Metrolinx
RAMS Risk Assessment Process

MX-SEA-STD-006

Revision 00
Date: 15/03/2022

RAMS Risk Assessment Process
MX-SEA-STD-006

Publication Date: March 2022

Preface

This is the first edition of the RAMS Risk Assessment process published as part of Metrolinx RAMS (Reliability, Availability, Maintainability and Safety) Standards. It describes a process for hazard and RAM risk source identification, analysis, and evaluation of risk associated with new design and changes to the design, operation, or maintenance of Metrolinx assets, systems, and subsystems. The application of this process assures acceptable RAM and safety risk levels are met.

The purpose of Metrolinx RAMS Standards is to formalize the framework to adequately manage RAMS performance of all Metrolinx assets for the entire life cycle starting from concept, through risk assessments, stage gate approvals, design and specifications, construction, systems integration, validation, acceptance, operation, maintenance, performance monitoring and decommissioning. Metrolinx RAMS standards, which are built as an adaptation of European Standard EN 50126-1:2017, provide internal Metrolinx staff and external stakeholders involved in design, construction, operation and maintenance of Metrolinx assets with a common understanding and a systematic process for RAMS management. Ultimately, they provide a systematic approach for specifying RAMS requirements and demonstrating that these requirements are achieved.

This document was developed by the Systems Engineering Assurance Office, Engineering and Asset Management Division, Rapid Transit Operations, Metrolinx.

Suggestions for revision or improvements can be sent to the Metrolinx Systems Engineering Assurance office, Attention: Director of Systems Engineering Assurance who shall introduce the proposed changes to the Metrolinx Systems Engineering Assurance office. The Director of the Systems Engineering Assurance office ultimately authorizes the changes. Be sure to 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.

March 2022

Amendment Record

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

Contents

Section **Page**

Preface ..... **i**

Documents **1**

Acronyms and Abbreviations **2**

Definitions **3**

1. Overview **9**
1.1 Purpose 9
1.2 Scope 9
1.3 Key Responsibilities 11

2. The RAMS Risk Assessment Process **11**
2.1 RAMS Risk Assessment Process & The System Life Cycle Flow Chart 11
2.2 RAMS Risk Assessment Process & The System Life Cycle Narrative 13
2.3 RAMS Risk Analysis & Evaluation Process Flow Chart 15
2.4 RAMS Risk Analysis & Evaluation Process Narrative 16

3. Input to RAMS Risk Assessment **17**
3.1 Input Information Sources 17
3.2 Reference Material 17
3.3 Application of RAMS Risk Assessment 18

4. Risk Source Identification & Classification **20**
4.1 Overview 20
4.2 Risk Source Identification (includes consequence analysis) 20
4.3 Risk Source Classification 23

5. Risk Analysis & Risk Acceptance Principles (RAP) **25**
5.1 Overview 25
5.2 Codes of Practice 26
5.3 Similar Reference System 26
5.4 Explicit Risk Estimation 27

6. Risk Evaluation & Treatment **29**
6.1 Overview 29
6.2 Comparison with Risk Acceptance Criteria (RAC) 29
6.3 Risk Treatment 30
6.4 Risk Transfer 31

7. RAMS Risk Assessment Deliverables & Output to Other Processes **33**
7.1 Overview 33
7.2 RAMS Risk Assessment Deliverables 33
7.3 Output to Other Processes 33

Appendix A Rail Network Core Hazards List **36**

Figures

Figure 1-1 The interrelation of RAMS management process and system life cycle - the V-Cycle representation [Source: BS EN 50126-1:2017] 10
Figure 2-1 The RAMS Risk Assessment Process throughout the system life cycle 12
Figure 2-2 The RAMS Risk Analysis & Evaluation Process 15
Figure 4-1 Example of a context diagram for the replacement of a switch machine [SOURCE: Network Rail CSM-RA Awareness Training] 22
Figure 4-2 Example of a Risk Model [Source: BS EN 50126-2:2017] 23

Tables

Table 0-1 Supporting Documents 1
Table 0-2 Acronyms and Abbreviations 2
Table 0-3 Definitions 3
Table 4-1 Summary of Risk Source Identification & Classification Fields 20
Table 5-1 Summary of Risk Analysis Fields 25
Table 6-1 Summary of Risk Evaluation, Treatment, and Transfer Fields 29
Table 7-1 Template for Hazard Logs & RAM Risk Source Logs 35

Documents

TABLE 0-1 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)	Parent Standard
BS EN 50126-2:2017	Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety	Parent Standard
CKH-ASMT-PRC-001	Asset Data and Information Standards	Reference
CKH-ENG-FRM-008	Standards Deviation Request Form	Reference
CKH-ENG-PRC-001	Procedure for Requesting Deviations to Metrolinx Standard Technical Requirements	Reference
CPG-QAT-FRM-106	CPG Terms Glossary	Reference
CSA EXP11:20	Canadian method for risk evaluation and assessment for railway systems (CMREA)	Related Process
Commission Implementing Regulation (EU) No. 402/2013	The Common Safety Method (CSM) for Risk Evaluation and Assessment Note: as amended by the Commission Implementing Regulation (EU) 2015/1136 of July 13, 2015	Reference
MX-SEA-STD-001	FRACAS Process	Related Process
MX-SEA-STD-002	FMECA Process	Related Process
MX-SEA-STD-003	RAM Plan Process	Related Process
MX-SMS-G001	Metrolinx Safety Department Risk Assessment Guide	Reference
CKH-RISK-PRC-001	Capital Projects Group Risk Management Procedure	Reference
September 11, 2019	Enterprise Risk Management Policy	Reference
September 2019	Enterprise Risk Management Framework	Reference
TBD	Roles and Responsibilities Matrix (RACI) for RAMS tasks	Document

Acronyms and Abbreviations

TABLE 0-2 ACRONYMS AND ABBREVIATIONS

Acronym	Full Name
ALARP	As Low As Reasonable Practicable
CCF	Common Cause Failure
CLOS	Customer Level of Service
CMREA	Canadian Method for Risk Evaluation & Assessment
CoP	Code of Practice
CPG	Capital Projects Group
CSM or CSM-RA	Common Safety Method
DC	Direct Current
ERE	Explicit Risk Estimation
ETA	Event Tree Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability study
KPI	Key Performance Indicator
OEM	Original Equipment Manufacturer
PSO	Phase Shift Overlay
RAC	Risk Acceptance Criteria
RAM	Reliability, Availability and Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RAP	Risk Acceptance Principle

Definitions

TABLE 0-3 DEFINITIONS

Term	Definition	Source
Acceptance	Status achieved by a product, system or process once it has been agreed that it is suitable for its intended purpose.	BS EN 50126-1:2017
Accident	An unwanted or unintended sudden event or a specific chain of such events that have harmful consequences, including consequences to people, property, or the environment.	CSA EXP11:20 Note: railway specific categories of accidents removed from definition to be applicable for all Metrolinx
Approval	Permission for a product or process to be marketed or used for stated purposes or under stated conditions.	BS EN 50126-1:2017
Asset	Any physical or tangible item that has potential or actual value to Metrolinx (excluding intellectual property, inventory to be sold, human resources, and financial instruments), as well as IT systems and software.	CKH-ASMT-PRC-001 Note: refer to CKH-ASMT-PRC-001 Asset Data and Information Standards for additional asset-related definitions.
Asset Class Teams	Metrolinx business units who have been designated as being accountable for the completeness and accuracy of information about a given class of assets.	CKH-ASMT-PRC-001
Asset Hierarchy	Hierarchical grouping of Metrolinx assets, organized within parent-child relationships.	CKH-ASMT-PRC-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 50126-1:2017

TABLE 0-3 DEFINITIONS

Term	Definition	Source
Barrier	[1] Physical or non-physical means, which reduces the frequency of a hazard and/or a likely accident arising from the hazard and/or mitigates the severity of likely accidents arising from the hazard. [2] A technical, operational or organizational risk control measure outside the system under assessment that either reduces the frequency of occurrence of a hazard or mitigates the severity of the potential consequence of that hazard. Note: these definitions specify hazards and accidents, but also apply for other RAM related risk sources and consequences.	[1] BS EN 50126-1:2017 definition of "safety barrier" (NOTE added) [2] CSA EXP11:20 (NOTE added)
Code of Practice	A written set of rules that, when correctly applied, can be used to control one or more specific hazards and RAM risk sources.	CSA EXP11:20 (adapted to specify "RAM Risk sources" in addition to hazards)
Common Cause Failure	Failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause.	BS EN 50126-1:2017
Consequence Analysis	Analysis of events which are likely to happen after a hazard or RAM risk source has occurred.	BS EN 50126-1:2017 (adapted to add "RAM risk source" in addition to hazards)
Corrective maintenance	Maintenance carried out after fault detection to effect restoration.	BS EN 50126-1:2017
Design	Activity applied in order to analyze and transform specified requirements into acceptable solutions.	BS EN 50126-1:2017
Error	Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition.	BS EN 50126-1:2017
Failure	Loss of ability to perform as required.	BS EN 50126-1:2017
Failure Mode	Manner in which failure occurs.	BS EN 50126-1:2017
Fault	Abnormal condition that could lead to an error in a system.	BS EN 50126-1:2017
Function	Specified action or activity which can be performed by technical means and/or human beings and has a defined output in response to a defined input.	BS EN 50126-1:2017

TABLE 0-3 DEFINITIONS

Term	Definition	Source
Incident	An unwanted or unintended event with a potential of causing harm to people, property and/or environment. Events where harm to people, property and/or environment has occurred, are referred to as 'accidents'.	N/A
Interfaces	All points of interaction during a system or subsystem life cycle, including operation and maintenance, where different participants of the Metrolinx network will work together in order to manage the risks. This includes points of interaction between or among participants, between or among subsystem components, between or among subsystems, and between or among systems.	[2] CSA EXP11:20 (adapted by changing "rail sector" to "Metrolinx network")
Hazard	Condition that could lead to an accident. Note: see definition of "RAM risk source" for conditions that could lead to an incident or failure. RAM risk source is RAM equivalent to hazard as covered in EN50126-1:2017.	BS EN 50126-1:2017 (NOTE added)
Hazard Analysis	Process of identifying hazards and analysing their causes, and the derivation of requirements to limit the likelihood and consequences of hazards to a tolerable level. Note: similar process aspects are also considered in risk assessment. In this standard the term is applied in life cycle phases after "requirements specification".	BS EN 50126-1:2017
Hazard Log	Document in which hazards are identified, decisions made, solutions adopted and their implementation status are recorded or referenced. Note: see definition of "RAM risk source log" for RAM equivalent to hazard log.	BS EN 50126-1:2017 (NOTE added)
Integration	Process of assembling the elements of a system according to the architectural and design specification, and the testing of the integrated unit.	BS EN 50126-1:2017
Investment Panel (Metrolinx)	The Investment Panel ("IP") is management's ultimate accountable governance body for benefits management of business cases across the entire capital project lifecycle.	Investment Panel ToR (03-1-2019)
Life Cycle	Series of identifiable stages through which an item goes, from its conception to disposal.	BS EN 50126-1:2017

