Lifecycle Stage	Requirements Activities	V&V Activities
Stakeholder needs and requirements definition	• Identify System Stakeholders and define needs • Define required characteristics and context of use of capabilities and concepts in the life cycle stages, including operational concepts. • Identify system Constraints • Prioritise Stakeholder needs and transform into clearly defined requirements.	• Define Critical performance measures • Stakeholder agreement that their needs and expectations are reflected adequately in the requirements is achieved. • Any enabling systems or services needed for stakeholder needs and requirements are available. • Traceability of stakeholder requirements to stakeholders and their needs is established.
System requirements definition process	• Define the system description, including system interfaces, functions and boundaries, for a system solution • Define System requirements (functional, performance, process, non-functional, and interface) and design constraints.	• Define Critical performance measures • Analyse system requirements • Any enabling systems or services needed for system requirements definition are available. • Traceability of system requirements to stakeholder requirements is developed.
Architecture definition process	• Generate system architecture alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet system requirements, and to express this in a set of consistent views. • Concepts, properties, characteristics, behaviours, functions, or constraints that are significant to architecture decisions of the system are allocated to architectural entities. • Identify System elements and	Confirm: • Stakeholder concerns are addressed by the architecture. • Architecture viewpoints are developed. • Context, boundaries, and external interfaces of the system are defined. • Architecture candidates are assessed • Architecture views and models of the system are developed. • Alignment of the architecture with requirements and design

Lifecycle Stage	Requirements Activities	V&V Activities
	their interfaces	characteristics is achieved. • Any enabling systems or services needed for architecture definition are available. • Traceability of architecture elements to stakeholder and system requirements is developed
Design definition process	• Design characteristics of each system element are defined. • System requirements are allocated to system elements. • Design enablers necessary for design definition are selected or defined. • Interfaces between system elements composing the system are defined or refined. • Design alternatives for system elements are assessed. • Design artefacts are developed.	• Any enabling systems or services needed for design definition are available. • Traceability of the design characteristics to the architectural entities of the system architecture is established
System analysis process	• System analyses needed are identified. • System analysis assumptions and results are validated. • System analysis results are provided for decisions.	• Any enabling systems or services needed for system analysis are available. • Traceability of the system analysis results is established.
Implementation process	• Implementation constraints that influence the requirements, architecture, or design are identified. • A system element is realized. • A system element is packaged or stored.	• Any enabling systems or services needed for implementation are available. • Traceability is established.
Integration process	• Integration constraints that influence system requirements, architecture, or design, including interfaces, are identified. • Any enabling systems or services needed for integration are available. • A system composed of implemented system elements is integrated. • The interfaces between the system and the external environment are checked. • Integration results and anomalies are identified.	• Approach and checkpoints for the correct operation of the assembled interfaces and system functions are defined. • The interfaces between the implemented system elements that compose the system are checked. • The interfaces between the system and the external environment are checked. • Traceability of the integrated system elements is established.
Verification process	• Provide objective evidence that a system or system element fulfils its specified requirements and	• Constraints of verification that influence the requirements, architecture, or design are

Lifecycle Stage	Requirements Activities	V&V Activities
	characteristics. • The Verification process determines that the "product is built right". The Validation process determines that the "right product is built	identified. • Any enabling systems or services needed for verification are available. • The system or system element is verified. • Data providing information for corrective actions is reported. • Objective evidence that the realized system fulfils the requirements, architecture and design is provided. • f) Verification results and anomalies are identified. • Traceability of the verified system elements is established.
Validation process	• Provide objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment.	• Validation criteria for stakeholder requirements are defined. • The availability of services required by stakeholders is confirmed. • Constraints of validation that influence the requirements, architecture, or design are identified. • The system or system element is validated. • Any enabling systems or services needed for validation are available. • Validation results and anomalies are identified. • Objective evidence that the realized system or system element satisfies stakeholder needs is provided. • Traceability of the validated system elements is established

Table No. 7 Project Lifecycle Requirements, Verification and Validation Related Lifecycle

5.2 Safety and RAM

EN 50126 Basis

This followed the guidance provided in Figure 9 of EN 50126 which presents the railway delivery lifecycle stages and outlines Safety and RAM activities/deliverables to be prepared and undertaken at each stage.

A subset of the lifecycle stages and related activities and deliverables (in bold text) are outlined in Table 8 below. These were systematically followed to assess compliance. Audit findings are presented in section 5 of this report.

Lifecycle Stage	Key Safety Activities and Deliverables	Key RAM Activities and Deliverables
System definition and application conditions	• Evaluate past experience data for safety • Perform Preliminary Hazard Analysis (PHA) • Establish (overall) **Safety Plan**	• Evaluate past experience for RAM • Perform preliminary RAM analysis • Set RAM Policy
Risk Analysis	• Perform system hazard and safety risk analysis. • Set up Hazard Log • Perform risk assessments	N/A
System Requirements	• **Specify (and elicit) system safety requirements (overall)** • Define Safety Acceptance Criteria • Define safety related functional requirements • Establish safety management	• **Specify system RAM requirements** • Define RAM acceptance criteria • Define system functional structure • Establish **RAM programme** • Establish **RAM Management Plan**
Apportionment of System Requirements	• Apportion of system safety targets and requirements • Specify sub-system and component safety requirements • Define sub-system and component safety acceptance criteria	• Apportion of system RAM targets and requirements • Specify sub-system and component RAM requirements • Define sub-system and component RAM acceptance criteria
Design and Implementation	Implement safety plan by review, analysis, testing and data assessment including: • Hazard log • Hazard analysis and risk assessment • Justify safety related design decisions • Undertake programme control (covering safety management and control of sub-contractors and suppliers) • Prepare generic safety case • Prepare generic application safety case	• Implement RAM programme by review, analysis, testing and data assessment including: ○ Reliability and availability ○ Maintenance and maintainability ○ Logistic support • Undertake RAM programme management and control of sub-contractors and suppliers.
Manufacturing	• Implement safety plan by review analysis and testing • Use the hazard log.	• Perform environmental stress screening • Perform RAM improvement testing • Commence Failure Reporting and Corrective Action System (FRACAS)

Lifecycle Stage	Key Safety Activities and Deliverables	Key RAM Activities and Deliverables
System Validation (including safety acceptance and commissioning)	• Prepare Application Specific Safety Case.	• Perform RAM Demonstration

