OLRT CONSTRUCTORS CONSTRUCTEURS

Confederation Line Phase 1

Case for Safety

Prepared by:	Mike Williamson – Systems Engineering Consultant	[signature]
Reviewed by:	Steve Leonard – Project Manager	[signature]
Approved by:	John Blowfield – RAMS Lead	[signature]
Authorised by:	Derek Wynne – Systems Engineering and Assurance Lead	[signature]
Agreed / Accepted by:	Sean Derry – SNC Lavalin Systems Assurance Director	Sean T. Derry
	Name, Title	Signature

Document No.	OLR-05-0-0000-REP-0017	Rev: 4
OLRT-C CONSTRUCTORS This document may contain confidential and commercially sensitive information.		14 Aug 2019

J Bergeron Aug 20TH 2019

LICENSED PROFESSIONAL ENGINEER J. BERGERON PROVINCE OF ONTARIO

REVISION HISTORY

Rev	Date	Description	Prepared by	Reviewed by	Approved by	Authorised by	Agreed by
0	17-Apr-2019	Initial Issue	C. Shaw	S. Leonard	J. Blowfield	D. Wynne	S. Derry
1	25-Apr-2019	Doc header consistency update	C. Shaw	S. Leonard	J. Blowfield	D. Wynne	S. Derry
2	23-May-2019	Revised in response to City CRE comments received 14/05/2019	C. Shaw	S. Leonard	J. Blowfield	D. Wynne	S. Derry
3	02-Aug-2019	Revised in response to CRE comments ref: OLR-05-0-0000-CRE-0080	C. Shaw	S. Leonard	J. Blowfield	D. Wynne	S. Derry
4	14-Aug-2019	Update and prep for RSA	M Williamson	S. Leonard	J. Blowfield	D. Wynne	S. Derry

EXECUTIVE SUMMARY

This Confederation Line Phase 1 Case for Safety addresses all elements of the railway including stations, Communications and control, signalling, rolling stock and infrastructure. The objective of this Case for Safety is to demonstrate the necessary Safety Related Application Conditions (SRAC) have been implemented and it therefore presents a Safety Justification for Revenue Service Availability (RSA), subject to stated limitations that can be found in the Confederation Line Phase 1 Operational Restrictions Document [12]. The Case for Safety relating to Operations and Maintenance are outside the scope of this document.

The Confederation Line Phase 1 Case for Safety presents evidence and reasoning for the justification that Confederation Line Phase 1 can be operated in a safe manner and that safety risks associated with such endeavour have been demonstrated to be acceptable. Integrated Hazard Log Summary Report [41] presents and concludes the overall safety hazard risk ranking and risk assessment undertaken through the course of the Engineering Safety Management lifecycle. It is supported by two subsidiary Safety Cases; the CBTC Systems Safety Hazard Analysis (Thales) [31] and the Alstom Citadis LRV Consolidated Safety File [32] for the Rolling Stock, Appendix A & B respectively summarise these. All other Primary System Safety Justifications are also considered in order to endorse safe operation of the railway.

The Confederation Line Phase 1 Case for Safety explains the Systems Engineering approach used to demonstrate the Confederation Line Phase 1 railway is fully integrated (compatible) and safe to operate through implementation of the V life-cycle model including Requirements Engineering, System Design, Verification & Validation, Safety Hazard Assessment, Test & Commissioning and Systems Assurance. The overall Safety Assurance element of this Case for Safety relies heavily on satisfactory evidence in the form of Design Certification Letters (DCL), Construction Certification Letters (CCL), Integration Certification Letters (ICL), and Test and Commissioning Systems Integration Test (SIT) and Systems Acceptance Test (SAT) evidence to confirm the successful implementation and integration of all systems. Any outstanding certification or residual testing required is identified in the ESAC Outstanding Items [13] but are considered to have detrimental effect upon safety.

In order to ensure the ongoing safety of the travelling public it is necessary to gather data on the effectiveness of certain systems and behaviour of the public hence additional activities specified in the Confederation Line Phase 1 Operational Restrictions Document [12] must be carried out for a limited period. By establishing a monitoring and review process (DRACAS) the ongoing safe operation of the railway can be assured by identifying the effectiveness of SRACs, whether or not they are sufficient, and determining when temporary restrictions can be lifted or whether they need extending.

Based upon the evidence presented, it is considered that Ottawa Confederation Line Phase 1 Railway is acceptable for revenue service subject to adherence to any Restrictions, Conditions and Limitations identified in the in Confederation Line Phase 1 Operational Restrictions Document [12] and resolution of issues identified in the Engineering Safety and Assurance Case Outstanding Items~~Engineering Safety and Assurance Case Outstanding Items~~ [13].

CONTENTS

1. INTRODUCTION

This Case for Safety structure is generally in accordance with Communication, signalling and processing systems. Safety related electronic systems for signalling [4] but tailored to fit a total railway system and its constituent parts. It presents evidence that the Confederation Line Phase 1 is safe to operate and maintain. Assessment of the operations and maintenance elements are to be provided by City of Ottawa in their Operator Safety Case and the Safety Management system for which they are responsible, and the Rideau Transit Maintenance (RTM) Safety Case.

The Case for Safety forms part of the Confederation Line Phase 1 Engineering Safety and Assurance Case [2].

1.1 PURPOSE

The purpose of this Confederation Line Phase 1 Case for Safety is to demonstrate the functionality of the railway systems integrated design and implementation is acceptably safe and that safety risks have been reduced to a level which is acceptable as defined in the Confederation Line Phase 1 Hazard Management ProcedureConfederation Line Phase 1 Hazard Management Procedure [1]. It records the Engineering Safety Management (ESM) activities undertaken to demonstrate the railway is fully integrated (compatible) and safe to operate.

The ESM approach demonstrates compliance with the requirements of the Project Agreement [6] by systematically identifying potential safety hazards and ensuring the risk associated with each hazard is mitigated to an acceptable level by design, operator action or maintenance activity.

This Case for Safety summaries the safety justifications for the Primary Systems, Critical Sub-systems and the top-level safety analysis in order to provide a complete summary of the engineering safety management activities and the resulting findings.

This Case for Safety is based on the process outlined in the Confederation Line Phase 1 Systems Safety Programme PlanConfederation Line Phase 1 Systems Safety Programme Plan [24] and focuses on providing argument for the safety of the integrated functional design of the Confederation Line Phase 1. It is underpinned by railway systems safety reports provided by the RTG-EJV, Alstom and Thales for their respective engineering work packages.

Where possible safety evidence/arguments are not repeated here, instead reference is made to evidence/arguments where provided.

1.2 SCOPE

1.2.1 Specific Inclusions

This Confederation Line Phase 1 Case for Safety covers the whole integrated Railway System defined by the Configurable Items Database [14] within the following categories:

1. Tunnel Systems
2. Track Systems

3. CTBC
4. Trains
5. Energy
6. Communications and Control
7. Stations
8. Train Control Centre (TSCC) and Backup Control Centre (BCC)
9. Maintenance and Storage Facility (MSF)

This Case for Safety also considers the interfaces and interactions of those interfaces between the Confederation Line Phase 1 Railway Systems and the Infrastructure and rolling stock Maintainers, operators and the environment.

1.2.2 Specific Exclusions

Systems, sub-systems or equipment outside the scope of the Confederation Line Phase 1 System Breakdown Structure [14] including those identified in Table 1.

Table 1: Equipment and Studies Outside of Scope

System Level	Sub-Systems Level
Train Wash Facility	Alstom Train Care
Wheel Lathe Facility	Alstom Train Care
Maintenance Shed Lifting Facilities	Alstom Train Care
P25 Voice Communications Network	City of Ottawa, OLRT-C Transpo
Fare Collection and Ticket Gates System	City of Ottawa OLRT-C Transpo

Assessment, certification and delivery of Operations and Maintenance (O&M) activities defined within the O&M Manuals and/or Transferred Safety Hazards that have been agreed with the Hazard Review Panel (HRP) are outside the scope of this Case for Safety.

The day-to-day operational safety management of the Confederation Line railway is not the responsibility of Ottawa Light Rail Transit-Constructors (OLRT-C) and is not addressed within this Case for Safety.

1.3 CONDITIONS

This Case for Safety relates to the build standard defined by the Confederation Line Phase 1 baseline recorded in PDM Plus as described in section 3.12 of the Confederation Line Phase 1 Engineering Safety and Assurance Case [2]. It is a condition that the as-built configuration baseline that underpins the ESAC and Case for Safety including subordinate Safety Justifications does not change.

The Confederation Line Phase 1 Railway has been correctly maintained throughout the pre-revenue service period.

Further conditions of operation are identified in the Confederation Line Phase 1 Operational Restrictions Document [12].

1.4 DOCUMENT STRUCTURE

This document provides the Case for Safety for the Confederation Line Phase 1 and forms a major input to the Ottawa Confederation Line Phase 1 Engineering Safety and Assurance Case (ESAC) [2].

The Confederation Line Phase 1 Safety and Assurance framework is shown in Figure 1.

