Metrolinx FMECA (Failure Modes, Effects, and Criticality Analysis)

MX-ALM-STD-003

Revision 02
December 2024

Metrolinx FMECA (Failure Modes, Effects, and Criticality Analysis)
MX-ALM-STD-003

Publication Date: July 2020
Revision Date: March 2022, December 2024

Preface

This is the third edition of the *Metrolinx FMECA (Failure Modes, Effects, and Criticality Analysis)*. This standard is now part of the Reliability Engineering Standards, a function of the Asset Lifecycle Management Office. The Document Number has been changed from MX-SEA-STD-002, Rev 01 to MX-ALM-STD-003, Rev 02. Document content has been updated to align templates and processes developed with best practices.

The purpose of the Reliability Engineering Standards is to formalize the framework to adequately manage RAM (Reliability, Availability, Maintainability) performance of all Metrolinx assets for the entire life cycle. Metrolinx Reliability Engineering standards are built as an adaptation of European Standard EN 50126-1:2017 and modified to suit all asset classes and internal Metrolinx processes. They provide internal Metrolinx staff and external stakeholders involved in the design, construction, operation, and maintenance of Metrolinx assets with a common understanding and a systematic process for Reliability Engineering management. It is intended for suitably qualified professionals that are familiar with the subject matter. These documents are not substitutes for all applicable local codes, standards, and manuals.

The *Metrolinx FMECA (Failure Modes, Effects, and Criticality Analysis)* is maintained by the Reliability Engineering team, Asset Lifecycle Management Office, Asset Management and Maintenance Division, Metrolinx.

Suggestions for revision or improvements, including a description of the proposed change along with information on the background of the application and any other useful rationale or justification, can be sent to the Metrolinx Asset Lifecycle Management Office, Attention: Director Asset Lifecycle Management. The Director of Asset Lifecycle Management ultimately authorizes the changes. Proposals for revisions or improvements to include your name, company affiliation (if applicable), e-mail address, and phone number.

December 2024

Contents:

List of Figures

List of Tables

Documents

Table 0-1 Supporting Documents

Reference	Document Title	Relation
BS EN IEC 60812:2018	Failure modes and effects analysis (FMEA and FMECA)	Reference
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-ALM-STD-001	Metrolinx Asset Information Standard	Reference
MX-EST-FRM-005	Standards Deviation Request Form	Reference
CKH-ENG-PRC-001	Procedure for Requesting Deviations to Metrolinx Standard Technical Requirements	Reference
MIL-STD-1629	Procedures for Performing a Failure Mode, Effects and Criticality Analysis	Reference
MX-ALM-STD-002	Metrolinx FRACAS Process	Related Process
MX-ALM-STD-005	Metrolinx RCA Process	Related Process
MX-SEA-STD-006	RAMS Risk Assessment Process	Related Process
MX-SMS-G001	Risk Assessment Guide	Reference

Acronyms and Abbreviations

Table 0-2 Acronyms and Abbreviations

Acronym	Full Name
CA	Criticality Analysis
CCF	Common Cause Failure
CLOS	Customer Level of Service
CPG	Capital Projects Group
EAM	Engineering and Asset Management
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
KPI	Key Performance Indicator
LCC	Life Cycle Cost
MMS	Maintenance Management System/Software
RAM	Reliability, Availability and Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RCA	Root Cause Analysis
RCM	Reliability Centered Maintenance
SME	Subject Matter Expert

Definitions

Table 0-3 Definitions

Term	Definition	Source
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 are designated as being accountable for the ownership and management of a given class of assets, and for the completeness and accuracy of information of the same class of assets.	CKH-ASMT-PRC-001 Asset Data and Information Standards
Asset Hierarchy	Hierarchical grouping of Metrolinx assets, organized within parent-child relationships.	CKH-ASMT-PRC-001
Causal Chain	The path of influence running from a root cause to problem symptoms.	
Common Cause Failures	Failures of multiple assets or systems, which would otherwise be considered independent of one another, resulting from a single cause.	IEC 60812:2018
Common Mode Failures	Failures of different assets or systems are characterized by the same failure mode.	IEC 60812:2018
Control	[1] Design features, or other existing provisions, which can prevent or reduce the likelihood of the failure mode or modify its effect. [2] Actions that are available or can be taken by an operator to negate or mitigate the effect of a failure on a system. Note: controls can also be referred to as compensating provisions.	IEC 60812:2018 MIL-STD-1629 Rev A
Corrective Action	A documented design, process, procedure, or materials change implemented and validated to correct the cause of failure or design deficiency. Note: in the context of FMECA, corrective actions are sometimes referred to as "treatment" or "mitigation" as an action to modify the likelihood and/or effects of a failure mode [IEC 60812:2018].	MIL-STD-721

	Note: corrective actions are sometimes distinguished from preventive actions and referred to collectively as CAPA (i.e., for Root Cause Analysis [MX-ALM-STD-005]); however, the FMECA process uses the term corrective action in reference to both corrective and preventive actions.	
Criticality	[1] Importance ranking is determined using a specified evaluation criteria. [2] Failure Mode Criticality: A relative measure of the consequences of a failure mode and its frequency of occurrences. [3] Asset Criticality: Is based on the significance of the impact on the achievement of the organization's objectives in the event of failure, regardless of the likelihood.	IEC 60812:2018 MIL-STD-1629 Rev A ISO 55000
Detection Method	Means by which a failure mode or incipient failure becomes evident.	IEC 60812:2018
Failure	[1] Loss of ability to perform as required. [2] The event, or inoperable state, in which any item or part of an item does not, or would not, perform as previously specified.	[1] BS EN 50126-1:2017 [2] MIL-STD-721
Failure Cause	Set of circumstances that lead to failure.	IEC 60812:2018
Failure Effect	Consequence of a failure, within or beyond the boundary of the failed item.	IEC 60812:2018
Failure Mode	[1] Manner in which failure occurs. [2] The manner by which a failure is observed. Generally, describes the way the failure occurs and its effect on equipment operation.	[1] BS EN 50126-1:2017 [2] MIL-STD-1629 Rev A
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
Hierarchy Level	Level of sub-division within an asset hierarchy. Note: definition adapted for Metrolinx RAMS processes to replace the term "item" with the term "asset."	IEC 60812:2018
Human Error	Discrepancy between the human action taken or omitted, and that intended or required.	IEC 60812:2018

