IN CONFIDENCE

Contract No. 5646

Ottawa Light Rail Transit (OLRT)

Systems Engineering and Assurance Health Check Report

Prepared for: OLRT-C

Document Number	SEMP/048/001
Version	1.0
Date	November 2017

Document Control

		Originated by		**Reviewed by**	
		Name, Role and Organisation	**Initials**	**Name, Role and Organisation**	**Initials**
Original	**Version 1.0**	Stuart Gilbey Consultant SEMP Ltd	SG	Mark Selkirk Consultant SEMP Ltd	MS
		Derek Wynne Consultant SEMP Ltd		Paul West Consultant SEMP Ltd	PW
Accepted By		**Name, Role and Organisation**	I confirm that I accept the contents of this document and that it can be issued to OLRT.		**Initials**
		Sean T Derry Assurance Lead OLRT			
Date		**Document Status**		Released	

Amendment History

Version	Description	Initials	Date
1.0	First Issue	SG / DW	14/11/2017

Executive Summary

SEMP Ltd were engaged by Ottawa Light Rail Transit Constructors (OLRT-C) to provide a Systems Engineering Health Check for the Confederation Line project.

The City's SA has been requested by OLRT-C to provide an interim assessment of OLRT-C progress in light of the OLRT-C 180 day Notice of Revenue Service Availability. This Systems Engineering Health Check will form the basis for the OLRT-C and City's SA engagement workshop arranged for 15-17th November 2017.

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 revenue service availability date. The health check performed did not consider Construction Management / Leadership. However, whilst not specifically reviewed, during the course of performing the Health Check the significant influence and contribution of design and integration management / leadership issues was noted.

This report presents the findings of the Systems Engineering Health Check and provides Route to Delivery scenarios.

Several areas of Systems Engineering deficiency have been identified by previous internal / external reviews. There are embryonic mitigation initiatives in place for some but not all of the gaps identified, and it should also be noted that where initiatives are being pursued these are both underfunded and under resourced.

Summarising, the level of System Engineering on the project to date is considered to be substantially below the minimum acceptable level for a project of this size and complexity. This is especially evident at the Railway System level and for early phases of the lifecycle (requirements and design). This is likely to have significantly increased integration risk on the project in addition to OLRT-C being unable to provide appropriate Assurance evidence to the Client and SA.

Given the advanced stage of the project, it is essential that robust effort is applied to agreeing the optimum set of Systems Engineering recovery activities and deliverables with the Client / SA at the above mentioned engagement workshop, thus enabling the project to conclude.

Contents

1 Introduction

1.1 Purpose

This report presents the findings and recommendations of the Systems Engineering Health Check commissioned by OLRT-C, to provide an assessment of the current status of Systems Engineering activities for the Confederation Line project. The objective of the 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 revenue service availability date;
- Identify any areas within the scope of the health check which require improvement and provide recovery strategies.

The City's SA has been requested by OLRT-C to provide an interim assessment of OLRT-C progress in light of the OLRT-C 180 day Notice of Revenue Service Availability. This Systems Engineering Health Check will form the basis for the OLRT-C and City's SA engagement workshop arranged for 15-17th November 2017.

1.2 Project Context

Ottawa Confederation Line Phase 1 will provide a Low Floor Light Rail Vehicle (LFLRV) Light Rail Transit (LRT) service between Tunney's Pasture and Blair stations. The 12.5-kilometre line will include a 2.5km mined tunnel beneath downtown Ottawa and an LRT Maintenance and Storage Facility (MSF) at Belfast Road, shown in Figure 1 below.

Phase 1 includes thirteen stations, with four located in the underground section and Blair Station, Hurdman Station and Tunney's Pasture Station integrating with the Bus Rapid Transit system. The Confederation Line links up with the north-south running O-Train at Bayview Station.

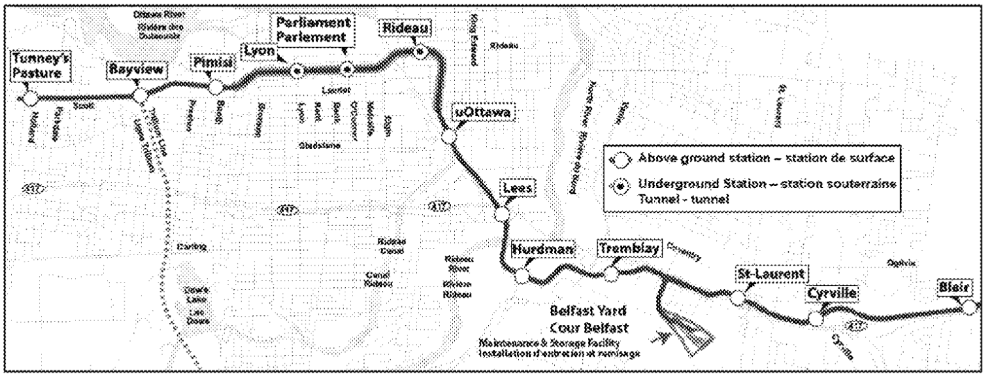


Figure 1 - Confederation Line Phase 1

A portion of the existing Bus Rapid Transit system (BRT) will be converted into the LRT and existing roads have been widened to accommodate the remaining buses. A THALES Seltrac signalling system will be installed and the trains, supplied by Alstom, will normally operate in Automatic Train Operation (ATO) mode. This is being opened through a 30-year Design-Build-Finance-Maintenance agreement with Rideau Transit Group (RTG).

Phase 1 creates the central section of the Confederation Line. East and West extensions are planned for 2022 and 2023 respectively. These extensions will see the line continue from Trim Road to Moodie and Baseline Stations adding over 27-kilometers of new rail to the Phase 1 scheme.

1.3 Systems Engineering on Infrastructure Projects

Infrastructure systems like the Confederation Line are characterised by large scale projects often with loosely defined boundaries, evolving system architectures, long implementation and asset life periods and multiphase lifecycles. A significant proportion of time and cost is spent during the construction phase.

Within infrastructure projects, many of the engineering disciplines (civil, structural for example) have well-established, traditional practices and are guided by industry codes and standards. Systems Engineering practices are more developed in the high technology subsystems that involve software development - communication based train control systems, for example.

The benefit of applying Systems Engineering to infrastructure projects lies in the structured approach to delivering and operating a multidisciplinary, integrated and configurable system.

1.4 Scope of the Health Check

The Confederation Line project is currently in the construction, installation, test and commissioning phases with a planned revenue service availability date of 24 May 2018. In this context, the review was conducted to assess the completeness and maturity of Systems Engineering processes and outputs, focussing on delivering an integrated, safe, operational railway system.

Railway Systems consist of people, processes and assets. The OLRT project is primarily responsible for delivering the railway assets - infrastructure, trains etc. The people and processes required to operate and maintain the railway assets are the responsibility of the City of Ottawa and Rideau Transit Maintenance (RTM) respectively.

The scope of the health check was limited to Systems Engineering and excluded other primary functions such as programme and project management which would be necessary to obtain a more complete picture of the project.

The health check focussed on providing assurance confidence. While some areas were explored in some detail, this review is not considered to be a full, comprehensive audit.

In addition to the health check, the second output of the review was to provide recovery strategies to address any issues identified.

The scope of the health check was defined and agreed in consultation with the OLRT Systems Assurance Lead.

1.5 Glossary

Table 1 lists the acronyms, abbreviations and defined terms used in the report.

Table 1 – Glossary

Term	Definition
ATO	Automatic Train Operation
BRT	Bus Rapid Transit system
CENELEC	European Committee for Electrotechnical Standardization.
CM	Configuration Management
DOORS	Dynamic Object Oriented Requirements System
EJV	Engineering Joint Venture
EMC	Electromagnetic Compatibility
FAT	Factory Acceptance Test
FRACAS	Failure Reporting, Analysis and Corrective Action System
GIDS	Guideway Intrusion Detection System
HAZID	Hazard Identification
HF	Human Factors
ISA	Independent Safety Advisor
LFLRV	Low Floor Light Rail Vehicle
LRT	Light Rail Transit
MSF	Maintenance and Storage Facility
O&M	Operation and Maintenance
OLRT	Ottawa Light Rail Transit
OLRT-C	OLRT Constructors
Ops	Operations
PA	Project Agreement (the contract)
PEO	Professional Engineers Ontario
PHA	Preliminary Hazard Analysis
RAM	Reliability, Availability, Maintainability
RAMS	Reliability, Availability, Maintainability, Safety
RTG	Rideau Transit Group
RTM	Rideau Transit Maintenance
SA	Safety Auditor
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SE	Systems Engineering
SEMP	Systems Engineering Management Plan
SIL	Safety Integrity Level
SIT	System Integration Test
SOP	Standard Operating Procedure
T&C	Test and Commissioning
TUV	Technischer Überwachungsverein
V&V	Verification and Validation

1.6 Reference Documents

The following documents are referenced within this report.

Table 2 – Reference Documents

Number	Title	Version
	Ottawa LRT Project Agreement	
ISO/IEC/IEEE 15288	Systems and software engineering — System life cycle processes	2015
EN 50126	Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS). Basic requirements and generic process	1999
EN 50128	Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems	2011
EN 50129	Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling	2003

2 Review Conduct

2.1 Review Arrangements

Review Dates	16 October 2017 to 20 October 2017
Location	OLRT Project Office 1600 Carling Av Ottawa
Review Team	Derek Wynne BSc (Hons) MIET MINCOSE Stuart Gilbey BEng (Hons) MIET MINCOSE

2.2 Review Method

The health check consisted of a review of selected project documentation together with a series of interviews with project staff. The schedule for the review is included in Appendix 1 and a record of the interviews conducted is contained in Appendix 3.

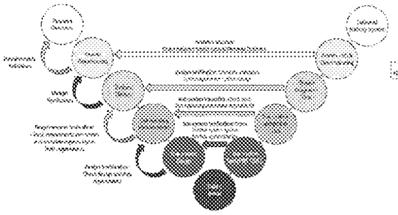
The Project Agreement requires compliance with ISO 15288 Systems and software engineering — System lifecycle processes and CENELEC standards. These standards have therefore been used as the basis for assessment.

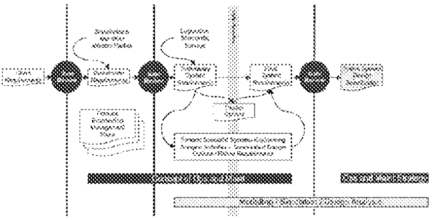
3 Review Findings

3.1 Presentation

The findings of the health check are structured based on the demonstration of the Fit for Operation Argument described in Section 3.2 below.

To provide context to the review findings, graphical representations of the applicable phases and processes of the generic lifecycle (highlighted yellow) are provided.





3.2 Fit for Operation Argument

Systems Assurance both at the Railway System and primary System specific levels is provided by a combination of Product and Process assurance requirements. Figure 2 shows the structure of the fit for operation argument used as the basis of the assessment.

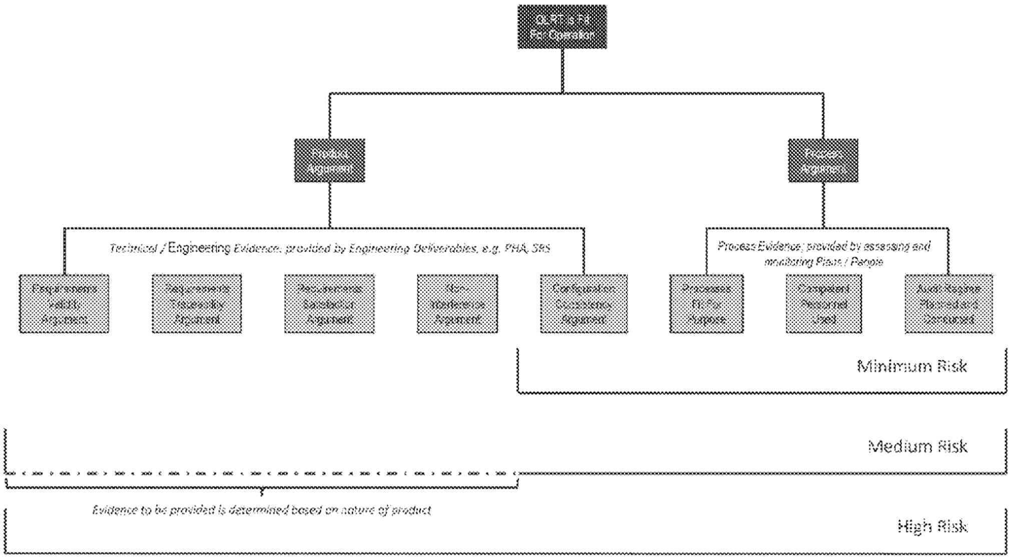

OLRT is Fit For Operation
Product Argument
Process Argument
Technical / Engineering Evidence: provided by Engineering Deliverables, e.g. PHA, SRS
Process Evidence; provided by assessing and monitoring Plans / People
Requirements Validity Argument
Requirements Traceability Argument
Requirements Satisfaction Argument
Non-Interference Argument
Configuration Consistency Argument
Processes Fit For Purpose
Competent Personnel Used
Audit Regime Planned and Conducted
Minimum Risk
Medium Risk
Evidence to be provided is determined based on nature of product
High Risk

Figure 2 - Fit for Operation Argument Structure

The five fundamental product assurance objectives which a system must fulfil, have been used to assess OLRT Systems Assurance, namely:

- Requirements Validity;

- Requirements Traceability;
- Requirements Satisfaction;
- Non-interference with any system function by unrelated functions;
- Configuration Consistency.

