Rail Safety Consulting

a Division of TUV Rheinland Mobility, Inc.

Safety Audit Report

Safety Audit Report of the

Ottawa Stage 1 LRT System

Doc.-ID:	1728-002
Revision:	5.0
Date:	13 September 2019

TÜVRheinland®
Rail Safety Consulting

Date	Rev.	Prepared	Reviewed	Description / Modification
2017-11-24	1.0	S. Mammoliti		1st Release to support the Service Notice Date milestone. Updated to reflect reviewer comments.
2017-11-29	2.0	S. Mammoliti		Updated to address confusion regarding terms of reference and scope.
2018-10-30	3.0 D1	S. Mammoliti		Updated to reflect progress made up to Design Integration Review (DIR) Meeting.
2019-04-02	4.0 D1	S. Mammoliti		Updated to reflect findings from Safety Audit held March 4 thru March 25, 2019.
2019-09-13	5.0	S. Mammoliti		Update for passenger-carrying operations.

TÜVRheinland®
Rail Safety Consulting

Table of Contents

1 PROJECT DEFINITION

The City of Ottawa has contracted with Rideau Transit Group General Partnership (RTG) to Design, Build, Finance, and Maintain Stage 1 of the Confederation Line Light Rail Transit (LRT) system.

As per the Safety Auditor Terms of Reference RFP [Ref. 1], TUV Rheinland is performing a Safety Audit to confirm that RTG is compliant with the Safety Requirements prior to the Revenue Service Availability date.

1.1 Scope

The intent of this Safety Audit Report is to capture the results and subsequent conclusions of the auditor in conducting the tasks set out in the Safety Audit Plan [Ref. 3]. The Safety Audit Plan requires a review of the design and implementation of the Ottawa Stage 1 LRT (OLRT) in order to verify that the system has been implemented to meet safety requirements specified in the Project Agreement [Ref. 2]. This review includes an examination of the design and analysis documentation as well as the development and safety processes employed by RTG and its partners.

This is the final revision of the Safety Audit Report issued in support of passenger-carrying operations.

1.2 Glossary

AAPP	Authority Approval Process Plan
ESAC	Engineering Safety & Assurance Case
IHA	Interface Hazard Analysis
IHL	Integrated Hazard Log
OLRT	Ottawa Light Rail Transit
OLRT-C	Ottawa Light Rail Transit – Constructors
PA	Project Agreement

RAM	Reliability, Availability, and Maintainability
RSSB	Rail Safety and Standards Board
SeMS	Security Management System
SMS	Safety Management System
SOP	Standard Operating Procedure
WBS	Work Breakdown Structure

1.3 Referenced Documents

[Ref. 1]	Safety Auditor for Stage 1 LRT	RFP No. 01317-91893-P01
[Ref. 2]	Ottawa Light Rail Transit Project – Project Agreement	TOR01: 4868348: v55
[Ref. 3]	Safety Audit Plan of the Ottawa Stage 1 LRT System	1728-001 Rev 1.0
[Ref. 4]	Ottawa Light Rapid Transit – Project System Safety Program Plan	OLR-05-0-0000-MPL-0006 Rev 01
[Ref. 5]	Ottawa Light Rapid Transit – Project System Safety Certification Plan	OLR-05-0-0000-MPL-0003 Rev 06
[Ref. 6]	Ottawa Light Rapid Transit – Project Integrated Hazard Log	OLR-05-0-0000-REG-0004 Rev 6
[Ref. 7]	Ottawa Light Rapid Transit – Authority Approval Process Plan	OLR-05-0-0000-MPL-0008 Rev 01
[Ref. 8]	Ottawa Light Rapid Transit – Authority Approval Process Plan (AAPP) Work Breakdown Structure (WBS)	Rev E dated 2017-09-29

