Failure Mode and Effect Analysis (FMEA) Procedure

This Version:				
Ver.	Created	Comment	Distribution	Corresponding...
1.0	2016-12-11	First released version	CTA	Editor: George Pruteanu Checker: F. Dazzi Approver: U. Straumann

Keywords:
FMEA, FME(C)A, Failure, Fault, Error, Preventive Maintenance, Corrective Maintenance, Level Maintenance, LRU, LLRU, MTBF, MTTR

Version History:				
Ver.	Date	Comment	Distribution	Corresponding...
0.1	2016-07-14	First draft	PO	Editor: G. Pruteanu Checker: N. Serre
0.2	2016-07-19	Initial comments taken into account	PO	Editor: G. Pruteanu Checker: N. Serre
0.3	2016-09-14	Implemented last PC meeting comments and feedback	PO	Editor: G. Pruteanu Checker: N. Serra

Table of Contents

1 Introduction

This document describes the procedure to perform the Failure Mode and Effects Analysis (FMEA) in Cherenkov Telescope Array (CTA).

The FMEA is an excellent hazard analysis and risk assessment tool to pin-point individual failure modes for corrective action. Additionally, it is a comprehensive and systematic method to establish relations between failure causes and their effects. However, the inability to deal with multiple-failure scenarios or unplanned cross-system effects, requires this tool to be used in conjunction with other analytical tools whilst developing reliability estimates (e.g. Full Tree Analysis).

1.1 FMEA Objectives

The objective of the FMEA is to consider all significant Line Replaceable Unit (LRU) or Lowest Line Replaceable Unit (LLRU) failures, one at the time, assess the effects on the overall product / system and detect conditions where a Single Point of Failure (SPF) can result in interruptions and / or produce a hazardous situation.

1.2 FMEA Scope

The FMEA procedure applies to all design solutions and studies during product design, prototype development, manufacturing and project delivery. The techniques can be applied at various stages of the development to provide effective guidance to the design process.

1.3 Terms and Definitions

The following terms and definitions, are most probably to be used in the FMEA process. For terms listed below please use the CTA Glossary in Jama for definitions:

Active Corrective Maintenance Time

Availability

Common Cause Failure

Corrective Maintenance

Deferred Corrective Maintenance

Degraded Mode

Downtime

Error

Failure

Failure Mode and Effects Analysis

Failure Modes, Effects and (Criticality) Analysis

Failure Rate

Fault

First Level Maintenance

Human Error

Line Replaceable Unit

Lowest Level Replaceable Unit

Maintenance

Maintenance Logistic Time

Mean Time Between Failures

Mean Time to Failure

Mean Time to Repair

Observing-Affecting Failure

Preventive Maintenance

Reliability

Risk Priority Number

Second Level Maintenance

Single Point of Failure

Systematic Failure

Third Level Maintenance

2 References

This section presents all applicable standards, CTA documents / reports, including reference design, used in the development of the FMEA.

Ref. #	Type	Document Title	ID Number
[1]	Standards	Electronic Reliability Design Handbook	MIL-HDBK-338
[2]		Reliability Prediction of Electronic Equipment	MIL-HDBK-217F
[3]		Reliability Modeling and Prediction	MIL-STD-756B
[4]		Engineering Safety Management, Issue 3, Yellow Book	ISBN 0953759504
[5]		Failure Mode/Mechanism Distribution 1991	FMD-91
[6]	CTA Documents	Quality Plan	MAN-QA/110405
[7]		Glossary (Basic Definitions/Acronyms)	Jama (CTA portal)
[8]		Failure Reporting and Corrective Action System (FRACAS	TBD
[9]		Spare Part Management Plan	TBD
[10]		RAMS Analysis Plan	TBD

Table 2.1 – Standards and CTA Documents

3 FMEA Key Aspects and Assumptions

The main key aspects and assumptions used in the FMEA are:

- The FMEA reviews **single failures** and their resulting effects on the system.
- The FMEA covers LRU and LLRU functional failure assuming failure mode occurred 100% (is not in a degraded mode[1] status).
- The FMEA assumes that the CTA product is built, meets the design specification and is operated according to CTA future instructions.
- It is recommended to follow the Product Breakdown Structure (PBS) of the telescopes and instruments and develop FMEAs to the **most convenient level** (including component level - i.e. mirror actuator). The main criterion should be the "**common function**", but it should not necessarily be the only one (e.g. Elevation, Azimuth Drive, Camera Mechanics, Camera Photo-detectors, Camera Signal Processing). If it is decided to do FMEA to LRU's level, consider also the interfaces and when "roll-up" to assembly level ensure that they are not double-counted.
- With the **right preparation**, the **right team**, the **right procedure** and **done correctly**, FMEAs will save money, speed up product development, increase safety, and achieve high reliability in products and processes. However, done improperly, they can waste time and not add value.