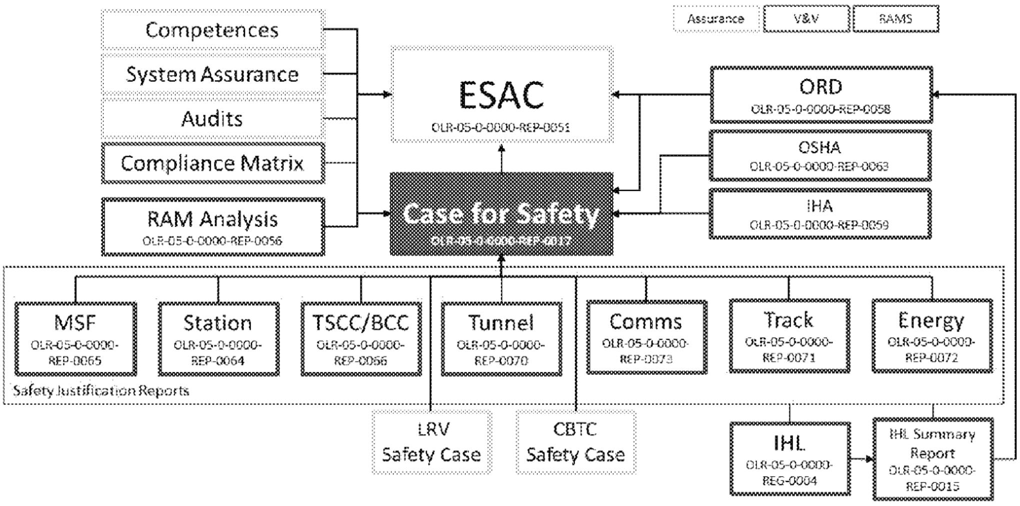

Figure 1: Document Hierarchy

1.5 GLOSSARY

Table 2: Glossary

Abbreviation	Meaning
AREMA	American Railway Engineering and Maintenance-of-Way Association
ATIS	Automatic Transmitter Identification System
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
BCC	Back-up Control Centre
BMS	Building Management System
BRT	Bus Rapid Transit system
CBTC	Communication Based Train Control
CCL	Construction Certification Letter
CCTV	Closed Circuit Television
CTS	Communications Transmission System
DCL	Design Certification Letter
DRACAS	Data Recording and Corrective Action System
DSR	Derived Safety Requirements
EJV	Engineering Joint Venture
EMC	Electro-Magnetic Compatibility
ESAC	Engineering Safety Assurance Case
ESM	Engineering Safety Management
HMP	Hazard Management Procedure
HOL	Hydro Ottawa Limited
IAC	Intruder Access Control
IEEE	Electrical and Electronics Engineers
IHA	Interface Hazard Analysis
IHL	Integrated Hazard Log
IRJ	Insulated Rail Joint

Abbreviation	Meaning
LFLRV	Low Floor Light Rail Vehicle
LRT	Light Rail Transit
LRU	Line Replaceable Unit
LRV	Light Rail Vehicle
MIL-STD	Military Standard
MSF	Maintenance and Storage Facility
PA	Public Address
OCS	Overhead Catenary System
OFS	Ottawa Fire Service
OLRT-C	Ottawa Light Rail Transit – Constructors
PA	Project Agreement
PHA	Preliminary Hazard Analysis
PIDS	Passenger Information Display System
PTI	Platform Train Interface
QRA	Quantitative Risk Assessment
RAMS	Reliability, Availability, Maintainability and Safety
RISKAC	Risk Acceptance Criteria
RSA	Revenue Service Availability
RTG	Rideau Transit Group
RTM	Rideau Transit Maintenance
SAT	Systems Acceptance Test
SCADA	Supervisory Control And Data Acquisition
SEMP	Systems Engineering Management Plan
SIL	Safety Integrity Level
SIT	Systems Integration Test
SOP	Standard Operating Procedures
SRAC	Safety Related Application Condition
TSCC	Transit Services Control Centre

Abbreviation	Meaning
TSR	Technical Safety Report
TVS	Tunnel Ventilation System

1.6 REFERENCE DOCUMENTS

All project documents are at latest issue unless where otherwise stated. All codes and standards refer to the version in use at the time in which the PA was agreed.

Table 3: Reference Documents

	Document Title	Document No.
[1]	Confederation Line Phase 1 Hazard Management Procedure	OLR-05-0-0000-PRC-0001
[2]	Confederation Line Phase 1 Engineering Safety and Assurance Case	OLR-05-0-0000-REP-0051
[3]	Confederation Line Phase 1 Integrated Hazard Log	OLR-05-0-0000-REG-0004
[4]	Communication, signalling and processing systems. Safety related electronic systems for signalling	EN50129
[5]	Confederation Line Phase 1 Risk Acceptance Criteria (RISKAC)	OLR-05-0-0000-MPL-0037
[6]	Project Agreement	TORO1; 4868348: v55
[7]	PA Technical Compliance Matrix	OLR-90-0-0000-CMP-0002
[8]	Confederation Line Phase 1 Operations and Support Hazard Analysis	OLR-05-0-0000-REP-0063
[9]	Systems and Software Engineering - System Lifecycle Processes	ISO/IEC/IEEE 15288:2008
[10]	Confederation Line Phase 1 V&V Management Procedure	OLR-50-0-0000-MPL-0006
[11]	Safety Integrity Level Allocation Report	REJ-05-0-0000-REP-0327
[12]	Confederation Line Phase 1 Operational Restrictions Document	OLR-50-0-0000-REP-0058
[13]	Engineering Safety and Assurance Case Outstanding Items	OLR-05-0-0000-REG-0025
[14]	Confederation Line Phase 1 Configurable Items Database	OLR-50-0-0000-REP-0058
[15]	Technical Compliance Report	OLR-05-0-0000-REP-0054
[16]	Confederation Line Phase 1 System Breakdown Structure	OLR-09-0-0000-DIA-0001
[17]	Day In The Life Of (DITLO) Report	OLR-05-0-0000-REP-0050
[18]	TVS Preliminary Hazard Analysis	RES-52-2-0000-REP-0292
[19]	Thales Preliminary Hazard Analysis (CBTC)	3CU 05018 0025 DUZZA
[20]	Rail Log	OTRC-Q200-18-WI
[21]	Hazard Review Panel (HRP) - Terms of Reference	SEMP-P0050-DOC-0002
[22]	Interface Hazard Analysis (IHA)	OLR-05-0-0000-REP-0059

	Document Title	Document No.
[23]	Standard for Fixed Guideway Transit and Passengers Rail Systems	NFPA 130
[24]	Confederation Line Phase 1 Systems Safety Programme Plan	OLR-05-0-0000-MPL-0012
[25]	Confederation Line Phase 1 Reliability Availability and Maintainability Report	OLR-05-0-0000-REP-0056
[26]	Confederation Line Phase 1 Systems Engineering Management Plan	OLR-50-0-0000-MPL-0005
[27]	The specification and demonstration of reliability, availability, maintainability and safety (RAMS)	EN50126
[28]	Department of Defense - Standard Practice - System Safety	MIL-STD-882E
[29]	NFPA 502 standard for Road Tunnels, Bridges and other Limited Access Highways.	NFPA 502
[30]	Manual for the Development of System Safety Programs Plans for Commuter Railroads, APTA, Washington, USA, 2006	May 15th 2007
[31]	CBTC Systems Safety Hazard Analysis (Thales)	3CU 05018 0247 DUZZA
[32]	Alstom Citadis LRV Consolidated Safety File	ADD0000939280
[33]	Confederation Line Phase 1 Project Quality Plan	SEMP-P0050-PLA-0025
[34]	IEC61508: Functional safety of electrical/ electronic/ programmable electronic safety-related systems	IEC61508
[35]	Thales Ottawa Light Rail Transit Project System Hazard Analysis	3CU 05018 0026 DUZZA
[36]	Mainline Preliminary Hazard Analysis	OLR-05-0-0000-REP-0003
[37]	GIDS Preliminary Hazard Analysis	OLR-05-0-0000-REP-0004
[38]	RSSB Gap Analysis	OLR-05-0-0000-MPL-0038
[39]	Project - Technical Description (Alstom)	507528 -P001
[40]	RTM LRV Faults and Vehicle Minimum Operating Standard	RTM-18-0-0000-SOP-LRV
[41]	Integrated Hazard Log Summary Report	OLR-05-0-0000-REP-0015
[42]	Confederation Line Phase 1 Reliability Availability and Maintainability Report	OLR-05-0-0000-REP-0056
[43]	Confederation Line Phase 1 Requirements Management Plan	OLR-50-0-0000-MPL-0007
[44]	Confederation Line Phase 1 V&V Management Plan	OLR-50-0-0000-MPL-0006
[45]	Configuration Management Plan (Thales)	3CU 05018 0020 QMZZA
[46]	Configuration & Change Management Plan (Alstom)	TBC

	Document Title	Document No.
[47]	RTGE CTS and Subsystems Configuration Management Plan	RES-53-0-0000-REP-0299
[48]	Design Change Management Procedure	OLR-QMS-GP700-SP02
[49]	Ottawa Light Rail Transit Project Specific Procedure: Field Directives	OLR-QMS-GP700-SP03
[50]	Ottawa Light Rail Transit Project Specific Procedure: Site Instructions	OLR-QMS-GP700-SP04
[51]	NFPA 130 Compliance Report	OLR-05-0-0000-CMP-0002
[52]	Stations Safety Justification Report	OLR-05-0-0000-REP-0064
[53]	TSCC and BCC Safety Justification Report	OLR-05-0-0000-REP-0066
[54]	Maintenance & Storage Facilities (MSF) Safety Justification Report	OLR-05-0-0000-REP-0065
[55]	Tunnel Safety Justification Report	OLR-05-0-0000-REP-0070
[56]	Track Safety Justification Report	OLR-05-0-0000-REP-0071
[57]	Energy Safety Justification Report	OLR-05-0-0000-REP-0072
[58]	Communication & Control Systems Safety Justification Report	OLR-05-0-0000-REP-0073
[59]	EJV System Safety Plan	REJ-05-0-0000-REP-0328
[60]	System Safety Program Plan (CBTC)	3CU 05018 0023 DUZZA
[61]	Alstom Safety Assurance Management Plan	ADD0000938677
[62]	MSF Preliminary Hazard Analysis Report	OLR-05-4-0000-REP-0001
[63]	Confederation Line Phase 1 System Assurance Management Plan	OLR-05-0-0000-MPL-0020
[64]	Confederation Line Phase 1 Competency Management Plan	OLR-05-0-0000-MPL-0040
[65]	Confederation Line Phase 1 System Breakdown Structure	OLR-09-0-0000-DIA-0001

2. SYSTEM DEFINITION

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 includes a 2.5km mined tunnel beneath downtown Ottawa and an LRT Maintenance and Storage Facility (MSF) at Belfast Road, shown in Figure 2.

