METROLINX

Metrolinx
Safety Requirements Specification: Product Description

MX-SEA-PD-112

Revision 00

Date: April 2023

Safety Requirements Specification: Product Description

MX-SEA-PD-112

Publication Date: May 2023

Amendment Record

Revision	Date (DD/MM/YYYY)	Description of changes

Preface

This is the first edition of the Metrolinx Safety Requirements Specification Product Description (MX-SEA-PD-112). It forms part of a suite of guidance documents that describe the procedures to be followed to comply with Metrolinx's Reliability, Availability, Maintainability and Safety (RAMS) requirements.

The purpose of this document is to describe the Safety Requirements Specification which states the safety functions to be implemented to control the risks identified by a risk assessment. Project proponents may need to generate this document when they are undertaking a technical change to the railway system or modifying a maintenance regime or undertaking an operational change to the railway system.

Suggestions for revision or improvements can be sent to the Metrolinx Systems Engineering Assurance office at Engineering.Assurance@metrolinx.com. The Director of the Systems Engineering Assurance office authorizes the changes. Include a description of the proposed change, background of the application and any other useful rationale or justification. Be sure to include your name, company affiliation (if applicable), e-mail address, and phone number.

April 2023

Contents

Documents ..... **iv**

Acronyms and Abbreviations ..... **v**

Definitions ..... **vi**

1 Safety Requirements Specification **1**

1.1 Purpose 1
1.2 Applicability 1
1.3 Supporting Material 1
1.4 Products 1
1.5 Key Responsibilities 2
1.6 Competence 2
1.7 Structure 3
1.8 Contents 3
1.9 Quality Criteria 4
1.10 Document Management 4

Tables

Table 1 Supporting documents iv

Table 2 Acronyms and Abbreviations v

Table 3 Definitions vi

Table 4 Document phases 5

Documents

Table 1 Supporting documents

Document Number	Document Title	Relation
BS EN 50126-1:2017	Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) (PHASE 1: Adoption of European Standard EN 50126-1:2017)	Parent Standard
MX-SEA-STD-100	RAMS Process Standard	Related Standard
MX-SEA-GDC-112	Safety Requirements Specification Guidance	Guidance
MX-SEA-TPL-112	Safety Requirements Specification Template	Template
MXSD-SSA-L1-STD-0001	Railway Risk Assessment Standard	Supporting Standard
TBD	Safety Related Application Conditions Product Description	Product Description
ISO 9001:2015	Quality Management Systems — Requirements	Supporting Standard
MX-SEA-TOR-001	Metrolinx System Review Panel (SRP) Terms of Reference (ToR)	Review Panel ToR
April 5, 2023	Metrolinx Safety Certification Committee (SSC) Terms of Reference (ToR)	Certification Committee ToR

Acronyms and Abbreviations

Table 2 Acronyms and Abbreviations

Abbreviation	Full Name
AIP	Approval In Principle
CMREA	Canadian Method for Risk Evaluation and Assessment for Railway Systems
ISA	Independent Safety Assessor
RACI	Responsible, Accountable, Consulted and Informed
RAM	Reliability, Availability and Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
SCC	Safety Certification Committee
SDS	Single Design Solution
SRAC	Safety Related Application Conditions
SRP	System Review Panel

Definitions

Table 3 Definitions

Term	Definition	Source
Asset owner	Groups and individuals that are responsible for asset ownership, asset maintenance, inventory management, document control, asset handover and reliability engineering	MX-ALM-STD-001
Availability	Ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.	BS EN 50126:2017
Maintainability	Ability to be retained in, or restored to, a state to perform as required, under given conditions of use and maintenance.	BS EN 50126:2017
Project Company	The private sector entity which enters into the Project Agreement with Infrastructure Ontario and Lands Corporation and Metrolinx to design, build and where applicable, finance, operate or maintain a Project. The special-purpose entity which has entered into a Project Agreement with the Contracting Authority.	CKH-QMA-FRM-003
Project Manager	Appointed by Metrolinx as its representative and is responsible for the delivery of the Project within the prescribed Schedule and budget. Metrolinx employees fulfilling the role of the Project Manager may also be considered the Cost Centre Manager, if this person is also delegated signing authority in accordance with the Metrolinx Corporate Administrative Manual, Administrative Management, Approval Authorization Controls and Designations. It is noted that non-Metrolinx employees fulfilling the role of the Project Manager are not considered Cost Centre Managers. In such cases refer to	CKH-QMA-FRM-003

	approved Project Chart of Accounts for the Program for the designated Cost Centre Manager.	
Reliability	Ability to perform as required, without failure, for a given time interval, under given conditions.	BS EN 50126:2017
Safety	Freedom from unacceptable risk that is related to human health or to the environment).	BS EN 51026:2017
Subsystem	Part of a system, which is itself a system	BS EN 50126:2017
System	Set of interrelated elements considered in a defined context as a whole and separated from their environment	BS EN 50126:2017