[Ref. 9]	Ottawa Light Rapid Transit – System Engineering and Assurance Health Check Report	SEMP/048/001 Rev 1.0 DRAFT
[Ref. 10]	Not Used	Not Used
[Ref. 11]	Railway Applications – Communication, signalling and processing systems – Safety related electronic systems for signalling	CENELEC EN 50129:2003
[Ref. 12]	System Engineering & Assurance Governance Document Tree – Railway Level	OLR-05-0-0000-WBS-0002 Rev C
[Ref. 13]	Security Management System	OCT-X000-00-PGM Rev 0.5 DRAFT
[Ref. 14]	Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)	CENELEC EN 50126:2002
[Ref. 15]	Project Agreement Analysis & Allocation	OLR-05-0-0000-REP-0009 Rev 1.0
[Ref. 16]	PA Technical Compliance Matrix	OLR-90-0-0000-CMP-0002 Rev 35
[Ref. 17]	OLRT Safety Requirements Matrix	OLR-05-0-0000-REP-0053 Rev 4
[Ref. 18]	OLRT - Project Hazard Management Procedure	OLR-50-0-0000-MPL-0009 Rev B

[Ref. 19]	OLRT – Project System Assurance Management Plan	OLR-XX-X-XXX-REP-xxxx Rev B 2018-03-21
[Ref. 20]	OLRT – Project System Engineering Management Plan	OLR-50-0-0000-MPL-0005 Rev 1.0
[Ref. 21]	OLRT – Project Competency Management Plan	OLR-05-0-0000-MPL-0040 Rev 0
[Ref. 22]	OLRT – Configuration Management Recovery Plan	OLR-09-0-0000-MPL-0004 Rev 1
[Ref. 23]	OLRT – Configuration Change Control Recovery Plan	OLR-05-0-0000-MPL-0036 Rev 1
[Ref. 24]	OLRT – Project Technical Compliance Report	OLR-05-0-0000-REP-0054 Rev 4
[Ref. 25]	O-Train Line 1 Operator Safety Case	OTC-Q208-00-REP Ver 2.0
[Ref. 26]	Confederation Line Phase 1 Case for Safety	OLR-05-0-0000-REP-0017 Rev 4
[Ref. 27]	Ottawa Light Rail Transit Project Reliability, Availability and Maintainability Report	OLR-05-0-0000-REP-0056 Rev 4
[Ref. 28]	Ottawa Light Rail Transit Project Confederation Line 1 Engineering Safety and Assurance Case	OLR-05-0-0000-REP -0051 Rev 3
[Ref. 29]	OLRT – RSSB Hazard Gap Analysis Evaluation	OLR-05-0-0000-MPL-0038 Rev 0

[Ref. 30]	OLRT – Project Interface Hazard Analysis	OLR-05-0-0000-REP-0059 Rev 4
[Ref. 31]	Thales - Ottawa Light Rail Transit Project Specific Application Safety Case Report	3CU 05018 0247 DUZZA Rev 001
[Ref. 32]	Thales – Safety Memo for ATS SW Build 5.05.02	Letter: OLRT-Thales-1118 Dated 2019-July-19
[Ref. 33]	Alstom – OLRT Consolidated Safety File	ADD0000939280 Rev C
[Ref. 34]	Alstom – Ottawa Light Rail Vehicle Safety Authorisation	RSA-TEM-003 Subcontract No. 507528-P001 Dated 2019-Sept-11
[Ref. 35]	OLRT – Project Integrated Hazard Log Summary Report	OLR-05-0-0000-REP-0015, Rev 3
[Ref. 36]	OLRT – Project Operations and Support Hazard Analysis	OLR-05-0-0000-REP-0063 Rev 3
[Ref. 37]	OLRT – Project Ottawa Confederation Line Phase 1 Operational Restrictions Document	OLR-05-0-0000-REP-0058 Rev 3

2 AUDIT RESULTS AND RECOMMENDATIONS

The results and recommendations associated with the audits are contained in this section.