Phase 1 includes thirteen stations, with three considered as Under Ground Stations, one considered as an Enclosed Station, 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, and with VIA rail at Tremblay.

The Ottawa Confederation Line Phase 1 consists of Guideway, Stations and Line of Route systems between Tunney's Pasture and Blair Stations, MSF Connector, LRV Phase 1 Fleet, MSF buildings and Yard, TSCC and BCC in accordance with the Project Agreement [6] for Confederation Line Phase 1.

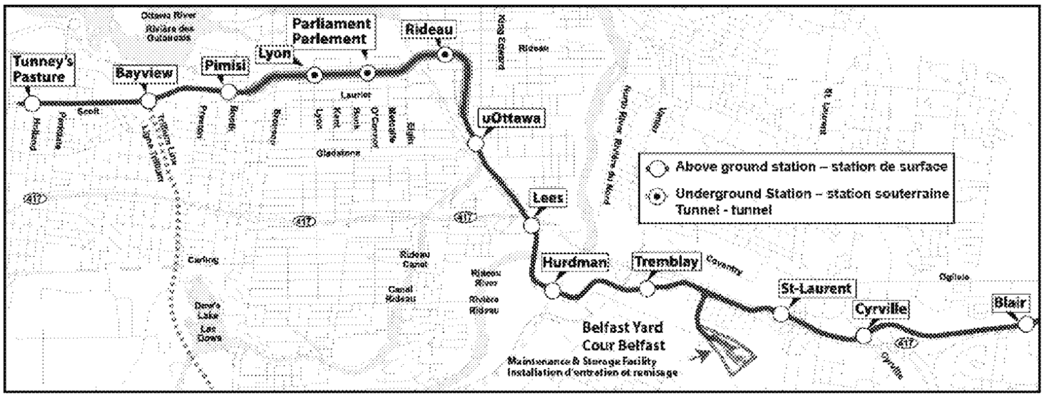

Figure 2: Confederation Line Phase 1 Route Map

2.1 KEY PARTIES

Design of the majority of Ottawa Confederation Line Phase 1 infrastructure has been the responsibility of an Engineering Joint Venture (EJV) partnership between SNC Lavalin, Dragados and EllisDon.

Alstom Citadis Spirit low floor articulated rail vehicles are used to provide up to 300 passengers per LRV unit.

Communications Based Train Control (CBTC) moving block train control systems is provided by Thales.

Transit Services (OC-Transpo) provide all main line control staff, LRV Drivers, transit law and other customer service personnel.

Rideau Transit Maintenance (RTM) are responsible for maintenance of all systems and infrastructure including the LRV fleet.

2.2 DESIGN STRATEGY

The Confederation Line Phase 1 project has sought to minimise risk in terms of project schedule and cost, long-term safety and operational performance, by maximising the use of type approved and commercially available equipment that has been proven on operating railways within Canada or overseas. Systems have been selected for their pedigree of proven use and reputation for reliable performance and has been implemented through the equipment and supplier selection acceptance processes.

The design processes have set out to deploy equipment in standard configurations maximising the use of component redundancy with adequate fault detection to mitigate the risk of hidden faults.

2.3 MAINTENANCE PHILOSOPHY

The Ottawa Confederation Line Phase 1 infrastructure has been designed to minimize the maintenance burden and logistic footprint. Maintenance has been rationalised to repair by LRU replacement at first line as far as is technically feasible, and preventive maintenance minimised by design and widespread implementation of SCADA monitoring capability.

This approach is considered to reduce safety risks to on-track personnel by minimising the time within hazardous environments whilst maximising benefit to passengers through on-time running and cost effectiveness. Assets have been selected for their inherent ease of maintenance whilst the infrastructure layout has been designed to permit necessary access, walking routes and provision for human factors.

2.4 OPERATING CONTEXT

Overall performance and cost effectiveness of Confederation Line Phase 1 is enhanced by embedding Supervisory Control And Data Acquisition (SCADA) as the fundamental feature of the operations concept. This approach automates equipment monitoring, many operating functions and enhances the overall operator decision-making.

2.5 PRIMARY SYSTEMS

This Case for Safety is supported by the following documents:

- Primary System Safety Justification Reports for Stations [52], TSCC/BCC [53], MSF [54], Tunnels [55], Track [56], Energy [57] and Communications [58]. The main sub-system elements considered within scope of each of these primary system level reports are shown in Table 4 on the following page
- Confederation Line Phase 1 Operations and Support Hazard Analysis [8]
- Confederation Line Phase 1 Interface Hazard Analysis [22]
- Standalone Safety submission from the train supplier with the Alstom Citadis LRV Consolidated Safety File for rolling stock and discussed in section [32].
- Standalone Safety submission from the signalling supplier with the (Thales) CBTC Systems Safety Hazard Analysis (Thales) [31] and discussed in section [32].

The overall railway level architecture is shown in Confederation Line Phase 1 System Breakdown Structure~~Confederation Line Phase 1 System Breakdown Structure~~ [65]. The sub-systems within scope of each primary system are identified in Table 4.

Table 4: Primary Systems Definition

System Level	Sub-Systems Level
Tunnel Systems	TVS Walkways Lighting Signage
Track Systems	Track forms Switches and crossings Drainage Buffer stops Derailment containment and Point heating.
Signalling & Train Interface	CBTC Secondary Detection Switch operation Train Borne Signaling
Trains	Light Rail Vehicle Units
Energy	Power Distribution System Overhead Catenary System
Communications and Control	Passenger Information Display System (PIDS) Closed Circuit Television (CCTV) Telephony System SCADA GIDS
Stations	At Grade Enclosed (see 2.3 definition) Under Ground
TSCC	Including BCC
MSF	Sanding, Inspection and Wash Bay SIW. Light Maintenance Bays LM1 and LM2. Wheel Truing Bay. Bogie Overhaul Heavy Maintenance Bays, including cranes, OCS interlock protection and stinger supply

2.6 LIGHT RAIL VEHICLES

The Confederation Line Phase 1 uses Alstom Citadis Spirit low floor articulated rail vehicles with a capacity of 300 passengers per LRV Unit.

The Citadis Spirit cars are electrically motorized vehicles which use 1500-volt DC power supplied from 8 traction power substations on the main line and 2 traction power substations in the yard. Power is distributed by an Overhead Catenary System (OCS).

Each LRV Unit is 49 meters in length with 7 passenger doors per side. During weekdays, trains will generally run made up of two LRV units providing a total passenger capacity of 600 passengers per train.

2.7 TRAIN CONTROL

The Confederation Line Phase 1 is controlled by CBTC supplied by Thales. CBTC system is a moving block automatic train control system which enables the Confederation Line Phase 1 to operate with a sustained operational headway (time between trains) of two minutes or less.

The system is designed to achieve an end to end travel time not exceeding 23 minutes in Automatic Train Operation (ATO) mode. It will provide for several modes of operation, from fully automated to fully Driver controlled.

All revenue trains shall be staffed by OC Transpo LRV Drivers who will oversee and/or drive trains with defined tasks and responsibilities, ensuring system safety in each of the various modes of operation.

The normal mode of operation in revenue service will be ATO. In this mode, LRV Drivers will oversee train operation, operate various vehicle systems, and control passenger door operation and train departure from the stations.

The Confederation Line TSCC is located at 875 Belfast Road in the existing Transit Services (OC Transpo) BRT Operations Centre. Transit Services management and control room staff will operate out of this facility. The BCC is located in the MSF in Belfast Yard.

Train operations in Belfast Yard (MSF) will be controlled by Rideau Transit Maintenance (RTM). RTM Yard Controllers work out of the Yard Control Centre in the MSF. The future intention will be for trains moving beyond the handover points in Belfast Yard to run unmanned and fully automated mode (UTO). However, for Phase 1 entry into service CBTC trackside equipment is not fitted throughout the yard for such operation.

2.8 ENVIRONMENT

There are 13 Ottawa Confederation Line Phase 1 Stations. Lyon, Parliament and Rideau Stations are Underground within a 2.5 km long downtown tunnel section, St-Laurent station is enclosed beneath a shopping complex, and the each of Tunney's Pasture, Bayview, Primisi, uOttawa, Lees, Hurdman, Tremblay, Cyrville, and Blair are at or above ground level.

Part of the railway is under the Ottawa Canal and below the rising water table and thus appropriate waterproofing and flood protection measures.

The environmental conditions present a range of challenges:

- Extremes of heat, cold and relative humidity
- Dust and particulate contamination
- Snow and ice on exposure
- High wind
- Saline conditions
- Shock and vibration
- Seismic activity
- Electromagnetic Interference.

2.9 FUNCTIONS

SIL have been assigned to safety-related functions in the Confederation Line Phase 1 SIL Allocation Report [11] and was based upon knowledge of the risk factors associated with high level functions with regards to random and systematic failures in line with CENELEC 50126 [27].

SIL levels have been assigned to functions and devolved into the systems, sub-systems and components that support each function. SIL allocation has been used to ensure that adequate protections had been implemented in order to protect patrons and maintenance personnel from hazardous conditions.

Verification of the compliance to the SIL allocations us verified in Confederation Line Phase 1 Technical Compliance Matrix [7].

2.10 SYSTEM BOUNDARIES AND INTERFACES

Interfaces for the communications and control system are shown in Figure 3. Hazards associated with Confederation Line Phase 1 interfaces are assessed in Interface Hazard Analysis (IHA) [22].