Likelihood	Chance of something happening Note: likelihood is sometimes referred to as probability	IEC 60812:2018 (note added)
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
RAMS Acceptance Criteria	Pre-established RAMS standards and requirements (including risk) an asset or system must meet. If the applicable RAMS acceptance criteria are not met, corrective action is required.	
Redundancy	Provision of more than one means for performing a function	IEC 60812:2018
Root Cause	The initiating cause in the causal chain that leads to an undesirable situation or condition; the point in the causal chain where corrective action reasonably be implemented and expected to correct and prevent recurrence of the undesirable situation or condition	
Scenario	Possible sequence of specified conditions under which the asset or system functions are performed. Note: definition adapted for Metrolinx RAMS processes to replace the term "item" with the term "asset or system."	IEC 60812:2018 (edited)
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

1. Overview

1.1 Purpose

1.1.1 The FMECA process provides a systematic method by which an asset or system is broken down by hierarchy level, and the failure modes and effects are identified, analyzed, and ranked for prioritization of potential corrective action.

a) The FMECA process is a tool used for failure criticality and RAMS Risk Assessment. The primary function of FMECA is for early identification of failure modes with the potential to result in undesirable and unacceptable risk, so they may be eliminated or minimized through design correction at the earliest possible time. FMECA is also used to trigger and optimize new or redesign decisions and maintenance strategies, as well as to assist in asset management life cycle cost (LCC) estimations.

1.1.2 The FMECA is composed of two analyses, the Failure Modes and Effects Analysis (FMEA) and the Criticality Analysis (CA).

a) The purpose of the FMEA is to determine how assets and systems have failed and/or may fail to perform their function and the effects of these failures to identify any required corrective actions for implementation to eliminate or minimize the likelihood or severity of adverse failure effects going forward; and

b) The purpose of the CA is to enable prioritization of the failure modes for potential corrective action.

1.1.3 The intended audience for this process document is:

a) Asset Class Teams;

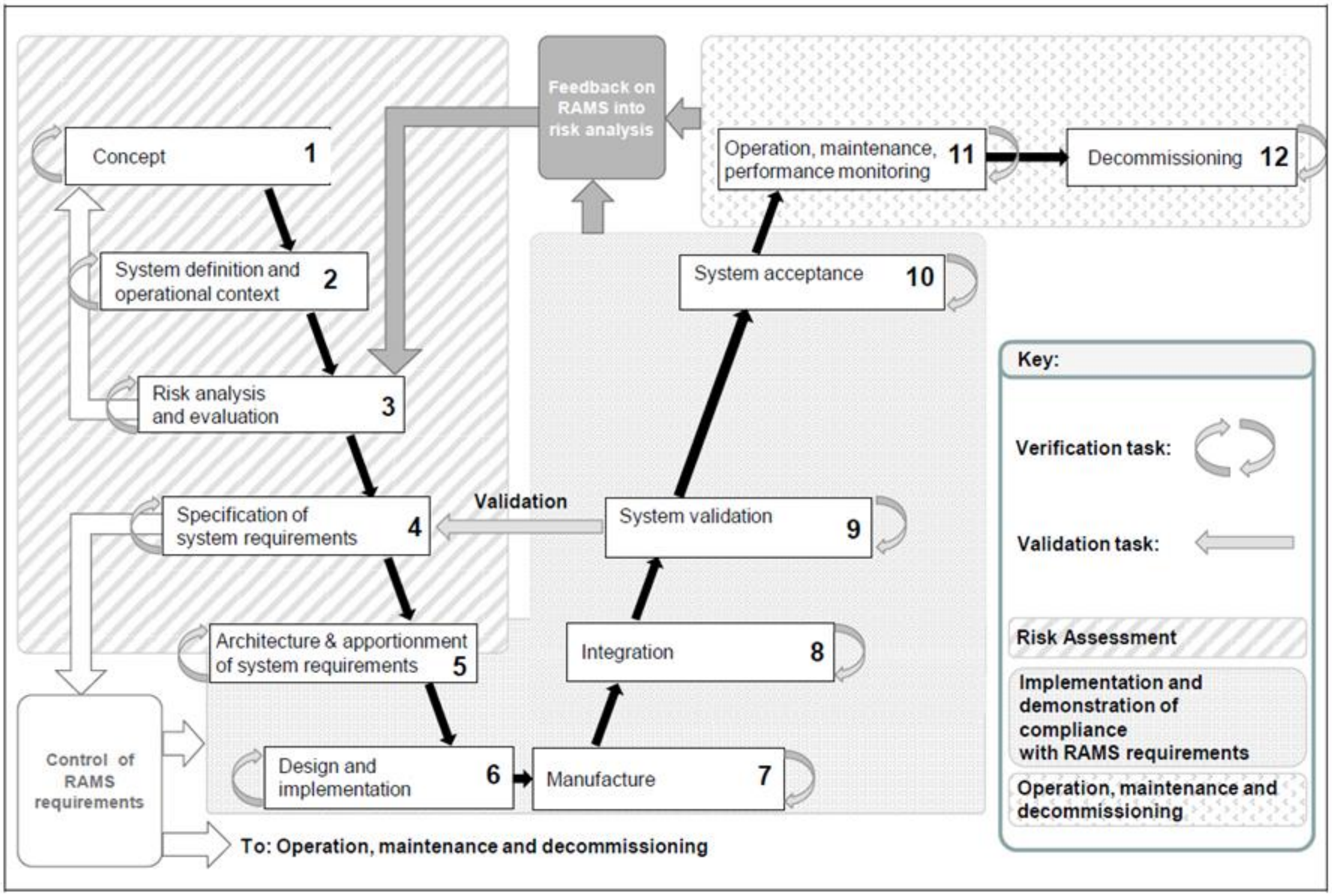
b) Safety & Security Team;

c) Delivery Team;

d) Sponsorship Office; and

e) Maintenance Team.

