The purpose of this SAMPLE document is to show in the public domain a typical FMDEA background developed by:

LIUTAIO
“FUNCTIONAL SAFETY SERVICES”

For preparing this SAMPLE report,

LIUTAIO experience

was used.

Table of Contents

1. Document purpose 3
2. Abbreviations 3
3. Glossary 3
4. References 3
5. FMEDA background 4
5.1 Introduction 4
5.2 What do FMEA, FMECA and FMEDA have in common? 4
5.2.1 To stablish the analysis scenarios. 5
5.2.2 Define “Target System” and its structure. 5
5.2.3 Perform the “Failure Modes and Effects” study 5
5.2.4 Perform the “Failure Modes and Effects” assessment. 6
5.3 Which is the difference between FMEA, FMECA and FMEDA? 6

1. Document purpose

The purpose of this sample document is to show in the public domain an outline about FMDEA methodology that is applied by LIUTAIO “Functional Safety Services.

For preparing this SAMPLE document LIUTAIO experience was used.

2. Abbreviations

Refer to sample document: 0418D10SD01 Abbreviations

3. Glossary

Refer to sample document: 0418D10SD02 Glossary

4. References

[1] LIUTAIO – Functional Safety Services
0418D10SD01 Abbreviations - Sample Document
Rev.01

[2] LIUTAIO – Functional Safety Services
0418D10SD02 Glossary - Sample Document
Rev.01

[3] IEC-60812 2006 Procedure for Failure Mode and Effects Analysis (FMEA)

[4] IEC-61078 2006 Reliability Block Diagram and Boolean Methods

[5] William M. Goble, and Harry Cheddie.
Safety Instrumented Systems Verification - Practical Probabilistic Calculations
ISA 2005.

5. FMEDA background

5.1 Introduction

FMEDA stands for "Failure Modes, Effects and Diagnostics Analysis".

A FMEDA is a systematic detailed procedure that is an extension of the classic FMEA procedure, which purpose is to calculate the failure rates of a "Target System". The "Target System" can be a device or group of devices which perform a more complex function.

This methodology was first developed for electronic devices and recently extended to mechanical and electro-mechanical devices.

A FMEDA assessment of a device or arrangement (group of devices) provides the required failure data (or Reliability data) needed for "SIL verification", "SIL Certification" or to calculate the device contribution in a "Safety Instrumented Function" (SIF) when the SIF's SIL rating is calculated.

5.2 What do FMEA, FMECA and FMEDA have in common?

FMEA stands for "Failure Modes and Effects Analysis".

FMECA stands for "Failure Modes, Effects and Criticality Analysis".

From the methodology point of view, the FMEA, FMECA and FMEDA are the same thing.

The common methodology can be applied prior or during the design, construction or final installation of the "Target System".

The common methodology analyses and reviews the failure modes of each component that is part of a device, to determine each component failure modes in order to rank the chance of failure of all components.

When the methodology is applied to an arrangement of devices, in addition to identify Failure Modes-Effects, a "Reliability Block Diagram" (RBD) of that arrangement shall be developed to evaluate the interaction among the devices. For example:

- Actuator-Positioner-Valve arrangement.
- Pipe Fittings-Pumps-Valves arrangement in a hydraulic power unit.
- Design of an "Uninterrupted Power Supply" (UPS) arrangement.
- Effect of potential failures in components of any electronic or mechanical devices/Circuits in an airplane.

In the common methodology the basic steps are:

1) To establish the analysis scenarios.
2) Define "Target System" and its structure.
3) Perform the "Failure Modes and Effects" study.
4) Perform the "Failure Modes and Effects" assessment.

5.2.1 To establish the analysis scenarios.

The way a device or arrangement fails in an operation/environment condition CAN CHANGE WHEN THE SAME DEVICE OR ARRANGEMENT is working is a different operation/environment condition.

A "Pre-Defined Scenario" shall establish the operation/environment condition where the analysis will take place.

For example:

a) A motor normally running, instead of the same motor normally stopped.

b) A fail close Actuator-Valve arrangement normally opened, instead of the same arrangement normally closed.

c) Failure modes of a mechanical device will be critical in cryogenic conditions, instead of in 0-100 DegC operation conditions.

5.2.2 Define "Target System" and its structure.

The "Target System" can be:

a) A simple device assembled with simple components.

For example: a "Solenoid Valve", and actuator, and exhaust valve, etc.

b) A complex device, where some device's components are complex enough to consider those components as a device.

For example: the analysis target is an airplane, and the "Global Positioning System" (GPS) and the "Propulsion System" are components of the airplane.

5.2.3 Perform the "Failure Modes and Effects" study.

For each simple device a "Failure Mode and Effects Table" (FMET) shall be developed, and this table shall be applied for each "Analysis Scenario" to consider in the study.