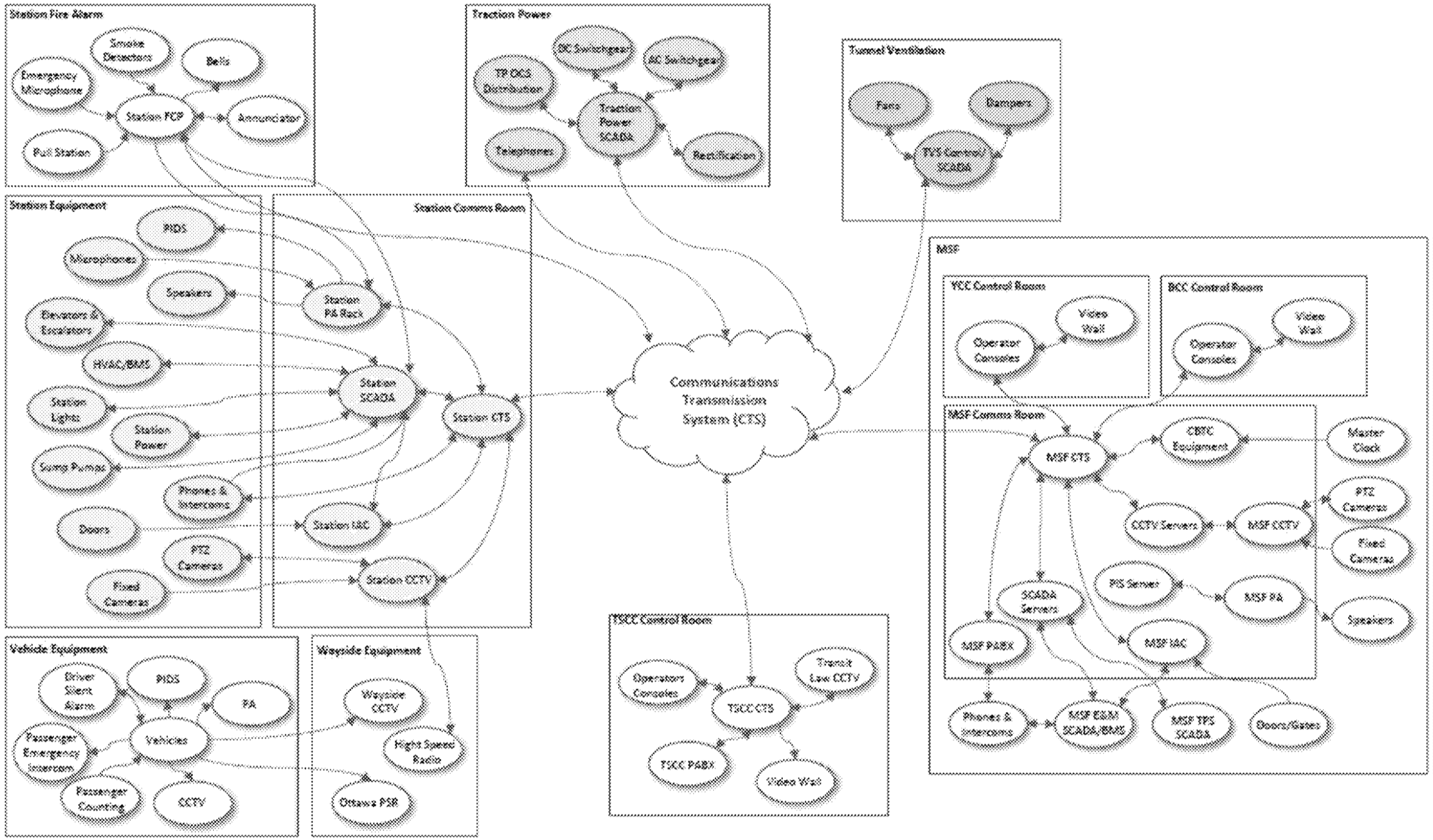

Figure 3: Communications and Control System Interfaces

3. SAFETY MANAGEMENT

Engineering Safety Management (ESM) has been applied in line with The specification and demonstration of reliability, availability, maintainability and safety (RAMS) EN 50126 [27] and Communication, signalling and processing systems. Safety related electronic systems for signalling [4] to demonstrate that:

- The integrated Railway system design is acceptably safe and that associated risks have been identified, managed and controlled to an acceptable risk level (including at the interfaces), throughout the development lifecycle
- Railway level hazards have been managed via the Integrated Hazard Log in accordance with the Confederation Line Phase 1 Hazard Management ProcedureConfederation Line Phase 1 Hazard Management Procedure [1] and:
  - Can demonstrate compliance with appropriate codes and standards mandated in the Project Agreement [6]
  - Can refer to the use of the systems or sub-systems used on other rail projects of similar type, size and operation
  - Where necessary further risk reduction measures have been identified taking into account the practicability of implementation and ensuring the risk reduction benefits provided are commensurate with the effort, cost and time required to implement.
- The integrated Railway system design and implementation satisfies all relevant safety requirements (i.e. operational limits, procedures, protection devices, mitigation provisions, etc. which reduce the frequency or consequences of hazards) managed in the PA Technical Compliance Matrix [7] and documented in the Technical Compliance Report [15]
- All safety requirements identified at Primary Systems level (during hazard identification and assessment activities) have been captured in the respective Hazard Logs and where applicable transferred in the form of Derived Safety Requirements (DSRs) or Safety Related Application Conditions (SRAC). DSRs or SRACs have been transferred and accepted by the Owner, Maintainer and/or Operator to establish suitable and sufficient standard operating practices and procedures in the form of Standard Operating Procedures (SOP), in order to manage safety risk to an acceptable level.

Where the risks associated a hazard cannot be satisfactorily mitigated by any of the methods given above the risk has been subjected to a comparative risk analysis. The comparative risk analysis demonstrates that although these risks are assessed to be above the acceptable level due to frequency of occurrence and severity, they are at least the same or lower level of risk compared to similar forms of mass transit transportation.

3.1 ROLES & RESPONSIBILITIES

Resources have been managed in accordance with the Confederation Line Phase 1 Competency Management PlanConfederation Line Phase 1 Competency Management Plan [64]. Further information on the competency management frameworks can be found in section 13 of the Confederation Line Phase 1 Engineering Safety and Assurance Case [2].

Systems consist of people, processes and assets. OLRT-C is primarily responsible for delivering the railway assets – infrastructure and trains.

Roles and responsibilities of Confederation Line Phase 1 stakeholders is provided in section 1 the Confederation Line Phase 1 Engineering Safety and Assurance Case [2].

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.

3.2 SAFETY LIFECYCLE

The Railway System safety lifecycle followed the V lifecycle detailed in the Confederation Line Phase 1 System Assurance Management Plan~~Confederation Line Phase 1 System Assurance Management Plan~~ [63] and Confederation Line Phase 1 Systems Safety Programme Plan~~Confederation Line Phase 1 Systems Safety Programme Plan~~ [24].

The Safety and RAM process objectives were to demonstrate that the Project is in line with EN50126 [27] and EN 50129[4] as specified in the PA [6] and in line with engineering best practice described in the Confederation Line Phase 1 Systems Engineering Management Plan~~Confederation Line Phase 1 Systems Engineering Management Plan~~ [26]. This Case for Safety demonstrates those objectives have been achieved.

The full extent of ESM activities carried out by system-wide contracts can be found in the respective System Safety Plans for EJV, Thales and Alstom, EJV System Safety Plan [59], System Safety Program Plan [60] and Alstom Safety Assurance Management Plan[61], respectively.

These documents are compliant to EN 50126 [27] where applicable to a railway product application.

Some proven and commercially available systems, sub-systems and equipment utilised in the Confederation Line Phase 1 may not have been developed and proven in accordance with EN 50126 [27] and EN 50129 [4]. Safe operation will be verified by comparison to reference systems through cross acceptance where long term safe operation has been demonstrated on other railways.

3.3 SAFETY REQUIREMENTS

3.3.1 Safety Process Requirements

The following safety standards are applicable to the Confederation Line Phase 1 Project:

1. EN50126: The specification and demonstration of reliability, availability, maintainability and safety (RAMS) [27]
2. EN50129: Communication, signalling and processing systems. Safety related electronic systems for signalling [4]
3. IEC61508: Functional safety of electrical/ electronic/ programmable electronic safety-related systems~~IEC61508: Functional safety of electrical/ electronic/ programmable electronic safety-related systems~~ [34]

4. MIL-STD-882E: Department of Defense - Standard Practice - System Safety [28]
5. Manual for the Development of System Safety Programs Plans for Commuter Railroads, APTA, Washington, USA, 2006 [30].

3.3.2 Safety Design Requirements

Safety requirements applicable to Railway Systems are derived from but not limited to the following:

- Project Agreement [6]
- Codes of practice mandated by the Project Agreement [6]
- DSRs applicable to hazards identified through contractor ESM activities and recorded in the Confederation Line Phase 1 Integrated Hazard Log [3]
- Confederation Line Phase 1 Integrated Hazard Log [3] DSR process
- RSSB Gap Analysis [38]
- OFS requirements fulfilled by the NFPA 130 Compliance ReportNFPA 130 Compliance Report [51]
- NFPA 502 standard for Road Tunnels, Bridges and other Limited Access Highways. [29].

The objectives of the requirements process for both safety and non-safety has been demonstrated to be fulfilled by:

1. Capture of existing requirements sets into a single repository and establishing a consistent baseline
2. Derivation of new requirements sets where these are necessary
3. Demonstrating traceability between requirements and other artefacts and addressing identified gaps.

The Confederation Line Phase 1 V&V Management Plan [10] defines the Verification and Validation (V&V) strategy and activities applied.

The primary objectives of the V&V processes were to ensure the Confederation Line Phase 1, as designed, built and installed, meets the specified safety requirements of the Project Agreement [6], all relevant codes and standards, and satisfies the DSRs and SRACs identified.

Requirements and Verification and Validation processes (V&V) are described in section 3 of the Confederation Line Phase 1 Engineering Safety and Assurance Case [2].