Table No. 8 Project Lifecycle Safety and RAM Related Lifecycle

5.3 Audit Output

Requirements and V&V

Audit Theme	ISO15288 Applicable Clause	Reviewed Document	Observation/Objective Evidence	RAG	Remedial Action /Recommendation
Requirements Management Plan and Process	N/A	OLR-50-0-0000-MPL-0007 Rev B Requirements Management Plan	**Partially compliant** A Requirements Management Plan was produced by EJV in November 2017 but was not completed or issued. The OLRT-C RMP was released in February 2018 and EJV are now following this plan. While the plan is compliant to ISO15288, awareness of the plan and the processes was primarily limited to the systems integration team.	A	**Observation No.1** Ensure EJV project team are aware of the RMP. **Observation No.2** The RMP provides for a tailored approach for each primary system. EJV to document how the requirements process has been tailored for each primary system.
Verification and Validation Plan and Process	**6.4.9** Provide objective evidence that a system or system element fulfils its specified requirements and characteristics.	OLR-50-0-0000-MPL-0006 OLRT-C VVMP	**Compliant** A Verification and Validation Plan was stated to have previously been produced by EJV, but no evidence of the document was provided during the audit. The OLRT-C VVMP was released in February 2018 and EJV are now following this plan. While the plan is compliant to ISO15288, awareness of the plan and the processes was primarily limited to the systems integration/V&V team.	G	**Observation No.1** Ensure EJV project team are aware of the VVMP.
Client Requirements	**6.4.2** Define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment. Identify stakeholders, or stakeholder classes, involved with the system throughout its life cycle, and their needs.	EJV DOORS	**Partially compliant** Client requirements have been provided to EJV in the form of the Project Agreement. The Project Agreement is held within the project DOORS database. The PA requirements in DOORS have previously been updated with agreed changes identified in the PADI log but it could not be confirmed whether this included the latest changes.	A	**Observation No.3** Ensure the PA held within DOORS incorporates any agreed changes as defined in variations, PADI Log, RFI etc.
Client Requirements	**6.4.2** Define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment. Identify stakeholders, or stakeholder classes, involved with the system throughout its life cycle, and their needs.	PA Agreement ; NFPA130	**Partially compliant** The Project Agreement requires compliance to a broad range of standards. There are defined processes for determining compliance to many of these standards (building/occupancy permits for example). For certain key, high risk or safety critical standards such as NFPA130 an overall statement of compliance is unlikely to be sufficient and these standards need to be managed on a clause by clause basis.	A	**Observation No.4.** Taking a risk-based approach, identify any key, high risk, safety critical standards/codes where an overall statement of compliance is insufficient, for example NFPA130, and include these standards in the requirements management process.

Audit Theme	ISO15288 Applicable Clause	Reviewed Document	Observation/Objective Evidence	RAG	Remedial Action /Recommendation
Client Requirements	**6.4.2** Define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment. Identify stakeholders, or stakeholder classes, involved with the system throughout its life cycle, and their needs.	PA Agreement ; NFPA130	**Partially compliant** There has been an exercise to identify the primary systems associated with each clause in the PA. However, apportionment of requirements within the PA that span the scope of EJV, Thales and Alstom have not taken place. Two examples of how EJV had determined their contribution and boundary in meeting a PA requirement that spanned Thales/Alstom/EJV were observed. The first was believed to have been agreed via email, the second by developing an ICD. It was not known whether the other party (Thales) had accepted the ICD. There is a risk of gaps in scope where railway level PA requirements have not been formally apportioned.	A	**Observation No.5** Review all ICDs to ensure that all parties have agreed and accepted the ICDs. The jointly signed records of agreement are not evidenced
Stakeholder Needs and Requirements Definition	**6.4.2** Define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment. Identify stakeholders, or stakeholder classes, involved with the system throughout its life cycle, and their needs.	Inputs to the Design process	**Partially compliant** No formal capture and analysis of stakeholder requirements has taken place. There is evidence of documented stakeholder input to the design process through reports and comment resolution sheets. Stakeholder input was also claimed to have been provided through meetings and emails. There is a risk of insufficient consideration of stakeholder needs and inability to demonstrate those needs have been met.	A	**Observation No.6** For each Primary System, identify and list the sources of stakeholder requirements (CRE's, reports, minutes of meetings etc.) that have been used as an input to the design process and review to ensure all stakeholder needs have been addressed. **Observation No.7** Taking a risk-based approach, identify any key stakeholder requirement sources that will require compliance statements against each clause and capture as part of the requirements management process.
System Requirements Definition	**6.4.3** Transform the stakeholder, user-oriented view of desired capabilities into a technical view of a solution that meets the operational needs of the user. This process creates a set of measurable system requirements that specify, from the supplier's perspective, what characteristics, attributes, and functional and performance requirements the system is to possess, in order to satisfy stakeholder requirements. As far as constraints permit, the requirements should not imply any specific implementation.	Inputs to the Design process	**Not compliant** System requirements have not been defined for any of the Primary Systems within EJV's scope. System requirements for the Comms System are in the process of being developed and this was shown during the audit. System requirements for TVS and Traction Power are planned to be produced.	R	**Observation No.8** Taking a risk-based approach, complete development of the system requirement specifications primary systems assessed as being high risk.

Audit Theme	ISO15288 Applicable Clause	Reviewed Document	Observation/Objective Evidence	RAG	Remedial Action /Recommendation
System Requirements Definition	**6.4.3** Transform the stakeholder, user-oriented view of desired capabilities into a technical view of a solution that meets the operational needs of the user. This process creates a set of measurable system requirements that specify, from the supplier's perspective, what characteristics, attributes, and functional and performance requirements the system is to possess, in order to satisfy stakeholder requirements. As far as constraints permit, the requirements should not imply any specific implementation.	Inputs to the Design process	**Not compliant** Requirements derived from the safety and RAM process have not been captured.	R	**Observation No.9** Ensure all requirements derived from the safety and RAM process are captured, flowed down to the applicable Primary Systems and have been satisfied in design.
Requirements Traceability	Missing clause number	DOORS	**Not compliant** Functional analysis has been used to derive additional requirements and these are traced to the interface register and back to the PA. This is not currently held in DOORS. Procurement specifications reviewed do not include traceability back to the primary system requirements.	R	**Observation No.10** Import the functional analysis back into DOORS. **Observation No.11 .** Import procurement specifications into DOORS and trace back to the Primary System requirements.
Requirements Satisfied in Design	**6.4.9** Provide objective evidence that a system or system element fulfils its specified requirements and characteristics. **6.4.11** Provide objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment.	Activity / exercise review – no specific document number applicable	**Partially compliant** An exercise is currently ongoing to review the design of each primary System against the relevant requirements in the PA and to declare a statement of compliance against each requirement. As no apportionment of the PA to primary systems has occurred, compliance statements are only for the contribution that primary system is making rather than an overall statement of compliance.	A	**Observation No.12** Extended the design verification exercise to demonstrate compliance back to stakeholder requirements where applicable and derived requirements.
Requirements Satisfied in Design	**6.4.9** Provide objective evidence that a system or system element fulfils its specified requirements and characteristics. **6.4.11** Provide objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment.	Sampling of requirements	**Partially compliant** During the audit, a number of requirements from the PA were selected to demonstrate how the requirement had been satisfied in design. It was not possible to easily demonstrate traceability during the audit meetings for some requirements - The evidence will need to be reviewed when provided.	A	**Observation No.13** Provide requested design evidence to enable examples of design verification to be completed.