1 Safety Requirements Specification

1.1 Purpose

1.1.1 The purpose of the Safety Requirements Specification document is to state all safety requirements for the system to be used on the project. The safety requirements are defined to control the hazards which are identified and recorded in the Hazard Record as part of the risk assessment process. Effectively establishing and managing safety requirements allows for traceability throughout the project lifecycle to support safe design, testing (verification and validation), acceptance and the safe operation of the system.

1.1.2 The Safety Requirements Specification states the safety functions that shall be implemented to control the risks identified by the risk assessment. Examples of typical parameters to characterise safety requirements are provided in Annex B of EN 50126.

1.1.3 Well defined Safety Requirements allow the Project Company and Metrolinx to have shared understanding of the system being developed and contributes to reducing the likelihood of missed or unclear requirements that may lead to the inability to properly mitigate hazardous scenarios. Safety Requirements that are clearly defined contribute to the safe operation and overall safety of the system.

1.2 Applicability

1.2.1 This product is mandatory for any project that undertakes a technical change to the railway system (i.e., introduction of a new subsystem, renewal of an existing subsystem, a modification to an existing subsystem, or introduction of a new or modified maintenance regime) or undertakes an operational change to the railway system.

1.1.1 This product is not applicable for established routine maintenance activities including like-for-like replacement of components.

1.1.2 This product is considered good practice when developing or modifying any complex system.

1.3 Supporting Material

1.3.1 The Safety Requirements Specification template is located in MX-SEA-TPL-112.

1.3.2 Guidance on completing the Safety Requirements Specification is located in MX-SEA-GDC-112.

1.4 Products

1.4.1 The Safety Requirements Specification is a product of the System Assurance process. Guidance on this process is available via MX-SEA-STD-100.

1.5 Key Responsibilities

1.5.1 The Project Company is responsible for the production of the Safety Requirements Specification. Preparation of the Safety Requirements Specification may be delegated; however, the Project Company is responsible for its content and quality.

1.5.2 The Project Company is the organization that is responsible for the contracted scope of work at the time of development. Project Company shall ensure that the Safety Requirements Specification is produced in accordance with applicable standards required by the contract (in compliance with the roles and responsibilities as defined in EN 50126:2017).

1.5.3 The Project Management may be performed by Metrolinx or may be contracted, for example in a Design/Build, whereby Metrolinx Project Management would ensure contract provisions for the Safety Requirements Specification are met and would not develop the Safety Requirements Specification.

1.5.4 Some of the Asset Owner obligations and responsibilities may be transferred through contracting, whereby the contract contains Reliability, Availability, Maintainability and Safety (RAMS) and operating requirements. The Metrolinx Asset Owner would participate in endorsing the Safety Requirements Specification whereas a contracted party responsible for RAMS would develop the Safety Requirements Specification as directed by the Project Management.

1.5.5 The System Review Panel (SRP) has delegated authority from the Safety Certification Committee (SCC) and is responsible for endorsing the Safety Requirements Specification. The System Review Panel ensures that the Safety Requirements Specification is compliant with the project requirements, applicable legislation, and national, industry, and Metrolinx standards. The SRP may also identify uncertainties, issues, and assumptions that may arise as the project progresses that should be addressed.

1.5.6 The full Responsible, Accountable, Consulted, and Informed (RACI) information that sets out the interaction between all stakeholders involved in the production and endorsement of the Safety Requirements Specification is available in MX-SEA-STD-100.

1.6 Competence

1.6.1 Safety Requirements shall be defined by personnel with technical competence in the system and an understanding of safety management, preferably as part of a multi-disciplinary team. The review shall also be completed by personnel with competence in safety management and sufficient understanding of the system to assess whether the safety requirements shall fully address the hazard. The competency of the people involved in the process shall be recorded in the Safety Requirements Specification.

1.7 Structure

1.7.1 The structure of the Safety Requirements Specification is described in the Safety Requirements Specification Guidance document located in MX-SEA-GDC-112.

1.7.2 The document requires the following section titles:

a) Introduction;

b) System description

c) Risk assessment approach;

d) Safety targets and Requirements;

e) Safety Related Application Conditions;

f) Assumptions; and

g) Safety Demonstration Process and Acceptance Criteria.