4 FMEA Procedures

The person in charge of reliability should work together with work-package Project Manager in organizing a team that consists of 4 to 6 members, selected based on appropriate knowledge and the contribution they can make to the design FMEA. The team should represent the following functional responsibilities within the work-package:

- Design
- Procurement
- Maintenance
- Quality
- Manufacturing / Supplier

The team initiates the FMEA process following the steps and recommendations below.

[1] See *Degraded Mode* definition.

4.1 Overview of the Design

This is one essential step in this process preparation for a successful FMEA start:

1. Help ensure all team members are familiar with the product and its design.
2. Identify each of the main components of the design and associated interfaces, determine their function(s) and document all this.
3. Make sure the team has in depth knowledge of all components and interfaces defined in the FMEA scope.
4. It is recommended to use blue-prints, functional diagrams, schematics for this overview.
5. Add reference numbers to each LRU / LLRU and interface using a PBS numbering allocation scheme.
6. Use the prototype and previous experience.
7. Invite a **subject matter expert** to answer any questions that may arise.

4.2 Brainstorm Potential Failure Modes

A potential failure mode represents any manner in which the component or product could fail to perform its intended function(s). The following are recommended activities to follow during a brainstorm session:

1. Before the start of the brainstorming session, overview the documentation for clues about potential failure modes.
2. Consider potential failure modes for each component and interface.
3. Remember that many components will have more than one failure mode.
4. Document each one.
5. Potential failure modes must not be left out because they rarely happen: this is an important moment to be thorough and to not allow for short-cuts.
6. As input to the brainstorming activity use the existing lessons learned data, warranty reports and reports that identify things that have gone wrong, such as damages and reworks or tests results.
7. Additionally, the team should consider what may happen under difficult usage conditions or special environmental conditions and how the product might fail when it interacts with other products.

4.3 List Potential Effects of Failure

The effect is related directly to the ability of that specific component to perform its intended function. An effect is the impact a failure could have, should it occur. Some failures will have an effect on the operating of the product, others on the environment and / or on the product itself.

Note: *The effect should be stated in terms that are clear and meaningful to product performance. If the effects are defined in general terms, it will be difficult to identify (and reduce) true potential risks.*

4.4 Assign Severity Rankings

The ranking scales are mission critical for the success of a FMEA, because they establish the basis for determining risk of one failure mode and effect relative to another. The same ranking scales of the FMEA should be used consistently throughout an organization. This will make it possible to compare the Risk Priority Numbers (RPNs) from different FMEAs.

The “severity ranking” is based on a relative scale ranging from 1 to 4. A ranking of “4” means the effect has a dangerously high severity leading to a hazard without warning. Conversely, a ranking of “1” means the severity is extremely low. The scales provide a relative, not an absolute classification, as is shown in Table 4.1.

SEV	Severity Criteria
4	- Major risk responses are required to be made quickly.
	- Potential failure mode affects safe operation or involves non-compliance with government regulations.
	- Major damage to the telescope might occur.
	- Data loss for more than three weeks is likely to happen.
	- Loss of life or accident causing permanent disability.
	- Large reduction in safety margin.
3	- Minor damage to telescope might occur.
	- Data loss for more than one week but less than three weeks is likely to happen.
	- No lost time injury or illness per local regulation of Occupational Health and Safety Administration criteria.
	- Significant reduction in safety margin or functional capability.
2	- Data loss for more than one working day but less than one week is likely to happen.
	- First Aid Event per OSHA criteria.
	- Slight reduction in safety margin or functional capability.
	- Major increase in workload.
1	- Failure can be fixed in less than one working day.
	- Minor degradation of the telescope performance.
	- Discomfort or nuissance.
	- Minor increase in workload.

Table 4.1 – Severity Scale and Criteria.