Audit Theme	ISO15288 Applicable Clause	Reviewed Document	Observation/Objective Evidence	RAG	Remedial Action /Recommendation
Requirements Satisfied in Design	**6.4.9** Provide objective evidence that a system or system element fulfils its specified requirements and characteristics. **6.4.11** Provide objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment.	Issues Management Process missing or not available	**Partially compliant** A compound requirement relating to emergency ventilation was examined and found to be declared compliant even though part of the requirement was not compliant. Although an issue was raised against this, the compliance status should be set to partial or pending.	A	**Observation No.14** Provide issues management process. **Observation No.15** Review design compliance statements for compound clauses to confirm compliance statement is correct.
Requirements Satisfied in Design	**6.4.9** Provide objective evidence that a system or system element fulfils its specified requirements and characteristics. **6.4.11** Provide objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment.	Issues Management Process missing or not available	**Not compliant** No evidence was provided of the link between verification and validation events and status. The SIT procedures are currently being updated and are planned to include traceability back to the requirements.	R	**Observation No.16** Create the Verification and Validation matrix in DOORS in accordance with the VVMP providing traceability from tests back to requirements.
Requirements Satisfied in Implementation	**6.4.9** Provide objective evidence that a system or system element fulfils its specified requirements and characteristics. **6.4.11** Provide objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment.	No Evidence provided	**Partially compliant** EJV are responsible for generating procurement specs but procurement is managed by OLRT-C. EJV are asked to review test and compliance data back from suppliers but do not formally accept. EJV are not responsible for verification and validation of the implemented system although as EoR are responsible for signing off that the design has been correctly implemented.	A	**Observation No.17** Clarify the division of roles and responsibilities relating to review and acceptance of product verification and compliance data from suppliers. **Observation No.18** Clarify the division of roles and responsibilities relating to review and acceptance of the implemented system.
Requirements Satisfied in Implementation	**6.4.9** Provide objective evidence that a system or system element fulfils its specified requirements and characteristics. **6.4.11** Provide objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment.	No Evidence provided	**Partially compliant** It was stated during the audit that the approach to demonstrate compliance to PA requirements was the subject of a letter to the City (Memo 13) currently being updated.	A	**Observation No.19** Conduct a risk-based assessment of assurance against the compliance approach detailed in Memo 13 in order to confirm the sufficiency of this approach.

Safety

Audit Theme	50126 Applicable Clauses	Relevant PA Clauses	Document Reviewed	Findings	RAG	Observations
Audit Planning	**5.3.7** The requirements detailed in this standard are written in order to support an audit process. The Railway Authority and the railway support industry for the system under consideration shall agree and implement an Audit Plan which addresses the application at the requirements of this standard, as adapted to the system	**PA (15-2 Part 4) Section 10.3ai, aii**	**Risk Based Intrusion Audit Plan could not be evidenced.**	**Not Compliant** • No Risk Based Intrusion Audit Programme • No Safety (50126) audits performed on the project since inception. • The project deemed Low Risk by the auditee led to a "light touch" assurance approach		**Observation No.20** No Risk Based Intrusion (RBI) Planned Audit programme covering for Systems Engineering (Safety).

Safety Planning	**5.3.4** The assessment of the application of this standard to the system under consideration shall: a) specify the lifecycle phases which are required to realize the system under consideration, providing a justification for the lifecycle phases specified and demonstrating that the tasks undertaken within these lifecycle phases comply with the principles of -the requirements of this standard. b) specify the mandatory activities and requirements of each required !lifecycle phase, using Figure 9 and the relevant phase related information of clause 6 as a checklist, including c) justify any deviation from the activities and requirements of the standard. d) justify the adequacy of the tasks chosen for the application under consideration. **5.3.5** Within all applications of this standard, the following requirements are mandatory: c) the establishment and implementation of the Safety Plan is an essential component in the realization of dependable systems. require similar analysis activities.	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Plan - REJ-05-0-0000-REP-0328 Rev 1 (approved) and Rev 2 (unapproved)**	**Partially compliant** The audit focussed on the safety management process applied to the primary System and sufficiency of the Overarching EJV Safety Management Plan to the integrated Station scopes (13No). Limitations of the approach were observed due to: 1. The unique process of the individual Engineer of Records sign off of the fixed station infrastructure was inadequately addressed. 2. Safety Organisation has been defined in the System Safety Plan with link to the OLRT-C Safety Organisation. 3. There was no evidence of who the safety authority signatory was for an integrated asset (e.g. station with MEP and comms systems or shaft/portal with MEP and comms systems) *Post Audit Note: This was further discussed as part of Station Element System Safety Audit and it was not clear how the integrated Station as an Integrated System is certified as-built and commissioned.*	**A**	**Observation No.21** Update Safety Plan to provide detail the safety certification sign-off for an integrated asset
		PA (15-2 Part 4) **5.10** System Safety	**EJV Safety Plan - REJ-05-0-0000-REP-0328 Rev 1 (approved) and Rev 2 (unapproved)**	**Partially Compliant** The plan does not reflect the fact that some aspects of the safety management process are being retrospectively applied whilst others are early in the design stage, e.g. the development of the GIDS and IP 04 designs	**A**	**Observation No.21** The EJV Safety level plan should incorporate the difference in approaches to different primary system designs. (Levels in design) The document should also address management of lower level tier suppliers' safety management process.

Safety Planning	**6.2.3.4** (Content of Safety Plan) Policy and strategy for achieving safety. • Scope of the plan and system description. • Description of the system lifecycle, safety tasks to be undertaken within the lifecycle and roles, responsibilities, competencies and relationships of bodies undertaking tasks within the lifecycle. • Safety analysis, engineering and assessment processes to be applied during the lifecycle. • Process for the maintenance of safety-related documentation, including Hazard Log. • Interfaces with other related programmes and plans. • Subcontractor management arrangements. • Requirements for periodic safety audit, safety assessment and safety review, throughout the lifecycle and appropriate to the safety relevance of the system under consideration, including any personnel independence requirements. • Hazard identification and analysis; • Risk assessment and on-going risk management; risk tolerability criteria; • The establishment and on-going review of the adequacy of the safety requirements; • Safety assessment, to achieve compliance between system requirements and realization; safety audit, to achieve compliance of the management process with the safety plan; • Safety assessment to achieve compliance between sub-system and system safety analysis. • Details of all safety related deliverables from the lifecycle, including. • Process to prepare system Safety Cases. • Processes for safety approval of the system, safety approval of system modifications and analysing operation and maintenance performance to ensure realized safety is compliant with requirements.	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Plan - REJ-05-0-0000-REP-0328 Rev 1 (approved) and Rev 2 (unapproved)**	**Not Compliant** The Safety Plan does not differentiate divisions of responsibility and who will be responsible for demonstrating that the safety risk associated with the as-commissioned asset design is ALARP. EJV are only responsible for demonstrating that the safety risks associated with the design of an integrated asset is ALARP (i.e. at AfC approved drawing). OLRT-C are responsible for the T&C phase of the delivered finalised as-built design by EJV. Potential scope gap on the EJV scope, e.g. responsibility for Fire Hydrant in Tunnel to be clearly defined. Including the following (not exhaustive): - No independent safety assessor identified - System breakdown structure used was non-compliant. Although the Plan provides a good technical description of the Primary Systems, there is insufficient detail on the System Boundaries, the Physical and Functional Interfaces, the Environment, the set of inherent safety measures		**Observation No.22** EJV Safety Plan needs to clearly state the following: (1) During T&C when snag items are identified and potentially may have a bearing on system safety - how this will trigger an update of the Design Safety Report (2) How EJV will carry out the safety assessment with a design change that may result from T&C conducted by OLRT-C **Observation No.23** (3) Clearly state the Division of safety responsibility for the V lifecycle stages (i.e. EJV stated that they will only demonstrate that finalised/accepted design is acceptably safe"). This needs to be accepted by OLRT-C. (4) The responsibility for safety integration. (5) Mechanism for managing interface safety requirements. Audit Note: It was discussed with D Roy that a way to resolve this issue is to use D Ellis Matrix showing a list of assets and the division of safety responsibility between EJV and OLRT-C Update Safety Plan to provide detail on those activities that will be carried out retrospectively (e.g. PHA) and what stage the project is at currently. Provide a system definition for the EJV scope of works detailing the following: System Boundaries Underlying Assumptions (if applicable) Inherent Safety Measures