Figure 1 RAMS V-Cycle [Source: EN 50126:2017]



1.2 Scope

1.2.1 The FMECA process applies to technical failure modes of all Metrolinx existing and future assets. It does not apply to non-technical or non-reasonably probable failure modes and effects.

1.2.2 The FMECA process is applicable in every phase of the life cycle, from concept to decommissioning [Figure 1]. FMECA is typically an iterative process and shall be tailored to the nature of the design process, and for different program and contract types. Appendix B provides examples of tailoring the FMECA for different applications and requirements.

1.2.3 For optimal asset and system RAMS performance, the FMECA process shall be initiated as soon as the preliminary design information is available. This could be as early as life cycle phase 1, “Concept” at the higher hierarchy levels, then extended iteratively to the lower hierarchy levels as more information becomes available through each phase of the system life cycle through to phase 10, “System acceptance” [Figure 1].

1.2.4 The FMECA shall be validated through phase 11, "Operation, maintenance, performance monitoring" Figure 1] and updated as warranted for any novel failure modes and failure effects identified during operation and maintenance, as well as updated failure rate assumptions. Validating the accuracy of existing FMECA is particularly important for use in reference analysis for new concept and redesign decisions, as well as for supporting reliability centered maintenance planning. Novel failure modes and actual failure rates can be identified and monitored through the FRACAS Process [MX-ALM-STD-003].

1.2.5 Suggested sources of input information to support the FMECA process are detailed in Section 1.

1.2.6 Possible outputs from FMECA and their relationships to other RAMS processes are detailed in Section 2.3.1f).

1.2.7 There are two primary instigators for starting the FMECA process:

a) When a change to an existing asset or system, or new design is approved. This includes operational and maintenance changes for existing assets; and

b) If a novel failure mode or effect is identified for an existing asset or system, which can be identified regularly as part of the FRACAS Process.

1.2.8 The FMECA process is composed of three phases;

a) Planning the FMECA, which produces the FMECA Plan:

i. Planning a FMECA involves considering why an analysis is to be performed, what assets and/or systems are to be analyzed, at which hierarchy levels, and under what scenarios, and how the analysis should be most effectively and efficiently performed;

ii. Stakeholders shall be consulted, as appropriate, so that their objectives and interests in the analysis are properly understood and taken into account;

iii. When multiple iterations of the FMECA are to be performed, the FMECA plan shall specify when this is required and the purpose and scope of each iteration at a minimum but should include a full sub-plan for each required iteration (i.e., FMECA Plan for each system life cycle phase); and

iv. The output of the planning phase is the FMECA Plan, which describes a tailored, cost-effective application of the FMECA for the particular context. For details on the contents of the FMECA Plan, refer to Appendix A, Section A.1.

b) Performing the FMECA, which produces the FMECA Worksheets:

i. The appropriate level of detail for the analysis depends on the context and the results desired, as specified in the FMECA Plan. In general, greater detail in the level of sub-division of the subject of the FMECA provides an equivalent level of detail on possible failure modes and effects and more detailed corrective action strategies, but the analysis is more time-consuming to undertake.

ii. Performing the FMECA is usually an iterative process as the design matures through the design phase, and as actual performance data is gained through operational and maintenance experience; and

Note: FMECA iteration requirements shall be specified as part of the FMECA Plan.

iii. The output of performing the FMECA is the FMECA worksheets. When updating an existing FMECA, only those worksheets and steps which are affected by the information driving the updates are required to be performed. For details on the contents of the FMECA worksheets, refer to Appendix A, Section A.2.

c) Documenting the FMECA, which produces the FMECA reporting:

i. The objective of the FMECA Reporting is to document in a logical way all relevant information used for and produced from performing the FMECA;

ii. Since the FMECA is an iterative process, the documentation is developed progressively throughout the life of the asset or system, which is the subject of the analysis. The FMECA documentation shall be updated at times appropriate to the application and as per the purpose and scope as defined in the FMECA Plan (i.e., at each life cycle phase during design, as corrective actions are identified and implemented, during operation and maintenance as actual performance data and experience is gained, etc.); and

iii. The form and content requirements of the FMECA Reporting shall be decided as part of the FMECA Plan in accordance with the output requirements. For details on the contents of the FMECA Reporting, refer to Appendix A, Section A.3.

1.2.9 A template for FMECA Worksheets is provided in Appendix A, Section A.2. However, these should be tailored as warranted in accordance with the objectives for individual applications of the FMECA process.

1.2.10 Examples of tailoring the FMECA are provided in Appendix B [page 24] to illustrate some possible approaches to performing the FMECA.

1.3 Key Responsibilities

1.3.1 The Reliability 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 The responsibilities for applying and demonstrating compliance with the FMECA process change through phases of the system life cycle [Figure 1] and vary depending on the contract type. Responsibilities are generally being contracted out for the design phase and ending up with EAM in Operation phase .

1.3.3 This document uses the following terms to describe responsible parties who shall be involved in the FMECA process:

a) Analyst(s): the person(s) responsible for conducting the FMECA in compliance with this FMECA process. The analyst(s) shall be competent in FMECA and shall have adequate technical understanding to challenge other stakeholders and subject matter experts involved in the analysis;

   Note: the analysts themselves may be subject matter experts.

b) Subject Matter Experts: people with relevant knowledge and experience to cover all the aspects of the asset or system to be analyzed, including technical, social, economic, and environmental considerations, as required;

c) Approver: the person with responsibility for defining the purpose of the FMECA, authorizing the use of resources, and approving the FMECA deliverables (FMECA Plan, FMECA Worksheets, and FMECA Report(s)), as well as the recommended corrective actions, including justification where no corrective action is recommended; and

   Note: the approver must be a different person from the analyst(s).

d) Stakeholders: people or organizations that can affect or be affected by the results of the FMECA.

2. Input Information Sources

2.1 Overview

2.1.1 This section illustrates a variety of possible input information sources to consider in planning and performing an FMECA. It should not be regarded as a comprehensive MX-ALM-STD individual analyses shall be specified in the FMECA Plan, and actual sources of information used in performing the FMECA shall be recorded in the FMECA Reporting.