3.4 HAZARDS & RISK ASSESSMENT

The risk assessment process for Confederation Line Phase 1 involved:

- Identification of all hazards associated with the railway
- Maintaining the Confederation Line Phase 1 Integrated Hazard Log [3] identifying and controlling the risks associated with identified hazards

- Predicting the safety risks to people from hazards on a qualitative or quantitative basis
- Comparing safety risks against the Confederation Line Phase 1 Risk Acceptance Criteria (RISKAC)~~Confederation Line Phase 1 Risk Acceptance Criteria (RISKAC)~~ [5]
- Identifying mitigation measures and reducing safety risks to an acceptable level as defined in the Confederation Line Phase 1 Hazard Management Procedure~~Confederation Line Phase 1 Hazard Management Procedure~~ [1].

3.4.1 Risk Acceptance Principles

Evaluation and assessment of safety risks has been conducted throughout the system designs using one of the following risk acceptance principles, described in the Confederation Line Phase 1 Hazard Management Procedure~~Confederation Line Phase 1 Hazard Management Procedure~~ [1].

- The application of standards and codes of practice
- A comparison with similar systems (reference systems or "cross acceptance")
- Quantitative Risk Assessment (QRA)

The system-wide engineering design solutions were implemented in accordance with codes and standards mandated in the Project Agreement [6]. Risk acceptance criteria are given in the Confederation Line Phase 1 Hazard Management Procedure~~Confederation Line Phase 1 Hazard Management Procedure~~ [1].

Risk acceptance principles provide various means of demonstrating Safety risks are managed to an acceptable level. Individual hazards were risk ranked using the risk matrix defined in Confederation Line Phase 1 Hazard Management Procedure~~Confederation Line Phase 1 Hazard Management Procedure~~ [1].

3.4.2 Safety Control Measures

'Controls' are those measures applied when the system under consideration can provide no further safeguard/protection for risk reduction. In such cases further controls are required in the form of Operational Safeguards (e.g. speed restrictions, prevention of over-crowding, etc.) and improved maintenance provisions to reduce failure rates.

Exceptional and temporary controls of this nature are recorded in the Confederation Line Phase 1 Operational Restrictions Document [12].

3.4.3 Railway Hazard Log Structure

The project developed an Confederation Line Phase 1 Integrated Hazard Log (IHL) [3] derived from early PHAs and containing predominantly operational hazards expected of a railway level hazard log managed by the Primary Design, Build and Maintain Contractor.

For functional failure hazards, i.e. train exceeding its Movement Authority, rolling stock emergency door release failure etc, each of the Primary Systems Contractors (EJV, Thales and Alstom) managed the Primary systems failures in their own Hazard Logs.

An initial review could not identify a systematic approach to the hazard identification process used to populate the IHL and so an exercise was carried out to review the IHL and associated PHAs against known railway hazards derived from internationally recognised and established safety management reporting systems. To this end, the RSSB Gap Analysis [38] was produced.

This work has driven the hazard management process to a satisfactory conclusion. Where analysis has identified the need for an intervention by operations or maintenance, those elements of the hazards that retain a residual risk have been transferred as part of the transfer process in the form of Safety Related Application Conditions, e.g. the frequency of a maintenance action being specific to the prevailing environmental conditions or wheel grinding being specific to the wheel/rail hardness and profile specifically chosen for Confederation Line Phase 1.

Analysis reports contributing to the development of the IHL came from a number of sources such as the GIDS Preliminary Hazard Analysis [37]; TVS Preliminary Hazard Analysis [18]; Mainline Preliminary Hazard Analysis [36]; MSF Preliminary Hazard Analysis Report [62] and Thales Ottawa Light Rail Transit Project System Hazard Analysis [30] and CBTC Systems Safety Hazard Analysis (Thales) [31]. Other contributions came from City comments and the early IHL review meetings.

All Primary Systems Design and Build Contractors managed their own Hazard Logs as shown in the hierarchy, Figure 4. The Hazard Review Panel (HRP) - Terms of Reference [21] requires the panel to review hazards in accordance with the Confederation Line Phase 1 Hazard Management Procedure~~Confederation Line Phase 1 Hazard Management Procedure~~ [1].

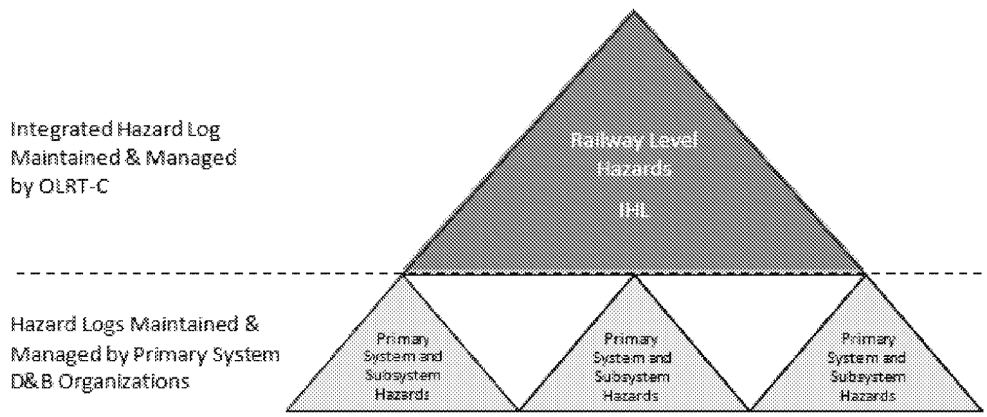

Figure 4: Hazard Log Structure between OLRT-C and Primary System Organisations

For a complete description of how the Hazard Management Process has been implemented, the final status of all IHL hazards and the SRAC transfers please refer to the Integrated Hazard Log Summary Report [41].

3.5 CONFIGURATION MANAGEMENT

Configuration Management is the top-level methodology using the principals of ISO 10007:2003: Quality Management Systems - Guidelines for Configuration Management. 2003; ISO/IEC/IEEE 15288: Systems and Software Engineering - System Lifecycle

Processes [9] and ISO/IEC/IEEE 26702 (IEEE1220): Application and Management of the Systems Engineering Process for assessing the impact of change to safety critical/related areas of operations.

The process strives to ensure that all of the railway systems including property, equipment, signalling etc. are accurately and completely documented against a consistent configuration management baseline.

Configuration Management and Change Control requirements have been flowed down to each vendor and are managed according to each suppliers accredited procedures; hence includes, Configuration Management Plan [45], Configuration & Change Management Plan (Alstom)~~Configuration & Change Management Plan (Alstom)~~ [46] and RTGE CTS and Subsystems Configuration Management Plan~~RTGE CTS and Subsystems Configuration Management Plan~~ [47].

Design Change Management throughout the construction phase is managed by OLRT-C in the form of Design Change Management Procedure [48], Ottawa Light Rail Transit Project Specific Procedure: Field Directives [49] and Ottawa Light Rail Transit Project Specific Procedure: Site Instructions [50].

A full description of the Change Control Process and how the Design Baseline has been established and controlled is shown in section 11 of the Confederation Line Phase 1 Engineering Safety and Assurance Case [2].

3.6 VALIDATION & VERIFICATION

The Confederation Line Phase 1 Requirements Management Plan~~Confederation Line Phase 1 Requirements Management Plan~~ [43] defines the requirements structure and processes applied by the Project. The Confederation Line Phase 1 V&V Management Plan~~Confederation Line Phase 1 V&V Management Plan~~ [44] defines the processes associated with satisfying and demonstrating compliance to requirements.

These Plans define the activities necessary to demonstrate traceability and progressive assurance using structured V&V processes.

A full description of the V&V Processes is given in section 3 of the Confederation Line Phase 1 Engineering Safety and Assurance Case [2].

4. QUALITY MANAGEMENT

Quality Management Processes are as defined in the Confederation Line Phase 1 Project Quality Plan [33].

A detailed synopsis of the Quality and Audit Processes implemented is given in section 14 of the Confederation Line Phase 1 Engineering Safety and Assurance Case [2].

5. TECHNICAL SAFETY REPORT

This section of the Case for Safety is the Technical Safety Report and has been constructed to be generally in line with EN 50129 [4] as far as it applies to an overall Railway Design, Build and Maintain undertaking thus covering all railway systems within Confederation Line Phase 1.

This Technical Safety Report addresses primary systems that combine to provide the requisite aggregate functionality to:

- Safely Operate the Confederation Line Phase 1 under normal, degraded and emergency modes of operation
- Provide an acceptably safe environment for patrons and railway staff and any third parties (e.g. members of the public)
- Demonstrate that risks to people from operation of the railway are acceptable as defined in the Confederation Line Phase 1 Hazard Management ProcedureConfederation Line Phase 1 Hazard Management Procedure [1]
- Manage degraded modes of operation both safely and in order to carry on a service
- Facilitate safe management of people in event of an Emergency or unexpected incident
- Provide a service level and comfort commensurate with a Light Rail suburban transit system
- Provide Operational Control facility at the TSCC, BCC and YCC to coordinate and control safe operation of the railway
- Provide facilities for the safe and efficient maintenance of the railway infrastructure, its assets and the rolling stock (including at the MSF).

Specific sections in the reports are illustrated in the list below and comprise:

- System description
- Evidence of correct functional operation
- Operational and external influences – weather, degraded modes of operation, etc
- The effects of failures
- Safety Related Application Conditions
- Derived Safety requirements
- Safety qualification tests
- Outstanding safety issues
- Any temporary or permanent control measures referred to in the Confederation Line Phase 1 Operational Restrictions Document [12].

The Technical Safety Report has been broken into nine 'contributing systems' and the results of the safety activities are given in the nine Primary Systems Safety Cases and Justifications.