Scope Definition		**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Plan - REJ-05-0-0000-REP-0328 Rev 1 (approved) and Rev 2 (unapproved)**	**Not Compliant** Clarity required on EJV Scope and Responsibilities in relation to the PA. Hazard Management Matrix, which identifies what is in and out of scope should also be incorporated in the System Safety Plan The SBS document is non-compliant to ISO 15288. It currently has no document number or unique identifier. The Auditor was aware of 2 versions with unclear configuration. This document needs mapping into the EJV Safety Plan after it achieves compliance.	R	**Observation No.24** Hazard Management Matrix to be provided. **Observation No.25** SBS required to be updated to achieve ISO 15288 compliance
Safety Organisation – Competency	**5.3.5** Within all applications of this standard, the following requirements are mandatory: a) responsibilities for carrying out all RAMS tasks within each phase of the lifecycle, including the interfaces between associated tasks, shall be defined and agreed for the system under consideration. b) all personnel with responsibilities within the RAMS management process shall be competent to discharge those responsibilities.	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Plan - REJ-05-0-0000-REP-0328 Rev 1 (approved) and Rev 2 (unapproved)**	**Not Compliant** The System Safety Plan does not reflect the potential for introduction of additional resources of varying competencies to address dynamic workload due to compressed project delivery timescales	R	**Observation No.26** Auditor requests a copy of the EJV Competency Matrix including Safety and RAM resources. To also include copies of relevant Project Organisational Charts and Update of the Safety Plan Organisation
Competency management		**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Plan - REJ-05-0-0000-REP-0328 Rev 1 (approved) and Rev 2 (unapproved)**	**Partially Compliant** As part of the general RAMS audit, a general observation was raised on Competency including: (1) Induction for New Engineers joining the project (2) Training Record Matrix (3) Competency Matrix including Safety and RAM	A	**Observation No.27** Information on competency management of personnel and induction of New Engineers including training requirements to be forwarded to Mary McGrath – Lead Auditor

Hazard Identification, Analysis & Management (inc OSHA):	**6.3.3.1** Systematic identification of all foreseeable hazards...including hazard from normal, emergency, misuse, fault conditions. **6.3.3.2** Determination and classification of risk tolerability. **6.3.3.3** Establishment of a hazard log and contents of hazard management plan.	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Process documents (EJV Track PHA Report)**	**General observation** - EJV went through the process in developing Track PHA. It was noted that the document although carried out retrospectively to safety assure the IFC Track Design was of a good standard and generally followed good engineering practice	**GP**	
				Not Compliant The EJV Track Preliminary Hazard Analysis does not include the Track System scope nor cover the safety requirements top down and bottom up as well any interface derived requirements. EJV stated that as part of the PHA for each Primary System (which is work in progress) an Interface Hazard Analysis (IHA) is also carried out. However, there was insufficient detail on the process for managing the transfer of interface hazards and risk control actions between different contracting entities (OLRT-C, RTM, OC-Transpo, Thales and ALSTOM)	**A**	**Observation No.28** PHA - Track scope definition requires update. Exclusions from the safety management perspective to be identified. Scope interfaces and interactions to be tabulated EJV need to clearly state the following: (1) Process for management and transfer of safety risks at the interface level (an example of S&C and interface to signalling point machine was discussed) (2) Process for management and acceptance of residual safety risks by RTM and OC-Transpo (i.e. operational and maintenance tasks).
		PA (15-2 Part 4) **5.10** System Safety	**EJV Safety process documents (EJV Track PHA Report)**	**Partially Compliant** The Track PHA Analysis has been undertaken at the high level but is yet to be detailed. Auditor expects the analysis to be developed to incorporate appropriate detail.	**A**	**Observation No.29** PHA Track development required

Hazard Identification, Analysis & Management (inc OSHA):	**6.3.3.1 Systematic identification of all foreseeable hazards...including hazard from normal, emergency, misuse, fault conditions.** **6.3.3.2 Determination and classification of risk tolerability.** **6.3.3.3 Establishment of a hazard log and contents of hazard management plan.**	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety process documents**	**Partially Compliant** The Track PHA listed a number of assumptions. However, it was highlighted that these were not assumptions but facts and should be reflected as such in the updated PHA	**A**	**Observation No.30** EJV to update the Assumptions Section clearly defining what is in scope and what is out of scope and is the responsibility OLRT-C for the Track PHA. Note: This general observation applies to all future PHAs that will be conducted by EJV.
		PA (15-2 Part 4) **5.10** System Safety	**EJV Safety process documents**	**Not Compliant** EJV as part of PHA carry out Interface Hazard Analysis (IHA) for each Primary System. Interface Control Documents are used to control and manage design risks across the interfacing parties. However, although EJV showed sample of ICD (e.g. TVS ICD), there were occasions where no evidence during the audit could be provided that each of the interface identified is acknowledged and accepted by the interfacing party (e.g. rolling stock). Similarly in the interface hazards identified, EJV could not provide detail on how each interface hazard would be mapped to the ICD document and how the transfer of risk associated with the hazard will be transferred to third parties	**A**	**Observation No.5** EJV to provide evidence that all interface identified in ICD documents have been accepted by third parties **Observation No.31** EJV to update the Safety Plan to provide detail on Interface Hazard Management including Transfer process
Fire Evacuation risks / routes	No Evidence provided	**PA (15-2 Part 4)** **5.10** System Safety	**Fire and Evacuation Risk Assessment**	**Partially Compliant** A specific discussion was held on the safety risks surrounding St Laurent Station which interfaces with a Shopping Centre. The fire evacuation route leads primarily into the shopping centre	**A**	**Observation No.32** EJV to provide a single document as evidence on how fire and evacuation risks have been managed in that specific station and in relation to the shopping centre