1.8 Contents

1.8.1 The contents of the Safety Requirements Specification are described in the Safety Requirements Specification Guidance document located in MX-SEA-GDC-112.

1.8.2 As a minimum, it shall contain the following:

a) Functional Requirements, including safety integrity requirements (what the system shall do to be safe, and how effective it needs to be). Functional Safety Requirements shall include:

   1) The expected functional behaviour of safety-related functions

   2) The behaviour of the safety-related functions in case of failures, divided into:

      i. The required safety integrity requirements

      ii. The required behaviour in case of no-hazardous failure (i.e., enforcement and retention of safe state)

b) Contextual Requirements (requirements/assumptions about the environment i.e., they cover maintenance and operational safety requirements and limitations); and

c) Technical Requirements (requirements relating to how the system is built and can be derived from maintainability, environmental conditions, potential threats created by the technology/system/subsystem regardless of their intended functions). Technical Safety Requirements comprise technical constraints for design/installation. They can include safety requirements such as:

   1) Conformity to external standards,

   2) Relevant regulations including OHSA (Occupational Health and Safety Act), Rules and Regulations

   3) Codes of Practice

1.8.3 The Safety Requirements shall:

a) Include all the safety requirements developed from the Hazard and Risk analyses that have been defined for the effective management of project hazards.

b) Describe the traceability of the safety requirements to the related hazards. The safety requirements shall be listed against the related hazard(s) or be referenced to the relevant hazards' ID.

c) Contain a unique identifier for each safety requirement.

d) Contain a unique identifying reference of the Hazard(s) it is mitigating. However, a safety requirement may be used to control several hazards.

e) For projects with existing systems, include existing safety requirements and indicate if they are maintained, updated, cancelled etc., and differentiate them from newly added and already existing safety requirements.

f) Include traceability to sources (clauses / references) of the safety requirements through mapping to relevant System Design documentation.

g) Include justification on the need for using each safety requirement including rationale that states its intent, justifies its inclusion or exclusion (if cancelled) and relevant assumptions that impact each safety requirement.

h) Include status of each safety requirement.

i) Include acceptance criteria for safety requirements including methods that were used to determine criteria.

j) Be written to conform to best practices i.e., each safety requirement is clear, accurate, complete, singular, unambiguous, free of grammatical/ spelling errors, free of contradiction, and able to be verified/validated etc.

Note: If there is difference between the safety requirements in the Hazard Record and Safety Requirements Specification then the Hazard Record shall take precedence as the live document; the Safety Requirements Specification can only be a snapshot at different project phases.

1.9 Quality Criteria

1.9.1 The quality management system used shall conform to ISO 9001:2015 rules or equivalent rules accepted by the Metrolinx Project Delivery Team and be appropriate for the system under consideration. The document shall identify all safety requirements defined in the risk assessment process with clear traceability to the relevant hazard(s).

1.10 Document Management

1.10.1 The Safety Requirements Specification is initially derived in Phase 4 (System Requirements), with requirements then apportioned to subsystems in Phase 5 (Architecture and Apportionment). The document is reviewed at the Single Design Solution (SDS) stage gate

by the project's Independent Safety Assessor (ISA) and is a requirement for stage gate progression.

1.10.2 The Safety Requirements Specification is dependent on the risk assessment activity conducted at Phase 3 (Risk Analysis). The outputs of the risk assessment lead the definition of the safety requirements. There shall be traceability between the Hazard Record (that began with the CMREA) and the safety requirements. In addition, the requirements specified are related closely to the development of the Safety Validation Plan, a document that is created in parallel to the Safety Requirements Specification during Phase 3.

1.10.3 Safety requirements are captured within various documents, rather than in a standalone deliverable. Where a project has an integrated system for managing requirements, it is good practice to include the safety requirements within the main requirements documents – this encourages people to read them alongside the other system requirements.

1.10.4 The level of detail for the safety requirements shall depend on the nature of the proposed system. Systems with novelty or complexity shall require more detailed requirements; systems using well understood components may be largely controlled through compliance to codes of practice.

1.10.5 The Safety requirements shall be managed as per MX-SEA-STD-007.

1.10.6 Once requirements are accepted at the Single Design Solution Review Gate, they must be version controlled and are subject to review as per the Contract Agreement.

1.10.7 Table 4 provides an overview of the Safety Requirements Specification document phases.

Document	Phase
Safety Requirements Specification	4 – System Requirements
Safety Requirements Specification (Refined)	5 - Apportionment

TABLE 4 DOCUMENT PHASES