Failure Modes & Criticality Analysis

Transport Roads & Maritime Services

ITS Procedural Guideline | **ILC-ITS-TP0-004-G01**

Contents

Introduction

The “Failure Modes and Effect (Criticality) Analysis” (FMECA) is termed as a bottom-up analysis of system reliability. The FMEA (Failure Mode and Effect Analysis) is based on a qualitative approach, whilst the FMECA takes a quantitative approach and is an extension of the FMEA; wherein a criticality and probability of occurrence is assigned for each given failure mode. The reference standard for FMECA is United States MIL-STD-1629. FMECA is an essential part of Reliability Centred Maintenance (RCM) and is a process used to determine the maintenance requirements of any physical asset in its operating context.

The FMEA/FMECA can be implemented as a functional and or physical analysis. Earlier in a design process a functional analysis approach would be taken. Better definition of the design and as more design details are confirmed permits a physical analysis to be implemented. The FMECA is most effective in providing a contribution to the final system configuration, with respect to reliability performance characteristics, during the actual design phase.

The purpose of FMECA is to identify potential design weaknesses through systematic analysis of the probable ways (Failure Modes) that a component or piece of equipment could fail. This would include the identification of the cause of the failure and its effect on the operational capabilities (functions) of an end item, be it a piece of equipment or a system. Each mission phase of the equipment or system would normally be taken into consideration.

The FMEA/FMECA is generally viewed as an analysis, which should be implemented during the design phase, to have maximum influence and impact on the final design. The FMEA/FMECA serves to input and support other engineering design activities for example:

- Safety Engineering: The FMECA would support the Safety Engineering efforts in analysis such as the Fault Tree Analysis. The failure modes with their assigned criticality would be seen as basic events.
- Testability Engineering: In the development of the FMECA, a column is reserved to annotate the method of failure mode detection/isolation. This information can be used to support a fault diagnostics procedure or validate the effectiveness of equipment built in test capability. Additionally, associated with safety, critical failure modes maybe identified that would otherwise go undetected, presenting themselves as potential hazards.
- Maintainability Engineering: As part of the maintainability analysis, critical to it’s undertaking, is the importance that detection and isolation is accurately reflected in the overall Mean Time To Repair calculations.
- Logistics Engineering: For each failure mode occurrence a resulting corrective maintenance task would be implemented. Of equal importance, in the development of Preventative Maintenance tasks through a Reliability Centred Maintenance approach the FMEA/FMECA plays a significant supporting role. Therefore the occurrence of failure modes, which are caused by wear-out characteristics would be identified and used to supplement the RCM effort.
- Availability Engineering: If an complex system architecture is developed, such as a high availability system employing the use of redundant elements, the FMECA is paramount in ensuring that there are no failure modes in the architecture that would degrade the final availability. This could be most beneficial in sensitive areas such as redundant cross over points (potential single point failures) etc.
- Design Engineering: The FMECA would support the design engineering effort to ensure that program design requirements are addressed. These could be in the support of requirements such as no single points of failure etc.

Process

According to the SAE JA1011 standard, which describes the minimum criteria that a process must comply with to be called a Reliability Centred Maintenance Process answers the following seven questions:

1. What are the functions and associated desired standards of performance of the asset in its present operational application (functions)?
2. In what ways can it fail to fulfil its functions (functional failures)?
3. What causes each functional failure (failure modes)?
4. What happens when each failure occurs (failure effects)?
5. In what way does each failure matter (failure consequences)?
6. What should be done to predict or prevent each failure (proactive tasks and task intervals)?
7. What should be done if a suitable proactive task cannot be found (default actions)?

The level or detail to which the FMECA should be performed would be based upon the purpose and objectives of the analysis. This may mean that certain elements in an system architecture are analysed to no lower than a higher functional level, or in the case of safety critical elements the FMECA maybe required to be developed to include the failure modes of piece-parts or discrete components.

The format required for carrying out FMECA is attached in Appendix A for reference. The failure likelihood levels as defined by MIL-STD-1629 standard are listed below in Table 1.

Table 1: Failure Likelihood Levels.

S. No.	Failure Level	Likelihood Description
	Level A	Frequent. The high probability is defined as a probability which is equal or bigger than 0.2 of the overall system probability of failure during the defined period
2.	Level B.	Reasonable probable. The reasonable (moderate) probability is defined as probability which is more than 0.1 but less than 0.2 of the overall system probability of failure during the defined period.
e	Level C.	Occasional probability. The occasional probability is defined as a probability which is more than 0.01 but less than 0.1 of the overall system probability of failure during the defined period.
4.	Level D.	Remote probability. The remote probability is defined as a probability which is more than 0.001 but less than 0.01 of the overall system probability of failure during the defined period.
5.	Level E.	Extremely unlikely probability. The extremely unlikely probability is defined as probability which is less than 0.001 of the overall system probability of failure during the defined period.