OSHA	**6.3.3.1 Systematic identification of all foreseeable hazards...including hazard from normal, emergency, misuse, fault conditions.** **6.3.3.2 Determination and classification of risk tolerability.** **6.3.3.3 Establishment of a hazard log and contents of hazard management plan.**	**PA (15-2 Part 4)** **5.10** System Safety	**OSHA**	**Partially Compliant** There was no detail on the EJV System Safety Plan on the need to carry out an OSHA	**A**	**Observation No.33** EJV System Safety Plan to be updated with provision of data on how OSHA will be carried out. Note: EJV Design Manager confirmed that OSHA will be carried out OLRT-C Safety Manager re-confirmed that OSHA shall be carried out all levels (i.e. OLRT-C, EJV, ALSTOM, THALES levels).
Preliminary Hazard Analysis (PHA)	**6.3.3.1 Systematic identification of all foreseeable hazards...including hazard from normal, emergency, misuse, fault conditions.** **6.3.3.2 Determination and classification of risk tolerability.** **6.3.3.3 Establishment of a hazard log and contents of hazard management plan.**	**PA (15-2 Part 4)** **5.10** System Safety	**PHA**	**Partially Compliant** It was recognised that Safety and RAM analysis is work in progress. However, for the Safety Analysis carried out to date (e.g. PHA) no evidence could be provided that the output of the PHA has been reviewed by the EJV Engineer of Record (Eng Team)	**A**	**Observation No.34** Provision of evidence required that output of the safety analysis has been reviewed by the Engineer of Record. It was recommended that this could be carried out through a small workshop which would speed up the process and support project delivery
System Integration PHA's for Integrated Safety Case	**6.3.3.1 Systematic identification of all foreseeable hazards...including hazard from normal, emergency, misuse, fault conditions.** **6.3.3.2 Determination and classification of risk tolerability.** **6.3.3.3 Establishment of a hazard log and contents of hazard management plan.**	**PA (15-2 Part 4)** **5.10** System Safety	**PHA**	**Partially Compliant** It was recognised in principle that a System Integration PHA will need to carry out in addition to the Primary Systems PHA. This will close the gap where Core Hazards (like Unauthorised Access) that may have not been assessed in Primary System PHAs	**A**	**Observation No.35** EJV to update the Safety Plan to detail on the System Integration PHAs that will be carried out to demonstrate completeness of the analysis Note - This will support the joint activity of producing the Integrated Safety Case (e.g. Station, TVS)
Hazard Log Structure	**6.3.3.1 Systematic identification of all foreseeable hazards...including hazard from normal, emergency, misuse, fault conditions.** **6.3.3.2 Determination and classification of risk tolerability.** **6.3.3.3 Establishment of a hazard log and contents of hazard management plan.**	**PA (15-2 Part 4)** **5.10** System Safety	**Hazard Log**	**Partially Compliant** It was recognised the EJV Hazard Log structure needs to be accepted by OLRT-C prior to doing any further work Note: The existing EJV Hazard Log is more of a FMECA than hazard Log	A	**Observation No.36** EJV to provide detail on Hazard Log Structure Note: It is recommended that a similar structure to that of OLRT-C IHL is used

Safety Requirements	**6.4** Safety requirements derivation **6.4.3.1** Requirements, for the system under consideration, shall include: • definition of the system and boundaries; mission profile; • functional requirements and supporting performance requirements, including safety functional requirements and safety integrity requirements for each safety function; logistic support requirements; • interfaces; • application environment; • tolerable risk levels for identified hazards; • external measures necessary to achieve the requirements; system support requirements; • details of the limits of the analysis; details of any assumptions made.	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Related Safety Process documents**	**Not Compliant** EJV started the safety activities very late on the project and therefore no safety requirements have been identified from the Hazard Identification and Analysis as these activities have only started		**Observation No.37** EJV to check and ensure that all safety requirements are identified and mapped to the Requirements V&V process to demonstrate that the safety measures/requirements have been included as part of the design development of systems and equipment under EJV scope.
Allocation and apportionment of safety requirements (including Interfaces)	**6.5.3** Allocation and apportionment of safety requirements to sub-systems and components	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Process documents**	**Not Compliant** EJV stated that they have carried out a SIL determination and allocation report. As part of the audit, EJV stated that they have allocated SIL 2 functionality for the SCADA and PLC Controller System. However, there is in sufficient detail on how EJV will demonstrate SIL 2 compliance at the product level and application level against the requirements of EN 50128 "Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems"(e.g. programming of the Digital Input and Digital Output Cards for the TVS functionality).		**Observation No.38** EJV to provide detail on how they will demonstrate compliance to SIL 2 functionality against EN 50128 "Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems." This includes EN50128 requirement to have an independent reviewer within the EJV organisation (separate from the project and design organisation)
Use Cases	**N/A**	**N/A**	**N/A**	**General Observation** -The Use Case document produced (and work in progress) is a good quality document and generally followed good engineering practice which can be used by supporting engineering functions (Safety, assurance, RAM) to carry out necessary engineering support activities.	**GP**	**RECORD** Use Cases to be finalised and baselined

Use Cases	**N/A**	**N/A**	**N/A**	**Partially Compliant** Demonstrate that all Use Cases have been identified and what criteria has been used to determine the list of Use Cases. Note - It was discussed and agreed in principle that consideration should be given to "DITLO Lite" to validate the completeness of the Use Cases. The Track PHA document identified a number of generic safety risks associated with the track design (e.g. broken rail). However, there was no traceability of how these safety risks have been managed in design and development of the track design including S&C. This was particularly important given that the PHA has been conducted on the as-built (IFC design) so the necessary traceability evidence is required for design requirements, to ensure that all safety risks were taken into account in the development primary systems. Discussion surrounding Energy Target Level Requirements drilled into link between this requirement and Regenerative Breaking and its impact on Station MEP assets (e.g. escalators). It was stated that Station electrical assets voltage tolerance was between 1000V and 1800V. However, it could not be confirmed whether during Regen Breaking this would tolerance would be exceeded.	**A**	**Observation No.39** Project to consider convening the DITLO Lite (or appropriate equivalent activity) to verify coverage of use cases. EJV to update the Track PHA and provide traceability to design requirements for each safety risk identified in the Table. Given this audit finding, EJV need to ensure that they have validated all Interface Requirements with their external and internal interface parties Post Audit Note: It was later confirmed that this Interface requirement has been validated (but only by email which is unacceptable for managing interface requirements)