4.5 Assign Occurrence Rankings

The “occurrence ranking” is based on the likelihood, or frequency, that the cause (or mechanism of failure) will occur. The potential cause needs to be identified in order to determine the “occurrence ranking”, because, just like the “severity ranking” is driven by the **effect**, the “occurrence ranking” is dependent on the **cause**. Identify issues that can cause multiple failures: “Common Cause Failures”.

If the cause is known, the frequency of occurrence of a specific failure mode can be better identified. The occurrence ranking scale, is on a relative scale from 1 to 10, as shown in Table 4.2. An “occurrence ranking” of “10” means the failure mode occurrence is very high - i.e. it happens all of the time. Conversely, a “1” means the probability of occurrence is remote.

4.6 Assign Detection Rankings

To assign “detection rankings”, consider the design and all related controls already in place for each failure mode and **only then** assign a “detection ranking” to each control. The “detection ranking” needs

OCC.	Rank Name	Failure Rate (/hour)	MTBF (hours)	Occurrence aprox. once every:
1	Unlikely	< 0.000003	> 360000	~ 100 years
2	Low (few failures)	0.000004	270000	75 years
3		0.000006	180000	50 years
4	Moderate (occasional failures)	0.000009	108000	30 years
5		0.000014	72000	20 years
6		0.000028	36000	10 years
7	High (repeated failures)	0.000278	3600	1 year
8		0.000556	1800	6 months
9	Very High (relatively consistent failures)	0.003333	300	1 month
10		0.014286	70	1 week

Table 4.2 – Occurrence Scale and Criteria.

to be regarded as an evaluation of the ability of the “design controls” to prevent or detect the mechanism of failure.

- “Prevention controls” are always preferred over “detection controls”. Prevention controls prevent the cause or mechanism of failure or the failure mode itself from occurring; they generally impact the frequency of occurrence. Prevention controls come in different forms and levels of effectiveness.
- “Detection controls” detect the cause, the mechanism of failure, or the failure mode itself after the failure has occurred.

A “detection ranking” of “1” means the chance of detecting a failure is almost certain. Conversely, a “4” means the detection of a failure or mechanism of failure is absolutely uncertain as shown in Table 4.3.

DET	Detection Criteria
4	- Design control will not or/and cannot detect a potential cause mechanism and subsequent failure mode.
	- There is no design control for this feature.
	- It is necessary to dismount parts of the telescope to detect the cause of the failure.
3	- Remote or very low chance that the design control will detect the failure or the root-cause.
	- Cannot be monitored from central control. Visual inspection needed but no need to dismount anything.
2	- Moderate or low chance that the design control will detect the failure or the root-cause.
	- Central control monitoring difficult (for instance, different causes might be the reason for the error message).
1	- High chance that the design control will detect the failure or the root-cause.
	- Central control monitoring easy (specific error message for root cause).

Table 4.3 – Detection Scale and Criteria.

4.7 Calculate the Risk Priority Number

The RPN provides a relative failure mode risk ranking, helps prioritize and focus improvement efforts and is calculated as the product of the Severity, Occurrence and Detection Ranking.

Since each of the three relative ranking scales ranges from 1 to 10 or 1 to 4, the RPN will always be between 1 and 160. The higher the RPN, the higher the relative risk.

4.7.1 RPN Threshold

An RPN threshold is to be established for each FMEA as follows:

- Rank in descending order all failure modes based on RPN (RPN(1) highest number to RPN(n) the lowest one).
- Calculate the cumulative sum starting RPN(1), RPN(2), · · · RPN(n), until the sum represents at least 80% of the sum of all RPNs in the FMEA.
- The RPN threshold will be the one where at least 80% is met (see next table as an example)

Failure Mode (FM)	7.1.2.1	7.1.2.4.3	7.1.2.3	7.1.4.3	7.1.4.4	7.1.4.3.2	RPN TOTAL
FM RPN	100	80	56	40	4	3	283
Cumulative Percentage RPN	35%	64%	83%	98%	99%	100%	

Table 4.4 – RPN threshold set-up example.

The above example sets the RPN threshold of 56. For all failure modes with a RPN above this threshold (our example: “7.1.2.1”, “7.1.2.4.3” and “7.1.2.3”) an action plan has to be developed to reduce their RPN under 56. In this example, failure modes with RPN under the 56 but with a severity of “4” should be added to the above list.