The Technical Assurance Cases at Railway and primary System levels should be developed during the Preliminary Design phase. For each phase, these Technical Cases should be supported by Sub-system Technical Assurance Cases which are populated with the identities of specific items of evidence as these become available.

The Technical Assurance Cases provide the principal schedule of evidence to demonstrate the Fit for Operation Argument (the Completeness Argument).

In addition, there are three fundamental process assurance objectives which the delivery organisation must satisfy, which have been used to assess OLRT Systems Assurance, namely:

- Fit for Purpose Processes;
- Competency;
- Audit Regime.

For maximum risk systems which are new or novel and/or have significant safety involvement, the full scope of the assurance argument is required. For minimum risk systems, it may be sufficient for the fit for operation argument to be based on the process argument together with the configuration consistency argument from the product argument. The majority of projects fit in between the minimum and maximum scope of assurance.

Given that OLRT is in the later stages of delivery it was determined that there was little merit in assessing the Competency and Audit Regime of OLRT-C. The Systems Engineering Health Check was therefore conducted on a Product Argument coupled with Fit for Purpose Processes Argument basis. Throughout the remainder of this report, each of the supporting Assurance Arguments will be considered. When aggregating these supporting arguments, it is clear that the Assurance Argument OLRT Fit for Operation cannot be made at this time

OLRT Fit for Operation Argument – *not ready*

3.3 Process Argument

It is necessary to show that Appropriate Engineering Processes have been developed and applied for all the Systems Engineering lifecycle stages, see BS ISO/IEC/IEEE 15288:2015.

The strategy of Process Arguments "Arguments that appropriate series of processes have been correctly executed by trained, experienced and competent personnel (Process Argument)" are based upon a series of arguments that:

- The processes have been correctly executed;
- The processes have been executed by trained, experienced and competent personnel;
- Audits have been planned and conducted;
- The process arguments have been used and linked as supporting evidence to the "Product Argument".

Throughout the remainder of Section 3.3 of this report each of the supporting Process Assurance Arguments will be considered. When aggregating these supporting arguments, it is clear that the OLRT Process Argument cannot be made at this time.

OLRT Process Argument – *not ready*

3.3.1 Fit for Purpose Processes

Life Cycle Management

ISO 15288: 5.4, 6; defines the objective of life cycle management as "define, maintain, and assure availability of policies, life cycle processes, life cycle models, and procedures for use by the organization."

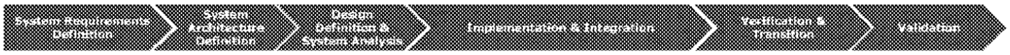

System Requirements Definition
System Architecture Definition
Design Definition & System Analysis
Implementation & Integration
Verification & Transition
Validation

Figure 3 - ISO 15288 Generic Lifecycle

As a minimum, we would expect to see a definition of:

- Life cycle phases and high level processes;
- Technical review gates;
- Key engineering deliverables;
- Organisation.

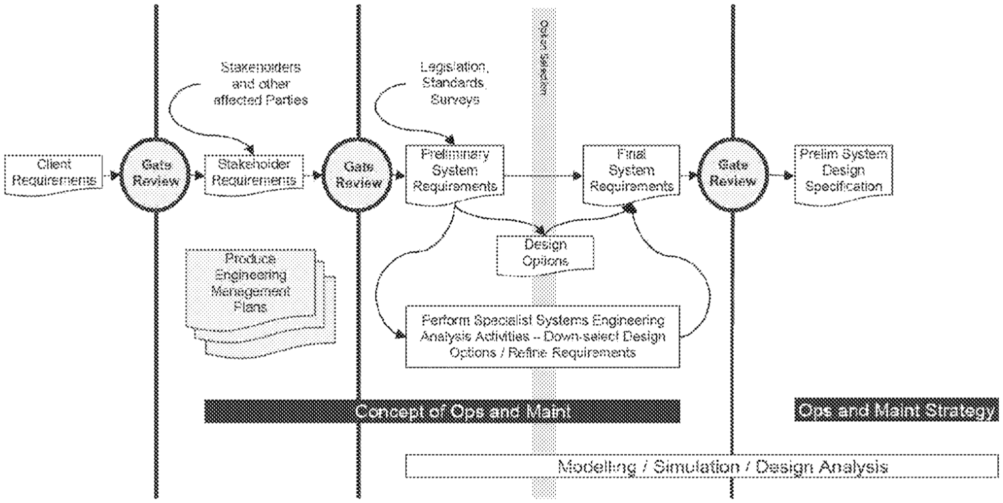


Figure 4 - Engineering Lifecycle Management

Completeness: several Engineering Management Plans were found to be absent. No evidence of an overarching engineering management plan such as a Systems Engineering Management Plan (SEMP) was provided. None of the interviewees were able to direct us to a formal description of how engineering is performed on the project.

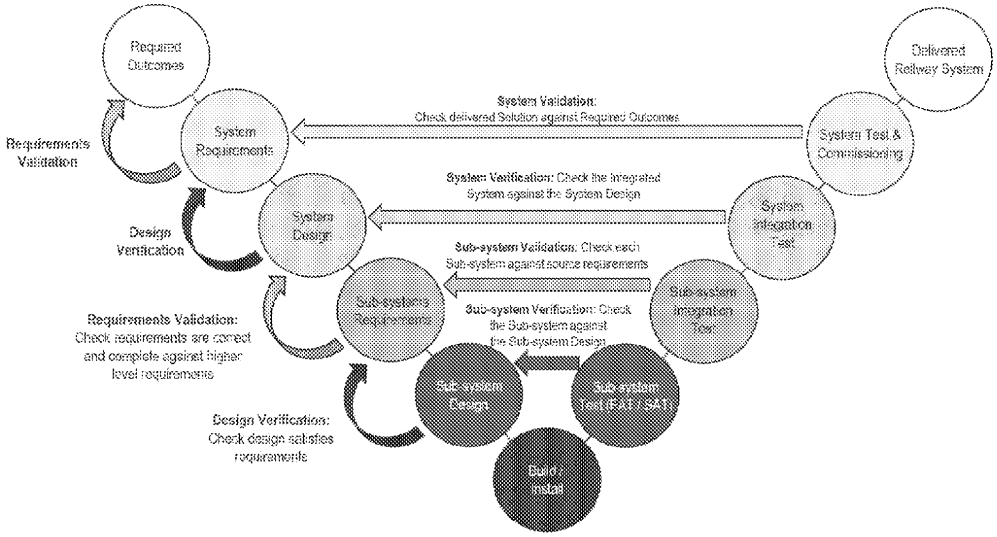
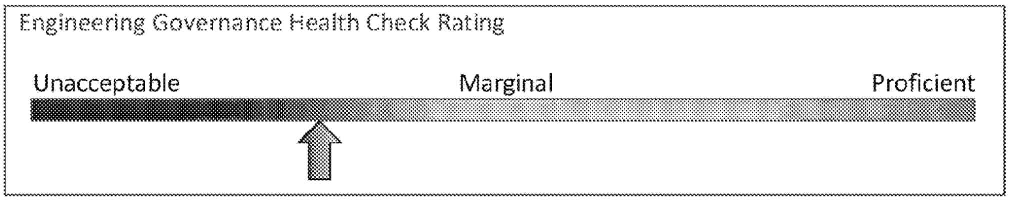


Figure 5 - Generic V Lifecycle

Some lower level plans were provided (Safety, V&V). Of those plans that do exist the majority were found to be unsuitable and requiring a rewrite. It is understood that work is now underway to develop some but not all project level engineering plans.



Adherence: of the plans that do exist there is little evidence of them being adhered to - both as defined or 'in the spirit of'.

Furthermore, it is evident that the project has not adhered to the design reviews specified within the contract, nor has it undertaken any form of Systems Engineering / Interdisciplinary design reviews.

As a consequence, OLRT Fit for Purpose Processes Argument - cannot be made at this time.

OLRT Fit for Purpose Processes Argument – *not ready*

3.3.2 Competency

Given that OLRT is in the later stages of delivery, it was determined that there was little merit in assessing the Competency of OLRT-C: the Systems Engineering Health Check was therefore conducted on a Product Argument coupled with Fit for Purpose Processes Argument basis.

OLRT Competency Argument – *not assessed*

3.3.3 Audit

Given that OLRT is in the later stages of delivery, it was determined that there was little merit in assessing the Audit Regime of OLRT-C. The Systems Engineering Health Check was therefore conducted on a Product Argument coupled with Fit for Purpose Processes Argument basis.

OLRT Audit Argument – *not assessed*

3.4 Product Argument

The Arguments demonstrating the delivered Railway possesses the required properties (Product Argument) should be based upon a strategy of product-based assurance supported by dependant arguments.

The objective is to show that the project identifies the solutions by addressing the principal assurance objectives:

- Requirement Validity;
- Requirement Traceability;
- Requirement Satisfaction;
- Non-interference;
- Configuration consistency.

Throughout the remainder of Section 3.4 of this report, each of the supporting Product Assurance Arguments will be considered. When aggregating these supporting arguments, it is clear that the OLRT Product Argument cannot be made at this time.

OLRT Product Argument – *not ready*

3.4.1 Requirements Validity

Requirements validation is an iterative process which takes place throughout the lifecycle of the project. During requirements capture, elicitation, analysis and specification, constant questioning and clarification of the requirements data should be performed in order to check its validity.

Requirements Validity is therefore the determination that Requirements at Railway / System / Sub-system are complete and correct in order to develop the solution and satisfy the Client.

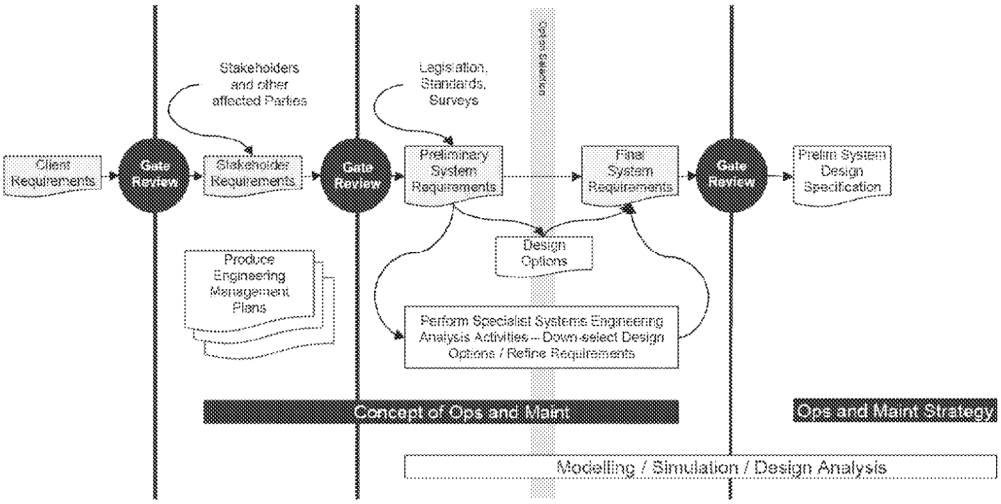

Stakeholders and other affected Parties
Legislation, Standards, Surveys
Option Selection
Client Requirements
Gate Review
Stakeholder Requirements
Gate Review
Preliminary System Requirements
Final System Requirements
Gate Review
Prelim System Design Specification
Design Options
Produce Engineering Management Plans
Perform Specialist Systems Engineering Analysis Activities – Down-select Design Options / Refine Requirements
Concept of Ops and Maint
Ops and Maint Strategy
Modelling / Simulation / Design Analysis

Figure 6 - Requirements Products

The contractual requirements document is the Project Agreement (PA). This contains requirements at multiple levels - railway, primary system, subsystem. The functional requirements from the PA have been captured in the requirements management tool, DOORS.

While attempts have previously been made to engage with operators and maintainers, no further requirements have been elicited. The risk associated with the lack of stakeholder requirements elicitation is that the requirements set is incomplete. The assumption is that the PA alone is a complete, validated set of requirements for the project. There is evidence that this assumption is invalid as more functionality has been added into procurement specifications than is required by the PA.