Change Control/Config Management:	**5.3.5** Within all applications of this standard, the following requirements are mandatory: e) an adequate and effective configuration management system shall be established and implemented, addressing RAMS tasks within all lifecycle phases. The scope of configuration management will depend on the system under consideration but shall normally include all system documentation and all other system deliverables.	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Process documents**	**Partially Compliant** Doc No EGV Safety Plan REJ-05-0-0000-REP-0328 Rev 1.0 Approved & Rev 2.0 Unapproved was sighted as having signatories problem	**A**	**Observation No.40** EJV need to ensure that all parties work to the most up to date Safety Plan
Design Engineering changes	**5.3.5** Within all applications of this standard, the following requirements are mandatory: e) an adequate and effective configuration management system shall be established and implemented, addressing RAMS tasks within all lifecycle phases. The scope of configuration management will depend on the system under consideration but shall normally include all system documentation and all other system deliverables.	**4.1.1 Management of Design Changes**	**Configuration Management Plan OLR-QMS-GP100-SP04_0**	**Partially Compliant** EJV stated that the design engineering changes that may result from snag items/non-conformities during T&C and which may potentially have a bearing on system safety functionality will be managed as per the OLRT-C Configuration Management Plan which is currently under development (Doc. No **OLR-QMS-GP100-SP04_0**). EJV have their own process for managing design changes from Concept to IFC'd accepted design and the documents that cover this were (1) Design Management Plan, (2) Design Execution Plan and (3) Design Quality Plan. However, no evidence could be cited where any changes that may have had a bearing system safety was reviewed by a System Safety and RAM Professional EJV stated that the safety analysis currently being done on Primary Systems is based on the latest design documentation. However, it could not be demonstrated during the audit that the safety and RAM analysis was reflective of the as-built design	**A**	**Observation No.41** EJV to confirm which sections within the three Plans refers to the requirement for Safety and RAM professional to have a stakeholder input to the proposed design change prior to implementation. Note: RAMS Team (D Roy) have joined late in the project OLRT-C to ensure that the Configuration Management Plan that is currently under production calls for safety assessments to be carried out on potential major design change that may arise from the T&C commissioning Phase. Note: D Ellis stated that he sits in the Change Control Board and is the Design Safety Representative for EJV EJV to provide evidence that system safety and RAM Analysis is reflective of the as-built design and the system has the necessary safety and reliability features called for in the outcome of the safety/RAM analysis

Test results from Test and Commissioning activities meeting safety requirements	**N/A**	**N/A**	**Information Management and Document Control** **ISO9001**	**Not Compliant** Given the status of the project, T&C is currently being carried out. However, safety is not being made aware of whether the test results are meeting the safety requirements. It was observed that the flow of information between the Design Engineering and RAMS teams was not optimised/co-ordinated, with the risk of mis-alignment in analyses outcomes,	R	**Observation No.42** Note it is recognised that this is a known issue. However, given the status of the project this issue needs to be resolved asap such that safety can start building up the whole safety claim-argument-evidence for Core Hazards There needs to be greater collaboration between the EJV Design Engineering and the Safety and RAM teams, particularly in relation to requirements management and final design/build configuration.
Safety Case	**6.6.3.5** Preparation of generic system safety case (and content) & justification that systems meets safety requirements **6.9.3.3** Application safety case and content	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Process documents**	**Not Compliant** EJV System Safety Plan stated that a Safety Report (Safety Case) shall be produced for each Primary System. The audit focused on one particular aspect and that is the Safety Report for Mechanical Electrical and Communications (including Public Health Systems). Although a Safety Report will be provided for each Primary System, this left a gap on which SR document will provide the "Case for Safety" for the Integrated Asset. In particular the Station with its Civil, Structural, Architectural and Integrated Mech, Elec and Public Health and Comms will form an Integrated Asset/System providing the functionality for Passenger Egress/Access to Station, Passenger egress/access from Platform to Train, Passenger, Maintainer and Station Staff Evacuation and Fire Services Intervention	R	**Observation No. 43** EJV to provide detail on the safety argument for the integrated Station System/Asset
Safety Argument for all primary systems	**6.6.3.5** Preparation of generic system safety case (and content) & justification that systems meets safety requirements **6.9.3.3** Application safety case and content	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Process documents**	**Partially Compliant** General observation - Figure 4 of the Safety Plan needs to state that the Safety Report will only be provided for the Design Case and excludes the T&C phase	A	**Observation No. 21** Update Safety Plan and Figure

Safety Argument for all primary systems	**6.6.3.5** Preparation of generic system safety case (and content) & justification that systems meets safety requirements **6.9.3.3** Application safety case and content	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Process documents**	**Partially Compliant** Generally, EJV as the Design Authority will provide the safety argument for all Primary Systems. However, some suppliers of subsystems will need to provide safety case documentation to substantiate the safety claims and arguments in EJV Hazard Log, PHA and final Safety report for each Primary Systems. One example discussed was the SIL 2 for the SCADA functionality and later on the audit on day 2, SIL2 functionality was discussed for the TVS PLC Controller. The Rev 2.0 Safety Plan does not provide detail on the process of managing supplier system safety	**A**	**Observation No.44** EJV need to provide detail on Supplier Safety Management and the safety documentation and certification that will be provided by suppliers to support EJV safety claims and arguments at the Primary System Level **Observation No. 21** No process identified on how the management of the supplier for system safety is implemented.
Safety reports for each type of station	**6.6.3.5** Preparation of generic system safety case (and content) & justification that systems meets safety requirements **6.9.3.3** Application safety case and content	**PA (15-2 Part 4)** **5.10** System Safety	**Safety reports for each type of station**	**Not Compliant** A general gap was identified in the audit, whereby the three different types of Station was considered as an Integrated Station Element that work together to perform the functionality of the Station (i.e. Safe Passenger Access/Egress in/out of Station, Passenger Platform Train Interface, Safe Maintenance, Station Staff Access/Egress and Fire and Evacuation for passengers/maintainers/ station, Security) A safety report supported by the necessary safety analysis is required	**A**	**Observation No. 45** A Safety Report shall be produced for each station type by EJV which will include the Civil, Architectural, Mechanical, Electrical and Public Health as well as the communication systems. Key risks that will need to be demonstrated shall be around the functionality of the station and will include Fire and Evacuation Risks.

Safety Validation Activities (including software)	**6.9.3.1** Safety validation against requirements	**PA (15-2 Part 4)** **5.10** System Safety	**EJV Safety Process documents**	**Not Compliant** EJV stated that they will be only responsible for hazard resolution for the detailed design phase not the T&C phase. EJV stated that as OLRT-C will be responsible for T&C it is OLRT-C responsibility to provide T&C evidence to support closure of hazards and its related derived safety requirements. Note: System Integration Test (SIT) logs will be reviewed by OLRT-C (not in all cases).		**Observation No. 46** EJV to provide this detail in the next revision of the System Safety Plan and obtain OLRT-C acceptance. **Observation No. 21** Note: The process of closing out hazards and related derived safety requirements for T&C process needs to be established
Integrated safety argument	**N/A**	**N/A**	**N/A**	**Partially Compliant** It was observed that there is lack of clarity between EJV and OLRT-C as to who will provide the integrated safety argument for the Integrated Asset (key example being Station, TVS etc). This issue was discussed in different parts of the audit. As part of the System Integration Audit held on the 19th April afternoon session, the auditor provided a system context diagram of a typical station to demonstrate the important of providing the integrated safety argument. Similarly, a simple diagram representing the safety loop (safety instrumented function - SIF) was presented for the TVS function General consensus was that this would be a joint EJV/OLRT-C activity	**A**	**Observation No. 47** All OLRT-C and EJV Design Engineering / Safety Team must determine how best to execute this joint and important activity which will be a key input to the railway level summarised safety case