TABLE 0-3 DEFINITIONS

Term	Definition	Source
Likelihood	Chance of something happening. Note: "likelihood" is sometimes referred to as "probability" or "frequency".	IEC 60812:2018 (NOTE added)
Maintainability	Ability to be retained in, or restored to, a state to perform as required, under given conditions of use and maintenance.	BS EN 50126-1:2017
Maintenance	Combination of all technical and management actions intended to retain an item in, or restore it to, a state in which it can perform as required.	BS EN 50126-1:2017
Network	[1] An interconnected or interrelated group of assets, systems, and subsystems needed to ensure safe and reliable operation or service. [2] The lines, stations, terminals, and all kinds of fixed equipment needed to ensure safe and continuous Metrolinx operation.	[1] N/A [2] CSA EXP11:20 (adapted to replace "operation of the Railway System" with "Metrolinx Operation")
Preventive maintenance	Maintenance carried out to mitigate degradation and reduce the probability of failure.	BS EN 50126-1:2017
RAM Plan	Documented set of time scheduled activities, resources and events serving to implement the organizational structure, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given RAM requirements relevant to a given contract or project.	BS EN 50126-1:2017
RAM risk source	Condition that could lead to an incident, service interruption, or failure. Note: see definition of "Hazard" for safety equivalent.	N/A
RAM risk source log	Document in which RAM risk sources are identified, decisions made, solutions adopted and their implementation status are recorded or referenced. Note: see definition of "Hazard log" for safety equivalent to RAM risk source log.	N/A
Reliability	Ability to perform as required, without failure, for a given time interval, under given conditions.	BS EN 50126-1:2017
Repair	Direct action taken to effect restoration.	BS EN 50126-1:2017

TABLE 0-3 DEFINITIONS

Term	Definition	Source
Residual Risk	Risk remaining after risk control measures have been taken.	BS EN 50126-1:2017
Restoration	Bringing an item into a state where it regains the ability to perform its required function after a fault.	BS EN 50126-1:2017
Risk	Combination of expected frequency of loss and the expected degree of severity of that loss. Note: the term "likelihood" is used in most Metrolinx risk documentation in place of "frequency".	BS EN 50126-1:2017 (NOTE added)
Risk Acceptance Criteria (RAC)	The terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further.	CSA EXP11:20
Risk Acceptance Principle	The rules used in order to determine whether or not the Risk related to one or more specific hazards and RAM risk sources is acceptable.	CSA EXP11:20 (adapted to add "RAM risk sources" in addition to hazards)
Risk Analysis	Systematic use of available information to identify hazards and RAM risk sources, and to estimate the risk.	BS EN 50126-1:2017 (adapted to add "RAM risk sources" in addition to hazards)
Risk Assessment	Overall process comprising a risk analysis and a risk evaluation.	BS EN 50126-1:2017
Risk Based Approach	Process for ensuring the safety of products, processes and systems through consideration of the hazards and their consequent risks. Note: the approach is applicable to RAM aspects in an analogous manner.	BS EN 50126-1:2017
Risk Evaluation	Procedure based on the risk analysis to determine whether the tolerable risk has been achieved.	BS EN 50126-1:2017
Risk Management	Systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating and controlling risk.	BS EN 50126-1:2017

TABLE 0-3 DEFINITIONS

Term	Definition	Source
Risk Treatment	Process for identifying and implementing measures to reduce the level of risk resulting from hazards and RAM risk sources. Note: in the context of RAMS Risk Assessment, risk treatment is sometimes referred to as "risk response", "risk control", "risk reduction", or "risk mitigation" as a process to modify the likelihood and/or severity of hazards and RAM risk sources.	N/A
Safe State	Condition which continues to preserve safety.	BS EN 50126-1:2017
Safety	Freedom from unacceptable risk. Note: risk related to human health or to the environment.	BS EN 50126-1:2017
Safety Authority	Body responsible for delivering the authorization for the operation of the safety-related system.	BS EN 50126-1:2017
Safety Case	Documented demonstration that the product (e.g. a system, subsystem or equipment) complies with the specified safety requirements.	BS EN 50126-1:2017
Safety Plan	Documented set of time scheduled activities, resources and events serving to implement the organization, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project.	BS EN 50126-1:2017
Service Interruption	A service interruption is any failure resulting in the inability to provide a service to the normal standard (i.e. unplanned schedule changes, train/bus delays and cancellations, customer-facing device unavailable, etc.)	N/A
Severity	Relative ranking of potential or actual consequences of a failure. Note: the term "Impact" is sometimes used in place of the term "Severity" in some Metrolinx processes and documentation.	IEC 60812:2018 (NOTE added)
Subsystem	Part of a system, which is itself a system.	BS EN 50126-1:2017
System	Set of interrelated elements considered in a defined context as a whole and separated from their environment.	BS EN 50126-1:2017

For additional terms and definitions, please refer to the *CPG Terms Glossary* (refer to *CPG-QAT-FRM-106*, *CPG Terms Glossary*, for more details).

1. Overview

1.1 Purpose

1.1.1 The purpose of the RAMS Risk Assessment Process is to provide a standardized process for evaluating asset, system, and subsystem related hazards and RAM risk sources and documenting the treatment actions required to minimize risk in design. This, in turn, maximizes RAMS performance in operation & maintenance and ensures Metrolinx enterprise and network level risk tolerance and CLOS KPIs are met.

1.1.2 The RAMS Risk Assessment Process follows the Canadian Method for Risk Evaluation and Assessment (CMREA) [ref. CSA EXP11:20] for risk analysis through codes of practice, similar reference system, and/or explicit risk estimation, where past explicit risk estimation for existing assets, systems, and subsystems may then be used as similar reference systems for analysis of new or redesigned assets, systems, and subsystems.

1.1.3 This process also results in a log of all identified risk sources, which in combination with well-defined risk tolerance(s) helps to guide risk management decision-making.

1.2 Scope

1.2.1 The RAMS Risk Assessment Process is only applicable to RAMS risk associated with any new design or any change to the design, operation, or maintenance of Metrolinx assets/systems/subsystems [ref. Section 3.3 for details on when RAMS Risk Assessment should be applied].

1.2.2 The RAMS Risk Assessment Process applies to all phases of the system life cycle [Figure 1-1]. Planning and documenting the scope, boundaries, risk acceptance criteria, and other inputs for the RAMS Risk Assessment begins at phase 1 and continues through the phase 2. The initial risk analysis and evaluation is performed at phase 3 to define system requirements to meet the defined risk acceptance criteria for phase 4 and phase 5. Any significant change to the asset/system/subsystem during phase 4 or phase 5 must be re-assessed to ensure the risk acceptance criteria are met through the specified design requirements. Similarly, any significant change in life cycle phases 6 thorough 12 must be re-assessed and treatment action taken to ensure the design meets the required risk acceptance criteria.

Note: If risk acceptance criteria cannot be achieved, the risk acceptance criteria may be revised or the project may be rejected, however the processes of risk acceptance criteria revision and project rejection are out of scope of the RAMS Risk Assessment Process.

1.2.3 Further details on the application of the RAMS Risk Assessment Process through the system life cycle can be found in sections 2.1 and 2.2 of this document and suggested sources of input information and reference material are detailed in section 3.

1.2.4 The RAMS risk analysis & evaluation is composed of the following major steps. Details on the application of these steps can be found in section 2.3 & 2.4 of this document.

a) Risk source identification & classification [ref. Section 4 for details]

b) Selection of Risk Acceptance Principle(s) (RAP) & risk analysis [ref. Section 5 for details]

c) Risk evaluation by comparison with risk acceptance criteria [ref. Section 6.2 for details]

d) Identification and selection of risk treatment action(s) [ref. Section 6.3 for details]

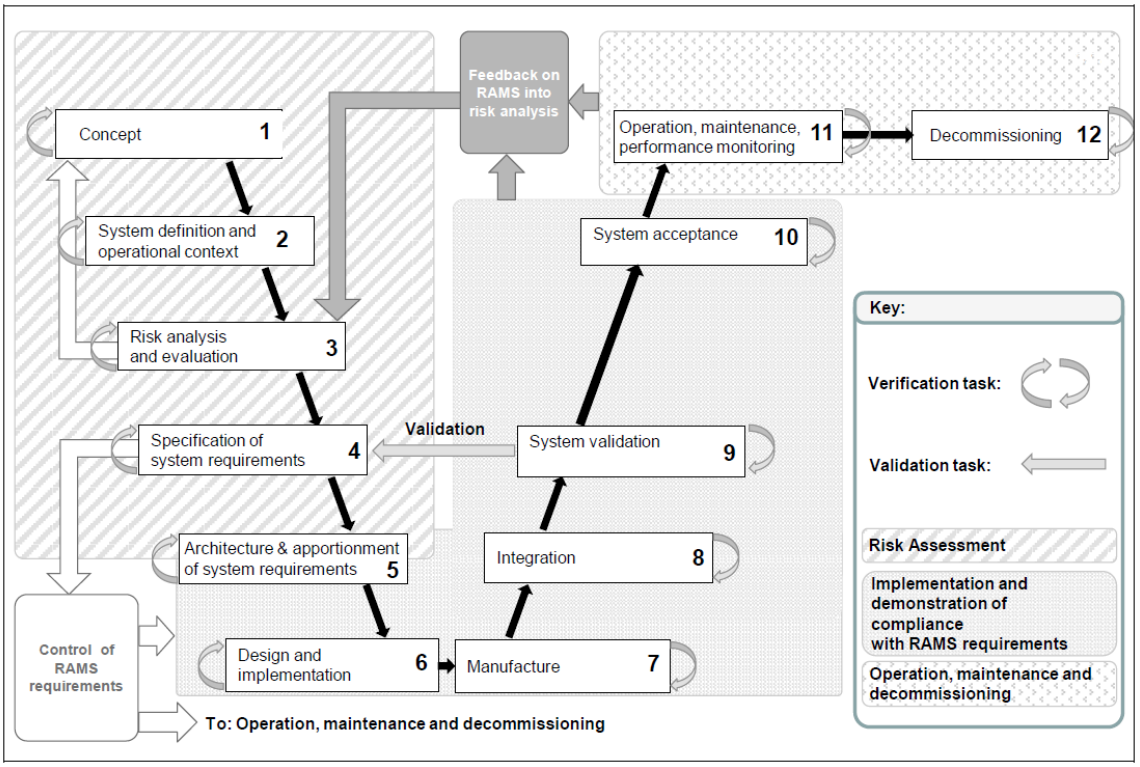
1.2.5 The output deliverables from the RAMS Risk Assessment Process are detailed in section 7 of this document, which include and are not limited to:

a) Hazard Log including Safety Requirements

b) RAM Risk Source Log including RAM Requirements

1.2.6 These deliverables in turn provide an input to many other processes, as detailed in section 7.3. Additionally, RAMS Risk Assessment documentation for assets in phases 11 & 12 provide valuable information for similar new design and design change decisions to reduce the analysis required for future RAMS Risk Assessments of similar systems.