4.8 Develop the Action Plan

Taking action(s) means reducing the RPN. The RPN can be reduced by lowering any of the three parameters (severity, occurrence or detection) individually or in combination with one another.

- A reduction in the severity ranking is often the most difficult to attain. It usually requires a design change.
- A reduction in the occurrence ranking is accomplished by removing or controlling the potential causes or mechanisms of failure.
- A reduction in the detection ranking is accomplished by adding or improving prevention or detection controls.

Note: *The failure modes of which the criticality contains severity of “4” should also be considered for an action plan regardless the RPN level.*

A decision of work-packages “**not to address**” for RPN reduction the failure modes exceeding RPN threshold, can be taken “**only in agreement and with the approval**” of the Project Office (PO) Head of RAMS[1], following strong evidence and justification of the decision (risk analysis reports, subject matter expertise test results or any other justification support previously agreed between the PO and the work-package).

4.9 Take Action Plan

The action plan outlines what steps are needed in order to implement the solution as well as people responsible to do so and corresponding estimated completion time. A simple solution will only need a simple action plan while a complex solution needs more thorough planning and documentation. Most action plans identified during a FMEA will be of the simple “who, what & when” category.

[1] Reliability, Availability, Maintainability and Safety (RAMS).

4.10 Calculate the Resulting Risk Priority Number

To recalculate the RPN, reassess the severity, occurrence, and detection rankings for the failure modes after the action plan has been completed. Calculating the resulting RPN using readjusted ranking numbers would confirm the action plan had the desired results.

5 FMEA Report

When a FMEA assembly level is completed (i.e. Camera, Optics, etc), an FMEA report must be provided to PO for gateway reviews. The information to be provided in the FMEA Report is mainly the following:

1. Main schematics and a detailed description of the assembly analysed.
2. A Reliability Bloc Diagram (RBD) for the assembly. An RBD is a method of modelling how components or assembly failures combine to cause system failure. The structure of RBD defines the logical interaction of failures within a system that are required to sustain system operation.
3. A summary of all findings and recommendations following the FMEA analysis.
4. All justifications and supports for previously agreed decisions “not to take actions” to reduce the RPN.
5. FMEA worksheets completed with all significant failure modes, root causes and effects, failures and RPN management on the overall.

6 The FMEA is a Live Document

The FMEA should be updated:

- at the conceptual stage;
- when changes are made to the design;
- when new regulations are instituted;
- when feedback from operators and maintenance personnel indicates.

A FMEA Worksheet

The following are header explanations for the FMEA worksheet.

A.1 Failure Mode Identification

Ref# (ID): each identified failure mode should be assigned a unique reference number on the FMEA worksheet. Use the PBS identification numbers.

Component (LRU / LLRU) are:

- LRU is the smallest faulty unit the maintenance personnel can identify and correct at the First Level of maintenance to restore system availability within a given Mean Time to Repair (MTTR). Each LRU should be designed for ease of replacement and fault isolation.
- LLRU is the smallest faulty unit the maintenance personnel can identify and isolate at the Second and Third Level of maintenance within a given MTTR.

Potential Failure Mode: description of the failure mode or failure mechanism of the LRU / LLRU or identified interfaces.

A.2 Failure Mode Effects

Local Effect: description of the effect when the failure does not affect other subsystem(s) (i.e. redundant or standby components).

Next Higher Level Effect: description of how the failure does affect “same level” or “next higher level” sub-system(s).

Overall System Escalation: description how the failure does affect entire system.

Severity (SEV): please, see Section 4.4.

A.3 Root Causes Identification

Potential Root Causes: description of the possible cause of the failure. It may include specific component failures, interface faults, or more general maintenance or operational errors.

Occurrence (OCC): please, see Section 4.5.

A.4 Criticality

This parameter is used to measure the criticality of failure modes and is the product between Severity and Occurrence and it will be used when ranking to pin-point failure modes with same RPN but high criticality.

A.5 Failure Management

Diagnostic / Detection: indication at what level the failure can be detected or observed. For instance:

- **Local:** the failure has visibility or can be detected with regular tools on-site.
- **Central:** alarms or any other visible information are sent to the central control room, helping to pin-point the failure or root cause.

Mitigation: set of activities or compensating provisions that are required to restore the system.

Comments: any other comment or justification for mitigation actions or detection process.