There are currently of the order of 1200 changes related to the PA. The requirements team are not automatically notified of these changes and therefore not all of the changes have been captured in DOORS.

There is no clear set of railway system requirements. Railway system requirements provide a definition of the functionality, performance and characteristics of the railway to be delivered including RAM and Safety targets. They provide a basis for development of the railway system architecture and design.

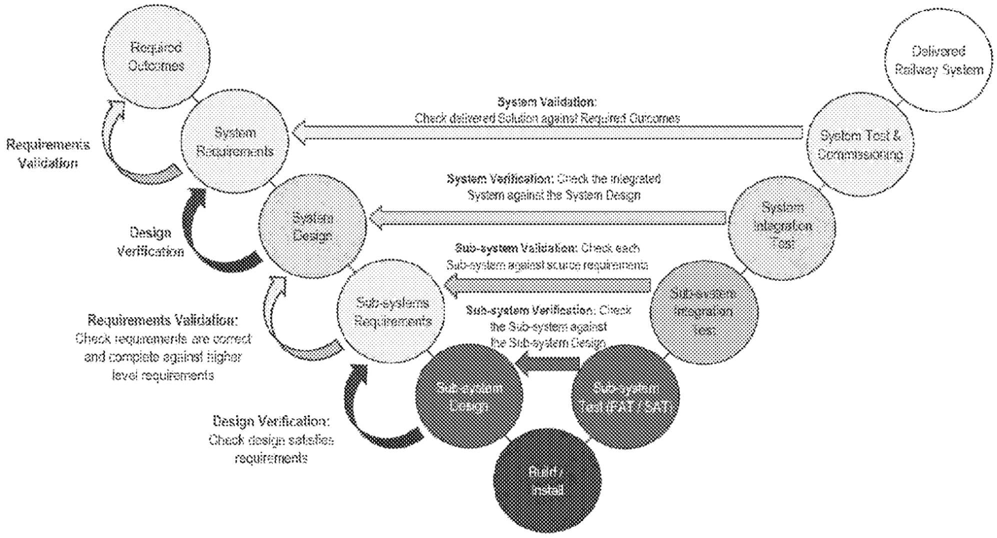
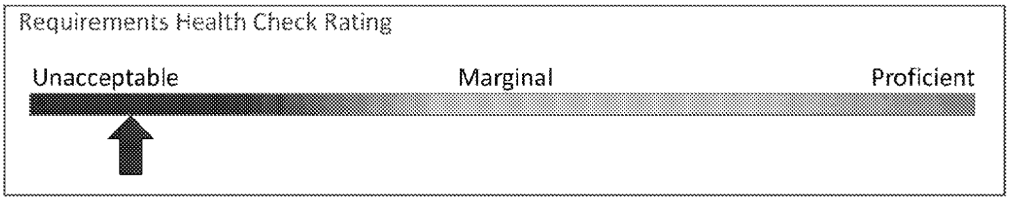

Required Outcomes
Delivered Railway System
System Validation:
Check delivered Solution against Required Outcomes
Requirements Validation
System Requirements
System Test & Commissioning
System Verification: Check the integrated System against the System Design
Design Verification
System Design
System Integration Test
Sub-system Validation: Check each Sub-system against source requirements
Sub-systems Requirements
Sub-system Integration Test
Requirements Validation:
Check requirements are correct and complete against higher level requirements
Sub-system Verification: Check the Sub-system against the Sub-system Design
Sub-system Design
Sub-system Test (FAT / SAT)
Design Verification:
Check design satisfies requirements
Build / Install

Figure 7 - Requirements Validity

Procurement specifications for primary systems and subsystems have been generated from the relevant requirements in the PA with limited analysis or derivation. The procurement specifications are not currently held in DOORS. The requirements team do not have visibility of the subsystem requirements.

Thales and Alstom have stated that some requirements within their respective procurement specifications are not applicable. It is not clear how this has been reflected back into the PA.



The technical requirements captured from the Project Agreement are not a complete set: it is therefore essential that further requirements capture / elicitation / derivation occurs along with requirements levelling / rationalisation - to remove duplication / confliction.

No evidence of a Requirements Management Plan for the project was provided.

Requirements Validity Argument – *not ready*

3.4.2 Requirements Traceability

Requirements traceability is a sub-discipline of Requirements Management; it records relationships between many kinds of development artefacts, such as requirements, specification statements, designs, tests, models and developed components.

Expanding on the above statement, requirements should be linked to their sources, be they captured from source documents or elicited from stakeholders or derived from specialist Systems Engineering analysis. Subsequently rtequirements should be linked to their solution. ~It should be noted that a large complex programme of work such as OLRT is expected to have such information at multiple levels of abstraction such as Railway, System and Sub-system and thus linkage will exist both within and between these layers.

This linkage underpins Requirements Traceability:

> *"6.4.2 Stakeholder needs and requirements definition process*
>
> > *6.4.2.3 Activities and tasks*
> >
> > > *f) Manage the stakeholder needs and requirements definition. This activity consists of the following tasks:*
> > >
> > > > *2) Maintain traceability of stakeholder needs and requirements.*
> > > >
> > > > > *NOTE Through the life cycle, bi-directional traceability is maintained between the stakeholder needs and requirements and the stakeholders and sources, organizational strategy, and business and mission problems and opportunities. Additional traceability to systems making up the system solution facilitates the transition to the System Requirements Definition process. This is often facilitated by an appropriate data repository"*
>
> *BS ISO/IEC/IEEE 15288:2015.*

Furthermore:

"6.4.3 System requirements definition process

6.4.3.3 Activities and tasks

d) Manage system requirements. This activity consists of the following tasks:

2) Maintain traceability of the system requirements.

NOTE Through the life cycle, bi-directional traceability is maintained between the system requirements and the stakeholder requirements, architecture elements, interface definitions, analysis results, verification methods or techniques, and allocated, decomposed, and derived requirements. This helps ensure that all achievable stakeholder requirements are met by one or more system requirements, and all system requirements meet or contribute to meeting at least one stakeholder requirement. This is often facilitated by an appropriate data repository"

BS ISO/IEC/IEEE 15288:2015.

By applying the principals outlined in applicable standards, referred to above, it can be determined that OLRT currently has immature Requirements Traceability within and between Railway, System and Sub-system levels and therefore:

Requirements Traceability Argument – *not ready*

3.4.3 Requirements Satisfaction

The demonstration of requirements being fulfilled begins in the design stage and continues through the subsequent system development stages of construction, testing & commissioning and operation. Hence, Requirements Satisfaction is evidenced through employing a robust Verification and Validation process and its various methods - such as analysis, modelling, simulation, test and inspection etc.

3.4.3.1 Verification and Validation (V&V)

ISO 15288: 6.4.9, 6.4.11

Ensuring that the 'right solution has been developed' (Validation) and 'developing the solution right' (Verification) are essential activities in any infrastructure programme. These activities are performed throughout the project lifecycle, to provide early and increasing confidence that the system is being developed correctly and to ensure that ultimately the outcomes required by the Client will be delivered.

For the purpose of Requirements Satisfaction, Verification is defined as;

"6.4.9 Verification process

6.4.9.1 Purpose

> *The purpose of the Verification process is to provide objective evidence that a system or system element fulfils its specified requirements and characteristics.*
>
> *The Verification process identifies the anomalies (errors, defects, or faults) in any information item (e.g., system requirements or architecture description), implemented system elements, or life cycle processes using appropriate methods, techniques, standards or rules. This process provides the necessary information to determine resolution of identified anomalies"*
>
> *BS ISO/IEC/IEEE 15288:2015.*

Whereas Validation is defined as:

"6.4.11 Validation process

6.4.11.1 Purpose

> *The purpose of the Validation process is to 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.*
>
> *The objective of validating a system or system element is to acquire confidence in its ability to achieve its intended mission, or use, under specific operational conditions. Validation is ratified by stakeholders. This process provides the necessary information so that identified anomalies can be resolved by the appropriate technical process where the anomaly was created"*
>
> *BS ISO/IEC/IEEE 15288:2015.*

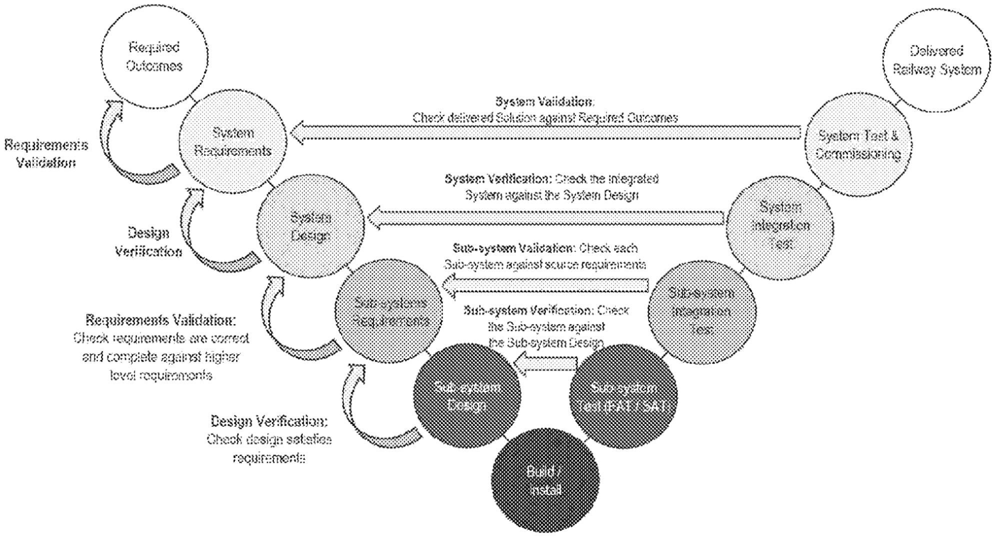

Required Outcomes
Delivered Railway System
System Validation: Check delivered Solution against Required Outcomes
System Requirements
System Test & Commissioning
Requirements Validation
System Verification: Check the integrated System against the System Design
System Design
System Integration Test
Design Verification
Sub-system Validation: Check each Sub-system against source requirements
Sub-systems Requirements
Sub-system Integration Test
Requirements Validation: Check requirements are correct and complete against higher level requirements
Sub-system Verification: Check the Sub-system against the Sub-system Design
Sub-system Design
Sub-system Test (FAT / SAT)
Design Verification: Check design satisfies requirements
Build / install

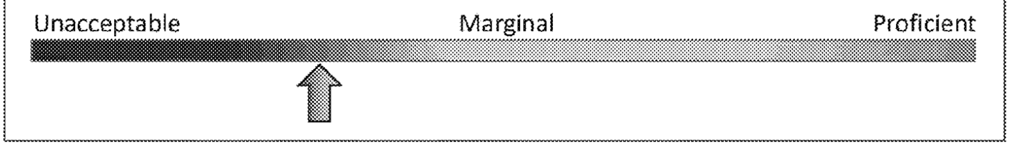
Figure 8 - Verification and Validation

Compliance data has been received from some suppliers against the procurement specifications but this is not complete in DOORS. Compliance data for the primary Systems (other than Vehicle and Signalling) is not complete.

No evidence of planning and tracking of V&V activities was provided.

No acceptance criteria have yet been developed against the PA and there has been no attempt to agree acceptance criteria with the City.

Verification & Validation Health Check Rating



Sections 3.4.3.2, 3.4.3.3, 3.4.3.4 and 3.4.3.5 below consider Requirements Satisfaction in each of the development stages following the requirements definition stage. It should be noted that these sub-categories of Requirements Satisfaction may be considered at more than one level of abstraction, e.g. Railway, System and Sub-system. The aggregation of these supporting arguments enables determination that OLRT currently has an immature Requirements Satisfaction at Railway, System and Sub-system levels, therefore the OLRT Requirement Satisfaction Argument cannot be made at this time.

Requirements Satisfaction Argument – *not ready*

3.4.3.2 Requirements Satisfied in Design

ISO 15288: 6.4.4, 6.4.5

System architecture activities define a comprehensive solution based on principles, concepts and properties logically related and consistent with each other. The solution architecture has features, properties and characteristics satisfying (as far as possible) the problem or opportunity expressed by the system requirements. It focusses on the high-level structure in systems and system elements.