2.1.2 Information pertaining to functions, characteristics, and performance is required for all hierarchy levels considered, up to the highest level within the scope, so that the analysis can properly address failure modes that affect any of those functions.

2.1.3 Collection of information continues throughout the FMECA process, as the analysis will often highlight where extra information is needed.

2.2 Failure Data Sources

2.2.1 Existing FMECA on the same, or similar assets and systems can be used as source material.

2.2.2 Sources of failure mode information include:

a) For new design, reference may be made to other assets or systems with similar function and structure to their performance under appropriate conditions;

b) For existing design, the failure modes might be known from previous FMECA; However, checks must be carried out to seek any differences between the old and new applications, which could result in different failure modes;

c) Operating data, experience, and SME knowledge, including incident and accident databases, maintenance and failure databases, and other FRACAS Data & Reports [MX-ALM-STD-002];

d) Testing data collected during design;

e) Industry publications and standards; and

f) Checklists based on generic failure modes for specific types of assets and systems, including Metrolinx specific references such as INFOR closing codes.

2.3 Asset or System Specification Information

2.3.1 Considerations for asset or system specification information may include:

a) Description of the asset or system to be analyzed, its objectives and role in the system and Metrolinx network as a whole;

b) Breakdown of the hierarchy levels of the asset or system and their characteristics, performances, technical specifications, functions, and functional limitations (i.e., environmental operational limits, etc.);

c) The logical, physical, and functional connections between the hierarchy levels under analysis (i.e., reliability block diagrams, functional block diagrams, flow charts, system charts, etc.);

d) Inputs to and outputs from the asset or system, at the various hierarchy levels to be analyzed;

e) Redundancy level and nature of spare equipment, redundant equipment or processes, or parallel processing paths;

f) Interfaces with other assets, systems, and the operational environment; and

g) Any changes in function or structure for the operational scenarios under analysis.

2.4 Scope, Purpose, and RAMS Acceptance Criteria Information

2.4.1 Considerations for the scope, purpose, and RAMS acceptance criteria information may include the following:

2.4.2 The position and importance of the asset or system within the operational context of the Metrolinx network;

2.4.3 The required outcome(s) of the FMECA (see Section 2.3.1f) for examples);

2.4.4 The defined RAMS acceptance criteria and criticality analysis framework. Resources for this information include:

a) The Asset Risk Framework provides a framework for assessing asset-related risk based on likelihood and severity; and

b) The Enterprise Risk Framework in Risk Assessment Guide [MX-SMS-G001] provides a framework for assessing enterprise-level risk based on likelihood and severity (Note: the term "impact" is used instead of severity in the Enterprise Risk Framework.)

Figure 2 Qualitative 4x5 Criticality Analysis Matrix Framework [Source: IEC 60812-2018]

Likelihood	Severity: Catastrophic	Major	Marginal	Minor
High	X	X	1	2
Medium	X	X	1	2
Low	X	X	1	2
Very Low	X	1	1	2
Remote	1	2	2	3

IEC

Category X: "Unacceptable";
Category 1: "Undesirable";
Category 2: "Acceptable";
Category 3: "Minor".

Note: If non-Metrolinx standard failure criticality analysis framework or RAMS acceptance criteria are used, then the FMECA Plan shall include details on how to interpret the ratings for comparison to the Asset Risk Framework and Enterprise Risk Framework to facilitate criticality ranking and corrective action prioritization across different analyses. Any criticality analysis framework used must include at least three (3) and not more than ten (10) categories for both severity and likelihood, resulting in a minimum 3x3 criticality matrix, and a maximum 10x10 criticality matrix.

3. Outputs from FMECA

3.1 Overview

3.1.1 This section illustrates a variety of possible outputs and use cases for the FMECA process beyond the FMECA Reporting contents detailed in this process document. This should not be considered a comprehensive list of allowable outputs or use cases.

3.1.2 The output and use requirements for individual analyses shall be specified in the FMECA Plan, and those required outputs shall be documented as part of the FMECA Reporting.

3.2 FMECA within the Design Process

3.2.1 The FMECA process may be used as a tool for explicit risk estimation and evaluation as part of the RAMS Risk Assessment process for new assets or system design or redesign.

3.2.2 The objective of FMECA during design is to identify corrective action recommendations for the failure modes within a system and the potential critical failures, which can be eliminated or minimized by design changes at the earliest possible time.

3.2.3 If a design change is not technically or economically feasible to meet the RAMS acceptance criteria, the associated risk can be transferred from the design phase to operation and maintenance through other corrective action recommendations, such as recommending maintenance tasks for the maintenance plan.

3.2.4 FMECA can be leveraged to identify Reliability Critical Items (RCI) and Safety Critical Items (SCI).

3.3 FMECA within Reliability Centered Maintenance

3.3.1 The ability to develop a successful maintenance plan using reliability-centred maintenance (RCM) requires a clear understanding of the functions, failures and consequences expressed in terms of the organization’s objectives in the operation of the asset or system.

3.3.2 For application to RCM, the FMECA should be structured in such a way that all failure modes can be clearly linked to loss of function at an appropriate hierarchy level and that aspects such as detection methods and controls consider potential maintenance task recommendations.

3.4 FMECA within Operation, Maintenance & Performance Monitoring Life Cycle Phase

3.4.1 Validation of FMECA is supported by the FRACAS Process [MX-ALM-STD-002] through regular identification of novel failure modes and effects and calculation of actual failure rate data to confirm or correct likelihood estimates.

3.4.2 Continuous iterative updating of the FMECA worksheets and reports during the operation, maintenance, and performance monitoring life cycle phase [Figure 1] can be used to provide a comprehensive failure mode database for all assets. This data, in turn, can be used as input or reference information for future FMECA [detailed in Section 2.2], as well as other analyses such as Root Cause Analysis (RCA) [MX-ALM-STD-005].

3.4.3 The FMECA process may also be used as a tool for explicit risk estimation and evaluation as part of the RAMS Risk Assessment process for operation or maintenance changes (i.e., maintenance plan revisions, changes to existing assets or system utilization or environment, etc.)