Detection (DET): please, see Section 4.6.

A.6 Reliability Prediction

Item Failure Rate: quantification in numbers of failures per million hours.

Modal Apportionment: if there are multiple Failure Modes (FMs) for the same component, the modal apportionment is the percentage each one represents. For instance, a battery has multiple FMs, the percentage for each one and therefore their corresponding modal apportionment are as follows:

- Catastrophic Open: 10%
- Catastrophic Short: 20%
- Leak: 20%
- Low Output: 50%

Note that all known FM should add to 100%

Effective Modal Failure Rate: quantification based on a standard set of Failure Modes / Mechanisms Distribution (FMD) used to better evaluate and down-select the failure modes to be addressed if RPN is higher than "RPN threshold" (see reference FMD-91 on Table 2.1).

$$\text{Effective Modal Failure Rate} = (\text{Item Failure Rate }) \times (\text{Modal Apportionment}) \tag{A.1}$$

Data Source: classification of Failure Rate Data Source. It can be:

- E: Estimated (using Standard Prediction Methods);
- S: Supplier;
- C: Calculated based on existing failure information.

A.7 Failure Classification

(Ss) Severity impact on Safety (Yes / No): if the severity classification is driven by the impact on safety (Ss), the answer is "Yes".

(Sr) Severity impact on Reliability (Yes / No): if the severity classification is driven by the impact on reliability (Sr), the answer is "Yes".

SPF (Yes / No): if the failure mode leads to the entire product (e.g. telescope) to fail, the answer is "Yes".

A.8 RPN Management

Action(s) Recommended: proposed action(s) to be taken if the failure mode RPN is above the "RPN threshold" level. Those action(s) are supposed to reduce the assigned severity, detection or occurrence ranking numbers. The goal is that the "resulting RPN" is less than "RPN threshold".

Action(s) Taken: selected action(s) taken in order to reduce the RPN in the severity, in the detection or in the occurrence scale.

New Severity (SEV): reassessment of the severity number after the corrective action was implemented.

New Occurrence (OCC): reassessment of the occurrence after the corrective action was implemented.

New Detection (DET): reassessment of the detection after the corrective action was implemented.

Resulting RPN: multiplication of newly assessed severity, detection and occurrence rankings.

Name of System/Subsystem analysed	Failure Mode and Effects Analysis	Prepared By:		Date:	
		Reviewed By:		Date:	
		Approved By:		Date:	

Failure Mode Identification			Failure Mode Effects				Root Causes Identification			Failure Management						Reliability Prediction				Failure Classification			RPN Management						
Ref# (ID)	Component (LRU/LLRU)	Potential Failure Mode	Local Effect	Next Higher Level Effect	Overall System Escalation	Severity (SEV)	Potential Root Causes	Occurence (OCC)	Criticality (SEV*OCC)	Diagnostic/ Detection		Mitigation	Comments	Detection (DET)	Actual RPN	Item Failure Rate	Modal Apportionment	Effective Modal Failure Rate	Data Source	(Ss) Severity impact on Safety (Yes/No)	(Sr) Severity impact on Reliability (Yes/No)	(SPF) Single Point of Failure (Yes/No)	Action(s) Recommended	Action(s) Taken	Responsibility	New Severity (SEV)	New Occurence (OCC)	New Detection (DET)	Result
										Local	Central																		
									0						0														0
									0						0														0
									0						0														0
									0						0														0
									0						0														0
									0						0														0
									0						0														0
									0						0														0
									0						0														0
									0						0														0
									0						0														0
									0						0														0
									0						0														0
									0						0														0

Table A.1 – FMEA Worksheet.

Glossary

assembly	Jama Glossary
CTA	Cherenkov Telescope Array
failure	Jama Glossary
FM	Failure Mode
FME(C)A	Failure Mode, Effects and (Criticality) Analysis
FMEA	Failure Mode and Effects Analysis
hazard	Jama Glossary
LLRU	Lowest Line Replaceable Unit
LRU	Line Replaceable Unit
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
PBS	Product Breakdown Structure
PC	Project Committee
PO	Project Office
product	Jama Glossary
RAMS	Reliability, Availability, Maintainability and Safety
RBD	Reliability Bloc Diagram
RPN	Risk Priority Number
SPF	Single Point of Failure
work-package	Jama Glossary