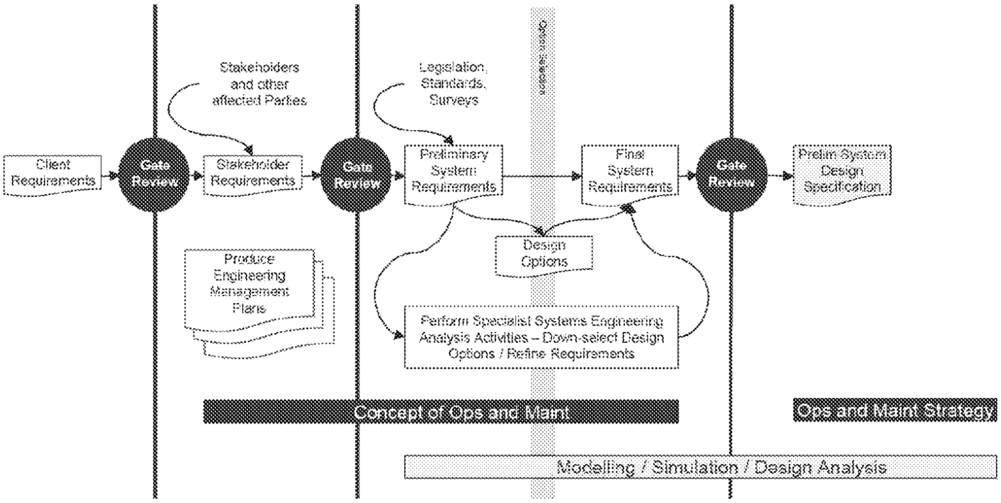

Stakeholders and other affected Parties
Legislation, Standards, Surveys
Option Selection
Client Requirements
Gate Review
Stakeholder Requirements
Gate Review
Preliminary System Requirements
Final System Requirements
Gate Review
Prelim System Design Specification
Design Options
Produce Engineering Management Plans
Perform Specialist Systems Engineering Analysis Activities – Down-select Design Options / Refine Requirements
Concept of Ops and Maint
Ops and Maint Strategy
Modelling / Simulation / Design Analysis

Figure 9 - Design Deliverables

At the railway level, there has previously been limited architecture and design definition. This increases the risk that individually specified systems will not successfully integrate together to satisfy railway level requirements and provides no means of apportioning railway level requirements down to systems.

Work is now starting in this area to develop architectures where they add value in de-risking integration, particularly focussed on the Communications and SCADA systems. Use cases are also being developed to provide a behavioural model. This work is considered to be underfunded and under resourced.

The design process for engineers is governed by Professional Engineers Ontario (PEO) and the Design Management Plan.

Fixed facilities designs are claimed to be fit for purpose, meeting contractual requirements, codes and standards. There is less confidence in the other primary Systems areas (other than Vehicle and Signalling).

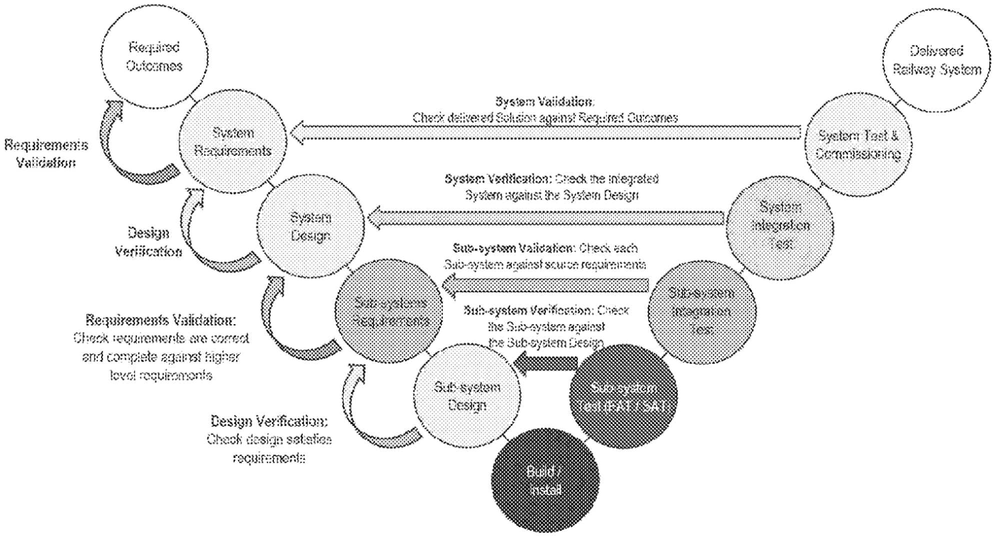

Required Outcomes
Delivered Railway System
System Validation: Check delivered Solution against Required Outcomes
System Requirements
System Test & Commissioning
Requirements Validation
System Verification: Check the integrated System against the System Design
System Design
System Integration Test
Design Verification
Sub-system Validation: Check each Sub-system against source requirements
Sub-systems Requirements
Sub-system Integration Test
Requirements Validation: Check requirements are correct and complete against higher level requirements
Sub-system Verification: Check the Sub-system against the Sub-system Design
Sub-system Design
Sub-system Test (FAT / SAT)
Design Verification: Check design satisfies requirements
Build / Install

Figure 10 – Requirements Satisfied in Design

3.4.3.2.1 Interface Management

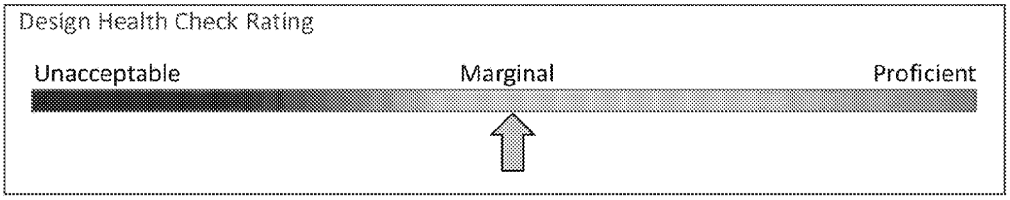
ISO 15288: 6.4.2, 6.4.3

Successful management of interfaces is critical to the success of any project but is an area which is commonly overlooked or badly managed. Interface management can help highlight underlying critical issues much earlier in the project.

An interface register has recently started to be generated for the project.

Although there are still some open points, interfaces between the primary rail systems (Rolling Stock and Computer Based Train Control (CBTC)) are being actively managed.

Again, the key risk area appears to be around the primary Systems areas (other than Vehicle and Signalling).



It is apparent that OLRT has no Railway level design. A measure of confidence can be assumed with the procurement of two (2) primary System elements from Thales and Alstom and the Requirements Compliance Matrices they have produced. It should be noted that these are fundamentally flawed, as these are based entirely on the OLRT Project Agreement and have not been embellished with further elicited or derived requirements. There is limited (at best) to no (worst) design compliance evidence available for the remainder of the OLRT solution at primary System level. In this area Sub-system design compliance evidence is provided via Designer Certificates which should provide a measure of confidence, but are lacking formal Requirements Compliance Matrices.

It can therefore be determined that OLRT currently has immature Requirements Satisfaction in Design within and between Railway, System and Sub-system levels, therefore the OLRT Requirements Satisfied in Design Argument cannot be made at this time.

Requirements Satisfied in Design Argument – *not ready*

3.4.3.3 Requirements Satisfied in Implementation

ISO 15288: 6.4.7

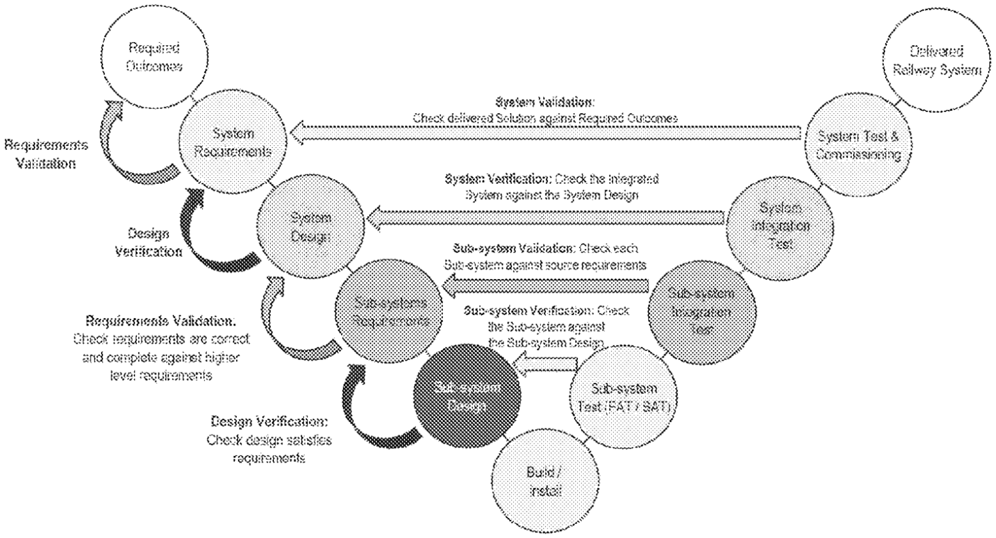
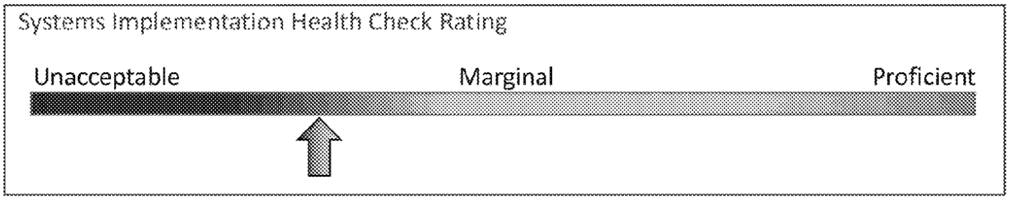

Required Outcomes
Delivered Railway System
System Validation:
Check delivered Solution against Required Outcomes
Requirements Validation
System Requirements
System Test & Commissioning
System Verification: Check the integrated System against the System Design
Design Verification
System Design
System Integration Test
Sub-system Validation: Check each Sub-system against source requirements
Sub-systems Requirements
Sub-system Integration Test
Requirements Validation: Check requirements are correct and complete against higher level requirements
Sub-system Verification: Check the Sub-system against the Sub-system Design
Sub-system Design
Sub-system Test (FAT / SAT)
Design Verification: Check design satisfies requirements
Build / install

Figure 11 – Requirements Satisfied in Implementation

The lack of railway level requirements and design has impacted the implementation and integration phases of the project. Additional work is required during implementation to attempt to identify and resolve gaps in the specifications. This by its nature is "bottom up" rather than "top down" integration.

Reduced coherence between the designed elements makes integration extremely challenging and in the case of a large scale rollout, the integration may be beyond the capability of the implementation team to deliver. Further, once integrated, the through life cost of the system may be higher.

The procurement department is non-technical with no engineering resource. This has led to omissions such as O&M manuals not being included in the contract.



It is readily apparent that Design Integration has crossed in to this activity. Design drawings, some with compounded changes not yet incorporated and many with insufficient detail, are being worked to and subsequently 'red-lined': there is no formal recording of Compliance to Requirements, rather there is robust effort to make the design work. This approach carries with it much risk as it is being conducted without visibility / formal understanding of decision implications, although it is readily apparent that the Implementation Team are striving to deliver a product that works.

It can therefore be determined that OLRT currently has immature Requirements Satisfaction in Implementation within and between Railway, System and Sub-system levels, therefore the OLRT Requirements Satisfied in Implementation Argument cannot be fully made at this time.

Requirements Satisfied in Implementation
Argument – not fully ready

3.4.3.4 Requirements Satisfied in Test & Commissioning

ISO 15288: 6.4.8

A Test and Commissioning Plan is in place which lists the System Integration Tests (SITs). Operational scenario tests have not currently been developed.

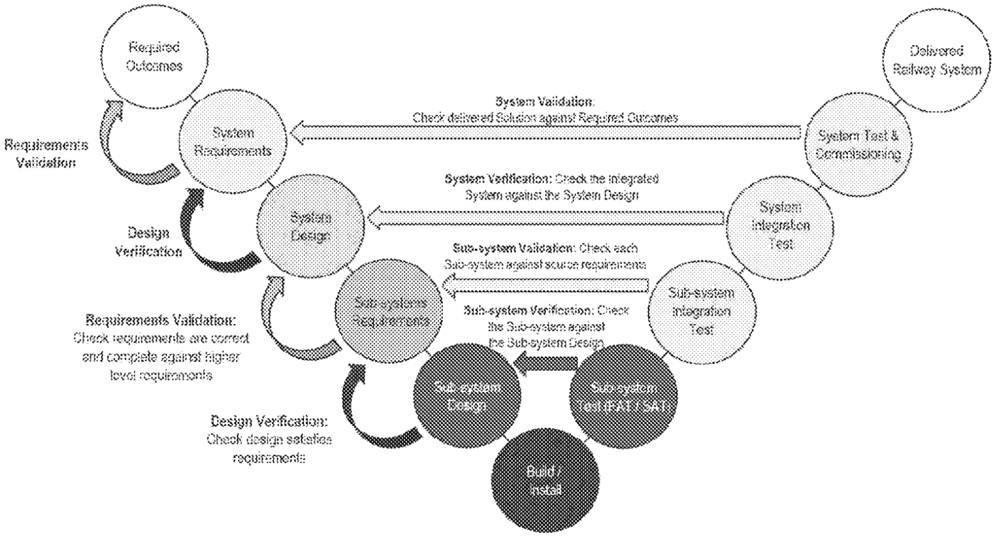

Required Outcomes
Delivered Railway System
System Validation: Check delivered Solution against Required Outcomes
Requirements Validation
System Requirements
System Test & Commissioning
System Verification: Check the integrated System against the System Design
Design Verification
System Design
System Integration Test
Sub-system Validation: Check each Sub-system against source requirements
Sub-systems Requirements
Sub-system Verification: Check the Sub-system against the Sub-system Design
Sub-system Integration Test
Requirements Validation: Check requirements are correct and complete against higher level requirements
Sub-system Design
Sub-system Test (FAT / SAT)
Design Verification: Check design satisfies requirements
Build / Install

Figure 12 - System Integration V&V

There is no traceability from the SITs back to the railway system requirements or to the PA and no process for recording test results against contractual requirements. In the absence of railway system requirements, the SITs have been mapped to the interface register.