For the sake of analysis the Severity of the error or failure can be divided into four different categories. These are listed in Table 2 (following).

Table 2: Severity Categories.

S. No.	Category	Severity Description
1.	Category I – Catastrophic.	A failure which may cause death or serious financial losses.
2.	Category II – Critical.	A failure which may cause severe injury, major property damage, or major system damage.
3.	Category III – Marginal.	A failure which may cause minor injury, minor property damage, and minor system damage which will result in a delay or loss of system availability.
4.	Category IV – Minor.	A failure not serious enough to cause injury, property damage, or system damage, but which will result in unscheduled maintenance or repair.

Based on the classification given in Table 1 and Table 2, the Criticality of any failure can be determined. Five different Likelihood Levels; based on the probability of occurrence of the failure are listed in Table 1. The four different Severity categories are based on loss or damage of human life or equipment and have been listed in Table 2. The Critically value of a given error with a certain estimated Likelihood of failure and Severity of the consequence of failure can be determined by looking up the number in the cell lying across the corresponding row and column. This number indicates the level of the Criticality and denotes the priority to be assigned to the Criticality. The number one stands for the highest priority while the number six stands for the lowest priority.

The matrix helps to prioritise the Failure Effects Mitigation for each error. Most immediate attention will be given to rectification of the Criticality with the highest priority.

Note that the Criticality priority increases as we move horizontally to the left and vertically to the top of the Matrix. This enables a qualitative analysis of the failures at a glance.

A standard failure mitigation procedure will be implemented in order to manage the identified risks.

Table 3: Criticality Matrix.

LIKELIHOOD	SEVERITY			
	Category I Catastrophic	**Category II Critical**	**Category III Marginal**	**Category IV Minor**
Level A Frequent	1. VERY HIGH	1. VERY HIGH	2. HIGH	3. TOLERABLY HIGH
Level B Reasonably Probable	1. VERY HIGH	2. HIGH	3. TOLERABLY HIGH	4. TOLERABLY LOW
Level C Occasional probability	2. HIGH	3. TOLERABLY HIGH	4. TOLERABLY LOW	5. LOW
Level D Remote Probability	3. TOLERABLY HIGH	4. TOLERABLY LOW	5. LOW	6. VERY LOW
Level E Extremely Unlikely	4. TOLERABLY LOW	5. LOW	6. VERY LOW	6. VERY LOW

LIKELIHOOD	SEVERITY			
	Category I Catastrophic	**Category II Critical**	**Category III Marginal**	**Category IV Minor**
Level A Frequent	1. VERY HIGH	1. VERY HIGH	2. HIGH	3. TOLERABLY HIGH
Level B Reasonably Probable	1. VERY HIGH	2. HIGH	3. TOLERABLY HIGH	4. TOLERABLY LOW
Level C Occasional probability	2. HIGH	3. TOLERABLY HIGH	4. TOLERABLY LOW	5. LOW
Level D Remote Probability	3. TOLERABLY HIGH	4. TOLERABLY LOW	5. LOW	6. VERY LOW
Level E Extremely Unlikely	4. TOLERABLY LOW	5. LOW	6. VERY LOW	6. VERY LOW

Effects Mitigation Action Plan

The Criticality value in the Criticality Matrix has been qualitatively classified into: Very High, High, Tolerably High, Tolerably Low, Low and Very Low. The degree of Criticality will define the mitigation to be undertaken. Generally, the mitigation will proceed as follows:

1. Eliminating the cause of the failure by changing the sub assembly component with a more reliable one. Elimination of cause of failure may also be possible by rewriting the firmware or software.
2. If it is not possible to eliminate the cause of failure it maybe possible to reduce the effect of the failure by making changes in the operational modes of the system or by increasing the redundancy of the system. These changes could result in changes in hardware, firmware or software.
3. If there is some residual failure effect left even after “1.” and “2.” above it can be mitigated by suggesting adequate preventative maintenance procedures. Details of the actions required during maintenance and the frequency of these actions needs to be provided.

A template for recording the actions to be taken for a Failure Effects Mitigation Action Plan is given in Appendix B.

Note: The mitigation can be carried out either by making changes in design, operational procedures, maintenance procedures, or with a combination of all three.