Figure 1-1 The interrelation of RAMS management process and system life cycle - the V-Cycle representation [Source: BS EN 50126-1:2017]



1.2.7 The Metrolinx Enterprise Risk Management Framework defines five categories of risk:

a) Project risks – risks relating to a project being completed on time and on budget.

b) Operational risks – risks relating to on-going operations.

c) Financial risks – Risks relating to and/or impacting funding of projects and operations, liquidity, financial reporting and movements in price of products and services, interest rates, currencies and commodities.

d) Strategic risks – Risks that threaten to disrupt the assumptions at the core of Metrolinx's strategy resulting in potential for financial loss or reputational damage.

e) Safety risks – Risks to the safety of Metrolinx's customers, staff, contractors and communities it operates and builds in.

1.2.8 The RAMS Risk Assessment Process concerns risks that fit within the enterprise risk categories of "operational risks" and "safety risks", with a secondary concern for "strategic risks" arising from asset performance (i.e. strategic financial risks associated with cost of maintenance).

1.2.9 The CMREA is concerned with the category of "safety risks" associated with hazards and accidents at the network level. The RAMS Risk Assessment Process is concerned with hazards and accidents at the asset, system, and subsystem levels. Therefore, CMREA network level risk assessment provides an input to the RAMS risk assessment at the assets, systems, subsystems level which together make up the network.

a) Residual risks at each level of assessment may impact each other (i.e. lower reliability systems result in lower performance at the network level and lower enterprise brand reputation). This relationship is managed by defining risk acceptance criteria and performance requirements at the network and enterprise levels to ensure that assets, systems, and subsystems are designed to meet the applicable network and enterprise level RAMS requirements.

1.2.10 The other enterprise risk categories of "Project Risk" and "Financial Risks" are out of scope of the RAMS Risk Assessment Process. Refer to CPG Risk Management Procedure [ref. CKH-RISK-PRC-001] for instruction on risk assessment for these risk categories.

1.3 Key Responsibilities

Note: This process is not specific to any contract type. For detailed responsibilities based on different contract types, refer to RAMS RACI document.

1.3.1 The RAMS team owns this process document and is responsible for ensuring this process meets or exceeds industry standards and applicable regulations, as well as ensuring compliance within Metrolinx.

1.3.2 For any new design, the individual that is responsible for the asset/system/subsystem design, at the stages when RAMS Risk Assessment is required, is responsible for demonstrating compliance with this process. This individual may change as the product goes through the system life cycle [ref. Figure 2-1 for details on the application on RAMS Risk Assessment through the system life cycle].

Note: This individual may be internal to Metrolinx or may be an external contractor (i.e. Project Co.)

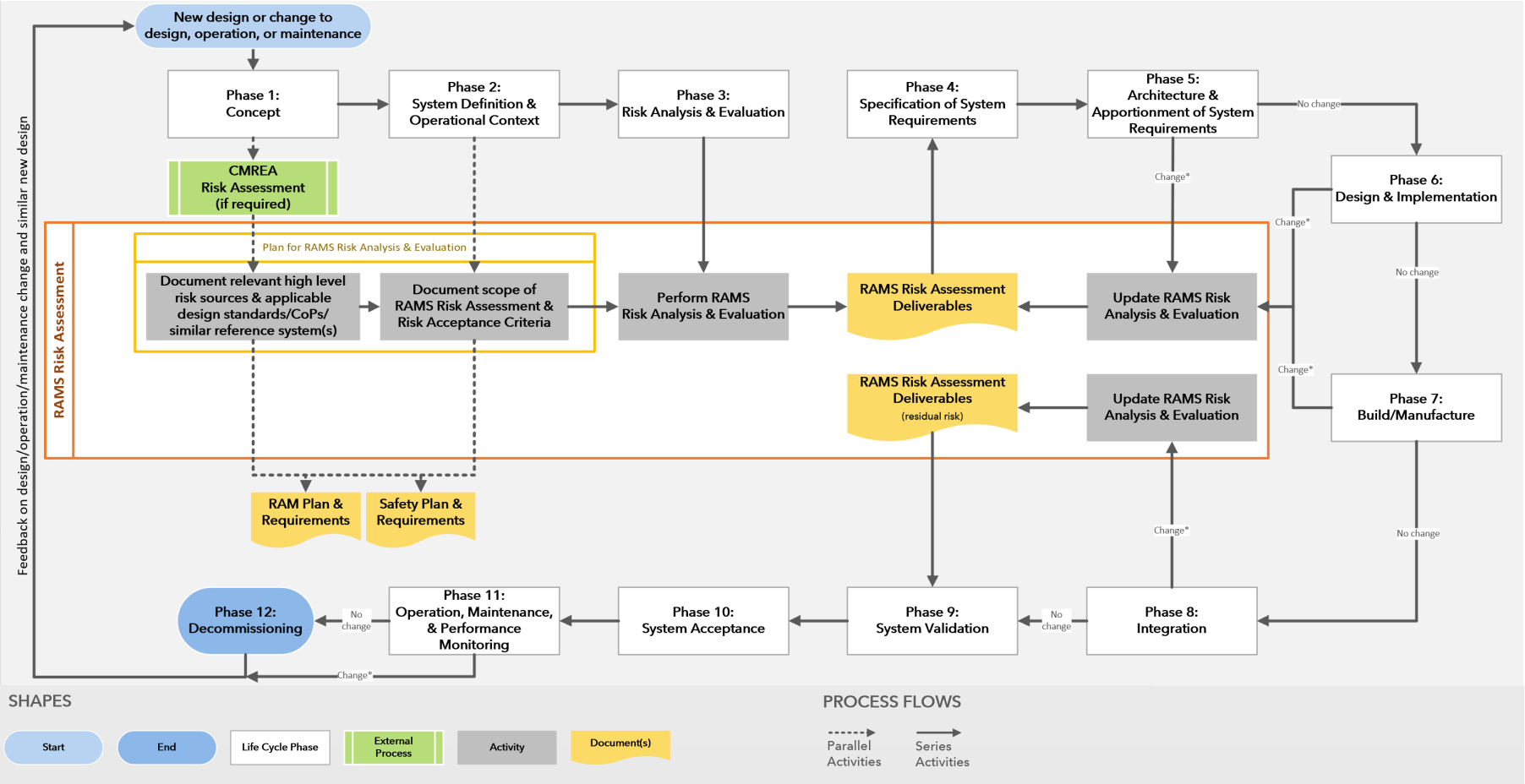
1.3.3 For any change to the design, operation, or maintenance of existing assets/systems/subsystems, the Asset Class Team is responsible for demonstrating compliance with this process.

2. The RAMS Risk Assessment Process

2.1 RAMS Risk Assessment Process & The System Life Cycle Flow Chart

2.1.1 FIGURE 2-1 illustrates the RAMS Risk Assessment Process throughout the system life cycle[1].

Figure 2-1 The RAMS Risk Assessment Process throughout the system life cycle



[1]For additional details on process activities, please refer to the process narrative on subsequent page(s).

*Change may occur at any point in life cycle at which point the RAMS risk analysis & evaluation shall be updated, only very likely occurrences are shown here for illustrative purposes. Change may result from new information, change to assumptions, change to design or operating conditions, change to risk acceptance criteria, etc. If the change does not alter any existing risk or introduce new risk, these results are to be documented and no further assessment is required at that time. This process does not apply for project schedule changes and any other changes which do not impact the design, interfaces, operating conditions, or maintenance of the asset/system/subsystem.

Note: this process map details RAMS Risk Assessment only, there are other RAMS deliverables associated with each life cycle phase detailed in other RAMS processes.

2.2 RAMS Risk Assessment Process & The System Life Cycle Narrative

2.2.1 RAMS Risk Assessment shall be initiated or revised for any new design or any change to design, operation, or maintenance of Metrolinx assets, systems, and subsystems. Although the RAMS Risk Analysis and Evaluation is first conducted at life cycle phase 3, the overall RAMS Risk Assessment Process is integrated throughout the entire life cycle. The process starts with planning for the analysis & evaluation as soon as the concept is defined at Phase 1 and continues with an iterative analysis & evaluation as additional details become available and as changes arise through the life cycle. The following steps describe the RAMS Risk Assessment Process throughout the system life cycle:

Note: this process narrative details RAMS Risk Assessment only, there are additional RAMS deliverables associated with each life cycle phase detailed in other RAMS Processes and summarized in BS EN 50126-1:2017.

1) Life Cycle Phase 1 – Concept: planning for the RAMS Risk Assessment should begin as early as possible in the system life cycle, including documentation of relevant high-level risk sources & requirements resulting from the network level CMREA risk assessment process and compiling a list of relevant reference material [ref. Section 3.2 for details] to be used in performing the RAMS Risk Analysis & Evaluation (starting at life cycle phase 3).
2) Life Cycle Phase 2 – System Definition & Operational Context: all the necessary input information sources required to perform the initial iteration of the RAMS Risk Analysis & Evaluation are compiled and documented, including the scope of the analysis and the risk acceptance criteria [ref. Section 3 for details]
3) Life Cycle Phase 3 – Risk Analysis & Evaluation: the Initial RAMS Risk Analysis and Evaluation is performed [ref. Sections 2.3 & 2.4 for details].

Note: any changes determined to not add or alter risk during the following life cycle phases shall be documented with justification.

4) Life Cycle Phase 4 – Specification of System Requirements: Deliverables from the RAMS Risk Analysis & Evaluation process include system and/or subsystem requirements to meet acceptable levels of risk in the design as input to specifying the system requirements.
5) Life Cycle Phase 5 – Architecture & Apportionment of System Requirements: When change occurs, the affected portion(s) of the RAMS Risk Analysis & Evaluation shall be updated. This includes the case where previously specified risk treatment measures cannot be fully complied with.
6) Life Cycle Phase 6 – Design & Implementation: When change occurs, the affected portion(s) of the RAMS Risk Analysis & Evaluation shall be updated. This includes the case where previously specified risk treatment measures cannot be fully complied with.
7) Life Cycle Phase 7 – Build/Manufacture: When the build is completed perfectly to the design specifications, no update to the RAMS Risk Analysis & Evaluation is required at this life cycle phase. However, if any change occurs during the build phase, then the

RAMS Risk Assessment shall be updated to ensure the risk acceptance criteria are met prior to integration.

8) Life Cycle Phase 8 – Integration: When change occurs, the affected portion(s) of the RAMS Risk Analysis & Evaluation shall be updated. This includes the case where previously specified requirements cannot be fully complied with. This update ensures that the residual risk is understood and documented prior to system validation and to inform system acceptance.

9) Life Cycle Phase 9 – System Validation: The residual (final) RAMS Risk Assessment provides an input to the system validation process through documentation that the design meets the specified requirements.

10) Life Cycle Phase 10 – System Acceptance: The residual (final) RAMS Risk Assessment provides an input to the system acceptance process through documentation that acceptable levels of risk have been achieved.

Note: if the system cannot be validated or accepted, the life cycle process may return to an earlier phase, at which point the RAMS Risk Assessment may require update.

11) Life Cycle Phase 11 – Operation, Maintenance & Performance Monitoring: Risks transferred to operations and maintenance shall be managed through performance monitoring [ref. MX-SEA-STD-001 FRACAS process]. Any change to design, operation, or maintenance during this life cycle phase shall trigger a revision to the RAMS risk assessment [ref. paragraph 2.2.1]. Additionally, prior RAMS Risk Assessment for existing Metrolinx assets, systems, and subsystems become resources for future RAMS Risk Assessment as similar reference systems [ref. Section 5.3 for details].