- Tunnel Safety Justification Report [55]
- Track Safety Justification Report [56]
- CBTC Systems Safety Hazard Analysis (Thales) [31].
- Alstom Citadis LRV Consolidated Safety File [32].
- Energy Safety Justification Report [57]
- Communication & Control Systems Safety Justification Report [58]
- Stations Safety Justification Report [52]
- TSCC and BCC Safety Justification Report [53]
- Maintenance & Storage Facilities (MSF) Safety Justification Report [54].

A brief summary of the scope and principle findings of each Primary Systems Safety Justification Reports is given below. The overall conclusions and recommendations of these documents and those from Systems Integration Test Reports and any subsidiary activities such as Site Surveillance Reports are given in Section 7 of this document.

5.1 TUNNEL SYSTEMS

The Ottawa Confederation Line Phase 1, a 12.5-kilometre Rail Transit (LRT) system and includes a 2.5km mined tunnel beneath downtown Ottawa. In addition, St. Laurent Station utilises below grade platforms and is fitted with a Tunnel Ventilation System and is treated as a tunnel.

Access to the MSF includes a tunnel below the VIA Rail line which is covered in the Maintenance & Storage Facilities (MSF) Safety Justification Report [54].

Tunnel Safety Justification Report [55] addresses the Guideway Intruder Detection System (GIDS); Tunnel walkways; Tunnel drainage; Tunnel lighting; Tunnel Signage; the Tunnel Ventilation System and Tunnel Structure. The Communication & Control Systems Safety Justification Report [58] contains information on communications and alarm protocols related to GIDS operation.

The Tunnel Safety Justification Report [55] identifies various control measures to protect against fire in the tunnel and to permit safe evacuation.

This includes the train control system (CBTC) avoidance of designated non-stopping areas, train fire alarms to train control and the resulting commands provided to the LRV under such circumstances.

It also includes the mitigation of LRV collision with animate and inanimate objects in the tunnel via the GIDS system.

The Tunnel Safety Justification Report [55] concludes that, for the scope of Phase 1, the Tunnel Systems can support the safe operation of the Confederation Line railway.

Recommendations resulting from the Tunnel Safety Justification Report [55] are given in section 7.2.1.

5.2 TRACK SYSTEMS

The Track Safety Justification Report [56] covers the Confederation Line Track system: 12.5 route kilometres of the Confederation Line Railway Phase 1 track systems running from Blair to Tunney's Pasture, and the connected MSF yard.

The Track Safety Justification Report [56] contains a detailed analysis of the track systems and considers the interfaces between the Confederation Line Railway track system and the Citadis Spirit LRV fleet, the system operators and maintainers and the environment.

The Track Safety Justification Report [56] concludes that, for the scope of Phase 1, the Track Systems can support the safe operation of the Confederation Line railway.

In addition, it details the maintenance considerations pertinent to the Project Agreement [6] specified choice of the AREMA standard resulting in the use of 115RE high strength rail (310 Brinell) in conjunction with operating a light weight train.

Recommendations related to maintaining track are provided in section 7.2.2.

5.3 CBTC

The Confederation Line Phase CBTC is provided by Thales Canada. Thales is one of the leading manufacturers of In-cab Signaling Systems and the Confederation Line Phase 1 signaling is based on the Thales SELTRAC system which is in worldwide use.

A detailed Signalling Systems Safety Case for the Confederation Line Phase 1 details Thales's safety management processes, test results and findings are provided in a separate document; the CBTC Systems Safety Hazard Analysis (Thales) [31].

CBTC Systems Safety Hazard Analysis (Thales) [31] concludes, quote "The evidence provided in this Safety Case demonstrates that the CBTC system satisfies the contractual safety requirements and safety targets, and that the CBTC is safe for the intended purpose, subject to compliance with SAC and SORs provided in Appendix F" of the report.

An overview of the System Safety Case findings is given in Appendix C of this document and recommendations related to the system are given in section 7.2.8.

5.4 ALSTOM CITADIS SPIRIT LRV

Alstom are one of the world's leading LRV manufactures. Confederation Line is the first Operator of the Citadis Spirit LRV, a new product specifically designed for the North American market, based on the widely used Citadis LRV series.

A full description is given in Project - Technical Description [39]. Results of the Alstom safety process and analyses are given in the Alstom Citadis LRV Consolidated Safety File [32].

Alstom Citadis LRV Consolidated Safety File [32] concludes, quote "The evidence provided in this Safety Case demonstrates that the Citadis Spirit LRV satisfies the contractual safety requirements and safety targets, and that it is safe for the intended purpose.

A summary of Alstom Citadis LRV Consolidated Safety File [32] and a synopsis of known Citadis Spirit issues are given in Appendix B and recommendations are given in section 7.2.9.

5.5 ENERGY SYSTEMS

The Energy Safety Justification Report [57] addresses the Energy System elements of the Confederation Line Phase 1.

The Energy System comprises the high voltage supply to the Confederation Line Phase 1, Traction Power Sub Stations, 1500V Overhead Catenary System, Grounding and Bonding and Electro-Magnetic Compatibility (EMC).

Evidence for and the reasoning behind the assertion that the Confederation Line Phase 1 Energy System is safe for operation is provided in the Energy Safety Justification Report [57] and the risks associated with the Energy System Primary Systems have been demonstrated to be acceptable.

Recommendations related to the Energy System are given in section 7.2.3.

5.6 COMMUNICATION & CONTROL SYSTEMS

A full description of the Communication and Control Systems and system safety processes undertaken to ensure safe operation are provided in the Communication & Control Systems Safety Justification Report [58]. The scope is:

- Provision of Communications infrastructure at all Confederation Line Phase 1 geographic locations in delivery or support of each of the following subsystems:
  - Communications Transmission Network (CTS)
  - Supervisory Control And Data Acquisition (SCADA)
  - Intruder Access Control (IAC)
  - Building Management System (BMS)
  - CCTV
  - Passengers Information
    - Public Address (PA)
    - PIDS
    - Telephony System
    - Advanced Traveller Information System (ATIS)
    - Wayside High-Speed Radio Data System

The Communication & Control Systems Safety Justification Report [58] concludes that "the Communications and Controls systems meet the requirements of the Project Agreement [6], whilst mitigating the hazards raised during the safety analysis of the works and is considered to be suitable for the onset of trial running and operational services".

Recommendations related to the Communications System are given in section 7.2.5.

5.7 STATION SYSTEMS

The Stations Safety Justification Report [52] provides an overview of each of the Confederation Line Phase 1 stations, identifies reports related to passenger movement (Pedestrian flow), addresses the Platform Train Interface (PTI), considers accessibility to and around the station and the LRV Operator station departure procedure.

The Stations Safety Justification Report [52] concludes:

The availability of Certificates of Occupancy indicates that all requirements related to building safety have been met and the stations have been constructed to a standard deemed by the respective Engineers of Record and the City of Ottawa to be safe for public use.

In addition, a rigorous hazard identification and mitigation process has been undertaken. All hazards associated with operation of the Confederation Line Phase 1 station buildings and the railway operation within the stations has been satisfactorily resolved and mitigated to an acceptable level.

Recommendations related to the Station systems are given in section 7.2.4.

5.8 TRAIN CONTROL CENTRE (TSCC & BCC)

The TSCC and BCC Safety Justification Report [53] summarises the safety evidence for the Ottawa Confederation Line Phase 1 Transit Services Control Centre and the Back-Up Control Centre (BCC). It describes how the integration team confirmed that a complete set of hazards were identified, assessed and managed in line with the Confederation Line Phase 1 Hazard Management Procedure~~Confederation Line Phase 1 Hazard Management Procedure~~ [1]. It is noted that the BCC is located in the MSF remotely from the TSCC which is located on Belfast Road (see next paragraph).

The Transit Services Control Centre TSCC provides the primary operation and control centre for revenue service of the Confederation Line Phase 1. It also operates and controls the mainline guideway during maintenance hours, which typically occur overnight.

The TSCC integrates the Confederation Line Phase 1 communications and control needs for the safe operation of the railway. It enables scheduling, command and control, supervision & data acquisition, communications, surveillance, power and emergency response of the Confederation Line Phase 1.

The only aspects of the Confederation Line that are not under primary operation and control from the TSCC are those located in the Maintenance and Storage Facility (MSF) buildings and Yard. These facilities are under the primary control of the Yard Control Centre (YCC).

The MSF Access Track is under joint control by the YCC and the TSCC. The TSCC is located in the OC Transpo building at 875 Belfast Road, a half kilometre east of the MSF building. Staff operating the TSCC will be from OC Transpo. Should the TSCC not be available for use, due to extenuating circumstances (e.g. prolonged loss of power, civil disaster, etc.), the Confederation Line Phase 1 includes an alternate location from which to continue operation at the BCC.

The BCC is located within the MSF building, adjacent to the YCC and has the basic functioning systems required to dispatch, monitor, and control operations of the Confederation Line Phase 1 LRVs.

The TSCC and BCC Safety Justification Report [53] concludes that, for the scope of Phase 1, the TSCC Systems can support the safe operation of the Confederation Line railway. Recommendations related to TSCC are given in section 7.2.6.

5.9 MAINTENANCE AND STORAGE FACILITY

The Maintenance & Storage Facilities (MSF) Safety Justification Report [54] covers the MSF and Yard.

The main purpose of the MSF is to provide maintenance of the LRV service fleet. The layout of the yard and the MSF structures accommodate the mainline connection track, and the revenue vehicle storage yard.

The MSF is constructed to support the covered storage of the LRV service fleet and consists of six stabling roads each with a berthing capacity for eight trains.

Access to the MSF from the mainline is provided by a connection track, which enters at the western end of the yard. Revenue Service vehicles exit and enter the site via this route. Cross over tracks near to the western edge of the site provide flexibility for vehicle movements, six turnouts have been provided within the yard.

The MSF is not fitted with a CBTC system and train movements within the MSF are controlled by Maintainer's procedures.