Due to the lack of railway level systems engineering there is a risk that component acceptance tests will pass but system integration tests will fail with multiple defects.

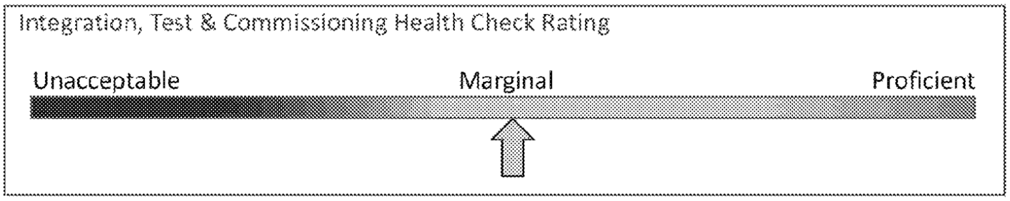
As there has been insufficient effort early in the lifecycle to "design for integration", system integration has been pushed to the right. There is now a risk that the T&C Team, as with the Installation Team, will need to dedicate significantly increased time "making it work" in addition to testing to confirm it works.

A Test Review Panel is being set up with the City to reviews test reports and status.

A defect review board has been established run by the T&C Team. The software tool used as the Failure Reporting, Analysis and Corrective Action System (FRACAS) is insufficient and the T&C Team have to augment the output with standard attributes.

The turnover process from the installation team to the T&C Team is working well.

The T&C Team chair interface management meetings between Thales and Alstom at field level.



With the immaturity of the Requirements set, discussed at various junctures in this report and the absence of an integrated design at both Railway and primary System levels, it is not possible to fully define tests to prove the integrated function and performance of OLRT. The Test & Commissioning Team are making strenuous efforts to bridge this gap, but there is a significant risk that this will result in a robust effort to make the design / installed components work together and will lack formal recording of Compliance to Requirements.

It can therefore be determined that OLRT currently has immature Requirements Satisfaction in Test & Commissioning within and between Railway, System and Sub-system levels, therefore the OLRT Requirements Satisfied in Test & Commissioning Argument cannot be fully made at this time.

Requirements Satisfied in Integration, Test & Commissioning Argument - not fully ready

3.4.3.5 Requirements Satisfied in Operations

ISO 15288: 6.4.10

The Operations Concept is a broad outline of an organization's assumptions or intent in regard to an operation or series of operations. It provides the basis for bounding the operating space, system capabilities, interfaces and operating environment.

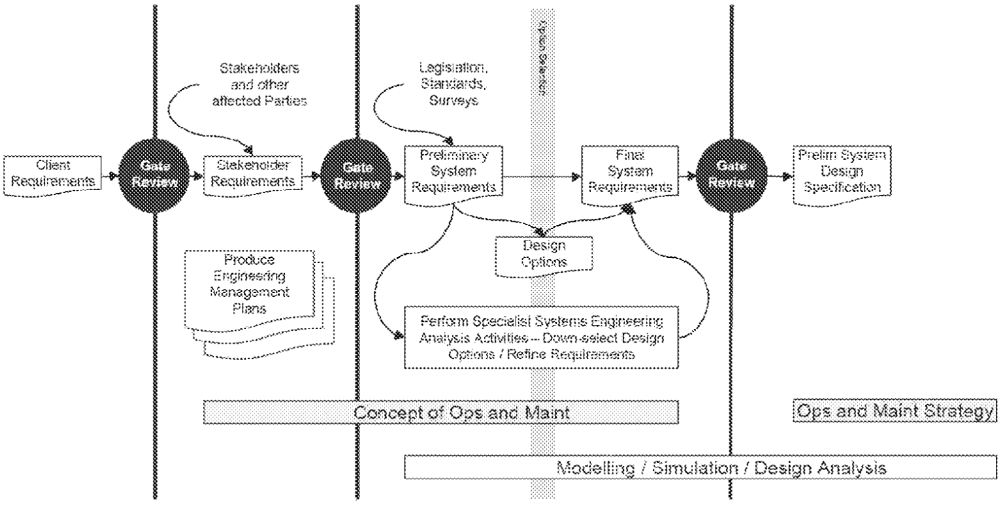
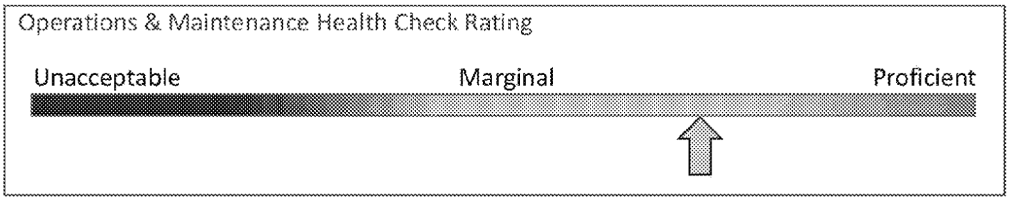

Stakeholders and other affected Parties
Legislation, Standards, Surveys
Option Selection
Client Requirements
Gate Review
Stakeholder Requirements
Gate Review
Preliminary System Requirements
Final System Requirements
Gate Review
Prelim System Design Specification
Design Options
Produce Engineering Management Plans
Perform Specialist Systems Engineering Analysis Activities – Down-select Design Options / Refine Requirements
Concept of Ops and Maint
Ops and Maint Strategy
Modelling / Simulation / Design Analysis

Figure 13 - Operations and Maintenance Products

An Operations Concept and a Maintenance Concept were both stated to be in existence. As there are no Railway System requirements, it is not possible to confirm via traceability whether the content of these documents has been incorporated into the design.



OLRT has not yet entered in to service; it is therefore too early to assess whether Requirements have been satisfied during operation.

Requirements Satisfied in Operations Argument – *TBC*

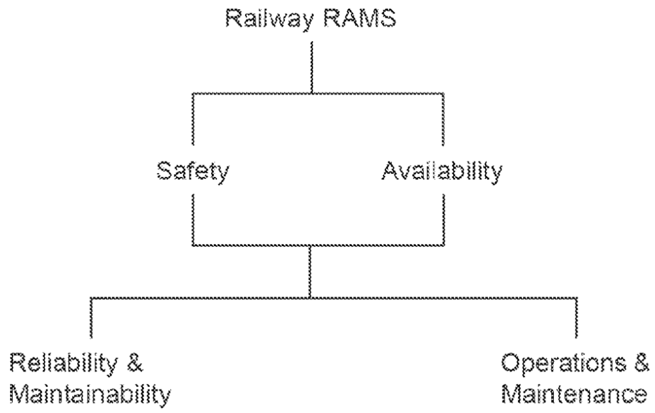
3.4.4 Non-Interference

The demonstration of the OLRT Non-Interference Argument is comprised of RAMS and associated systems elements such as Human Factors and EMC: the objective is to show that the Railway is both Safe and Available, in a Reliable manner providing appropriate Maintenance is undertaken.

4.3 Elements of Railway RAMS

> *Safety and availability are inter-linked in the sense that a weakness in either or mismanagement of conflicts between safety and availability requirements may prevent achievement of a dependable system. The inter-linking of railway RAMS elements, reliability, availability, maintainability and safety in shown in figure below*

BS EN 50126-1 1999



Inter-relation of Railway RAMS Elements BS EN 50126-1 1999

Sections 3.4.4.1, 3.4.4.2, 3.4.4.3 and 3.4.4.4 below consider the various sub-categories of the Non-Interference argument. It should be noted that these sub-categories may be considered at more than one level of abstraction, e.g. Railway, System and Sub-system. The aggregation of these supporting arguments enables determination that OLRT is currently immature at Railway, System and Sub-system levels and the OLRT Non-Interference Argument cannot be made at this time.

OLRT Non-Interference Argument – *not ready*

3.4.4.1 Safety

The demonstration of Railway Safety begins in the requirements stage and continues through the subsequent system development stages of design, construction, testing & commissioning and operation. Hence, Safety is evidenced through employing a robust Safety Analysis and Hazard Management process, and its various methods - such as System Hazard Analysis, Fault Tree Analysis, Failure Modes Effects Criticality Analysis, allocation of SIL levels etc.

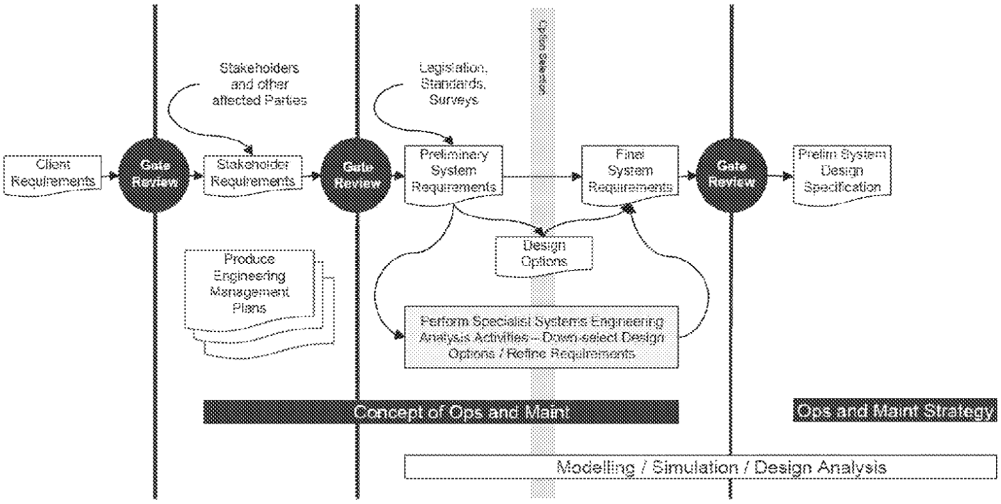

Stakeholders and other affected Parties
Legislation, Standards, Surveys
Option Selection
Client Requirements
Gate Review
Stakeholder Requirements
Gate Review
Preliminary System Requirements
Final System Requirements
Gate Review
Prelim System Design Specification
Design Options
Produce Engineering Management Plans
Perform Specialist Systems Engineering Analysis Activities – Down-select Design Options / Refine Requirements
Concept of Ops and Maint
Ops and Maint Strategy
Modelling / Simulation / Design Analysis

Figure 14 - Specialist Engineering Activities - Safety

Technical / Engineering Safety Management is defined as:

4,3,6 Technical concepts of safety are based on a knowledge of:

a) all possible hazards in the system, under all operation, maintenance and environment modes.

b) the characteristics of each hazard in terms of severity of consequences.

c) Safety/safety related failures in terms of:

- All system failure modes that could lead to a hazard (safety related failure modes). This is a sub-set of all reliability failure modes (a));

- The probability of occurrence of each safety related system failure mode;

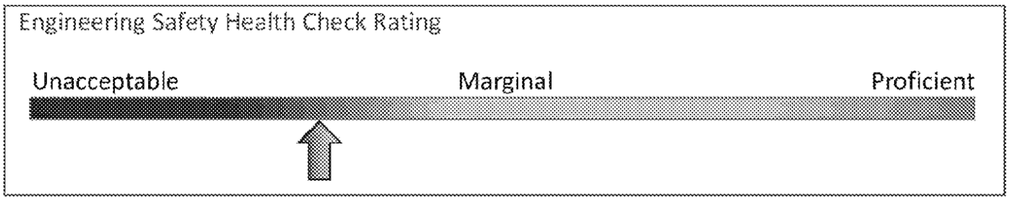
> *- Sequence and/or coincidence of events, failures, operational states, environmental conditions etc. in the application, that may result in an accident. (i.e. a hazard resulting in an accident);*
>
> *- The probability of occurrence of each of the events, failures operational states, environment conditions, etc. in the application.*
>
> *d) maintainability of safety related parts of the system in terms of:*
>
> *- the ease of performing maintenance on those aspects or parts of the system or its components that are associated with a hazard or with a safety related failure mode;*
>
> *- probability of errors occurring during maintenance actions on those safety related parts of the system;*
>
> *- time for restoring the system into a safe state.*
>
> *e) System operation and maintenance of safety related parts of the system in terms of:*
>
> *- human factors influence on the effective maintenance of all safety related parts of the system and safe operation of the system;*
>
> *- Tools, facilities and procedures for effective maintenance of the safety related parts of the system and for safe operation;*
>
> *- effective controls and measures for dealing with a hazard and mitigating its consequences."*
>
> *BS EN 50126-1 1999.*

A hazard log exists and incorporates hazards on other systems which have been identified by Thales and Alstom. It was stated that the hazard log is not currently structured and is now being reworked into a hierarchical categorisation. No fault tree or other formal analysis has been performed.