The structure of the FMET table can vary for a FMEA, for a FMECA and for and FMEDA.

In addition, the FMET structure can vary according to the "Target System" nature.

Initially the FMET is pre-filled by an FMEA/FMECA/FMEDA "Specialist", or "FME Specialist".

Next, a review/analysis session, like in a HAZOP, shall be performed to allow all representative involved in the project, manufacturing and/or operation of the "Target System" to review/adjust the pre-filled FMET as required.

Of course, the pre-filled FMET are provided to the session participants before the session takes place, but in general way individual comments **SHALL NOT** be considered before the session, because it is better and less time consuming to evaluate the integrated opinion of all session participants to look for the conclusions that consider all points of views.

The result of the "Failure Modes and Effects" study is a report with all reviewed/adjusted FMET tables and Conclusions/Decisions about the "Target" system".

If the "Target System" shall be modified after the "Failure Modes and Effects" study session, the procedure shall be repeated from above step in section 5.2.2. However, minor changes can be evaluated by the "FME Specialist" separately.

5.2.4 Perform the "Failure Modes and Effects" assessment.

The assessment and results are different for FMEA, FMECA and FMEDA. Refer to below section 5.3 for the differences among these assessments.

5.3 Which is the difference between FMEA, FMECA and FMEDA?

As described previously:

- In section 5.2.3: the FMET table can vary according to the "Target System" nature, and if it is performed a FMEA, FMECA or FMEDA.
- In section 5.2.4: The FMEA, FMECA and FMEDA results are different.

The possible different structures of the FMET tables for the FMEA, FMECA and FMEDA assessment **WILL NOT** be discussed in the document, because they are sensitive to the 'Target System" nature and "Analysis Scenarios". Nevertheless, the below description of the FMEA, FMECA and FMEDA assessments results can provide an idea of those tables structures.

The FMEA assessment results are the identification of all ways a "Target System" can fail. These ways are the Failure Modes-Effects.

The FMECA assessment results include the FMEA results and the ranking ALL Failure Modes-Effects. This ranking is used to identify the components (or Devices) with higher impact on "Target System" reliability, where changes or enhancement are required, to improve typically safety indexes like:

- "Average Probability of Failure on Demand" (PFDavg), or
- "Average Dangerous Frequency of Failure" (PFHavg), or
- "Mean Time to Failure Spuriously" (MTTFs), or
- "Mean Time to Failure Dangerously" (MTTFd), etc.

The FMECA can be developed to provide a qualitative or quantitative assessment, and in both cases, it shall provide the "Target System" criticality matrix to show in graphic way which are the components (or devices) with higher and lower impact in the "Target System" reliability.

The FMEDA assessment results include the FMEA results and the "Target System" reliability data. This data can be used for:

a) "Target System" SIL verification.
b) "Target System" SIL certification.
c) "Target System" reliability contribution to a "Safety Instrumented Function" (SIF) when the SIF's SIL rating is calculated.

The reliability data is provided as the quantification (typically FIT, failures per billion hours) of:

1) Safe Detected Failure rate.

Failure rate of "Target System" to move its operation condition from NORMAL to SAFE state, and Safety/Control system or Operator can be notified.

The target plant or equipment is protected.

2) Safe UnDetected Failure rate.

*Failure rate of "Target System" to move its operation condition from NORMAL to SAFE state, **BUT** Safety/Control system or Operator **WILL NOT** be notified.*

The target plant or equipment is protected.

3) Dangerous Detected Failure rate.

*Failure rate of "Target System" where it will remain in NORMAL state when a demand happens, **BUT** Safety/Control system or Operator can be notified to fix the problem or apply maintenance.*

*The target plant or equipment **IS NOT** protected, **BUT** the problem is identified, and there is a chance to fix the failure before a demand.*

4) Dangerous UnDetected Failure rate.

*Failure rate of "Target System" where it will remain in NORMAL state when a demand happens, and Safety/Control system or Operator **WILL NOT** be notified.*

*The target plant or equipment **IS NOT** protected, the problem is **HIDDEN**, and the only chance to identify and to fix the failure is when a "Proof Test" is performed.*

NOTE: If it is required, FMEDA assessment can be oriented to reveal which portion of "Dangerous Undetected Failures" can be identified by "Proof Test". In other word, FMEDA assessment could provide the "Proof Test Effectiveness" (Et) or "Proof Test Coverage" (PTC) of "Proof Test" on "Target System".

5) Annunciation failure rate.

*Failure rate of "Target System" that **WILL NOT** affect safety performance to move its operation condition from NORMAL to SAFE state. For example, a transmitter local display failure.*

6) Any other rate of identified failures that will not make the "Target System" to fail Safe or Dangerously.