Note: any assumptions shall be validated with actual performance data prior to use as a similar reference system in RAMS Risk Analysis & Evaluation Process.

12) Life Cycle Phase 12 - Decommissioning: Prior RAMS Risk Assessment for decommissioned Metrolinx assets, systems, and subsystems become resources for future RAMS Risk Assessment as similar reference systems [ref. Section 5.3 for details].

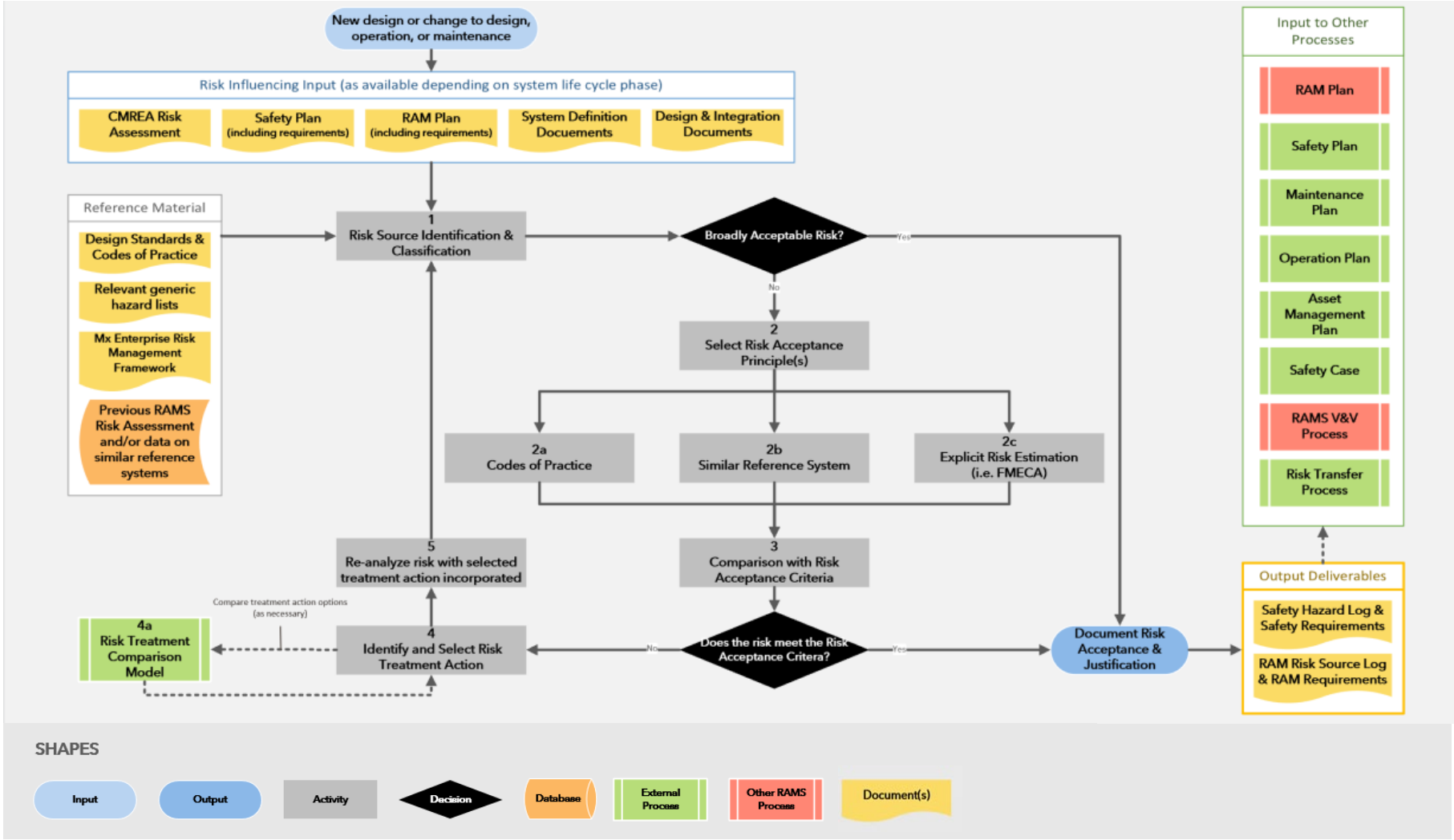
Note: any assumptions shall be validated with actual performance data prior to use as a similar reference system in RAMS Risk Analysis & Evaluation Process.

END: The process ends here

2.3 RAMS Risk Analysis & Evaluation Process Flow Chart

2.3.1 FIGURE 2-2 illustrates the RAMS Risk Analysis & Evaluation Process[2].

Figure 2-2 The RAMS Risk Analysis & Evaluation Process



[2] For additional details on process activities, please refer to the process narrative on subsequent page(s).

2.4 RAMS Risk Analysis & Evaluation Process Narrative

2.4.1 RAMS Risk Analysis and Evaluation shall be initiated or revised for any new design or any change to design, operation, or maintenance of Metrolinx assets, systems, and subsystems. The following steps describe the RAMS Risk Analysis & Evaluation Process:

1) Identify [ref. Section 4.2 for details] and classify [ref. Section 4.3 for details] all relevant hazards and RAM risk sources. For broadly acceptable risk, proceed to step 5), otherwise proceed to step 2).

2) For each hazard and RAM risk source identified as not broadly acceptable risk, select, document, and apply the appropriate Risk Acceptance Principle(s) (RAP) to analyze the risk. The RAP should be applied in the following order as applicable to reduce the risk to an acceptable level while avoiding excessive analysis required for Explicit Risk Estimation where it is not required. Any assumptions made as part of this analysis shall be documented.

   a) Codes of Practice [ref. Section 5.2 for details]
   b) Similar Reference System [ref. Section 5.3 for details]
   c) Explicit Risk Estimation [ref. Section 5.4 for details]

Note: at least one RAP must be used to analyze each source of risk (unless broadly acceptable risk).It is possible that multiple RAPs may apply to an individual source of risk, and very likely that each RAP will be applicable to at least one source of risk when conducting a RAMS Risk Assessment, particularly for complex assets/systems/subsystems design.

3) Compare the results of the risk analysis to the applicable Risk Acceptance Criteria (RAC). If the risk is within the RAC, proceed to step 5), otherwise proceed to step 4).

4) Where the risk exceeds the RAC, identify, document, and select treatment action(s) to reduce the risk.

   a) If multiple possible treatment action options are identified, risk treatment comparison models should be used as appropriate to inform selection decision [ref. BS EN 50126-2:2017 Annex A for methods to define Risk Acceptance Criteria, where ALARP is the Metrolinx accepted standard method]

5) Once treatment actions are selected, return to step 1) to identify any new sources of risk introduced by the treatment action, and proceed to re-analyze and re-evaluate the risk with the treatment action applied.

Note: this process may take several iterations, and if the RAC cannot be met then the change may be cancelled or the RAC may be revised to accept a higher level of risk in order to proceed. The processes of cancelling changes and altering the RAC are outside of the scope of the RAMS Risk Assessment Process.

6) Document and justify the acceptance of the residual sources of risk and level of risk within the design, including all requirements to meet the accepted residual risk.

END: The process ends here

3. Input to RAMS Risk Assessment

3.1 Input Information Sources

3.1.1 Input information sources change and evolve through the system life cycle. Any change to the input information sources at any time during the system life cycle shall result in an update to the RAMS Risk Analysis & Evaluation.

3.1.2 These information sources include, but are not limited to:

a) System definition & requirements documentation, including operational context. In accordance with the CMREA, this documentation shall specify at least the following details:

1) System objective (intended purpose);

2) System functions and elements, where relevant (including human, technical and operational elements);

3) System boundary including other interacting systems;

4) Physical interfaces (interacting systems) and functional interfaces (functional input and output);

5) System environment (for example energy and thermal flow, shocks, vibrations, electromagnetic interference, and operational use);

6) Existing safety measures and, after the necessary relevant iterations, specification of the network level Hazard Log & Safety Requirements identified by the CMREA Risk Assessment process; and

7) Assumptions that determine the limits for the RAMS Risk Assessment.

b) RAM Plan & RAM Policy, including RAM requirements [ref. MX-SEA-STD-003 RAM Plan Process for details]

c) Safety Plan & Safety Policy, including Safety requirements

d) Subsystem design documentation, including system requirements apportionment to sub-systems

e) Metrolinx Core Hazard Lists [ref. Appendix A for Rail Network Core Hazard List]

3.2 Reference Material

3.2.1 Reference material sources may change and evolve through the system life cycle. Any change to the reference material at any time during the system life cycle shall result in an update to the RAMS Risk Assessment.

3.2.2 These information sources include, but are not limited to:

a) Metrolinx Enterprise Risk Management Policy and Enterprise Risk Management Framework (including Risk Appetite/Tolerance and Risk Acceptance Criteria).

b) Previous RAMS Risk Assessment and/or data on past performance of similar systems [ref. MX-SEA-STD-001 FRACAS Process]

c) Applicable and relevant industry design standards and Codes of Practice

d) Relevant industry generic hazard lists (i.e. Rail Safety and Standards Board generic hazards for rolling stock, etc.)

3.3 Application of RAMS Risk Assessment

3.3.1 RAMS Risk Assessment shall be applied for all new assets/systems/subsystems.

3.3.2 For changes during life cycle phase 11 [FIGURE 1-1] "operation, maintenance, and performance monitoring", RAMS Risk Assessment applies to changes of technical, operational, and organizational nature, however for organizational changes, only those changes which could impact the operation or maintenance of the asset/system/subsystem under consideration shall be taken into account for RAMS Risk Assessment.

3.3.3 The potential impact of the change in question on the reliability, availability, maintainability, and/or safety shall be considered based on the following criteria as per CSA EXP11:20 CMREA:

a) criticality: a credible worst-case scenario in the event of failure of the design under assessment;

b) novelty used in implementing the change: this concerns both what is innovative in the industry and what is new for Metrolinx;

c) complexity of the change;

d) monitoring: the inability to monitor the implemented change throughout the system lifecycle and intervene appropriately;

e) reversibility: the inability to revert to the asset/system/subsystem before the change; and

f) additionality: assessment considering all recent changes to the design under assessment.