Safety requirements resulting from the HAZID process do not appear to have been captured. No traceability exists to confirm whether required safety measures have been incorporated into the design.

The Guideway Intrusion Detection System (GIDS) and traction power are required to be Safety Integrity Level (SIL) 2. Both have been assessed as not currently meeting this level.

During the review it emerged that the Standard Operating Procedures (SOPs) drafted by OLRT were in the process of being rewritten by the Operator, often substantially reduced in content. There is a risk that where a SOP has been written to provide a partial or full mitigation of a hazard, that the effectiveness of this mitigation is reduced during the rewriting process. There is also a danger that the reduced SOP will not mitigate the hazard and invalidate the safety claim.



The lack of OLRT Derived Requirements at Railway, primary System and Sub-system levels suggests the minimum requisite Safety Analysis and Hazard Management has not been undertaken. Preliminary Hazard Analysis has been undertaken but thereafter System Hazard Analysis, Fault Tree Analysis, Failure Modes Effects Criticality Analysis, allocation of SIL levels and so on have not been completed / undertaken.

It can therefore be determined that OLRT currently has an immature Safety Argument within and between Railway, System and Sub-system levels, therefore the OLRT Safety Argument cannot be made at this time.

OLRT Safety Argument – *not ready*

3.4.4.2 RAM

The demonstration of Reliability, Availability and Maintainability begins in the requirements stage and continues through the subsequent system development stages of design, construction, testing & commissioning and operation. Hence RAM is evidenced through employing a robust RAM Management process and its various methods - such as Mean Time Between Service Affecting Failure management, Fault Tree Analysis, Failure Modes Effects Criticality Analysis, etc.

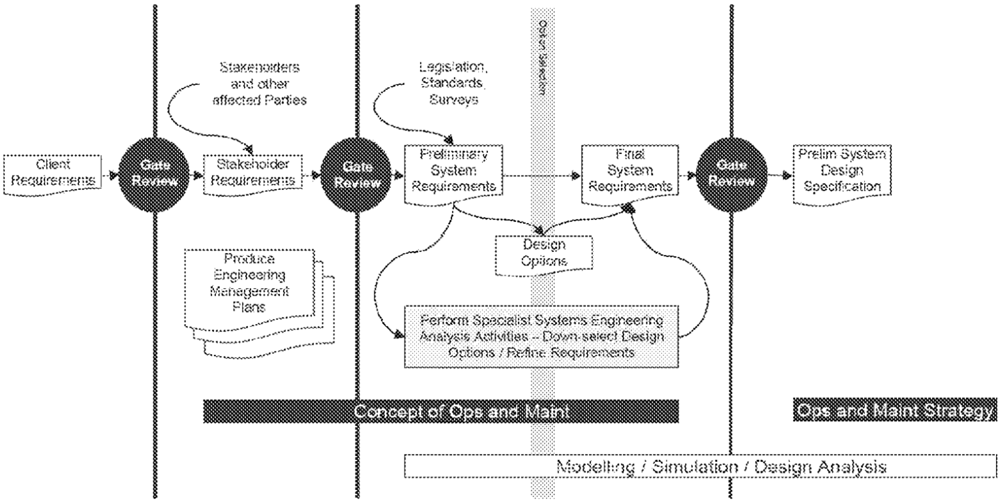


Figure 15 - Specialist Engineering Activities - RAM

Technical / Engineering Reliability, Availability and Maintainability Management is defined as:

> *"4.3 Elements of railway RAMS*
>
> *4.3.5 Technical concepts of availability are based on a knowledge of:*
>
> *a) reliability in terms of:*
>
> *- all possible system failure modes in the specified application and environment;*
>
> *- the probability of occurrence of each failure or alternatively, the rate of occurrence of each failure;*
>
> *- the effects of the failure on the functionality of the system.*
>
> *b) Maintainability in terms of:*
>
> *- time for the performance of planned maintenance;*
>
> *- time for detection, identification and location of faults;*
>
> *- time for the restoration of the failed system (unplanned maintenance).*
>
> *c) Operation and maintenance in terms of:*
>
> *- all possible operation modes and required maintenance, over the system lifecycle;*
>
> *- the human factor issues.*
>
> *BS EN 50126-1 1999.*

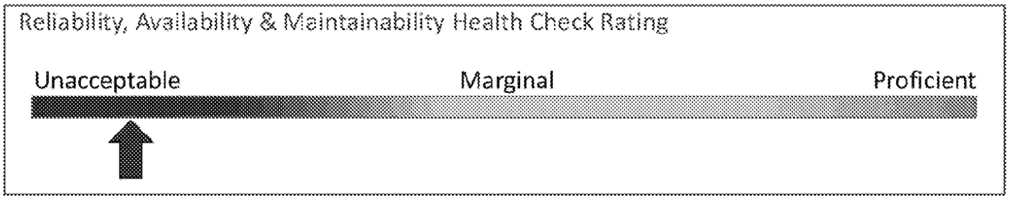
Analysis of how availability targets are to be met needs to be started early in the life cycle. RAM analysis determines the reliability targets for individual assets, redundancy and maintainability requirements including spares holdings, for example.

RAM analysis has not yet been performed for the project.

It was stated that Thales and Alstom have performed RAM analysis for their systems although the output of this analysis has not yet been studied.

Because of the lack of any RAM analysis, RAM targets were not set and are missing from some procurement specifications.

Attention also needs to be given to the strategy for reliability growth during trial running and the initial period of revenue service.


Reliability, Availability & Maintainability Health Check Rating

The minimum requisite Reliability, Availability and Maintainability analysis has not been undertaken.

It can therefore be determined that OLRT currently has an immature RAM Argument within and between Railway, System and Sub-system levels, therefore the OLRT RAM Argument cannot be made at this time.

OLRT RAM Argument – *not ready*

3.4.4.3 Human Factors

A Railway System is the sum of all of its parts: people plus processes plus products. Thus it is essential to manage the suitability of people to undertake certain functions, particularly those that are essential to Safe Operation and Maintenance. Furthermore, it is essential to manage Ergonomic aspects for those who will operate, maintain and use the railway.

Human Factors and Ergonomics is defined as:

4.4 Factors Influencing Railway RAMS

4.4.2 Categories of factors

4.4.2.11 The derivation of detailed human influencing factors should include, but not be limited to a consideration of each of the following human factors. It should be noted that the following checklist is non-exhaustive and should be adapted to the scope and purpose of the application;

a) allocation of system functions between human and machine;

b) effect on human performance within the system;

c) requirements on the system arising from competencies and reaction time;

d) requirements on the system arising from information processing capabilities;

e) effects on the system of human/system interface factors;

f) Human factors in system design and development."

BS EN 50126-1 1999.

The lack of OLRT Derived Requirements at Railway, primary System and Sub-system levels suggests the minimum requisite Human Factors and Ergonomics analysis has not been formally and demonstrably undertaken. For the purpose of this report it is assumed that both Alstom and Thales will have managed Human Factors and Ergonomics considerations thus this issue affects the remainder of OLRT.

It can therefore be determined that OLRT currently has an immature HF Argument, therefore the OLRT HF Argument cannot be fully made at this time.

OLRT HF Argument - not fully ready

3.4.4.4 EMC

In order to confirm that the Railway can be operated and maintained Safely and Reliably, it is also necessary to consider other influencing factors. One key factor is Electromagnetic Compatibility.

4.4 Factors Influencing Railway RAMS

4.4.2 Categories of factors

4.4.2.10 The derivation of railway specific influencing factors should include, but not be limited to, a consideration of each of the following specific factors. It should be noted that the following checklist is non-exhaustive and should be adapted to the scope and purpose of the application:

a) system operation;

b) environment;

c) application conditions;

d) operating conditions;

e) failure categories.

BS EN 50126-1 1999.

The lack of OLRT derived requirements at Railway, primary System and Sub-system levels suggests the minimum requisite EMC analysis has not been formally and demonstrably undertaken. For the purpose of this report it is assumed that both Alstom and Thales will have managed EMC considerations thus this issue affects the remainder of OLRT.

It can therefore be determined that OLRT currently has an immature EMC Argument, therefore the OLRT EMC Argument cannot be fully made at this time.

3.4.5 Configuration Consistency

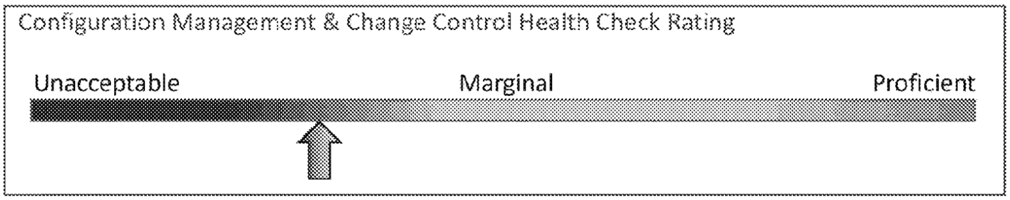
The purpose of Configuration Management (CM) is to manage and control system elements and configurations over the life cycle. CM also manages consistency between a product and its associated configuration definition. As a result of the successful implementation of the Configuration Management process, configuration baselines are established and changes to items under configuration management are controlled.

For all major projects it is essential to manage configuration of design and as built and manage the applicability of changes to the configuration. To achieve this, data baselines should be created at each gate / design review.

> *6.3.5 Configuration management process*
>
> *6.3.5.1 Purpose*
>
> *The purpose of Configuration Management (CM) is to manage and control system elements and configurations over the life cycle. CM also manages consistency between a product and its associated configuration definition*
>
> *6.3.5.2 Outcomes*
>
> *As a result of the successful implementation of the Configuration Management process:*
>
> *a) Items requiring configuration management are identified and managed.*
>
> *b) Configuration baselines are established.*
>
> *c) Changes to items under configuration management are controlled.*
>
> *d) Configuration status information is available.*
>
> *e) Required configuration audits are completed.*
>
> *f) System releases and deliveries are controlled and approved*
>
> *BS ISO/IEC/IEEE 15288:2015.*

The review found that individual documents and drawings are controlled and managed, however there does not appear to be any definition of overall technical baselines for the project.

Design baselines should normally be produced at each requirements and design review and again at key lifecycle stages (installation, integration etc.) to incorporate asset information, software and configuration data versions etc.



The lack of OLRT design reviews, including Systems Engineering / Interdisciplinary design reviews, has resulted in no configuration baselines of the OLRT Requirements or Design. This is subsequently reflected in the implementation activities with multiple compounded changes against single design drawings that are undecipherable.

It can therefore be determined that OLRT currently has immature Configuration Consistency within and between Railway, System and Sub-system levels, therefore the OLRT Configuration Consistency Argument cannot be made at this time.

OLRT Configuration Consistency Argument – *not ready*

3.5 Review Summary

Figure 16 illustrates both the minimum Systems Engineering maturity expected for the current lifecycle stage of the project together with actual maturity assessed during the health check.