All hazards identified that relate to the MSF facility were managed in accordance with the Confederation Line Phase 1 Hazard Management Procedure~~Confederation Line Phase 1 Hazard Management Procedure~~ [1] and the results can be seen in Integrated Hazard Log Summary Report [41].

The Maintenance & Storage Facilities (MSF) Safety Justification Report [54] concludes that, for the scope of Phase 1, the MSF Systems can support the safe operation of the Confederation Line railway. Recommendations related to MSF are given in section 7.2.7.

6. SYSTEM INTEGRATION

Section 5 of this Case for Safety provided a summary of the Primary Systems which considered the systems in 'a standalone' context, albeit while taking cognisance of the impact of failure on the railway as a whole. In order to look at the Confederation Line operation as a whole, rather than just the sum of its parts, a number of activities have been undertaken which look at the Confederation Line Phase 1 as a holistic system.

These activities are recorded in the following documents:

- Confederation Line Phase 1 Integrated Hazard Log [3]
- Day In The Life Of (DITLO) Report [17]
- Confederation Line Phase 1 Interface Hazard Analysis (IHA) [22]
- Confederation Line Phase 1 Reliability Availability and Maintainability Report [42]
- Confederation Line Phase 1 Operations and Support Hazard Analysis [8].

The process of determining the whole system is safely integrated and fit for purpose is by satisfactory completion of Systems Integration Tests (SIT) that demonstrate the safety functions perform as required along with assembly of the necessary design, construction and integration evidence to support all hazard mitigation and control measures.

The primary means of providing this evidence is tracked and reported in the PA Technical Compliance Matrix [7] and Technical Compliance Report [15]. The overall determination the Confederation Line Phase 1 is safe to operate from a risk acceptability point of view is confirmed in the Integrated Hazard Log Summary Report [41].

The Integrated Hazard Log Summary Report [41] describes the Confederation Line Phase 1 Integrated Hazard Log [3] hazard management activities. It traces the transfers of Safety Related Application Conditions via HRP records.

A summary of this process, the hazards identified, their risk ranking and the final analysis carried out to demonstrate the railway is safe to operate is shown in the Integrated Hazard Log Summary Report [41].

7. CONCLUSIONS & RECOMMENDATIONS

The conclusions of this Case for Safety are addressed below together with recommendations for further work.

7.1 CONCLUSIONS

The Confederation Line Phase 1 Railway has been demonstrated to be capable of safe operation by a comprehensive review and analysis of the system and hazards against the principles of EN 50126 [27] and EN 50129 [4].

This Case for Safety and the associated documents provide that evidence to support the following claims:

- The Confederation Line Phase 1 meets the requirements of the Project Agreement [6] and requirements that have been derived whilst mitigating the hazards raised during the safety analysis of the works.
- Hazard identification, analysis and mitigation processes have been undertaken in which evidence is presented that all Confederation Line Phase 1 hazards have been reduced to acceptable levels as evidenced by the IHL Summary Report [41].
- Assurance of correct design has been provided in the form of DCLs by Engineers of Record that confirm the electrical, structural and mechanical design has been generated in accordance with applicable Codes, Standards and Requirements as evidenced by the Technical Compliance Matrix [7].
- Assurance of correct construction has been provided in the form of CCLs by Engineers of Record that underwrite the general conformity of construction to the DCL as evidenced by the Technical Compliance Matrix [7].
- Successful completion of SIT/SAT is evidenced by the Technical Compliance Matrix [7]. Residual test requirements are identified in the ESAC Outstanding Items [13].
- OBC and OFS Occupancy Certificates have been granted confirming that the facilities are safe for use as evidenced by the Technical Compliance Matrix [7]. Any outstanding certification is identified in the ESAC Outstanding Items [13].
- Anything identified in the ESAC Outstanding Items [13] is considered to relate to completion of Confederation Line Phase 1 from a commercial perspective and does not have a detrimental effect upon safety.
- RAM analysis has been undertaken to the extent necessary to demonstrate that the necessary Confederation Line Phase 1 RAM performance inherently meets the safety requirements in the design.
- Safety risks have been reduced by using mature and proven systems that have been integrated using processes that have been demonstrated to be robust and traceable.
- Ottawa Confederation Line Phase 1 Railway is considered to be acceptably safe and suitable for the onset of Revenue Service subject to the conditions identified in section 1.3 and in the Confederation Line Phase 1 Operational Restrictions Document [12].

7.2 RECOMMENDATIONS

7.2.1 Tunnel System Recommendations

1. In winter the Tunnel Walkway should be de-iced as and when required to prevent slips, trips, falls in event of emergency.
2. A tunnel leak inspection and repair strategy should be developed to ensure the long-term tunnel structural integrity.
3. Tunnel water management arrangements should be considered to protect vital tunnel assets from water damage and corrosion.
4. Tunnel cable route should be kept free from excess water and suitable drainage of the cable troughs should be ensured.
5. Maintenance should carry out periodic inspection of the cableways to ensure cables are functional and drainage ways are kept clear.

7.2.2 Track System Recommendations

1. Ultrasonic rail testing is to be carried out every 3 months for the first 2 years and is then changed to a risk-based approach. Maintainer to amend plan going forward.
2. A working group should be established to monitor wheel and rail wear data. From this, specific remedial actions can be identified and agreed, such that they do not cause any worsening to one asset or the other. The Maintainer to establish working group prior to start of passenger operations. The remit of the working group is given as item 3 in table B2 of Track Safety Justification Report [56] .
3. The installation of protective troughing to all main line switch heater pipes, to prevent damage during tamping operations.
4. The monitoring of track position, in relation to OCS and masts is critically important. Datum plates could be used to facilitate ease of inspection.
5. The condition of the rail head through the core tunnel has been contaminated by work site debris, water ingress and tunnel lining remedial products. It is recommended the rail head grinding is carried out within 2 months of the opening to passenger operations.

7.2.3 Energy System Recommendations

1. Maintenance inspection of the overhead conductors in relation to track alignment to minimise the risk from de-wirement or collision with electrification posts is required in line with recommendation #4 in section 7.2.2.
2. Maintenance tasks are needed to regularly check for rail and bond discontinuities with sufficient frequency that the risk of dangerous touch potentials arising from broken bonds is maintained at an acceptable level.
3. A Maintenance Procedure to be in place to inspect or replace lightning arrestors after a known strike in the area.

4. The grounded rail system in the depot is separated from the insulated rail system of the main line by Insulated Rail Joints (IRJ). As failure of one of these insulations will ground the main line running rails, a regular maintenance test is required to confirm the integrity of the IRJs.
5. Regular maintenance inspections and measurements are required to ensure insulation values between rail and ground are maintained. A process for the identification of poor insulation and undertaking remedial work is required.

7.2.4 Station System Recommendations

1. During the initial running period, prior to RSA, a check should be made to ensure there are no issue with obscuration of the LRV Operator view on the CCTV system by ambient light conditions. This should continue to be monitored throughout the seasons and recorded, via the OC Transpo Rail Log [20] and DRACAS. Appropriate remedial action to be implemented.

7.2.5 Communications System Recommendations

No recommendation identified exclusive to Communications. Please refer to General Issues 7.2.10.

7.2.6 TSCC/BCC Recommendations

1. Noise levels and disturbance in TSCC room will need to be monitored during trial running.
2. Alarm management in the Confederation Line Phase 1 TSCC is to be managed in accordance with the Alarm Strategy to be produced by City/OC-Transpo.
3. TSCC operations should continue to be monitored during service and included in DRACAS.

7.2.7 MSF Recommendations

1. Hazards related to UTO and fitment of CBTC throughout the MSF are transferred to Confederation Line Phase 2.
2. Hazards relating to migration to Confederation Line Phase 2 will be addressed post Confederation Line Phase 1 RSA.

7.2.8 CBTC Recommendations

Track maintenance vehicles not fitted with transponders are effectively Non-Communication Objects (NCO), and therefore, the following steps are required to ensure safe operation of these vehicles:

1. A rigorous procedure put in place to ensure all LRVs are in the MSF before track maintenance machines are allowed on track.
2. Procedure must be implemented to prevent maintenance vehicles entering an otherwise protected work zone.

3. It is recommended that all track machines be fitted to allow them to be controlled via the Thales CBTC system at the earliest opportunity.

7.2.9 Alstom Citadis Spirit LRV Recommendations

Please refer to Appendix B extract from the Alstom Citadis LRV Consolidated Safety File [32] and the Confederation Line Phase 1 Operational Restrictions Document [12] for limitations.

7.2.10 General Recommendations

The following recommendations have been identified as part of the hazard analysis process:

1. It is recommended that for the initial running period additional staff are placed on the platform or on the LRVs to manage the safe transfer of patrons at the Platform Train Interface.
2. It is recommended Data Recording and Corrective Action System (DRACAS) be implemented in order to detect the precursor events that may lead to a safety-related incident and to promote continuous improvement in the management of safety and performance of the infrastructure.
3. It is recommended corrective maintenance tasks be prioritised according to the operational criticality of the function delivered by the failed asset in order to determine an acceptable "time at risk" and inform corrective maintenance scheduling, spares inventory levels and supply-chain setup arrangements. An analysis should be undertaken that builds upon the assessment presented within the Confederation Line Phase 1 Reliability Availability and Maintainability Report [25] to determine the tasks that must undergo immediate response and those that can be scheduled according to the convenience of the maintenance organisation

APPENDIX A – SIGNALLING SYSTEM SAFETY CASE

Thales has provided a CBTC Systems Safety Hazard Analysis (Thales) [31]. It provides the satisfactory conclusion as recorded below:

The Safety Case demonstrates that the CBTC system has been subject to a comprehensive quality and safety management program, in accordance with Quality Assurance Plan [C-3], CBTC Systems Safety Hazard Analysis (Thales) [31] and System Safety Plan [C-2]. The report summarises the results of system/subsystem hazard analyses, safety studies and hazard management activities. The quality and safety management activities are summarised in Quality Management Report (Section 3) of CBTC Systems Safety Hazard Analysis (Thales) [31] and Safety Management Report (Section 4) of CBTC Systems Safety Hazard Analysis (Thales) [31].