3.3.4 Examples where RAMS Risk Assessment applies at Metrolinx include but are not limited to:

a) Project de-scoping to accommodate project budget reduction that results in technical change. Examples include layout change or a floor removal impacting maintenance access and utilities shutoff valves accessibility, or reduction in the number of station elevators impacting availability and safety for accessibility and emergency egress, etc.

b) Design change, including introduction, elimination, or change of technology, such as USRC re-signalling project, replacing DC track circuits with PSO track circuits for track electrification, replacement of a non-OEM part with a similar part from an aftermarket supplier, installation of condition monitoring systems for existing assets, etc.

c) Maintenance changes such as introducing new maintenance procedures, changing preventive maintenance frequency, changing maintenance instruction checklists, etc.

d) Service increase or decrease, including introduction of a new service

e) New failure mode or operational safety concern identified through performance monitoring [ref. MX-SEA-STD-001 FRACAS Process] or through incident/accident reporting, as available.

f) Changes to rules, regulations, and policies related to the design, operation, or maintenance of existing Metrolinx asset classes that are retroactive

3.3.5 Examples where RAMS Risk Assessment does not apply at Metrolinx include but are not limited to:

a) Project schedule and personnel changes

b) Like for like replacements as part of state of good repair activities

c) Changes to rules, regulations, and policies related to the design, operation, or maintenance of existing Metrolinx asset classes that are not retroactive

4. Risk Source Identification & Classification

4.1 Overview

4.1.1 The level of detail in the RAMS Risk Assessment shall be adequate to enable the risk to be properly considered. The purpose is not to catalogue every trivial source of risk, nor is it expected that sources of risk beyond the limits of current knowledge will always be identified. The RAMS Risk Assessment shall reflect a reasonable analysis of hazards and RAM risk sources within the applied technology itself and the network in which it operates.

4.1.2 Whenever possible, RAMS Risk Assessments should be correlated with historical records of accidents & incidents, and the records of causes.

4.1.3 The entire RAMS Risk Assessment Process is iterative throughout the system life cycle, including risk source identification & classification as additional input information sources [ref. section 3 for details] is specified and/or any change occurs.

4.1.4 The following fields shall be documented at a minimum as part of the risk source identification & classification phase of the RAMS Risk Assessment:

TABLE 4-1 Summary of Risk Source Identification & Classification Fields
(ref. TABLE 7-1 for full Hazard Log & RAM Risk Source Log minimum fields template)

Identification	Risk Source ID	unique identifier for each hazard and RAM risk source
	Description	description of the risk source
	Core Hazard/RAM Risk Source	list the core hazard/RAM risk source that this specific risk source is tied to
	Primary Cause	description of the cause of the core hazard/RAM risk source
	Secondary Cause	description of the cause of the specific hazard/RAM risk source under analysis
	Consequence(s)	description of the consequence(s) if the hazard/RAM risk source where to occur **Note:** may be split into primary and secondary consequences as needed to best describe/understand the risk.
	Reference Source(s)	reference document(s) used to identify the risk source
	Risk Owner	the name of the individual person responsible for ensuring the risk level associated with the risk source meets the risk acceptance criteria
Classification	SME Categories	The subject matter expertise (SME) that is required to understand the risk
	Location(s)	Where the risk occurs
	Operational Scenario(s)/Mode(s)	When the risk occurs
	Life Cycle Phase(s)	When the risk source applicable in the system life cycle
	Safety/RAM	The RAMS parameter or combination of parameters impacted by the risk source
	Broadly Acceptable	Yes or No, with justification if yes

4.2 Risk Source Identification (includes consequence analysis)

4.2.1 All available input information sources [ref. section 3 for details] shall be used to identify all relevant hazards and RAM risk sources. Relevant industry generic hazard lists, CMREA risk assessment documentation, incident/accident databases, and previous RAMS risk assessments of reference systems are all excellent starting points for initializing list of

hazards & RAM risk sources, however any differences between the reference documentation and the specification of the asset/system/subsystem under assessment must also be considered to identify any new or obsolete hazards or RAM risk sources introduced by the differences.

4.2.2 Within the asset/system/subsystem under consideration, risk can be caused by a combination of:

a) operational causes (wrong operation or maintenance including the operational environment). Examples include but are not limited to:

1) Insufficient troubleshooting instructions leading to longer repair time, longer service disruption, and higher potential for misdiagnosis of failure cause leading to repeat failures and lower reliability.

2) Improper training or certification of operation and/or maintenance personnel leading to incorrect installation and high infant mortality rate, maintenance induced failures, higher service affecting failure rate, and higher occurrence of accidents and lost time injury frequency rate due to improperly trained staff.

3) Installation of an asset in an environment which exceeds the inherent design limitations leading to failures due to frequent overheating in summer, frequent freezing in winter, normal vibration levels causing frequent mechanical failures, etc.

b) technical and functional causes (internal to the system under consideration, including integration with interfacing systems) Examples include but are not limited to:

1) Incorrect specification of inputs from and outputs to interfacing systems leading to systems integration issues such as input power surge leading to catastrophic explosion accident, input power outage leading to complete system unavailability, or improper input power voltage/current leading to degraded system performance. The same examples can be considered risks of incorrect output if the power supply is the system under analysis.

2) Inadequate consideration of human factors in design and integration resulting in increased occurrence of human error, induced damage, incidents, and/or accidents when interacting with the asset/system/subsystem, including potential for increased occurrence of vandalism.

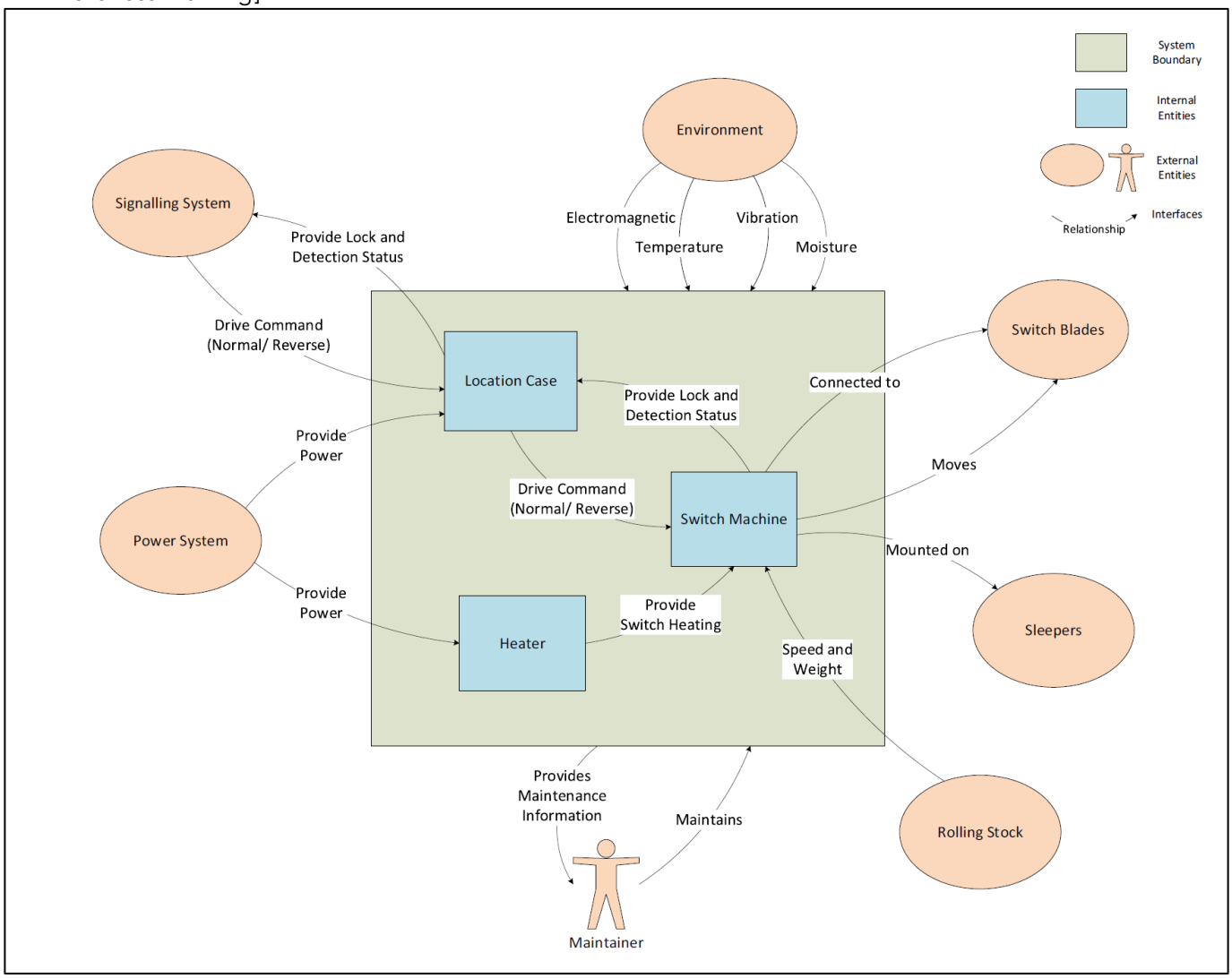
3) Inadequate specification of design or functional requirements leading to issues such as unexpected failure modes resulting in higher than acceptable failure, incident, and accident rates. For example, an elevator door requires door sensors to prevent closure if something is in the way, however without adequate specification of the sensitivity or coverage of the sensors, this could lead to the doors closing on small objects or objects not fully blocking the doors, which could lead to an accident like a child's finger being pinched in the doors.

4.2.3 Context diagrams are a useful tool to help identify hazards and RAM risk sources, which illustrate the boundaries between the asset/system/subsystem, showing the interfaces and entities it interacts with, including the operating environment.

4.2.4 FIGURE 4-1 illustates an example context diagram for the replacement of a switch machine. The system under assessment includes the switch machine itself, the heater, and the location case. These three parts interact with each other, but each also interface with other assets and systems. Interfaces and relationships are specified such as all three parts interact

with the external environment in which the switch machine system is installed, while the location case alone interfaces with the signalling system to command and communicate switch position movement.

Figure 4-1 Example of a context diagram for the replacement of a switch machine [SOURCE: Network Rail CSM-RA Awareness Training]



4.2.5 Additionally, where needed to support risk source identification a risk model should be defined. Causes, risk sources and accidents stand in a many-to-many relationship, such as:

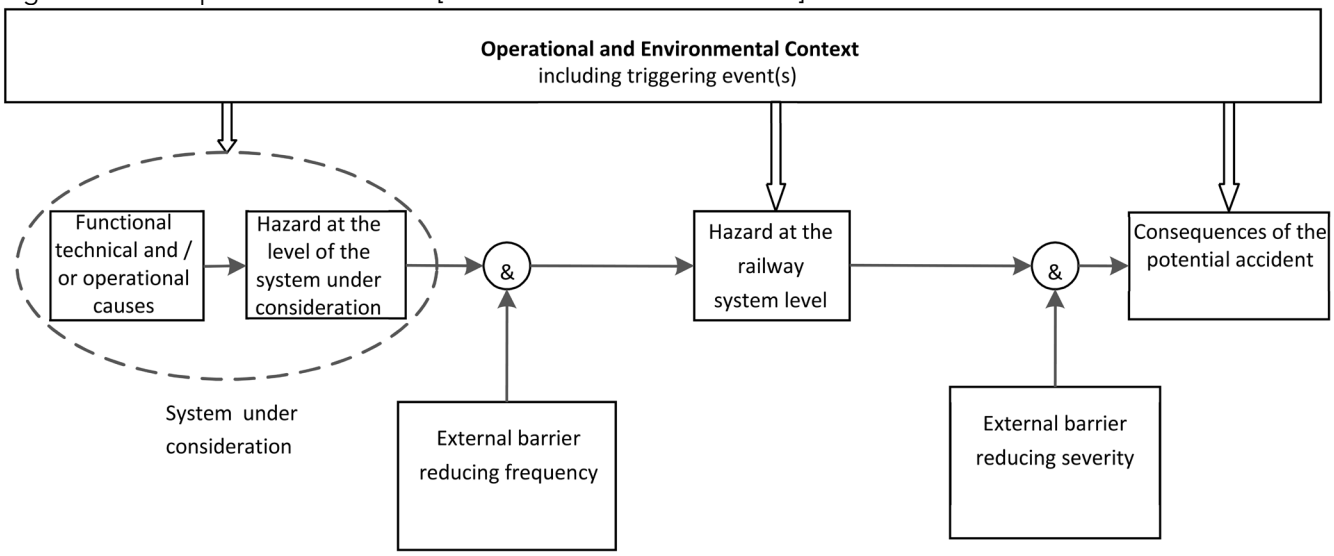
a) a single cause can trigger (or contribute to) several different risk sources;

b) a risk source can be triggered by several different causes;

c) a risk source can result in different types of accidents and/or incidents under different operational and environmental contexts;

d) an accident or incident can have different consequences under different operational and environmental contexts.