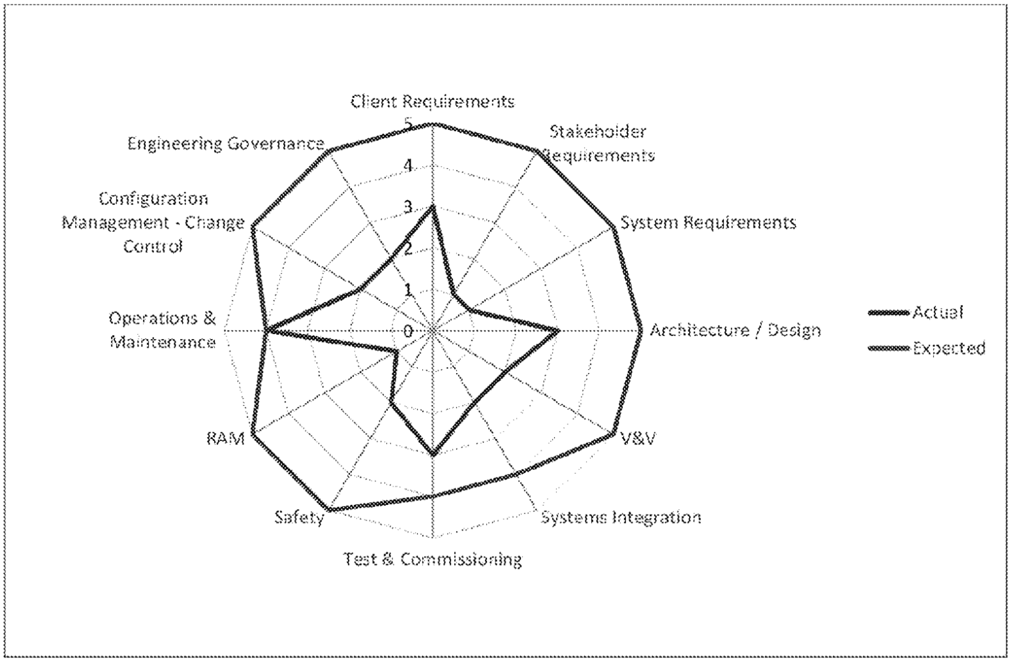


Figure 16 - Health Check Summary

Sections 3.3 and 3.4 of this have described the status of each of the OLRT Risk Based Assurance Arguments. By collating these individual argument statuses and depicting them alongside the Risk Based Assurance argument framework it is clear to see the difficulty in presenting robust assurance that can withstand scrutiny.

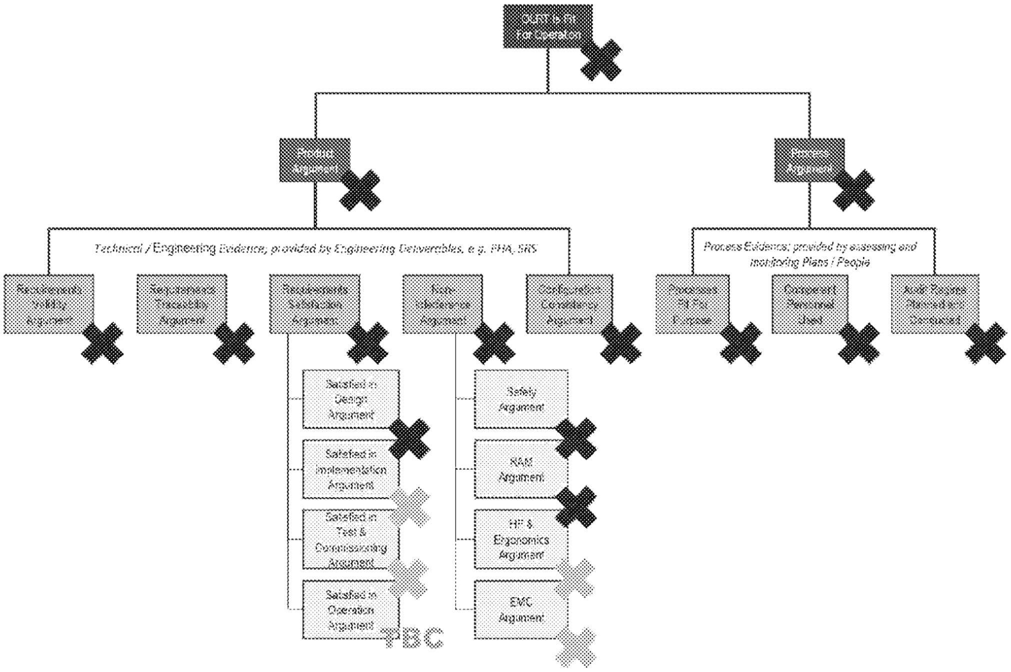

OLRT is Fit For Operation
Product Argument
Process Argument
Technical / Engineering Evidence; provided by Engineering Deliverables, e.g. PHA, SRS
Process Evidence; provided by assessing and monitoring Plans / People
Requirements Validity Argument
Requirements Traceability Argument
Requirements Satisfaction Argument
Non-Interference Argument
Configuration Consistency Argument
Processes Fit For Purpose
Competent Personnel Used
Audit Regime Planned and Conducted
Satisfied in Design Argument
Satisfied in Implementation Argument
Satisfied in Test & Commissioning Argument
Satisfied in Operation Argument
TBC
Safety Argument
RAM Argument
HF & Ergonomics Argument
EMC Argument

Figure 17 - Fit for Operation Argument Summary

The OLRT Systems Engineering reviewers have circa 50 years combined Systems Engineering experience and due to the nature of their work have had oversight of a significant number of major rail programmes: given the quantum and severity of deficiencies identified within the one (1) week Systems Engineering Health Check it is essential that robust effort is applied to identifying / agreeing the optimum set of Systems Engineering activities and resultant artefacts with the Client / SA enabling the project to conclude: section 4 of this report overviews the suggested Route to Delivery.

4 OLRT Route to Delivery

The level of Systems Engineering on the project to date is considered to have been below the recognised minimum acceptable level for a project of this size and complexity. This is especially evident at the railway system level and for early phases of the lifecycle - requirements and design. In our opinion this is likely to have increased the integration risk on the project, which may place increased pressure on the revenue service availability date.

There is generally a reasonable level of confidence in the two primary system suppliers – Thales and Alstom. Both companies have mature systems engineering processes and significant previous experience. The primary area of risk is around the remainder of the primary Systems and Sub-systems such as Communications and SCADA.

Given the stage the project is at, the focus now needs to be on identifying the set of activities to reduce the integration risk to an acceptable level and to enable an assurance case to be built.

4.1 Requirements Validity and Design Integration Verification Strategy

The diagram below and subsequent suggested actions should be undertaken 'in parallel': Top-down; Middle-out; Bottom-up. This will enable concurrency in application of recovery activities with a view to adhering to the Revenue Service date.

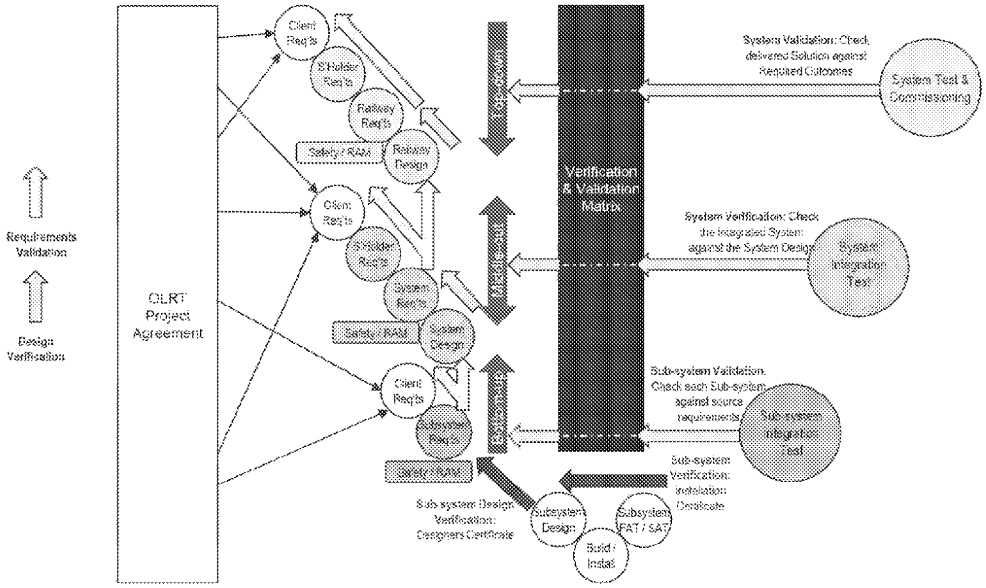

Requirements Validation
Design Verification
OLRT Project Agreement
Client Req'ts
S'Holder Req'ts
Railway Req'ts
Safety / RAM
Railway Design
Client Req'ts
S'Holder Req'ts
System Req'ts
Safety / RAM
System Design
Client Req'ts
Subsystem Req'ts
Safety / RAM
Sub-system Design Verification: Designers Certificate
Top-down
Middle-out
Bottom-up
Verification & Validation Matrix
System Validation: Check delivered Solution against Required Outcomes
System Test & Commissioning
System Verification: Check the integrated System against the System Design
System Integration Test
Sub-system Validation. Check each Sub-system against source requirements
Sub-system Integration Test
Sub-system Verification: Installation Certificate
Subsystem Design
Build / Install
Subsystem FAT / SAT

Figure 18 - Proposed Requirements Validity and Design Integration Strategy

The Route to OLRT Delivery strategy is based upon: maximising the use of existing formal Systems Engineering artefacts, whilst undertaking tasks to formalise other essential information along with its requisite traceability. These actions need to be agreed with the City / SA at the Engagement Workshop scheduled for 15-17th November 2017.

1. The OLRT Project Agreement is already captured into DOORS: this needs to be further analysed to ensure appropriate levelling and decomposition of captured requirements and updated to incorporate changes.

2. In parallel to 1. The Procurement Specifications will be captured into DOORS and linked back to the OLRT Project Agreement captured / analysed requirements.

3. OLRT Stakeholder Requirements will be captured / structured into DOORS from known sources - e.g. Maintenance Plan: these requirements will most likely be at the Railway and primary System level.

4. Railway level System Requirements will be derived that satisfy the Railway level Client and Stakeholder requirements.

5. In parallel to 4. Railway level Safety / RAM analysis will be undertaken with subsequent derived requirements being captured by 4.

6. Railway level physical and functional architectures (design) will be produced and linked back to the Railway level System Requirements.

7. Primary System level System Requirements will be apportioned by the Railway level Design and embellished by creating linkage back to both parent level and primary System level Client and Stakeholder requirements.

8. In parallel to 7. Primary System level Safety / RAM analysis will be undertaken with subsequent derived requirements being captured by 7.

9. Primary System level physical and functional architectures (design) will be produced and linked back to the primary System level System Requirements.

10. Sub-system level System Requirements will be apportioned by the primary System level Design and embellished by creating linkage back to both parent level and Sub-system level Client requirements.

4.2 Design Verification, Product Verification and Validation Strategy

By completing the above 10 waypoints, not only will a valid set of requirements and design integration verification have been achieved, the framework against which design verification, product verification and product validation can be proven will also be created.

11. OLRT Designers will complete a design checklist and design certificate to confirm that their design meets the Sub-system level System Requirements. Additionally, OLRT Designers will complete a checklist to confirm that Procurement Specifications are procuring appropriate products.

12. OLRT Installation Team will complete an Installation checklist and installation certificate to confirm that the installation meets the Sub-system design and Sub-system System Requirements. Any deviation is to be recorded on red-line drawings and will incur RAM and Safety analysis to ensure that the required emergent properties will not be compromised.

13. OLRT Test & Commissioning Team will then undertake:

    a. Sub-system Validation against Sub-system Requirements;

    b. Primary System Verification against the primary System Requirements and Design, ensuring that the installed Sub-systems integrate to achieve the aggregate intent;

    c. Primary System / Railway Validation against the Railway System Requirements and Design ensuring that the primary Systems integrate to achieve the aggregate intent.

14. All Verification and Validation confirmation will be captured into a Verification & Validation Matrix and linked back to the various levels of requirements, thus affording requirements traceability.