3.5 FMECA within Asset Management

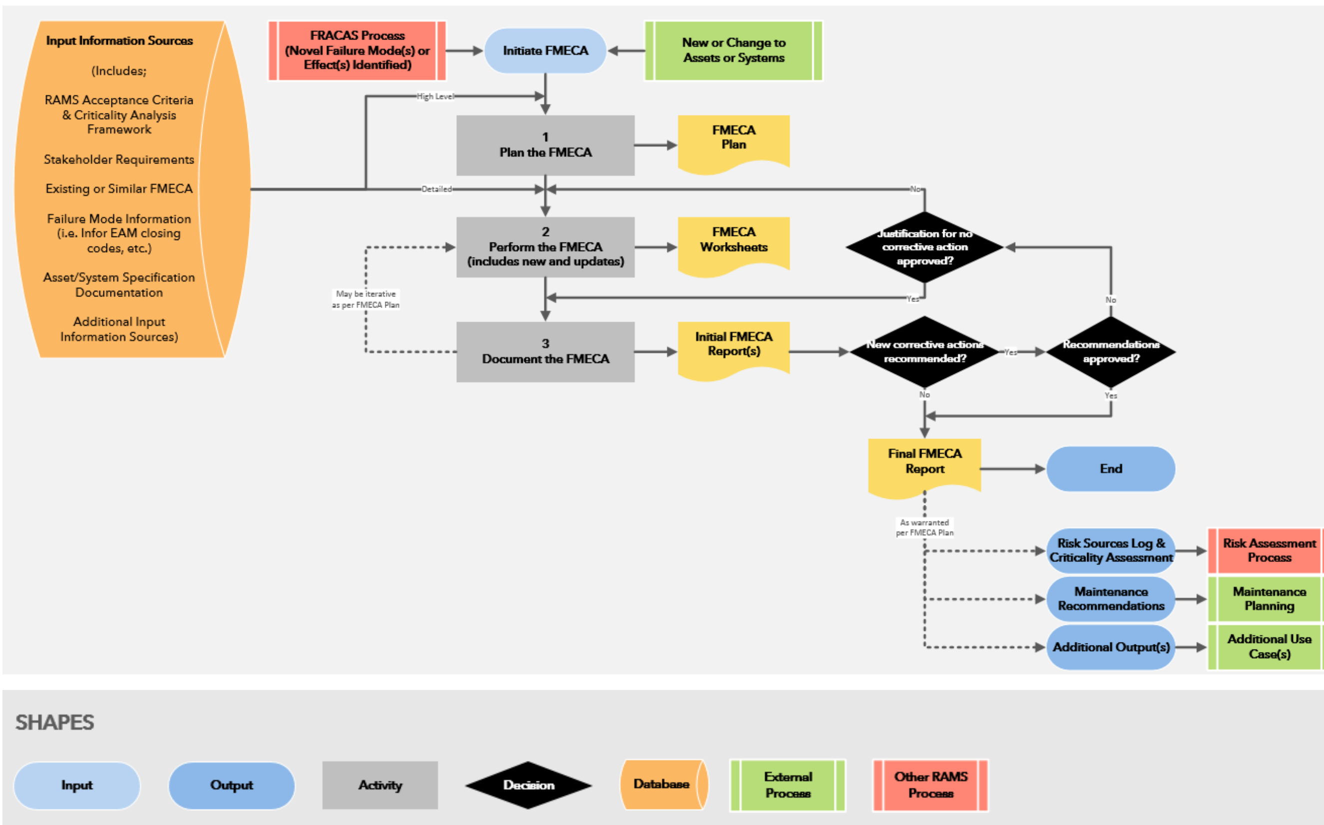
3.5.1 FMECA can support the development of Asset Management Plans by providing failure mode criticality scores through the use of the criticality analysis and as input to the Asset Risk Framework.

4. The FMECA Process

4.1 The FMECA Process Flow Chart

4.1.1 Figure A- illustrates the process steps for planning the FMECA[1].

Figure 3 The FMECA Process Map



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

4.2 The FMECA Process Narrative

4.2.1 The following steps detail the FMECA Process:

a) There are two primary instigators for initiating the FMECA process:

i. When a change to an existing asset or system, or new design is approved, this includes operational and maintenance changes for existing assets;

ii. If a novel failure mode or effect is identified for an existing asset or system, which can be identified regularly as part of the FRACAS Process [MX-ALM-STD-002];

b) Using the relevant input information sources available [detailed in Section 1], plan the FMECA. Refer to Appendix A, Section A.1 for details on the requirements for the FMECA Plan. Once the FMECA Plan has been completed and approved, proceed to step 4;

c) Using the relevant input information sources available [detailed in Section 1], perform the FMECA by producing or updating the FMECA Worksheets. Refer to Appendix A, Section A.2 for details on the requirements for the FMECA Worksheets. When the required FMECA Worksheets have been completed as specified in the FMECA Plan, proceed to step d);

d) Document the results of the FMECA in the Initial FMECA Report(s). Refer to Appendix A, Section A.3 for details on the requirements for the FMECA Reporting. Once the results are documented, proceed to step e);

Note: The FMECA Plan may specify an iterative approach to performing and documenting the FMECA (step 4 and step d)), requiring additional FMECA Worksheets to be produced or updated and the FMECA Reporting updated accordingly at different times. This does not prevent the process from continuing to step e) for the existing FMECA at each required iteration specified in the FMECA Plan.

e) If any new corrective actions are recommended in the latest FMECA Reporting, these shall be considered for acceptance and incorporation by proceeding to step f). If no new corrective actions are identified for recommendation from the latest FMECA Report, then this constitutes the Final FMECA Reporting, and the FMECA process ends here;

f) If the recommendations are not approved, proceed to step g). If the corrective action recommendations are approved, then the latest FMECA Reporting constitutes the Final FMECA Reporting, and the FMECA process ends here; and

Note: Some contents of the FMECA reporting may form outputs to other processes such as RAMS Risk Assessment and Maintenance Planning processes [see Section 2.3.1f) for details on additional potential outputs from FMECA and their use cases].

g) If the justification for no corrective action is approved, then this justification shall be documented in the FMECA by updating the FMECA Reporting per step d). If no corrective action is acceptable, then return to step 4 and update the FMECA Worksheets to identify alternate corrective action recommendations to meet the RAMS acceptance criteria.