Figure 4-2 Example of a Risk Model [Source: BS EN 50126-2:2017]



4.2.6 The consequences of each hazard and RAM risk source must also be identified through consequence analysis, which involves gathering and documenting data that describe the effects of each risk source. The recommended approach is to use FRACAS data and accident/incident data, wherever available, and/or to consult experts on the asset/system/subsystem under consideration, including the operational and environmental context.

4.2.7 Depending on the complexity of the scenarios under analysis, the consequence analysis is generally performed using bottom-up techniques or a combination of bottom-up and top-down techniques. Commonly used techniques include:

a) Failure Mode Effect & Criticality Analysis (FMECA) [ref. RAMS-2 FMECA Process]

b) Event Tree Analysis (ETA) [ref. IEC 62502:2010]

c) Fault Tree Analysis (FTA) [ref. IEC 61025:2010]

d) Hazard and operability study (HAZOP) [ref. IEC 61882: 2001]

Note: any separate consequence analyses performed in support of the RAMS risk assessment shall be included either as an appendix to the RAMS Risk Assessment documentation, or reference documented to an external location where the consequence analyses can be accessed for review.

4.3 Risk Source Classification

4.3.1 Each identified source of risk shall be classified to inform any required risk treatment decision in terms of:

a) The field(s) of subject matter expertise the risk source is associated with

b) Any specific location(s) the risk source is associated with

c) Any specific operational scenario(s) or mode(s) in which the risk source arises

d) The life cycle phase(s) in which the risk source arises

e) Whether the risk source impacts safety, RAM, or a combination

f) Whether the risk source is broadly acceptable or not.

4.3.2 If the risk analysis identifies cases with risk "broadly acceptable", there is no need to specify further requirements for those risk sources. The classification of broadly acceptable risk is only used when the consequence is so low or when the likelihood of occurrence is so low that it is not reasonably practicable to take any action to reduce the risk. Examples include:

a) Staircases built to code still pose a tripping hazard, however the risk of tripping is considered broadly acceptable.

b) The likelihood of being struck by lightning twice is so low that it is considered broadly acceptable.

5. Risk Analysis & Risk Acceptance Principles (RAP)

5.1 Overview

5.1.1 For each hazard and RAM risk source that is not broadly acceptable, one or a combination of the three Risk Acceptance Principles (RAP) must be used to analyse the risk. These should be applied in the order listed (as applicable) to reduce the risk to an acceptable level while avoiding excessive analysis required for Explicit Risk Estimation where it is not required.

a) Codes of Practice

b) Similar Reference System

c) Explicit Risk Estimation

5.1.2 In many cases, expert judgement will be required to analyse the risk in addition to available data and design specification. To make it a credible basis for risk assessment, expert judgement should be made as objective as possible. This implies:

a) Check / estimation should not be the opinion of a single person. Agreement among several (independent) experts and approved knowledge enhances the confidence in an assessment.

b) Experts have adequate knowledge of the area in question.

c) All necessary areas of expertise (which could arrive at differing classifications) should be included in the judgement.

d) If the expert judgement is applied to estimate the frequency and consequences of hazards and RAM risk sources, a clear understanding of the categories promotes a common interpretation.

e) The results of expert judgement are documented. This ensures the transparency and plausibility of the conclusions. It demonstrates the integrity and enables third parties to trace the conclusion.

f) This documentation shall include:

1) the participants and respective areas of expertise.

2) information like references to publications, sources, assumptions, deliberately excluded aspects with justification, rationale of conclusion, etc.

TABLE 5-1 Summary of Risk Analysis Fields
(ref. TABLE 7-1 for full Hazard Log & RAM Risk Source Log minimum fields template)

Risk Analysis	Selected Risk Acceptance Principle(s)	Codes of Practice, Similar Reference System, or Explicit Risk Estimation
	Initial Likelihood	Only in the case of Explicit Risk Estimation
	Initial Severity	Only in the case of Explicit Risk Estimation
	Initial Risk	Only in the case of Explicit Risk Estimation

5.2 Codes of Practice

5.2.1 Codes of Practice (CoP), when correctly applied, may be used to control one or more specific hazards and/or RAM risk sources.

5.2.2 Each Code of Practice shall meet the following requirements:

a) be a set of rules widely recognised in the network domain under assessment (i.e. railway), or be specifically accepted as a standard by Metrolinx and;

b) be relevant for the control of the hazard or RAM risk source in the design under consideration.

5.2.3 If one or more hazards or RAM risk sources are controlled by codes of practice fulfilling the requirements above, then the risks associated with these risk sources shall be considered acceptable and those risks do not need to be further analysed.

5.2.4 The use of the codes of practice shall be registered in the hazard log and/or RAM risk source log as safety and/or RAM requirements.

5.2.5 If the risk for a particular hazard or RAM risk source cannot be acceptably covered by the application of a Code of Practice, additional requirements shall be identified by applying additional Codes of Practice or other RAP. This can also occur when the related Code of Practice does not sufficiently cover the identified hazard and RAM risk sources (e.g. the Code of Practice is not applicable to the full range of risk sources).

5.3 Similar Reference System

5.3.1 The system under consideration may be compared with a reference system for risk assessment.

5.3.2 The similar reference system shall satisfy the following requirements:

a) it has already been proven in-use to have an acceptable safety and/or RAM performance level and would therefore still qualify for approval;

b) it has similar functions and interfaces as the system under consideration;

c) it is used under similar operational conditions as the system under consideration for a sufficient period of time such that it has given confidence with the range of observed accidents and incidents; and

d) it is used under similar environmental conditions as the system under consideration.

5.3.3 If a reference system fulfils the requirements listed above, then for the system under consideration:

a) the risks associated with the hazard and RAM risk sources covered by the reference system shall be considered as acceptable;

b) the RAM and safety requirements for the risk sources covered by the reference system shall be derived from the RAMS analyses or from an evaluation of safety & RAM performance records of the reference system; and

c) these RAM and safety requirements shall be registered in the hazard log and/or RAM risk source log as RAM and/or safety requirements.

Note: This approach implies that the information in paragraphs 5.3.2 and 5.3.3 above was recorded for the project that introduced the reference system and that the information has been retained.

5.3.4 If the system under assessment deviates from the reference system, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system by applying another reference system or one of the two other RAP. The risks associated with the hazards and RAM risk sources covered by the reference system shall, in that case, be considered as acceptable.

5.3.5 If at least the same RAMS risk level as the reference system cannot be demonstrated, additional requirements shall be identified for the deviations, applying one of the two other RAP.

5.4 Explicit Risk Estimation

5.4.1 If the risk sources are not covered by Codes of Practice of Similar Reference Systems, risk analysis shall be performed using the RAP of explicit risk estimation along with risk evaluation [ref. Section 6 for details]. The aim is to estimate the risk and ensure the risk is acceptable.

5.4.2 The explicit risk estimation shall satisfy the following requirements:

a) the methods used shall reflect correctly the system under consideration and its parameters (including all applicable operational modes such as start-up, standby, emergency, etc.);

b) the results shall be sufficiently accurate to serve as robust decision support. Minor changes in input assumptions or prerequisites shall not result in significantly different requirements.

5.4.3 When explicit risk estimation principle is used, it shall:

a) document the risk acceptance criteria to be used to establish the acceptability of the risk level for the consequences of the relevant risk sources;

b) demonstrate that the risk treatment measures applied sufficiently reduce the risk to meet the risk acceptance criteria;

c) document the results of the explicit risk estimation.

5.4.4 When the risk associated with a hazard, RAM risk source, or a combination of several is considered acceptable, the identified risk treatment measures shall be registered in the safety hazard and RAM risk source logs as requirements.

5.4.5 Quantitative explicit risk estimation is performed by estimating the frequency of occurrence and the severity of an accident/incident scenario. This shall be done for the consequences of all identified hazards and RAM risk sources, using data and/or expert judgment. There are many ways and hybrid approaches in which various types of analyses can be combined and structured to calculate risk estimates. Failure Modes, Effects, and Criticality Analysis (ref. MX-SEA-STD-002 FMECA Process) can be used for explicit risk estimation based on likelihood of occurrence and severity of consequence. Fault Tree Analysis is commonly used to calculate the likelihood of occurrence, as well as Event Tree Analysis to calculate the severity based on the probability of the hazards & RAM risk sources leading to accidents/incidents.

5.4.6 There are areas for which the quantitative approach is usually not feasible and risk estimation and acceptance arguments may remain qualitative. Qualitative explicit risk estimation shall be performed by use of expert judgement [refer to paragraph 5.1.2 for details on expert judgement]. Examples where a quantitative approach is usually not feasible include:

a) mechanical parts relying on material endurance and design tolerance properties over a stated product lifetime;

b) electrical hazards relying on technical measures to avoid electrocution, induced voltages, etc.;

c) operational rules (including operating staff, maintenance workers, etc.), where it could be difficult to demonstrate that the Tolerable Hazard Rates (THR) have been met;

d) hazards related to minor injuries of customers by contact with sharp edges, trip on slippery surfaces;

e) fire/explosion hazards relying on technical measures for their prevention.

5.4.7 Using explicit risk estimation results in a level of uncertainty, generally with higher uncertainty the earlier in the life cycle the explicit risk estimation is conducted to define the RAM and Safety requirements. The following approaches may be used individually or in combination to manage uncertainty in risk estimation:

a) Worst possible scenario - the most conservative approach for dealing with uncertainty:

1) It is assumed that if a risk source could lead to a number of possible accidents/incidents, the worst possible scenario (the scenario with the highest risk) should be considered;

2) If the likelihood of a risk source occurring is estimated as a range based on a statistical analysis of data, then the highest frequency of the range is used in the analysis; and

3) If the severity of a risk source is estimated by “expert judgement”, then the worst-case scenario assessment of any expert is taken.

b) Reasonable estimates - these estimates can include the likelihood of a particular risk source based on the operational profile and taking into account all factors that might avert or reduce the severity of an accident including human actions. Estimates of likelihood and severity are to be based on:

1) collected data for existing assets/systems/subsystems;

2) extrapolated data from similar situations on other networks or even similar use cases in comparable industries, calculated failure rates using generic failure rate prediction tools; and/or

3) expert judgement.

c) Reasonable worst case - an intermediate approach between worst possible scenario and reasonable estimates:

1) worst case is applied for one of the dominant factors in the analysis so as to introduce a reasonable measure of conservatism;

2) thereafter “reasonable estimates” shall be accepted for all other dominant factors, otherwise the whole analysis will degrade into the “worst case” analysis.