Software development plan – SIL 2	**50128 – SIL 2 software requirements**	**X**	**Software Development SIL2**	**Not Compliant** As part of the TVS Audit, it was stated that a Software Development Plan was being produced to demonstrate that software has been developed to the necessary software standards as listed in the PA. However, this Plan is being developed after completion of all PLC software programme development which calls into question on how the software development process will demonstrate compliance to SIL 2 software development requirements as per EN 51028	R	**Observation No. 48** For the next phase of software development, the software development plan to be demonstrated against SIL 2 EN 50128 software requirements

RAM

Audit Theme	50126 Applicable Clauses	Relevant PA Clauses	Document Reviewed	Findings	RAG	Observations
RAM Planning	**6.2.3.2** Undertake preliminary RAM analysis to support targets; 6.2.4.2 Develop RAM Policy for the system 6.4.1 Specify the RAM requirements and the overall demonstration and acceptance criteria for RAM for the system. Establish a RAM Programme Plan. 6.4.4.3 The RAM Programme shall include the tasks which are judged to be the most effective to the attainment of the RAM requirements for the system under consideration. The RAM Programme shall be agreed by the Railway Authority and the railway support industry for the system under consideration and shall be implemented throughout the lifecycle of the system.	**PA 15-2 Part 4 Articles 5 and 6**	**Document Number Unknown. Document under development by EJV**	**Not Compliant** The observations raised for the EJV System Safety Plan relating to Scope, System Boundaries and Definitions, Division of responsibility between IFC design and T&C will apply for the RAM Plan	R	**Observation No. 49** Update RAM Plan to address findings.
RAM Plan	6.4.1 Establish a RAM Programme Plan	**PA 15-2 Part 4 Articles 5 and 6**	**Document Number Unknown. Document under development by EJV**	**General observation** - The EJV RAM Plan is of a good standard, but further details on RAM processes required	**GP**	**RECORD**

RAM Organisation	The RAM program plan should contain the roles, responsibilities, competencies and relationships of organisations undertaking tasks within the lifecycle.	**PA 15-2 Part 4** **Article 5.11** Reliability and Availability	**EJV RAM Process documents**	**Not Compliant** EJV provided a walkthrough of the RAM process, organisation and activities by using the RAM Plan. A general observation was raised and agreed, that given majority of the safety and reliability engineering activities started late in the design development cycle and taking into account challenging timescales, does EJV have sufficient RAM and Safety professionals to ensure timely production of all safety and RAM documentation to support OLRT-C railway level safety and RAM documentation?		**Observation No. 50** EJV to carry out a review of the resource profile and where applicable bring into RAM/S resource support (external sub-contract/Internal resource in the SNC Lavalin Organisation or Permanent Resource) EJV to update the RAM and Safety Plan to explain the resource requirements process and its impact on RAM and Safety Organisation Note: OLRT-C will need to review the Safety and RAM resource profile to ensure that they themselves (as receivers of assurance documentation) can carry out a thorough review and acceptance of the bow-wave (cascade) of documentation that will be coming their way

RAM Analysis	**6.4.3.3** The following activities should be planned: • Reliability analysis and prediction, including: functional analysis and system failure definition; • top down analysis, for example fault tree analysis and block diagram analysis; • bottom up analysis, for example Failure Modes Effects Analysis (FMEA); • common cause failure or multiple failure analysis; • sensitivity analysis and trade-off studies; reliability apportionment; • human machine interface analysis; • stress analysis; • worst case prediction and tolerance analysis.	**PA 15-2 Part 4** **Article 5.11** Reliability and Availability	**No RAM Analysis**	**Not Compliant** EJV RAMS Engineer stated that RAM analyses activities were yet to commence. Therefore, the audit was focused on RAM Planning.		**Observation No. 51** RAM Analyses to commence as soon as practicable and reflect the latest designs configuration (including as built design variations on site).
RAM Calculation and FMEA Template	**6.4.3.3** The following activities should be planned: • Reliability analysis and prediction, including: functional analysis and system failure definition; • top down analysis, for example fault tree analysis and block diagram analysis; • bottom up analysis, for example Failure Modes Effects Analysis (FMEA); • common cause failure or multiple failure analysis; • sensitivity analysis and trade-off studies; reliability apportionment; • human machine interface analysis; • stress analysis; worst case prediction and tolerance analysis.	**PA 15-2 Part 4** **Article 5.11** Reliability and Availability	**Methodology agreement required**	**Partially Compliant** The methodology for calculating the reliability and availability of Primary Systems needs to be agreed with OLRT-C prior to initiating any RAM calculations The FMECA template requires acceptance by OLRT-C prior to initiating any FMECA work. EJV safety Assurance Director stated that FMECA would be carried out at lowest replacement unit level. For some systems and functions, engineering judgement will need to be taken to determine whether the FMECA may also need to be carried out in more detail (e.g. PLC controller for the TVS function and carrying out a hardware and software interaction FMECA for each Digital Input and Digital Output card)	**A**	**Observation No. 52** EJV to update RAM Plan and include section on RAM methodology and FMECA template. Define which systems and functions where more detailed FMECA shall be carried out (e.g. PLC controller for the TVS function and carrying out a hardware and software interaction FMECA for each Digital Input and Digital Output card)

RAM Maintenance Task Analysis	**50126**	**PA 15-2 Part 4** **Article 5.11** Reliability and Availability	**Stakeholder Management**	**Partially Compliant** A general observation was raised on the need for RTM to be a stakeholder in maintenance task analysis such that RTM can evaluate any impact that the outcome of the MTA will have on their produced Maintenance Procedures	**A**	**Observation No. 53** Ensure RTM is a stakeholder review of the MTA output
RAM Requirements	**6.4.1** a) specify the overall RAMS requirements for the system. b) specify the overall demonstration and acceptance criteria for RAMS for the system. c) establish the RAM Programme for controlling RAM tasks during subsequent lifecycle phases.	**Schedule 15-2 Part 4** **5.11** Reliability and Availability (a) Overall reliability of the CBTC Train Control System shall be such that with the provided redundancy, availability is 99.99% or greater. Availability calculations shall be based on the formula:	**EJV RAM Process documents**	**Not Compliant** EJV RAMS Engineer stated that RAM Requirements activities were yet to commence. Therefore, the audit was focused on RAM Planning.	**A**	**Observation No. 54, related to Observations 51, 52 & 53** EJV will need to comprehensively address the issue of RAM requirements in order to support adequate planning, activities and demonstration against requirements. **Observation No. 55** Clarification from Client should be sought with regards to specific RAM targets.
Apportionment of RAM Requirements	**6.5.1** a) allocate functional requirements to designated sub-systems, components and external facilities. b) allocate safety requirements to designated sub-systems, components and external risk reduction facilities. c) specify the designated sub-systems, components and external facilities to achieve complete system RAM requirements, including the impact of common cause and multiple failures.	**PA 15-2 Part 4** **Article 5.11** Reliability and Availability	**EJV RAM Process documents**	**Not Compliant** EJV RAMS Engineer stated that RAM Requirements allocation activities were yet to commence. Therefore, the audit was focused on RAM Planning.	**A**	**Observation No. 54** EJV will need to comprehensively address the issue of RAM requirements in order to support adequate planning, activities and demonstration against requirements. **Observation No. 55** Clarification from Client should be sought with regards to specific RAM targets.