Note: Per the purpose of the FMECA Reporting to document all relevant information used for and produced from performing the FMECA, the justification for changes to any corrective action recommendations per step g) shall also be documented in the FMECA reporting (step d).

Appendix A. FMECA Deliverables Outline

A.1 FMECA Plan Contents

A.1.1. Definition of the objectives and scope:

a) The stated objectives shall clearly identify the reason for the analysis and the ultimate deliverable(s) of the FMECA.

b) The scope defined shall identify the asset or system to be analyzed, the hierarchy level(s) at which the FMECA shall be performed, the analysis approach (i.e. bottom-up or top-down, quantitative or qualitative, etc.), and justify the use or exclusion of the Criticality Analysis portion of the process.

Note: Criticality analysis is useful, particularly where there are constraints on the possible corrective actions based on cost, technical difficulty, or time limitations. However, it may not be practical if all identified failure modes are to be treated or if there is insufficient information to make reasonable estimates of the criticality value.

A.1.2. Definition of the boundaries and scenarios

a) The boundaries should include inputs to and outputs from the asset or system, and explicitly specify which interfaces are within the scope of analysis and which are excluded. In some cases, with complex systems with multiple connections across the boundaries, it may be more valuable to define the boundaries from a functional standpoint to specify the inclusions and exclusions.

b) The scenario descriptions define the use cases for analysis. They should specify all internal and external stress factors that may affect failure modes and effects (i.e., environmental conditions, organizational constraints, human factors, etc.). Examples of scenarios that should be considered include but are not limited to:

i) Normal operation;

ii) Storage;

iii) Premature operation;

iv) Failure to operate at the prescribed time;

v) Intermittent operation;

vi) Failure to cease operation at a prescribed time;

vii) Loss of output or failure during operation;

viii) Degraded output or operational capability; and

ix) Other unique failure conditions, as applicable, are based on system characteristics and operational requirements or constraints.

A.1.3. Definition of the RAMS acceptance criteria for corrective action recommendation and prioritization:

a) The criteria for determining which failure modes require corrective action and priorities for action shall be defined prior to undertaking the analysis to enable consistent and justifiable selection of failure modes which require corrective action, and which do not; and

b) In the case where criticality analysis performance is part of the FMECA Plan, the method by which criticality rating will be estimated/calculated shall be specified.

Note: If a non-Metrolinx standard criticality analysis framework is used, then the FMECA Plan shall include details on how to interpret the ratings for comparison to the Asset Risk Framework and Enterprise Risk Framework to facilitate criticality ranking and corrective action prioritization across different analyses. Any criticality analysis framework used must include at least three (3) and not more than ten (10) categories for both severity and likelihood, resulting in a minimum 3x3 criticality matrix and a maximum 10x10 criticality matrix.

A.1.4. Definition of the documentation and reporting requirements: The FMECA plan shall define the expected outputs from performing the FMECA and how each output is expected to be used. The collective outputs shall form the FMECA Reporting.

A.1.5. Definition of the resources required for analysis:

a) The input information sources required for performing the FMECA shall be defined; and

b) The size of the team of analysts, specific competencies required, and any relevant stakeholders shall be defined.

A.1.6. The FMECA Plan can include additional descriptions of the factors which influence the approach to analysis, as applicable, which include but are not limited to:

a) Milestones to determine the required timing of analysis outcomes.

b) Contractual requirements;

c) CLOS and RAMS performance targets; and

d) Industry benchmarking performance targets.

A.2 FMECA Worksheets Contents

A.2.1. Identify the hierarchy level and operational mode(s) & scenario(s) under analysis, as well as analysis revision information.

A.2.2. Identify functions: a concise statement of each function performed. The functions can be derived from the functional specification or other available sources.

A.2.3. Identify failure modes for each function: list the ways in which each asset or system could fail to perform each function. The analysis objective is to identify all credible failure modes relevant to the analysis objectives. To assist in developing a complete list of credible failure modes, refer to input failure mode information sources [detailed in Section 2.2].

A.2.4. Identify existing detection methods and controls for each failure mode:

a) Detection methods are the means to identify the failure mode, failure, or incipient failure. Early detection of a failure or imminent failure allows for intervention to prevent or reduce the effects of the failure (i.e., warning lights or alarms, monitoring or diagnostics systems, audits, etc.); and

b) Controls are design features, or other existing provisions, which have the ability to prevent or reduce the likelihood of the failure mode or modify its effect (i.e., preventive maintenance, redundant or backup systems, alternative means of operation when detection identifies an issue, etc.)

Note: When controls or detection methods are considered inadequate, then new or improved controls or detection methods shall be determined and form the basis of corrective actions recommended.

A.2.5. Identify the failure effect(s) of each failure mode: the recorded description of each failure effect shall include sufficient information to enable an accurate assessment of the severity and significance of the consequences. The manner in which effects are recorded, and the types of effects to be considered shall be based on those described in the FMECA plan.

a) Where an individual failure mode has no detection method, and the failure effect is not evident, these events shall be recorded for further investigation or analysis. One approach is extending the FMECA to determine the effects of a second failure, which, in combination with the first failure, could result in an unsafe or unacceptable failure condition (i.e. failure of a protective device results in adverse consequences only in the event that both the protective device fails and the asset or system which it is designed to protect fails). Alternatively, other analysis types could be used to investigate the consequences of combinations of failures, such as Fault Tree Analysis.

Note: Rather than considering the effects as a whole, the effects of failure modes may be distinguished between the analysis hierarchy level (local effects), the Metrolinx network level (final/global effects), as well as at any intermediate hierarchy levels as warranted by the level of detail required in the analysis. Identification of local effects generally provides information, which can help when devising corrective actions, though there may not be any local effect beyond the failure mode itself. Identification of final/global effects generally provides a common reference point when considering the relative importance of individual failures.