6. Risk Evaluation & Treatment

6.1 Overview

6.1.1 Following risk analysis, the results are compared with the risk acceptance criteria to determine if the residual risk resulting from any individual risk source is beyond the acceptance criteria, and also to ensure the residual RAMS risk in the design is within the limits of the risk acceptance criteria, including broadly acceptable risk.

6.1.2 This is accomplished by comparing the results of the risk analysis with the risk acceptance criteria and defining additional RAM and/or Safety requirements through risk treatment measures as necessary until the residual risk is acceptable.

6.1.3 In the case of explicit risk estimation this evaluation is performed for each individual hazard and RAM risk source. However, in the case of codes of practice and similar reference system, the requirements defined by these RAP shall be the risk treatment measures applied to reduce the risk to an acceptable level.

TABLE 6-1 Summary of Risk Evaluation, Treatment, and Transfer Fields
(ref. TABLE 7-1 for full Hazard Log & RAM Risk Source Log minimum fields template)

Risk Evaluation & Treatment	Risk Treatment Actions	List all actions/measures that may be taken to treat the risk
	RAMS Requirements	Detail the risk treatment actions selected as RAM and/or Safety requirements for implementation to control the residual risk to an acceptable level
	Justification for Selection of RAMS Requirements	Justify the reasons only certain risk treatment actions were selected as RAMS requirements
	Compliance Evidence	Reference to documentation as proof of compliance with RAMS requirements
	Notes	Any additional comments or notes
	Assumptions	Detail or reference to documentation detailing all assumptions
	Status	Open, Controlled, Transferred, or Cancelled
Risk Transfer	Residual Risk Owner	The name of the individual person responsible for accepting ownership of the residual risk and any associated treatment actions
	Risk Transfer Details	Details of how the residual risk is being transferred to the identified owner
	Transfer Status	Pending, Accepted, Rejected

6.2 Comparison with Risk Acceptance Criteria (RAC)

6.2.1 In the case of explicit risk estimation, it may be possible to compare individual risk sources with individual RAC, however this is not always practical depending on how the RAC are specified.

6.2.2 In all cases, the RAM & Safety requirements shall be assessed with a holistic approach to the design under consideration such that residual risk of the whole system after introducing

RAM & Safety requirements is assessed, taking into consideration all identified hazards & RAM risk sources.

6.2.3 If the residual risk does not meet the RAC, then additional risk treatment action is required to reduce the total risk to an acceptable level [ref. Section 6.3 for details].

6.3 Risk Treatment

6.3.1 If the RAC are not met by the existing design, then treatment action must be taken to reduce the risk. There are several strategies for reducing risk depending on the RAMS parameter(s) affected, as detailed below. Additionally, in the case where multiple treatment action options exist, there are various methods that can be used to compare and select the appropriate action(s). One common method is ALARP (As Low As Reasonably Practicable), which is detailed in BS EN 50126-2:2017 Annex A.

6.3.2 The principal ways in which Safety risks can be reduced are:

a) improvement of reliability so that failures resulting in unsafe condition are less likely to occur;

b) improvement of availability so that the effects of failures resulting in unsafe condition are less severe;

c) introduction of safety control measures to reduce the likelihood of occurrence or severity of consequences (i.e. operational limitations, staff training/certification requirements, external barriers, etc.).

6.3.3 The principal ways in which RAM risks can be reduced are:

a) improvement in reliability, so that fewer failures occur with consequently fewer occasions for loss;

b) improvement in availability, so that when a failure does occur the resulting loss is smaller.

Note: improvement in maintainability is not covered independently as it is covered under improvement in availability; see 6.3.6c). Improvement to maintainability and/or reliability will also improve availability since it is a function of both (i.e. higher reliability overall will result in fewer service affecting failures and therefore increased service availability).

6.3.4 RAMS risk treatment is a balance of risk reduction through design optimization measures as well as risk transfer, such as creating and handing over a maintenance program with the design that will be applied in operation and maintenance.

6.3.5 There are four principal strategies for improving reliability:

a) designing system tolerances so that small deviations of parameters from their nominal values do not result in incorrect operation (applied in phase 6, Design and Implementation)

b) designing so that components are not expected to operate close to their limits e.g. rated load, temperature, etc. (phase 6, Design and Implementation)

c) application of good quality management practices to the procurement of materials and to the control of manufacturing and installation processes (phase 7, Manufacture)

d) condition monitoring, predictive maintenance, and preventive maintenance (phase 11, Operation, Maintenance and Performance Monitoring)

6.3.6 There are four principal strategies for improving availability:

a) provision of duplicate/redundant or back-up systems so that a single failure does not result in any loss of function (phase 5, Architecture and apportionment of system requirements).

b) provision of facilities for operation in a degraded mode in the event of a failure (phase 2, System definition and operational context, and phase 5, Architecture and apportionment of system requirements)

c) improving the maintainability of the system, so that the time required for repair and restoration of normal operation following a failure is reduced (phase 6, Design and Implementation)

d) provision of sufficient resources (such as competent staff, test equipment, spares, troubleshooting and fault isolation guidelines) so that the time required for repair and restoration of normal operation following a failure is reduced (phase 11, Operation, Maintenance and Performance Monitoring)

6.3.7 These strategies can be applied in combination. The order in which they are listed does not imply an order of preference.

6.3.8 If the selected risk treatment measures fall outside of the asset/system/subsystem design under assessment, then the associated risk must follow the risk transfer process and be accepted by the owner of the treatment measure [ref. Section 5.4 for details]. If the treatment action is not accepted, then different measures must be put in place to ensure acceptable risk levels are met in accordance with the RAC.

6.3.9 Accepted treatment measures are documented as RAMS design, operational, or maintenance requirements as part of the Hazard Log and RAM Risk Source Log [ref. Section 7 for details]. These risk treatment measure requirements then set the baseline for defining RAMS performance requirements. For example, risk treatment measures in the form of preventive maintenance requirements where the asset must be taken out of service at a regular frequency provides baseline for maximum hours of asset availability for service, which shall be taken into consideration in defining realistic asset Availability requirements.

6.4 Risk Transfer

6.4.1 In cases where risk is controlled by treatment measures/requirements external to the design under assessment, then these measures must be formally communicated and accepted by all affected parties before the risk can be considered accepted.

6.4.2 Common examples include:

a) Any maintenance requirements (i.e. preventive maintenance, staff training/certification, etc.) are transferred to the Operation & Maintenance life cycle phase. Any requirements to meet the RAC must be documented and accepted in the Maintenance Plan.

b) Any operational limitations or rules are also transferred to the Operation & Maintenance life cycle phase, and any associated requirements to meet the RAC must be documented and accepted in the Operational Plan.

c) Any external barriers introduced will change the design of interfacing assets and/or systems, therefore any new risk(s) introduced by the barriers to the interfacing assets/systems must be assessed and demonstrated to be acceptable.

7. RAMS Risk Assessment Deliverables & Output to Other Processes

7.1 Overview

7.1.1 The results of the RAMS Risk Assessment are a set of RAM and Safety requirements associated to clearly identified functions, systems or operating rules.

7.1.2 Based on the selected risk acceptance principles, these requirements can refer to codes of practice, to reference systems, or give explicit targets derived from an explicit risk estimation (ERE).

7.2 RAMS Risk Assessment Deliverables

7.2.1 Hazard Log & Safety Requirements, including list of safety-critical and safety-related assets

7.2.2 RAM Risk Source Log & RAM Requirements, including Reliability Critical Items List (RCIL)

7.2.3 The RAM & Safety requirements documentation specifies all accepted risk treatment actions, including a list of required design standards/codes of practice.

7.2.4 Table 7-1 provides a template for the minimum fields of information required for the Hazard and RAM Risk Source Logs. These logs may be kept separately or as a single log where the RAMS parameters impacted are clearly identified as safety and/or RAM.

7.3 Output to Other Processes

7.3.1 RAMS Risk Assessment produces a log of hazards and RAM risk sources, design standards & requirements to ensure the risk is managed to an appropriate level, and other risk treatment requirements to be transferred and managed through operating and maintenance plans. This then provides feedback into many other processes, including but not limited to:

a) Design change process: to meet Risk Acceptance Criteria (RAC) driving update to associated documentation & requirements including System Definition, RAM Plan, and Safety Plan, Safety Case, RAM Analysis, and the Asset Management Plan.

b) Risk Transfer process:

1) Updates to the maintenance plan to add and/or change maintenance staff training/certification requirements and/or maintenance activity requirements identified as required risk treatment action to meet RAC

2) Updates to the operating plan to add and/or change operational limitations, staff training/certification requirements, and/or operating procedures identified as required risk treatment action to meet RAC

c) RAMS Verification & Validation Process: the RAMS Risk Assessment provides RAM and safety requirements for validation.

d) Network level CMREA risk assessment process: iteration where additional hazards are identified at the RAMS risk assessment level, the need for new operational rules arises, and/or additional external measures are required to fulfill the RAM or Safety targets.

Table 7-1 Template for Hazard Logs & RAM Risk Source Logs

Identification (ref. Table 4-1 for detail in larger font)								**Classification (ref. Table 4-1 for detail in larger font)**						**Initial Risk Analysis (ref. Table 5-1 for detail in larger font)**				**Risk Evaluation & Treatment (ref. Table 6-1 for detail in larger font)**							**Residual Risk Analysis (ref. Table 5-1 for detail in larger font)**			**Risk Transfer (ref. Table 6-1 for detail in larger font)**		
Risk Source ID	**Description**	**Core Hazard/RAM Risk Source**	**Primary Cause**	**Secondary Cause**	**Consequence(s)**	**Reference Source(s)**	**Risk Owner**	**SME Categories**	**Location(s)**	**Operational Scenario(s)/Mode(s)**	**Life Cycle Phase(s)**	**Safety/RAM**	**Broadly Acceptable**	**Selected Risk Acceptance Principle(s)**	**Initial Likelihood**	**Initial Severity**	**Initial Risk**	**Risk Treatment Actions**	**RAMS Requirements**	**Justification for Selection of RAMS Requirements**	**Compliance Evidence**	**Notes**	**Assumptions**	**Status**	**Residual Likelihood**	**Residual Severity**	**Residual Risk**	**Residual Risk Owner**	**Risk Transfer Details**	**Transfer Status**
unique identifier for each hazard and RAM risk source	description of the hazard/RAM risk source	list the core hazard/RAM risk source that this specific risk source is tied to	description of the cause of the core hazard/RAM risk source	description of the cause of the specific hazard/RAM risk source under analysis	description of the consequence(s) if the hazard/RAM risk source where to occur NOTE: may be split into primary and secondary consequences as needed to best describe/understand the risk.	reference document(s) used to identify the risk source	the name of the individual person responsible for ensuring the risk level associated with the risk source meets the risk acceptance criteria	The subject matter expertise (SME) that is required to understand the risk	Where the risk occurs	When the risk occurs	When the risk source applicable in the system life cycle	The RAMS parameter or combination of parameters impacted by the risk source	Yes or No, with justification if yes	Codes of Practice, Similar Reference System, or Explicit Risk Estimation	Only in the case of Explicit Risk Estimation	Only in the case of Explicit Risk Estimation	Only in the case of Explicit Risk Estimation	List all actions/measures that may be taken to treat the risk	Detail the risk treatment actions selected as RAM and/or Safety requirements for implementation to control the residual risk to an acceptable level	Justify the reasons only certain risk treatment actions were selected as RAMS requirements	Reference to documentation as proof of compliance with RAMS requirements	Any additional comments or notes	Detail or reference to documentation detailing all assumptions	Open, Controlled, Transferred, or Cancelled	Only in the case of Explicit Risk Estimation	Only in the case of Explicit Risk Estimation	Only in the case of Explicit Risk Estimation	The name of the individual person responsible for accepting ownership of the residual risk and any associated treatment actions	Details of how the residual risk is being transferred to the identified owner	Pending, Accepted, Rejected

Note: minumum required fields shown, additional fields may be added as required to best detail the Hazard Log and RAM Risk Source Log and to build traceability from the railway level hazard log [ref CMREA].