2.1 Task 2 – Audit of Applicable Safety and Security Requirements

The following documents were reviewed as a part of this audit:

- OLRT – Project Integrated Hazard Log [Ref. 6]
- Project Agreement Analysis & Allocation [Ref. 15]
- PA Technical Compliance Matrix [Ref. 16]
- OLRT Safety Requirements Matrix [Ref. 17]
- OLRT Technical Compliance Report [Ref. 24]
- O-Train Line 1 Operator Safety Case [Ref. 25]

The Safety Requirements of the Project Agreement (PA) [Ref. 2] have been identified and expanded upon to a level that is sufficient for their allocation to the applicable subsystems of the OLRT as evidenced in the Project Agreement Analysis and Allocation [Ref. 15], the PA Technical Compliance Report [Ref. 16], and the OLRT Safety Requirements Matrix [Ref. 17]. Conformance with Technical Requirements is evidenced in the Technical Compliance Report [Ref. 24] while compliance with the specific Derived Safety Requirements (DSR) is contained in the Safety Requirements Matrix [Ref. 17].

The System Engineering and Assurance Health Check [Ref. 9] and previous revisions of this Report and had documented a delay in the development and completion of the Safety and Security Requirements and its associated impediment to system design and the audit of the Subsystem Safety Cases (Task 4), System and Operations Readiness and Hazard Tracking Matrix (Task 5a), and ultimately, the Main Safety Case (Task 5b).

Typically, the identification and elicitation of Safety Requirements occurs during the Concept and Design Phases of a project (Phases 1 through 6 of the Authority Approval Process Plan (AAPP) [Ref. 8]). The delayed development of the Safety Requirements also presented a risk that there would be an overreliance upon Standard Operating Procedures (SOP) to mitigate Safety Requirements as the opportunity to mitigate Safety Requirements through design measures was not feasible given the advanced design and deployment of

the System. An Operator Safety Case [Ref. 25] was produced for the City of Ottawa (see section 2.4) and concludes that "… OC Transpo has mobilized the necessary staff, with the appropriate skills, training and certifications, and with the appropriate rules and procedures in place to allow for the safe operations of the System in revenue service."

Consequently, the observations made in earlier version of this Audit Report regarding the delayed development of Safety Requirements have been addressed. The development and implementation of the Safety and Security Requirements are sufficient for passenger-carrying operations.

2.2 Task 3 – Audit of Safety Management System and Security Management System

The following documents were reviewed as a part of this audit:

- OLRT – Project System Safety Program Plan [Ref. 4]
- OLRT – Project System Safety Certification Plan [Ref. 5]
- Security Management System [Ref. 13]
- OLRT – Authority Approval Process Plan [Ref. 7]
- OLRT – AAPP Work Breakdown Structure [Ref. 8]
- OLRT – System Engineering and Assurance Health Check Report [Ref. 9]
- System Engineering & Assurance Governance Document Tree – Railway Level [Ref. 12]
- OLRT – Project Hazard Management Procedure [Ref. 18]
- OLRT – Project System Assurance Management Plan [Ref. 19]
- OLRT – Project System Engineering Management Plan [Ref. 20]
- OLRT – Project Competency Management Plan [Ref. 21]
- OLRT – Configuration Management Recovery Plan [Ref. 22]
- OLRT – Configuration Change Control Recovery Plan [Ref. 23]

Schedule 15-1, Article 3 of the PA identifies several standards that should be used to guide the OLRT Safety Management, specifically EN 50126 [Ref. 14]. This standard identifies system safety as being dependent upon not only hazard and safety analyses, but also a properly functioning Quality Assurance and Reliability, Availability, and Maintainability (RAM) program to ensure that the elements of the railroad that are responsible for the

safety are well defined (via a Quality Assurance Program) and are demonstrated to be reliable (via a RAM Program) in their respective execution of the safety functions.

Change Control and Configuration Control measures typically associated with a Quality Assurance Program were not executed during the early phases of the project. As a result, a Configuration Management Recovery Plan [Ref. 22] and Configuration Change Control Recovery Plan [Ref. 23] were created and executed. Their outputs were used in the in the review of the Engineering Safety & Assurance Case (ESAC) [Ref. 28] and the System Level Safety Case [Ref. 26] to ensure that the safety-critical and safety-related element system described in these document are under proper change control and configuration management.