Selection of Maintenance Tasks

The FMECA contributes towards selection of the appropriate maintenance interventions for the system. Once the functions that equipment is intended to perform are identified, the ways that it might fail to perform those intended functions and the consequences of these failures evaluated it is convenient to define the appropriate maintenance strategy for the equipment.

The analysis teams decision of which strategy (or strategies) to employ for each potential failure may be based on judgment and the experience of the individual members. The frequency of the preventative maintenance will depend on the degree of Criticality of the Failure Mode.

Maintenance Planning

Once the appropriate schedule maintenance tasks have been identified, the final step is to package them into a workable maintenance plan. This may involve choosing time intervals at which groups of tasks can be carried out most effectively and efficiently.

Appendix A: Failure Mode Effects (Criticality) Analysis

System:..... Performed By:.....

Ref. Drawing no:..... Date:.....

Description of unit			Description of failure			Effect of failure		Failure Levels.	Severity ranking.	Criticality Priority.
Ref No.	Function.	Operational mode.	Failure mode.	Failure cause or mechanism.	Detection of failure.	On the subsystem.	On the system function.			
1.	VMS Set up / Configuration.	Message Display.	VMS Unobtainable.	Wrong Controller ID, seed or offset.	Error flag raised.	VMS Display Disabled.	VMS Display Blanks out.	C.	Critical.	Tolerably High (3).
2.	Software Interface.	Comm Interface.	Software lockup.	Software bug.	Error message displayed.	Detection failure.	System failure.	D.	Critical.	Tolerably Low (4).
3.	Wireless Comm.	Communications.	Comm failure.	Power supply failure.	Power failure flag raised.	Comm failure.	System failure.	C.	Catastrophic.	High (2).

Note: These entries are for reference only.

Appendix B: Failure Effects Mitigation: Action Plan

System: ..... Performed By: .....

Ref. Drawing no: ..... Date: .....

Ref. No.	Failure mode	Criticality Priority	Failure Effects Reducing Provisions	Design Changes	Operational Changes	Maintenance Procedures/Changes	Action by	When
	VMS Unobtainable	3	Static advisory signage in case of VMS failure Regular Preventative Maintenance	Message be displayed for some time even when VMS is unobtainable	Static Signage be made mandatory for critical messages	Check for correct ID as part of routine maintenance	D: CJ O: AR M: AG	3/12/11 31/1/12 15/1/12
	Software lockup	4	More rigorous software testing Reboot the computer after one hour	Review procedure for testing and automatic system reboot in case of software lockup	Change operational procedures to reboot after 45 minutes if system does not reboot automatically	No Change required	D: CJ O: AR	30/6/11 31/12/12
	Comm failure	2	Backup batteries System generates alarm	Select more reliable Power supply and provide for back up batteries	Alternate communication path be made available	Review Preventative Maintenance procedures to check power supply and batteries	D: CJ O: RR M: AG	3/12/11 30/6/12 15/1/13

D: Design, O: Operation, M: Maintenance.

Note: These entries are for reference only.

About this release

Procedure Number:	ILC-ITS-TP0-004-G01
Procedure Title:	Failure Modes & Criticality Analysis
Author:	Traffic Management Branch
Technical Authorities	Traffic Facilities Asset Management

Issue	Date	Revision description
Issue 1	Sept 2012	Initial Release • This is the first issue of this document under the ILC-ITS Management System. • This document was previously in-use by Traffic Facilities Asset Management
Issue 2	March 2015	General logo and format updates

Note The issue date is normally considered to be the date on which a document is authorised or signed off. Under the ILC Management System, authorisation is indicated by the signature of the authorising manager on the document register. For simplicity then, the date of writing or revising a document is used as the issue date.

This document is published under the Infrastructure Life Cycle Management System and is subject to review and continual improvement. The current version of this procedure is that published on the RMS intranet.

Note: The Infrastructure Lifecycle Management System complies with the requirements of the ISO9001 standard. This standard is revised every four years. While system procedures within the ILC Management System are revised as necessary, to meet any changed requirements of the standard, references within the procedures refer only to ISO9001.

It should be confidently assumed by users that the term ISO9001 within a procedure refers to the most current version of the standard.

HAVE YOUR SAY!

TechInfo welcomes your feedback, ideas, suggestions and constructive comments. If you have any concerns about specifications or other RMS technical documents, using our Improvement Requests system will allow your suggestions to be referred to the person responsible even quicker.
Email: techinfo@rta.nsw.gov.au