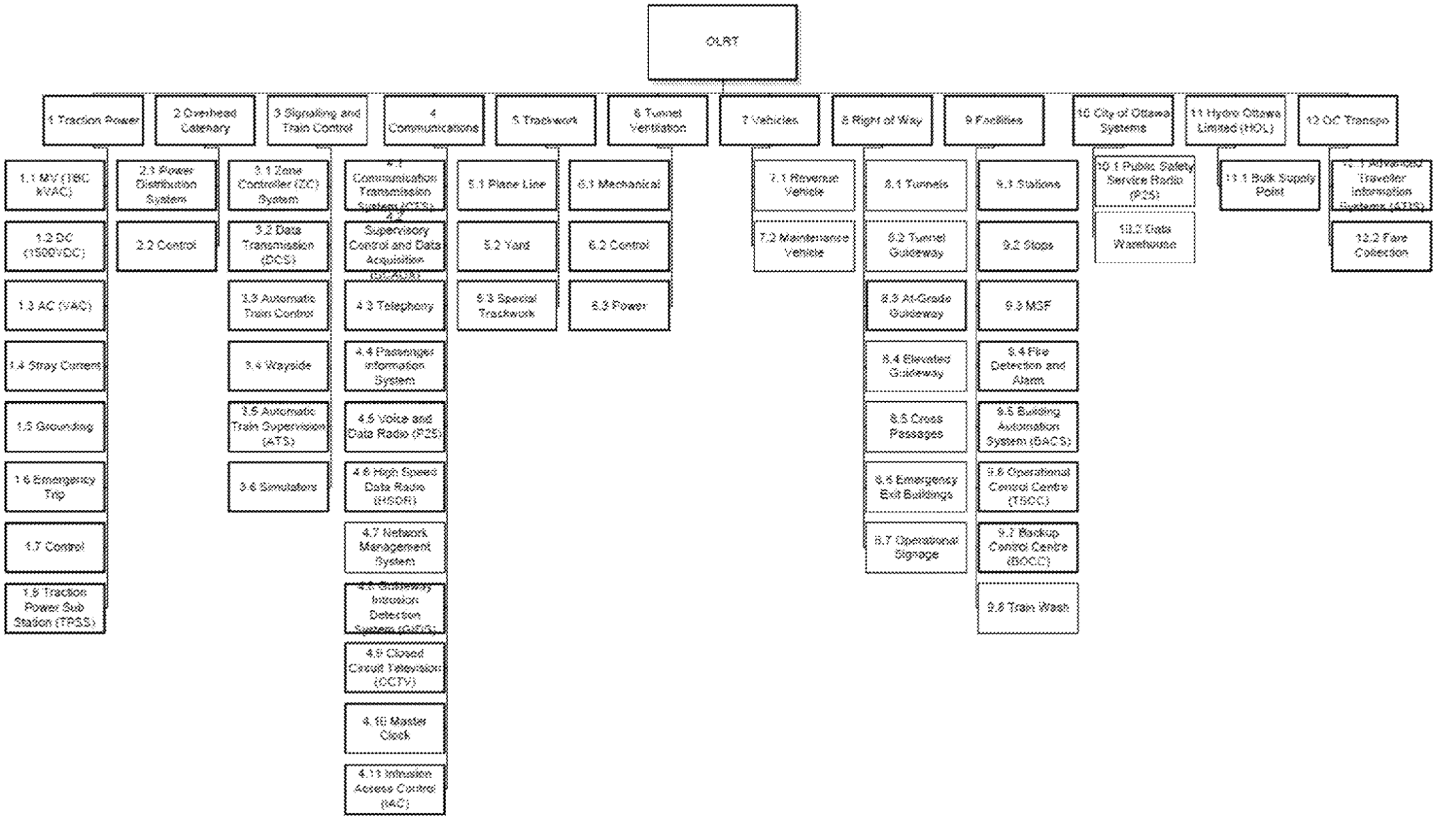
Appendix 1. Review Schedule

Table 3 – Review Schedule

Day	Morning	Afternoon
Mon	Systems Engineering and Assurance Management Plans at: OLRT Railway Level OLRT Major System / Asset Level Covering at least the following: Systems Engineering Management Plan (SEMP) Requirements Management Plan (RMP) Verification and Validation Management Plan (VVMP) Safety Management Plan (SMP) Reliability, Availability Maintainability Plan (RAMP) Human Factors Integration (HFIP) Electromagnetic Compatibility Control Plan (EMCP) Interface Management Plan (IFMP) System Design Management Plan (SDMP)	Systems Engineering and Assurance Management Competence / Capacity / Enablement at: OLRT Railway Level Covering at least the following: Systems Engineering Requirements Verification and Validation Safety RAM Human Factors EMC Interfaces System Design
Tues	Requirements Validity at: OLRT Railway Level OLRT Primary System / Asset Level Covering at least the following: Client / Stakeholder / System Captured / Elicited / Derived Concept of Operations Maintenance Concept Hazard Log Interface Register	Design Verification at: OLRT Railway Level OLRT Primary System / Asset Level Covering at least the following: System Architecture Interface Specifications Functional Block Diagrams Modelling / Simulation / Analysis Design compliance evidence
Wed	Specialist Analysis at: OLRT Railway Level OLRT Primary System / Asset Level Covering the following HF Analysis / Assessments RAM Analysis Safety Analysis / Assessments EMC Analysis / Assessments	Product Verification at: OLRT Railway Level OLRT Primary System / Asset Level Covering at least the following: Factory Acceptance Site Integration / Acceptance Test results / compliance evidence

Day	Morning	Afternoon
Thurs	Product Validation at: OLRT Railway Level OLRT Primary System / Asset Level System Integration Railway Integration	Operational Readiness at: OLRT Railway Level OLRT Primary System / Asset Level Covering at least the following: Normal Operation Emergency Operation Degraded Operation Abnormal Operation Alignment to Hazard Log Standard Operating Procedures
Fri	Configuration / Change Management at; OLRT Railway Level OLRT Primary System / Asset Level Covering at least the following; Design Baselines As Built Baselines Migration Plans Issues / Assumptions / Dependencies / Constraints	Route Map for Delivery at; OLRT Railway Level OLRT Primary System / Asset Level Covering at least the following; Issues / Risks Omissions Safety Integration Outline Plan

Appendix 2. System Breakdown Structure


OLRT
1 Traction Power
1.1 MV (13 kVAC)
1.2 DC (1500VDC)
1.3 AC (VAC)
1.4 Stray Current
1.5 Grounding
1.6 Emergency Trip
1.7 Control
1.8 Traction Power Sub Station (TPSS)
2 Overhead Catenary
2.1 Power Distribution System
2.2 Control
3 Signaling and Train Control
3.1 Zone Controller (ZC) System
3.2 Data Transmission (DCS)
3.3 Automatic Train Control
3.4 Wayside
3.5 Automatic Train Supervision (ATS)
3.6 Simulators
4 Communications
4.1 Communication Transmission System (CTS)
4.2 Supervisory Control and Data Acquisition (SCADA)
4.3 Telephony
4.4 Passenger Information System
4.5 Voice and Data Radio (P25)
4.6 High Speed Data Radio (HSDR)
4.7 Network Management System
4.8 Guideway Intrusion Detection System (GIDS)
4.9 Closed Circuit Television (CCTV)
4.10 Master Clock
4.11 Intrusion Access Control (IAC)
5 Trackwork
5.1 Plane Line
5.2 Yard
5.3 Special Trackwork
6 Tunnel Ventilation
6.1 Mechanical
6.2 Control
6.3 Power
7 Vehicles
7.1 Revenue Vehicle
7.2 Maintenance Vehicle
8 Right of Way
8.1 Tunnels
8.2 Tunnel Guideway
8.3 At-Grade Guideway
8.4 Elevated Guideway
8.5 Cross Passages
8.6 Emergency Exit Buildings
8.7 Operational Signage
9 Facilities
9.1 Stations
9.2 Stops
9.3 MSF
9.4 Fire Detection and Alarm
9.5 Building Automation System (BACS)
9.6 Operational Control Centre (TSOC)
9.7 Backup Control Centre (BOCC)
9.8 Train Wash
10 City of Ottawa Systems
10.1 Public Safety Service Radio (P25)
10.2 Data Warehouse
11 Hydro Ottawa Limited (HOL)
11.1 Bulk Supply Point
12 OC Transpo
12.1 Advanced Traveller Information Systems (ATIS)
12.2 Fare Collection

Appendix 3. Record of Discussions

The review team conducted interviews with the following personnel.

Table 4 – Interview Record

Person	Organisation	Role	Topic
Sean T Derry	OLRT-C	Systems Assurance Lead	Assurance
Jonathan Sprakes	EJV, OLRT-C	Manager, Systems Engineering & Integration	Systems Engineering
Daniele Ferrara	EJV	Director of Railway Controls	Requirements, V&V, Design Integration
Frank Fitzgerald	OLRT-C	Systems Installation Director	Systems Installation
Stacey Bjornson	EJV	Requirements Manager	Requirements and V&V
Tim Scribner	OLRT-C	T&C Deputy Manager	T&C
John Selke	OLRT-C	Safety and T&C Coordinator	T&C, RAM, Safety
Tom Pate	RTM	Head of Maintenance	Maintenance
Louis Ranger	OLRT-C	Strategic Advisor	Ops
Eva Bognar	OLRT-C	Safety Engineer	Safety
Richard Duncan	OLRT-C	RAM Engineer	RAM
Florica Nye	OLRT-C	Design Coordinator	Engineering Management, Change Management
David Ellis	EJV	Design Manager	Design
Jacques Bergeron	OLRT-C	System Integration Director	System Integration

Appendix 4. Key Recommendations

Table 5 - Health Check Recommendations

Category	Issue	Summary	Risk	Recommendation
Lifecycle Management	Incomplete set of engineering management plans.	The project is missing key engineering plans, including the SEMP.	Key SE activities will be missed or not performed in a coherent manner.	Generate missing engineering management plans, focused on what needs to be completed to deliver revenue service.
	Multidisciplinary technical reviews have not been conducted.	There is an absence of multidisciplinary technical reviews, especially at the railway systems level.	Issues with integration are not identified until the integration test phase leading to increased cost and schedule pressure.	Define and conduct multidisciplinary design reviews.
Requirements	Lack of railway system requirements.	There is no clear set of railway system requirements. Railway system requirements provide a definition of the functionality, performance and characteristics of the railway to be delivered including RAM and safety targets. They provide a basis for development of the railway system architecture and design.	Incomplete definition of scope leads to failure to deliver an integrated, operable railway system.	Generate a set of railway level requirements focused on de-risking system integration

Category	Issue	Summary	Risk	Recommendation
	Lack of requirements traceability.	Limited traceability between requirements and design at different levels.	Scope is misaligned between subsystems leading to gaps in required functionality. Unable to demonstrate that all requirements have been satisfied in the design and delivered system.	Import procurement specifications into DOORS and trace back to PA.
System Architecture and Design Definition	Incomplete railway system level architecture.	At the railway level, there has been limited architecture and design definition.	Individually specified systems will not successfully integrate together to satisfy railway level requirements.	Continue to develop architecture and system design for key risk areas.
Verification and Validation	Acceptance criteria not defined.	The criteria for demonstrating that a PA requirement has been delivered, has not been agreed.	Disagreement between the project and client over whether requirements have been adequately met leads to inability to close out contract.	Identify acceptance criteria against PA and agree with client
	Insufficient V&V planning and reporting.	The events required to confirm satisfaction of requirements have not been identified.	Insufficient V&V events have been planned to demonstrate satisfaction of requirements.	Identify V&V events against railway system requirements and procurement specifications
Test and Commissioning	Missing traceability from SIT.	Lack of traceability from the SIT procedures back to the PA.	The planned set of SITs, do not fully test all requirements in the PA.	Provide traceability from SITs to railway system requirements

Category	Issue	Summary	Risk	Recommendation
	Increased integration during test and commissioning.	As there has been insufficient effort early in the lifecycle to "design for integration", integration has been pushed to the right.	The T&C team will need to dedicate significantly increased time "making it work" in addition to testing to confirm it works.	Consider introducing a field engineering team with authority to make design changes to support the T&C Team in resolving integration issues.
RAM	RAM analysis not performed.	There is an absence of RAM analysis to determine the reliability targets for individual assets, redundancy and maintainability requirements.	The railway as a whole does not meet its reliability, availability and maintenance targets.	Perform RAM analysis to assess the current characteristics of the railway and identify gaps.
	Reliability growth strategy.	The railway is unlikely to achieve its full reliability targets when first operational. A strategy to grow the reliability is required.	The railway as a whole does not meet its reliability and availability targets.	Develop Reliability Growth Strategy.

Category	Issue	Summary	Risk	Recommendation
Safety	Hazard Analysis	A hazard log exists but is not fully complete. It is currently in the process of being structured and reworked into a hierarchical categorisation. No fault tree or other formal analysis has been performed.	Some railway and primary system level hazards may not have been identified, leading to an increased level of safety risk in the delivered system.	Complete the full system hazard analysis (including fault tree analysis, FMECA) at railway and primary system level and update hazard log. Determine severity and probability of safety risks and identify risk mitigation measures to reduce all safety risks to a tolerable level.
	Hazard Mitigation	Safety requirements resulting from the HAZID process do not appear to have been captured. No traceability exists to confirm whether required safety measures have been incorporated into the design.	Mitigations for identified hazards have not been adequately incorporated into the design, leading to an increased level of safety risk in the delivered system.	Ensure all mitigation measures are captured as requirements and incorporated into the design.
Configuration Management	Requirements Change Management	Contract changes are not automatically advised to the requirements team for impact analysis and implementation.	The requirements baseline does not reflect the current contract status.	Update the PA change process to ensure the requirements team is part of the change impact analysis and is advised of all changes.

Category	Issue	Summary	Risk	Recommendation
	Baselines	No overall technical baselines exist for the project.	Requirements, design and implementation are not aligned, for example, two systems running software versions that are not compatible.	Establish configuration baselines, and control change to the baselines.