The System RAM Analysis Report [Ref. 27] was produced and forms part of the body of evidence of the Case for Safety [Ref. 26] and ESAC [Ref. 28] to demonstrate that the System can reliable perform its intended functions, including those necessary for the safety of the System.

Given the timelines associated with the execution of the Safety Programme, the Safety Plan was not in line with either the MIL-STD-882E or IEC 61508 standards that are called out as references in the Safety Plan. The approach has been tailored to use a Risk Based Assurance methodology. The methodology involves the review of the Hazard Log against a list of railroad hazards as tabulated by the Rail Safety and Standards Board (RSSB) [Ref. 29] to ensure that potential hazards had not been overlooked, followed by an allocation of mitigation responsibilities to Primary Systems, and a further review of the interactions between the Primary Systems via an Interface Hazard Analysis (IHA) [Ref. 30] to ensure that all interactions between Primary Systems that are related to safety-critical or safety-related functions have been assessed. The IHA has concluded that the interfaces between the Primary Systems are fit for purpose.

In addition to the OLRT Safety Plan [Ref. 4], a review of the OLRT Certification Plan [Ref. 5], and OC Transpo Security Management System [Ref. 13] were conducted and concluded that the Security Management System was fit for purpose. It should be noted that the scope of this report is to assure that OLRT-C, as the supplier of the System, has a

Safety Management System that is capable of delivering a safety system. The review of the OC Transpo Security Management System was included in this Audit Report in order to ensure that there was a mechanism by which OC Transpo was able to manage mitigation measures that involve SOPs. These SOP related mitigation measures were identified in the Integrated Hazard Log (IHL) [Ref. 6] as further discussed in Section 2.4.

The Work Breakdown Structure [Ref. 8], System Engineering and Assurance Health Check [Ref. 9], the System Engineering & Assurance Governance Document Tree [Ref. 12], and the Safety Plan and Certification Plan were also used to inform the early review of the Safety Management System. The approach presented in the System Engineering and Assurance Health Check and the System Engineering & Assurance Governance Document Tree were discussed during the Engagement Workshop (Nov 15 through Nov 17, 2017) and prescribed the Risk Based Assurance methodology described above used to define the minimum set of artifacts necessary to establish a systematic safety and systems assurance approach.

The review of the OLRT Safety Management System, as described above has demonstrated that the OLRT Safety Management System has been effective in implementing the System Safety Requirement, as described in Section 2.1.

2.3 Task 4 – Audit of Subsystem Safety Cases

The following documents have been provided as evidence that the Primary Systems have met their respective Safety Requirements (see Section 2.1):

- Thales OLRT Safety Case [Ref. 31]
- Thales Safety Memo for ATS SW Build 5.05.02 [Ref. 32]
- Alstom OLRT Consolidated Safety File [Ref. 33]
- Alstom Citadis Spirit – Ottawa Light Rail Vehicle Safety Authorisation [Ref. 34]
- OLRT EJV Confederation Line Phase 1 Case for Safety [Ref. 26]
- Security Management System [Ref. 13]

The Primary Systems consist of the Thales Signalling System, Alstom Light Rail Vehicle, and the EJV Systems (Maintenance and Storage Facility, Stations, Train Control Centre,

Backup Control Centre, Tunnel, Communications System, Track, and Energy). The Subsystem Safety Cases are documented in the Thales OLRT Safety Case [Ref. 31], Alstom OLRT Consolidated Safety File [Ref. 33], and EJV Case for Safety [Ref. 26] respectively. These documents present the safety justifications for each of the Primary Systems. The Thales and Alstom Safety Cases are further supported by subsequent certification letters for software releases and other changes from the baseline established in their respective Safety Cases (Thales Safety Memo for ATS SW Build 5.05.02 [Ref. 32] and Alstom Vehicle Safety Authorisation [Ref. 34]).