Appendix A Rail Network Core Hazards List

Source: Network Rail Core Hazards

Core Hazard Reference	Core Hazard	Core Hazard Definition
CH1	*Potential for collision between trains (Inappropriate separation between trains)*	This Core Hazard groups Causes, arising from or impacted by the change, which effect the safe separation between trains. This hazard includes the scenarios in which the determined separation between trains, normally provided by the signalling system, has broken down including for example, all instances of lost or degraded train detection. This Core Hazard is primarily expected to affect Passengers and Workforce. There is potentially a secondary effect on Members Of Public, were a collision to result in "something hazardous" going beyond the railway boundary.
CH2	*Potential for collision with object (Objects/Animals on the line)*	This Core Hazard groups Causes, arising from or impacted by the change, which affect the likelihood of objects or animals "find their way" on or near the running railway such that they could make contact with a passing train. This Core Hazard includes those occurrences where (not an exhaustive list): • The train is incompatible with the structure gauge; • The train may collide with buffers; • Debris from moving train and objects falling from trains; • Animals or objects being on the running railway and having some effect thereon; • Inappropriate construction and maintenance practices; • Dumping heavy loads onto railway. This Core Hazard excludes: • Potential for collision at level crossings; • Instances of objects on the track causing fires; • Collision with objects which cause derailment. There may be many instances of animals entering and leaving the railway having no effect at all and being entirely unnoticed. These scenarios are not included, neither are those in which other objects, such as litter, come to rest on the railway, but do not affect the system at all. This Core Hazard is primarily expected to affect Passengers and Workforce. There is potentially a secondary effect on Members Of Public, where a collision to result in "something hazardous" going beyond the railway boundary.

Core Hazard Reference	Core Hazard	Core Hazard Definition
CH3	*Potential for derailment*	This Core Hazard groups Causes, arising from or impacted by the change, where the relationship between the track and the train is compromised such that the train may be derailed. Examples of possible causes include (not an exhaustive list): • Over-speeding of the train; • Track degradation outside safe limits; • Faults at switches and crossings; • Signalling failures; • All instances of lost rail-wheel adhesion; • Objects on the line. This Core Hazard is primarily expected to affect Passengers and Workforce. There is potentially a secondary effect on Members Of Public, where a derailment to result in "something hazardous" going beyond the railway boundary.
CH4	*People-train incident at the platform interface*	This Core Hazard groups Causes, arising from or impacted by the change, which affect people at the platform train interface including, but not restricted to (not an exhaustive list): • Entering or alighting from trains; • Falling off platforms; • Being struck or run over by train (station areas only); • Crossing the lines at station (where authorised only); • Opening and closing of carriage doors; • Doors opened on the wrong side of the platform potentially leading to passengers or workers getting off the train on the wrong side, or falling out of the train onto the track. Also included here are incidents where doors which are on the same side of the train as the platform but which are not adjacent to the platform (e.g. when a train is longer than the platform) are unlocked or opened and passenger or worker leaves or falls out of the train; • Passenger or worker trying to board a moving train, potentially leading to apparel being caught on the door and dragged along the platform or opening the door then falling and being hit by the door or caught up in the door. This Core Hazard excludes Passengers and Workers who deliberately access restricted track areas. These events are within the scope of Unauthorised access to track. This Core Hazard is expected to affect Passengers and Workforce only.

Core Hazard Reference	Core Hazard	Core Hazard Definition
CH5	*People-train incident on the train*	This Core Hazard groups Causes, arising from or impacted by the change, which affect people on-train due to train movement. This includes, but is not restricted to (not an exhaustive list): • People protruding beyond train gauge during movement; • Loss of train compartment integrity (e.g. Carriage separation, broken windows); • Falls due to train lurching, jerking or rapid deceleration and instances of lost rail-wheel adhesion; • Doors opened early, potentially resulting in passengers and workers on the train falling out of the train; • Trains departing with a door open, potentially resulting in passengers or workers falling out of the train; • Doors opened during train movement, potentially resulting in passengers or workers falling out of the train; • Train carriage decoupling during movement, potentially leading to passengers or workers falling off the train; This Core Hazard excludes a collision with another train, derailment, collision with an object.
CH6	*Electrical Hazards*	This Core Hazard groups Causes which affect the safe separation of people from live electrical power supplies, arcing of traction power supplies. The scope of the core hazard includes the following (not an exhaustive list): • Occurrence of traction power arc (except where related to conductor rail/shoe gear Arcing); • Existence of touch potential; • Structure exposed to leakage current; • Inappropriate separation from direct current (DC) conductor rail; • Inappropriate separation from overhead line equipment (OHLE); • Inappropriate separation from ground potential. This Core Hazard may affect Passengers, Workforce and Members of the Public.
CH7	*Ignition of flammable material*	This Core Hazard groups Causes which affect the potential for ignition of flammable material potentially leading to fire or explosion on trains, in stations and trackside as well as in other Metrolinx properties. This Core Hazard is expected to impact on Passengers, Public and Workforce.
CH8	*Unauthorised access to track*	This Core Hazard groups Causes related to unauthorised access to track. This Core Hazard may affect Passengers, Workforce and Members of the Public.

Core Hazard Reference	Core Hazard	Core Hazard Definition
CH9	*Failure to protect workforce on track from train movements*	This Core Hazard groups Causes, arising from or impacted by the change, related to workforce when on or about the track. This includes but is not limited to (not an exhaustive list): • When acting as lookout or hand signaller; • When working on or about the track; • When authorised to walk on the track; • Those situations where the distance between the running rail and people is not sufficient to ensure the safety of passengers, workers or neighbourhood. This Core Hazard will impact on the Workforce only.
CH 10	*Potential for Structural failure*	This Core Hazard is intended to encompass all Causes, arising from or impacted by the change, relating to the failure of structures. This Core Hazard may affect Passengers, Workforce and Members of the Public. This Core Hazard includes those situations where structures are unstable creating a threat to passengers or members of public. This hazard shall not include instability of trains or the movement of materials on trains. Consideration should be given to the interface of this hazard with the hazards Object on line and Inappropriate separation between trains. All structures going beyond the railway boundary are covered here (not an exhaustive list): • Unsound / Unsecured Tree; • Unsound / Unsecured Tunnel; • Unsound / Unsecured Underbridge / Culvert; • unsound / unsecured overbridge; • Unsound / Unsecured Signalling Structure; • Unsound / Unsecured Electrification Structure.
CH 11	*Person struck/ impact with object hazards*	This Core Hazard groups Causes which affect the potential for persons to be struck or impacted by objects, including vehicles (but excluding trains). This Core Hazard is expected to impact Passengers, Public and Workforce.
CH 12	*Exposure to hazardous materials*	This Core Hazard is intended to encompass all Causes, arising from or impacted by the change, related to exposure to hazardous materials. The scope of this hazard includes events where (not an exhaustive list): • Workers are working in confined spaces, or are exposed to hazards such as fumes from batteries; • Exposure hot materials/ working; • Workers are in proximity to uncontrolled harmful substances. This includes those harmful substances carried by the railway (dangerous goods) as well as harmful substances routinely used in the running and maintenance of the railway (fuel oils, caustics, etc.); • Workers come into proximity to harmful substances through contaminated water or land. This Core Hazard will impact on the Workforce only.
CH 13	*Manual Handling*	This Core Hazard is intended to encompass all Causes related to manual handling injuries, including lifting. This Core Hazard will impact on the Workforce only.

Core Hazard Reference	Core Hazard	Core Hazard Definition
CH 14	*Inappropriate maintenance*	This Core Hazard is intended to encompass all Causes, arising from or impacted by the change, relating to maintenance issues such us (not an exhaustive list): • Inadequate training and/or manuals; • Inappropriate spares; • Inadequate configuration management; • Inappropriate/inadequate maintenance strategy; • Potential for track buckling.
CH 15	*Inadequate security protection of the railway system.*	This Core Hazard groups Causes, arising from or impacted by the change, related to security of signalling system operation. The scope of this hazard includes the following events (not an exhaustive list): • Hacking into software of the signalling system; • Unauthorised access to signalling equipment; • Unauthorised access to control rooms.
CH 16	*Operational delay*	This Core Hazard is intended to encompass all Causes, arising from or impacted by the change, which result in operational delays. This Core Hazard is expected to affect Passengers and Workforce only.
CH 17	*Antisocial behaviour*	This Core Hazard is intended to encompass all Causes, arising from or impacted by the change, which result in antisocial behaviour on all Metrolinx infrastructure, including assault, theft and vandalism. This excludes suicidal behaviour.
CH 18	*Electro-Magnetic Interference (EMI) caused to by railway operations*	This Core Hazard groups Causes related to Electro-Magnetic Interference (EMI) initiated by Railway Operations to Businesses, General Public, Adjacent Buildings, Hospitals. This core hazard has been developed to include those situations where EMI from the infrastructure or rolling stock could affect the safety of members of public directly. It does not include EMI caused by infrastructure or rolling stock to signalling and track circuits, or interference between the rolling stock and infrastructure. Such interference could be considered part of the causes for other hazards.
CH 19	*Potential for collision at Level crossings*	This Core Hazard groups Causes, arising from or impacted by the change, which affect the likelihood of collisions at level crossings, with persons, vehicles, objects or animals. All types of level crossing are included in the scope of this hazard.
CH 20	*Evacuation*	This Core Hazard groups Causes, arising from or impacted by the change, related to evacuation from any railway asset, including trains, stations and depots.
CH 21	*Slips, trips and fall hazard*	This Core Hazard groups Causes, arising from or impacted by the change, which affect the likelihood of slips trips and falls, including falls from height.
CH 22	*Suicidal behaviour*	This Core Hazard groups Causes, arising from or impacted by the change, which affect the occurrence of suicidal behaviour and suicide on Metrolinx infrastructure.