A.2.6. Identify failure causes: understanding how the failure occurs is useful in order to identify the best way to reduce the likelihood of failure or its consequences. However, the FMECA does not include a method for full causal analysis, and the cost-effectiveness of causal analysis should be considered (i.e. more effort could be dedicated to analyzing causes of failure modes that have a significant effect on functions and objectives than those with a lesser effect). For detailed causal analysis, as warranted per the FMECA Plan, refer to the RCA Process [MX-ALM-STD-005].

a) Common Cause Failures: The analysis should consider possible sources of common cause failure (CCF), where more than one failure occurs simultaneously or within a sufficiently short period of time, as to have the effect of simultaneous failures (i.e., extreme temperature operation, etc.). In the case where a control may fail from the same cause as a failure against which it is meant to protect, then that CCF should be included as a failure cause in the same manner as other causes, and the reasoning for its inclusion included in the documentation.

A.2.7. Perform the Initial Criticality Analysis (CA): which can be carried out either as part of the analysis for each failure mode as each is analyzed for its effects or following the identification of all failure modes.

a) Determine the severity of each failure effect: the severity determined for each failure mode shall represent the significance of its impact. To ensure consistent failure mode prioritization within the FMECA, severity shall be assessed using a clearly identified and common framework as specified in the FMECA Plan;

Note: the severity of an effect might appear more significant at low hierarchy levels if redundancy or other controls are only accounted for at higher levels in the hierarchy.

b) Estimate the likelihood of the failure mode: the time period for which the estimations are made shall be clearly stated in the FMECA, where the period selected shall be appropriate to the objectives of the analysis. The likelihood of occurrence of a failure mode can be estimated using a variety of methods and sources, including:

i) Testing data collected during design.

1) Operational failure rates (i.e., from FRACAS Process [MX-SEA-STD-001]);

2) Failure data for similar assets or systems with comparable use; and

c) Determine the criticality of the failure mode per the selected assessment framework as specified in the FMECA plan (generally calculated as severity x likelihood).

Note: The CA can be tailored to also consider detectability as a separate parameter in addition to likelihood and severity, depending on the complexity of the system and the objectives of the analysis, as detailed in the FMECA plan. However, when not considered separately, the detectability of the failure should be considered in estimating the severity of the effects.

A.2.8. Identify corrective action recommendations: where the reasons for recommending any potential corrective actions are based on the RAMS acceptance criteria as specified in the FMECA Plan. Corrective actions can include but are not limited to; design changes, actions to be taken during operation to prevent or reduce the effects of failure modes, or preventive maintenance as a means of control. Consideration should also be given to removing means of control that are ineffective or unnecessary. Corrective actions may result in one or more of the following:

a) Elimination of the failure mode;

b) Reduction of the likelihood of the failure mode; and

c) Elimination or reduction of the effects of the failure mode.

A.2.9. Perform the Final Criticality Analysis: by following the same process as paragraph A.2.7 while taking into consideration the incorporation of the recommended corrective action(s) impact to the likelihood and/or severity.

A.2.10. Figure A-1 illustrates an outline formatting for the FMECA worksheets. Other formatting is considered acceptable as long as it contains all the above specified fields at a minimum.

Figure A-1 Outline for FMECA Worksheets Minimum Contents

Revision: ______________ Prepared by: ______________ Approved by: _________ Date: _________

Asset/System Hierarchy: ____

Operational Mode(s) & Scenario(s):

Failure Mode & Effects Analysis					Initial Criticality Analysis			Corective Action Recommendations	Final Criticality Analysis		
Functions	Failure Modes	Failure Causes	Failure Effects	Existing Detection Methods & Controls	Likelihood	Severity	Criticality		Likelihood	Severity	Criticaility

A.3 FMECA Reporting Contents

A.3.1. Summarize details from the FMECA Plan, including justification for any deviation from the plan:

a) Identify the subject of the FMECA, including a description of the asset or system under analysis, the appropriate block, functional or flow diagrams which define the structure and interfaces, and any other information relevant to understanding the subject of the analysis;

b) Document all input information sources used, including issue/revision details;

c) Document a clear description of the scope and boundaries, noting any particular exclusions from the scope, including assumptions made in the relevant use scenarios;

d) Detail the RAMS acceptance criteria used to define when corrective action is needed or not; and

e) Document a clear, detailed description of the methodology underpinning the analysis and the framework for the CA;

A.3.2. Identify all personnel (analyst(s), manager(s), and persons with relevant competence) and stakeholders involved in the FMECA.

A.3.3. Identify any limitations or shortcomings in the FMECA to be addressed by future updates (i.e., at different hierarchy levels, etc.) or other analysis (i.e., Fault Tree Analysis for CCF and other multiple failures scenarios, etc.).

A.3.4. Summarize the FMECA results, including recommendations for further analysis, if appropriate, and recommended corrective actions, including clear responsibilities and due dates. When recommendations are incorporated, this shall be identified in the FMECA reporting. In the case that any recommendations are not incorporated, the justification shall be documented in the FMECA reporting.

A.3.5. List the failure modes, their effects, and, if appropriate, their causes and criticality.

A.3.6. Analysis records can also be included as an annex to the reporting in the form of FMECA Worksheets. Where these are extensive, or a database has been used, references to where the information can be found shall be provided.

A.3.7. There is no single reporting format because the full contents of the FMECA reporting will depend on the objectives and context of the analysis.

Appendix B. FMECA Tailoring & Example Criticality Analysis Frameworks

B.1 Overview

B.1.1. This appendix summarizes some of the aspects of tailoring an FMECA. For additional aspects and examples, refer to IEC 60812:2018.

B.2 Top-Down vs Bottom-Up Approaches:

B.2.1. Choosing a starting point for tailoring an FMECA depends upon the purpose and stage of the analysis and how the best value is achieved:

a) Where the starting point to the analysis is the top or mid-levels in the hierarchy, and the causes for the failure modes are limited to the failures in the next lower level(s); this is referred to in this document as a top-down approach;

b) Where the start point to the analysis is at the lowest level of the hierarchy relevant to the objectives, this is referred to in this document as a **bottom-up approach**; and

c) The top-down approach is normally used in the early stages of design and hence may produce a result that is incomplete in-depth and/or breadth as a result of deliberate limitation of scope or lack of available information. However, an early start to the analysis can have a positive impact on future costs. If the project continues to full scale development, the FMECA should be completed using the detailed 'bottom-up' approach so that it can fulfil its purposes.