These Subsystem Safety Cases and subsequent Certification Letters support the use of their respective Primary Systems in passenger-carrying operations.

2.4 Task 5a – Audit System and Operations Readiness and Hazard Tracking Matrix

In support of Hazard Tracking the following documents were reviewed:

- OLRT – Integrated Project Hazard Log [Ref. 6]
- OLRT – RSSB Hazard Gap Analysis Evaluation [Ref. 29]
- OLRT – Project Integrated Hazard Log Summary Report [Ref. 35]
- OLRT – Project Operations and Support Hazard Analysis [Ref. 36]
- OLRT – Project Ottawa Phase 1 Operational Restrictions Document [Ref. 37]

The hazards applicable to the System are identified in the Integrated Project Hazard Log [Ref. 6] (IHL). As noted in Section 2.2, this included a cross check of the items in the Hazard Log against those identified in in the RSSB Hazard Gap Evaluation [Ref. 29] to ensure the comprehensiveness of the hazard identification process. The closure of the identified hazards are documented in the Hazard Log Summary Report [Ref. 35] and is further supported by the Operations and Support Hazard Analysis [Ref. 36] and the Operational Restrictions Document [Ref. 37] to ensure that hazard mitigations which require procedural elements to control the hazard have been given due consideration.

These artefacts demonstrate that the hazards have been tracked to their respective resolutions, and along with the OC Transpo Operator Safety Case [Ref. 25], indicate that the System is ready for passenger-carrying operations.

2.5 Task 5b – Audit Main System Safety Case

The Engineering Safety & Assurance Case (ESAC) [Ref. 28] "lays out the main lines of reasoning and argument to support delivery of the Confederation Line Phase 1 Railway." The ESAC summarises the Safety, Assurance, RAM, and Verification and Validation evidence that support the OLRT-C assertion that the supplied System is fit for purpose. This includes OLRT-C's review of the references included in this Audit Report as well separate audits, competency assessments, and system assurance activities conducted by OLRT-C. The ESAC concludes assurance arguments presented in the ESAC "… satisfied the Confederation Line Phase 1 works are sufficiently assured to enable entry in service operations in accordance with the RSA."

The review of the artefacts identified in this Audit Report along with the review of the ESAC itself are positive and support the assertion of the ESAC that the System is fit for passenger-carrying operations.

3 CONCLUSIONS

3.1 Audit Conclusions and Recommendation

3.1.1 Task 2 - Applicable Safety and Security Requirements

Previous observations made in earlier version of this Audit Report regarding the delayed development of Safety Requirements have been addressed. The development and implementation of the Safety and Security Requirements are sufficient for passenger-carrying operations.

3.1.2 Task 3 - Safety Management System and Security Management System

The review of the OLRT Safety Management System, as described in Section 2.2, demonstrates that the OLRT Safety Management System has been effective in implementing the System Safety Requirement, as described in Section 2.1.

3.1.3 Task 4 - Subsystem Safety Cases

The Subsystem Safety Cases for the Primary Systems which include the Thales Signalling System, Alstom Light Rail Vehicle, and the EJV Systems (Maintenance and Storage Facility, Stations, Train Control Centre, Backup Control Centre, Tunnel, Communications System, Track, and Energy) support the use of their respective Primary Systems in passenger-carrying operations.

3.1.4 Task 5a - System and Operations Readiness and Hazard Tracking Matrix

The artefacts identified in Section 2.4 as part of the audit of the System and Operations Readiness and Hazard Tracking demonstrate that the hazards have been tracked to their respective resolutions, and along with the OC Transpo Operator Safety Case [Ref. 25], indicate that the System is ready for passenger-carrying operations.

3.1.5 Task 5b - Main System Safety Case

The review of the artefacts identified in this Audit Report along with the review of the ESAC itself are positive and support the assertion of the ESAC that the System is fit for passenger-carrying operations..

3.2 Revenue Readiness

Given the scope and findings of this Safety Audit Report, as summarised in Section 3.1 above, this Audit Report supports the use of the OLRT for passenger-carry operations.