The technical evidence to support CBTC safe operation and system entry into revenue service are summarised in the Technical Safety Report (Section 5). The Safety Case provides evidence of functional and technical safety to show the CBTC system is safe for its intended use. The design principles and safety concepts incorporated into design assure the safety of the CBTC system, including operation under normal and degraded modes. The design measures were verified and validated in accordance with the System Verification and Validation Plan [C-9] of CBTC Systems Safety Hazard Analysis (Thales) [31]. The Safety Case includes references to verification and validation evidence.

The evidence provided in this SASC, in conjunction with the software development process and verification and validation reports, demonstrate that software achieves the assigned Safety Integrity Level (SIL) and CBTC system fulfils the qualitative safety targets (Section 4.5.1) of CBTC Systems Safety Hazard Analysis (Thales) [31]. The evaluation of random failures (hardware equipment) shows that the CBTC system meets the quantitative safety targets (Section 5.2.3.11) of CBTC Systems Safety Hazard Analysis (Thales) [31].

This Safety Case covers the in-house and site testing of the current hardware and software configuration for system entry into Revenue Operation. The outstanding items were reviewed to determine the impact in terms of functional and technical safety. These items are not considered to have a safety impact or have temporary measures in place to provide the necessary protections to enter into revenue service.

The evidence provided in the Safety Case demonstrates that the CBTC system satisfies the contractual safety requirements and safety targets, and that the CBTC is safe for the intended purpose, subject to compliance with the SACs and SORs provided in Appendix F and Appendix G of CBTC Systems Safety Hazard Analysis (Thales) [31].

Further changes to the system configuration specified in CBTC Systems Safety Hazard Analysis (Thales) [31] will be covered by Safety Memos. These will summarise the activities performed for a specific configuration change (e.g. software release under configuration change control process) and evaluate the safety impact, including SORs.

APPENDIX B – ALSTOM CITADIS CONSOLIDATED SAFETY FILE

Alstom managed their own Hazard Log during the design and development process of the Citadis Spirit LRV and both Alstom and OLRT-C along with OC Transpo worked collaboratively to resolve safety issues where necessary.

One significant area of concern for all parties on all railways is the Platform Train Interface. This has been addressed extensively in the Confederation Line Phase 1 Integrated Hazard Log but a number of the hazards associated with this interface remain with Alstom to resolve, namely:

Passengers trapped between platform and train.

This is one aspect not specifically addressed in the IHL and so is summarized here. Referring to para 6.1.2.1.1 of the Alstom Citadis LRV Consolidated Safety File [32].

Passenger trapped between platform and train was analysed qualitatively by OLRT-C and Alstom, based upon a dimensional analysis and a case prepared for OC Transpo, using these arguments. OLRT-C developed a Safety Certificate (Safety Certificate 9207) that presented the dimensional analysis and ability to view the side of the car with the platform cameras. While Alstom and OLRT-C considered the hazard mitigated, OC Transpo required a design change to add a third layer to the bellows to reduce the Platform to Train gap to the minimum practical.

Referring to 6.1.2.1.1 photos can be seen of the before and after modification. While the nearly flush gangway bellows mitigated most of the risk of a passenger being trapped or falling between the platform edge and the side of the car, an entrapment hazard was identified with the straight bottom of the bellows. It is conceivable that a person could put their foot between the platform edge and the gangway bellows and the straight bottom of the gangway bellows would then prevent withdrawing the foot. The final design will have a curved bottom, so a foot cannot be caught on the bottom of the bellows. Refer to 6.1.2.1.1 for a photo of prototype.

Please refer to the Alstom Citadis LRV Consolidated Safety File [32] for all rolling stock safety issues that have been either independently or collaboratively resolved with stakeholders.

Waivers and Restrictions.

All known design issues with resolution still to be implemented on the vehicle, pertaining to closure of safety studies and related safety activities are listed in Table C1. These waivers have been considered tolerable at the start of revenue service with the exception of #4 which is yet to be agreed, providing they are implemented in a timely manner during the warranty period.

Table B1 - Alstom Citadis related Waivers

No.	Subject	Reference Chapter	Issue	Resolution
1	Drivers cab lighting	2.6.14.3.1	Dimmer does not permit complete shut off of cab light, causing reflection in the windshield at night and driver distraction.	The dimmer will be modified to permit complete shutdown of the cab ceiling lights.
2	Non flush gangway	2.6.2.1.1 & 6.1.2.1	Non flush gangway bellows allows a place for people to be trapped between gangway and the platform	Add a 3rd layer to bring the gangway bellows almost flush with the side of the train.
3	Carbody fire resistance	10.3.2	The underfloor area is not sealed to the side of the car, permitting a flashover under the floor to propagate up the vehicle sidewall	Add blocking plates and intumescent seals to prevent underfloor fire from entering the interior.
4	Suspension	Not addressed in the document	On occasions of AW03 loading due to not enough capacity in the suspension floor tilt recovery back to nominal level takes approximately 8 minutes. Roughly equivalent to two station stops. The resulting difference in LRV floor height to platform could be as much as 50mm.	A design solution has been identified and proposed. This entails removing one of the suspension compressors and replacing the mechanical space with an additional expansion vessel. The impact of removing one of the duel compressors on reliability and performance has been assessed and it has been concluded that the single compressor has significant over capacity in performance and duty cycle longevity to ensure no detrimental effect on the systems stated availability or reliability.

Drivers Cab Lighting #1

As recorded in 2.6.14.3.1 Alstom Citadis LRV Consolidated Safety File [32] there is a design solution for complete shutdown of cab lights. However, the current dimmer switches reduce the lux levels down significantly and considered to be tolerable for RSA.

Non-Flush Gangway #2

Significant improvements were made with the second layer bellows. The third layer introduced fills the void to the extent there will be approximately 150mm from the platform edge to the gangway bellows which is a 50% improvement over the second layer. There may be a need for extra vigilance by the Driver until the 3rd layer is introduced the whole fleet. The fitment of the modification is fairly quick process as it fits neatly over the existing layer; it is not a time-consuming replacement of the existing bellows.

Car Body Fire Resistance

The earlier fire resistance test resulted in modification to the underbody to ensure the LRV body achieved compliance, this being in the areas under the chassis where external train components are the likely source of fire. As far as meeting the fire resistance compliance for Confederation Line Phase 1 is concerned, the Citadis Spirit is suitable for entry into revenue service. However, Alstom on their own volition, as part of their ongoing improvement program are extending the fire resistance along the under chassis.

Intumescent paint has been used in order to maximise the car body fire resistance in response to the carriage floor and roof assemblies failing to fully conform to the fire resistance ratings. A maintenance regime has been established for periodic inspection of the intumescent paint and engineering evaluation of the requirement for re-application, as required.

The time scale of this is not considered to impact RSA for Confederation Line Phase 1 as there is no credible fire risk to the underneath of the LRV away from the high energy fire sources. However, for Phase 2 level crossings are incorporated in the route thus the risk of under carriage fire is increased from potential of highway vehicle induced fires spreading under the LRV chassis.

Suspension AW03 Loading

Alstom have given careful consideration to a viable solution that does not impact on the current vehicle certification, e.g. axle loading amongst other physical attributes which could give rise to the need for requalification of the vehicle.

The proposed solution maintains Alstom's design principles and engineering assessment of the solution has demonstrated the required change will not impact on the overall performance and reliability of the vehicle. However the change could take a significant time to implement through the whole fleet, possibly six months. During this period the unmodified trains will not be ADA compliant which compromises legislative compliance at Revenue Service.

That aside, considering the situation purely from a safety point of view, the impact on the majority population of mobility impaired fare paying passengers is not significant. All wheel chair users can easily accommodate a 50mm step up or down as can most mobility impaired passengers. There are some not so common mobility debilitating conditions for which a 50mm step up would be very difficult, e.g. Arthrogryposis but this by no means represents a significant number of the population, (approximately 1 in 3,000).

From a safety risk point of view the non-compliance is tolerable with risk assessment for up to six months if managed with extra Operator vigilance and recorded announcements to be played during peak operating hours when AW03 loading is likely to occur and during public events.

Certification

A Preliminary fleet Safety Certificate (rev 3) is current for all Ottawa Spirit trains 16/1/2019. This states that all Citadis Spirit trains for the Confederation Line Phase 1 are limited for test and commissioning use and training operations under a number of restrictions, including no passenger to be carried.

A full certificate is required for RSA.

The Maintainer has established RTM LRV Faults and Vehicle Minimum Operating Standard [40].

Maintenance and Operations Procedures

One area that needed particular consideration in the IHL was the auto coupling and vehicle recovery procedure and the time it takes to prepare an in service LRV and the rescue vehicle for coupling. Figure 5~~Figure 5~~ and Figure 6 below show an LRV with front panel in place and front panel removed the latter being a necessity for vehicle recovery.

Figure 5: Confederation Line Phase 1 Alstom Citadis Spirit LRV with Front Panel in Place

Figure 6: Confederation Line Phase 1 Alstom Citadis Spirit LRV with Front Panel Removed

In order to recover an LRV the front skirt of the failed LRV has be removed as does the corresponding panel from the towing unit. The coupling procedure was demonstrated in a depot environment to take around 20 minutes and that does not include getting equipment to and from the site. However, as it is intended to detrain passengers prior to the recovery taking place, it is purely a service affecting failure event. Should this procedure change, then the LRV recovery procedure should be revisited, RTM-OP-PRO-124 Train Evacuation refers.

APPENDIX C – COMMUNICATIONS SYSTEM INTEGRATION