B.3 Quantitative vs Qualitative Scales:

B.3.1. Assessment of CA parameters, such as severity and likelihood, might be based on quantitative, or qualitative measurement scales.

a) **Quantitative scales** may be useful when relevant operating experience, test data, or prediction is available, enabling a failure rate or probability to be assigned to specific failure modes; and

b) **Qualitative scales** may be useful when failures have to be prioritized, but detailed information is unavailable, or the asset or system is insufficiently defined to enable relevant quantitative data to be applied.

B.4 Criticality Assessment Frameworks:

B.4.1. The following figures illustrate examples of failure mode criticality assessment frameworks, in addition to the example of a failure mode criticality matrix as given

B.4.2. . For further examples, refer to IEC 60812:2018.

B.4.3. The following figures illustrate example categories bands for evaluating likelihood and severity.

Figure B-1 Example Likelihood Categories [Source: EN 50126:2017]

Example 1 - Likelihood (Frequency) of Hazardous Events with Examples for Quantification (Time-Based)

Frequency level	Description	Example of a frequency range based on a single item operating 24 h/day	Example of equivalent occurrence in a 30 year lifetime of a single item operating 5000 h/year
		Expected to happen	
Frequent	Likely to occur frequently. The event will be frequently experienced.	more than once within a period of approximately 6 weeks	more than about 150 times
Probable	Will occur several times. The event can be expected to occur often.	approximately once per 6 weeks to once per year	about 15 to 150 times
Occasional	Likely to occur several times. The event can be expected to occur several times.	approximately once per 1 year to once per 10 years	about 2 to 15 times
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.	approximately once per 10 years to once per 1 000 years	perhaps once at most
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.	approximately once per 1 000 years to once per 100 000 years	not expected to happen within the lifetime
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.	once in a period of approximately 100 000 years or more	extremely unlikely to happen within the lifetime

Example 2 - Likelihood (Frequency) of Hazardous Events With Examples for Quantification (Distance-Based)

Frequency level	Description	Example of a range of frequency
F1	Likely to occur often	more than once every 5 000 km per train
F2	Will occur several times	once every 25 000 km per train
F3	Might occur sometimes	once every 100 000 km per train

Figure B-2 Example Severity Categories [Source: EN 50126:2017]

Example 1 - Severity of Hazardous Events Related to RAM

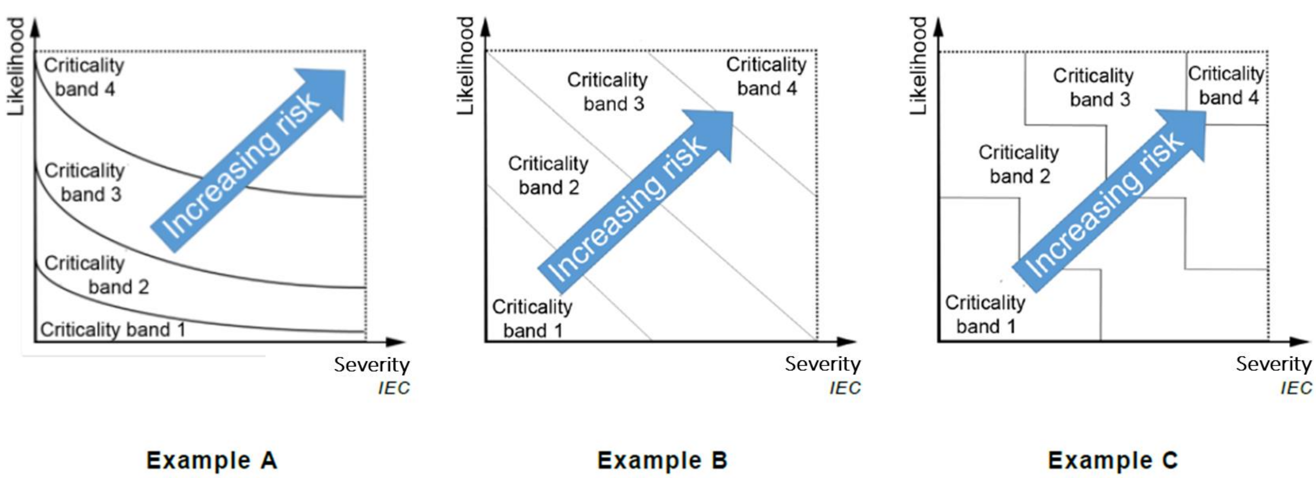
RAM severity category	Description
Significant (immobilising failure)	A failure that: • prevents train movement or • causes a delay to service greater than a specified time • and/or generates a cost greater than a specified level
Major (service failure)	A failure that: • prevents the system from achieving its performance and • does not cause a delay or cost greater than the minimum threshold specified for a significant failure
Minor	A failure that: • does not prevent a system achieving its specified performance and • does not meet criteria for Significant or Major failures

Example 2 - Severity of hazardous events related to Safety

Severity category	Consequences to persons or environment
S1	Many equivalent fatalities (likely more than about 10) or extreme damage to the environment.
S2	Multiple equivalent fatalities (likely less than about 10) or large damage to the environment.
S3	Single fatality or severe injury or significant damage to the environment.
S4	Minor injuries or minor damage to the environment
S5	Possible minor injury

B.4.4. Figure B-3 illustrates examples of failure mode criticality plots showing likelihood against severity, with criticality ranks being assigned according to bands within the plot. In this case, both the likelihood and severity are continuous quantitative scales.

Figure B-3 Example Criticality Plots for Failure Mode Criticality Assessment [Source: IEC60812:2018]



B.4.5. Another method of failure mode criticality analysis is by assigning a risk priority number (RPN). The common form of the risk priority number (RPN) is a product of the three ratings for severity (S), likelihood (L), and detection (D). The range of the RPN values depends on the measurement scales for the three parameters, which usually use ordinal rating scales of 1 to 10, producing overall RPN values ranging from 1 to 1,000.

$$RPN = S \times L \times D$$

– End of Document –