METROLINX

Metrolinx
Safety Subsystem Requirements: Product Description

MX-SEA-PD-140

Revision 00

Date: April 2023

Safety Subsystem Requirements: Product Description

MX-SEA-PD-140

Publication Date: April 2023

Amendment Record

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

Preface

This is the first edition of the Metrolinx Safety Subsystem Requirements Product Description (MX-SEA-PD-140). 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 document that collects all the Safety requirements and targets that the subsystems under safety validation shall meet. Project proponents may need to produce 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 Subsystem Requirements **1**

1.1 Purpose 1
1.2 Applicability 1
1.3 Supporting Material 2
1.4 Products 2
1.5 Key Responsibilities 2
1.6 Competence 3
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 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
MXSD-SSA-L1-STD-0001	Railway Risk Assessment Standard	Supporting Standard
ISO 9001:2015	Quality management systems — Requirements	Supporting Standard
MX-SEA-GDC-140	Safety Subsystem Requirements Guidance	Guidance
MX-SEA-TPL-140	Safety Subsystem Requirements Template	Template
MXSD-SSA-L3-TK-0004	Hazard Management Toolkit	Template
MX-SEA-STD-007	Requirements Management	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 Abbreviations

Abbreviation	Full Name
ALARP	As Low As Reasonably Practicable
DRM	Design Requirements Manual
ISA	Independent Safety Assessor
RACI	Responsible, Accountable, Consulted and Informed
RAMS	Reliability Availability Maintainability and Safety
SCC	Safety Certification Committee
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 approved Project Chart of Accounts for the Program for the designated Cost Centre Manager.	CKH-QMA-FRM-003

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 (related to human health or to the environment)	BS EN 50126:2017
Safety Related Application Condition	Those conditions which need to be met in order for a system to be safely integrated and safely operated	BS EN 50126:2017
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 Subsystem Requirements

1.1 Purpose

1.1.1 The goal of developing the safety subsystem requirements is to determine the safety integrity required for each function and subsystem to ensure that the integrated system meets the overall safety integrity targets.

1.1.2 The goal of safety subsystem requirements document is to establish an agreed upon set of detailed safety requirements for a subsystem, including acceptance criteria and rationale. The safety subsystem will be assessed for compliance with the requirements during system verification and validation.

1.1.3 System Requirements are used to ensure that all design inputs (e.g. safety requirements of the existing system, operating conditions, Project goals, codes & standards, Metrolinx DRM, analysis outcomes including risk analyses) are incorporated into the design. Effectively establishing and managing requirements allows for traceability through the project lifecycle to support design, testing (verification & validation), acceptance and safe operation of the system.

1.1.4 Well defined requirements allows the Project Company (ie. the Contractor) and Metrolinx to have a shared understanding of the system being developed. This reduces the likelihood of scope revisions, rework due to misunderstandings or missed requirements, and improves the ability for project leadership to plan and schedule work.

1.1.5 The overall objective of the Safety Subsystem Requirements document is therefore to:

a) describe the methods used to define the safety subsystem requirements, as required to achieve acceptance by Metrolinx;

b) collect in one place all the subsystem safety requirements;

c) define the subsystem safety acceptance criteria; and

d) refer to the safety policy to define the strategy to follow where the subsystem does not satisfy the safety requirements and targets.

e) ensure that system level requirements are decomposed and allocated to the different subsystems

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.

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

1.2.3 If safety requirements are identified for a project that is non-significant under the Canadian Method for Risk Evaluation and Assessment for Railway Systems (CMREA) then this product shall be required to capture and manage those requirements.

1.3 Supporting Material

1.3.1 The Safety Subsystem Requirements template is located in MX-SEA-TPL-140.

1.3.2 Guidance on completing the Safety Subsystem Requirements is located in MX-SEA-GDC-140.

1.4 Products

1.4.1 The Safety Subsystem Requirements document 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 Subsystem Requirements document. Preparation of the Safety Subsystem Requirements document may be delegated; however, the Project Company is responsible for its content and quality.

1.5.2 The Project Company is the organization 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 System Review Panel (SRP) has delegated authority from the Safety Certification Committee (SCC) and is responsible for endorsing the Safety Subystem Requirements Document. The System Review Panel ensures that the Safety Subsystem Requirements document is compliant with the project requirements, applicable legislation, 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.

1.5.4 The Project Management may be performed by Metrolinx or may be contracted. For example, in a Design/Build Contract, Metrolinx Project Management may choose not to develop the Safety Subsystem Requirements themselves, but instead ensure contract provisions for the Safety Subsystem Requirements are met by the Project Company.

1.5.5 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 Subsystem Requirements whereas a contracted party responsible for RAMS would develop the Safety Subsystem Requirements as directed by the Project Management.

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 Subsystem Requirement document is available in MX-SEA-STD-100.

1.5.7 System and Subsystem Safety Requirements, and hazards must be transferred and accepted between Metrolinx and the Project Company throughout the asset lifecycle to ensure clear ownership of hazards and the actions to mitigate them.

1.6 Competence

1.6.1 Safety Subsystem Requirements shall be defined by personnel with technical competence in the subsystem 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 subsystem to assess whether the safety requirements shall fully mitigate the hazard to ALARP. The competency of the people involved in the process shall be recorded in the Safety Subsystem Requirements document.

1.7 Structure

1.7.1 The structure of the Safety Subsystem Requirements document is described in the Safety Subsystem Requirements Guidance document located in MX-SEA-GDC-140.

1.7.2 The document requires the following section titles:

a) Introduction;

b) Subsystem 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 structure of the Safety Subsystem Requirements document is described in the Safety Subsystem Requirements Guidance document located in MX-SEA-GDC-140.

1.8.2 As a minimum, it shall contain the following:

a) Functional Requirements and supporting Peformance Requirements, including required safety integrity for each subsystem and function. Functional Safety Requirements shall include:

   1) The expected functional behaviour of safety-related functions

   2) Safety Integrity Level (SIL) for Electronic systems

   3) The behaviour of the safety-related functions in case of failures, divided into the required safety integrity requirements and The required behaviour in case of 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,

3) Codes of Practice.

4) Interface requirements that manage how subsystems interact

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) Demonstrate traceability of the Safety Subsystem Requirements to system level safety requirements.

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 a rationale that states its intent, justifies exclusion (if cancelled), relevant assumptions that impact each requirement, and reference to any documents, or analysis used to develop the requirements.

g) Include status of each safety requirement as per MXSD-SSA-L3-TK-0004

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

i) 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.

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 Subsystem Requirements shall be produced at Phase 5 (Apportionment) following the Safety Requirements Specification developed at Phase 4 (System

Requirements). The document is reviewed at the Single Design Solution (SDS) stage gate by the Project Company's Independent Safety Assessor (ISA) and is a requirement for stage gate progression.

1.10.2 The Subsystem Safety Requirements document is dependent on the Safety Requirement Specification produced at Phase 4 (System Requirements) which is resulted from risk assessment activity conducted at Phase 3 (Risk Analysis). The outputs of the risk assessment lead the definition of the safety requirements at system level, the subsystem safety requirements shall describe the strategy to capture the safety requirements for the subsystem concerned.

1.10.3 Safety requirements are captured within various documents. 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 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.

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

1.10.7 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.

1.10.8 Table 4 provides an overview of the Safety Subsystem Requirements document phases.

Document	Phase
Safety Requirement Specification	4 – System Requirements
Safety Subsystem Requirements	5 – Apportionment

TABLE 4: DOCUMENT PHASES