RAM Validation Activities	**6.4.3.2** Demonstration and acceptance process for the overall RAMS requirements facilitated by the system RAMS validation plan, should include: • a description of the system; • the RAMS validation principles to be applied to the system; • the RAMS tests and analysis to be carried out for the validation including details of the required environment, tools, facilities etc.; • the validation management structure including requirements for personnel independence; • details of the validation program (sequence and schedule); • procedures for dealing with non-compliance.	**PA 15-2 Part 4** **Article 5.11** Reliability and Availability	**EJV RAM Process documents**	**Not Compliant** EJV RAMS Engineer stated that RAM Validation activities were yet to commence. Therefore, the audit was focused on RAM Planning.		**Observation No. 54** EJV will need to comprehensively address the issue of RAM requirements in order to support adequate planning, activities and demonstration against requirements. **Observation No. 55** Clarification from Client should be sought with regards to specific RAM requirements. **Observation No. 56** The safety and RAM validation plans needs to be clearly documented and relevant to the systems engineering approach adopted by EJV in line with PA Requirements.
RAM Demonstration (Collaborative working groups)	**6.9.3.1** Requirement of this phase shall be to validate the total combination of sub-systems, components and external risk reduction measures according to the Validation Plan and record the validation process, including: • details of RAMS validation tasks against acceptance criteria, including RAM demonstrations and safety analysis; • details of process, tools, equipment used for validation tasks against acceptance criteria; • results of validation tasks for all acceptance criteria; any limitations and constraints applying to the system; action taken to resolve failures and incompatibilities.	**PA 15-2 Part 4** **Article 5.11** Reliability and Availability	**EJV RAM Process documents**	**Not Compliant** EJV Design Manager stated there are performance (RAM) requirements which need to be demonstrated. However, on the same question put to the EJV System Safety Manager/Director the answer was that there are no performance requirements to demonstrate EJV could not provide any detail on what the requirements are for the EJV scope of delivery for Reliability Demonstration		**Observation No. 57** Both Design Engineering and System Safety needs to work together as an Integrated Engineering & Assurance Team reducing any uncertainty. Design Engineering need to provide the necessary technical evidence for the safety team to deliver the necessary safety approvals for all Primary Systems and the final integrated asset solution. **Observation No. 58** EJV to update RAM Plan and include section on Reliability Demonstration

FRACAS	**6.4.3.3** A Failure Reporting Analysis and Corrective Action System (FRACAS) to be applied to the system from phase 7 of the lifecycle, with records including: technical data on system; reason for maintenance action; type of maintenance action; man-hours & elapsed time for maintenance action; maintenance down time; number and skill level of personnel; spare parts used; cost of consumables; reporting and corrective action. The arrangements to ensure co-ordination of individual RAM elements; details of all RAM related deliverables from the lifecycle; details of RAM acceptance tasks; interfaces with other related programmes and plans; constraints and assumptions made in the RAM programme	**PA 15-2 Part 4** **Article 5.11** Reliability and Availability	**EJV RAM Process documents**	**Not applicable. Not EJV Scope**	**N/A**	**Not in EJV Scope. This is a Railway Level activity.**

T

Table No. 9 Detailed Audit Report

6.0 Follow Up Audit

NONE planned ~ There is no follow up and close out audit planned by SEMP Audit team. OLRT-C have the responsibility of audit follow up and close out on any findings contained within this report.

7.0 Past Audits

There have been no Systems Engineering Type audits previously performed on the OLRT-C Project for EJV.

8.0 Audit Objective Evidence

During the course of the audit performance documents sampled (examples (but not limited to) are detailed in the below table which were examined, discussed and reviewed. Soft copy documents were supplied by the auditee for reference only to the SEMP Audit Team.

Day	Document Name/Number	Revision Number
Day 1	**Intro and Track work**	
	Design management Plans	No Data available during Audit performance, EJV to provide and send to Lead Auditor
	Non-Conformance Reports (NCR) LOG	No Revision referenced
Day 2	**Stations**	
	CPTED Reports	No Data available during Audit performance, EJV to provide and send to Lead Auditor
	FLSS Meeting Minutes	RES-51-0-0000-MEO-0001 RES-51-0-0000-MEO-0002 RES-51-0-0000-MEO-0003 RES-51-0-0000-MEO-0004 RES-51-0-0000-MEO-0005 RES-51-0-0000-MEO-0006 RES-51-0-0000-MEO-0007 RES-51-0-0000-MEO-0008 RES-51-0-0000-MEO-0009 RES-51-0-0000-MEO-0010 RES-51-0-0000-MEO-0011 RES-51-0-0000-MEO-0012
	Interface Control Docs (ICD)	No Data available during Audit performance, EJV to provide and send to Lead Auditor
	Passenger Modelling Analysis Report	No Data available during Audit performance, EJV to provide and send to Lead Auditor

	RTG/EJV Training Procedures and Records	No Data available during Audit performance, EJV to provide and send to Lead Auditor
	System Design Functionality Report	No Data available during Audit performance, EJV to provide and send to Lead Auditor
Day 3	**PS&D & TVS**	
	Ottawa CL RMP	
	Email Pertaining to Ottawa CL RMP	Email - Daniele Ferrara
	Ottawa CL RMP	No document number - But states REV A
	PS&D	
	DBC's	
	Ground Fault Calculations	No Data available during Audit performance, EJV to provide and send to Lead Auditor,
	Protection	No Data available during Audit performance, EJV to provide and send to Lead Auditor
	PA Compliance Checklists -PS&D	No Data available during Audit performance, EJV to provide and send to Lead Auditor
	TTE	No Data available during Audit performance, EJV to provide and send to Lead Auditor
	TVS	No Data available during Audit performance, EJV to provide and send to Lead Auditor
	ISO 9001 Certificate	CERT – 0096970 June 20th 2017
Day 4	**COMMS**	
	Reports from enclosures	No Data available during Audit performance, EJV to provide and send to Lead Auditor
	Cyber Security Audit overview OLRT IHL & TVA	OLRT Cyber Security Workshop #2 IHL & TVA
	OLRT Master Network Diagram (Draft)	Photo only
	RTGEJV NCR-CAR-PAR Log sample	No Data available during Audit performance, EJV to provide and send to Lead Auditor

Table No 10. EJV Documents reviewed during Audit performance

9.0 Attachments

Attachment No	Description	Dated
No 1	Audit Notification SEMP-PSL-2018-AUD-2001	4th April 2018
No 2	Signatory Attendance Logs - Audit performance Day 1 to Day 5	16th April to 20th April 2018
No 3	SEMP Initial Audit Report – Document Number: SEMP/048/00x dated 20th April 2018 – presented at Audit Closing Meeting	20th April 2018

Table No. 11 List of Attachments to this Report

END OF REPORT