Failure Mode Effects and Criticality Analysis (FMECA)

The Failure Modes and Effect Analysis, commonly referred to a FMEA, is one of the most utilized methods for conducting reliability analyses. The Failure Modes and Effects Criticality Analysis (FMECA) is an extension of the FMEA, focusing on the quantitative parameters for a criticality assigned to each probable failure mode, and is discussed below. A widely accepted military standard for conducting FMEAs is Mil-Std-1629. This military standard details the specifics in conducting a FMEA.

The FMEA/ FMECA is analytical tool, which implemented effectively is a powerful design engineering aid. The FMEA/ FMECA is extensively used in the aerospace, military, automotive and space sectors, as part of the system engineering function. These industries have their own variance on how to and why conduct a FMEA, however their intent is the same. For instance NASA focuses on the qualitative aspect of failure modes and their effect on a system, rather than a quantitative approach, which would not be the case in conducting a FMECA as opposed solely to a FMEA. Supporting the NASA FMEA process is a Critical Items List (CIL). This list contains all the failure modes that would have a catastrophic effect on a system or mission.

The Failure Modes and Effect (Criticality) Analysis is termed as a bottoms up analysis. The FMEA is based on an qualitative approach, whilst the FMECA takes a Quantitative approach and is an extension of the FMEA, assign a criticality and probability of occurrence for each given failure mode.

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

FMEA/ FMECA Utilisation

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 its 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 Centre Maintenance approach the FMEA/ FMECA plays a significant supporting role. Therefore the occurrence of failure modes, which are caused by wearout characteristics would be identified and used to supplement the RCM effort.

Availability Engineering: If a 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.

Functional or Physical Analysis

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. With better definition of the design and as more details are firmed up then this will permit 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.

Level of Detail

The level of 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 a system's architecture are analyzed to no lower than a higher functional level, or in the case of safety critical elements the FMECA may be required to be developed to include the failure modes of peace part or discrete components.

> **Example higher functional level failure modes:** A power distribution network, consisting of redundant elements. The purpose of the FMECA maybe to ensure that there are no single point failures in the network architecture which would otherwise have a profound impact upon the system availability.
>
> **Example failure modes of peace part:** Used in a pyrotechnic firing circuit employed in safety equipment, deployed on an offshore oil and gas rig. (E.g. firing mechanism to inflate a life raft). It maybe be necessary to analyze all of the components associated with this circuit and their individual failure modes, giving full consideration to the possible effects due to its operating environment and the dormancy. These components could include the pyrotechnic device itself, wiring harnesses, electronic sensor and firing mechanism.

Failure Modes

The following is a general list of the failure modes of various components.

Component	Failure Mode	Failure Cause
Relay	▪ Contacts Fail Shorted ▪ Contact Fail Open	▪ Contacts Welded ▪ Contacts Dirty/ Corroded
Transformer	▪ Coil Fails Open ▪ Coils Fails Shorted	▪ Open Circuit Coil ▪ Insulation Breakdown
Motor	▪ Bearing Failure ▪ Brushes Fails Open ▪ Coil Fails Open ▪ Coils Fails Shorted	▪ Worn Bearing; Lubrication Failure ▪ Dirty/ worn Brushes ▪ Open Circuit Coil ▪ Insulation Breakdown
Actuator - Hydraulic	▪ Leakage ▪ Fails to Return	▪ Worn/ Damaged Seal ▪ Line Blocked
Switch - SPDT	▪ Contacts Fail Shorted ▪ Contacts Fail Open ▪ Fails to Activate	▪ Contacts Welded ▪ Contacts Dirty/ Corroded ▪ Mechanism Failure
Cathode Ray Tube	▪ Blurred Image	▪ Focusing Screen Misaligned

Component	Failure Mode	Failure Cause
	▪ Incorrect Color ▪ Performance Degradation (luminance)	▪ Color Gun Failure ▪ Chemical Coating Degradation
Brake Mechanism	▪ Activation Failure	▪ Mechanism – Corroded, Worn, Fluid Line Blockage
	▪ Disengagement Failure	▪ Mechanism – Corroded, Worn, Fluid Line Blockage
Power Supply	▪ Incorrect Voltage ▪ Output Voltage Loss ▪ Output Unregulated ▪ Excessive Noise – Electrical	▪ Regulator Failure ▪ Component Failure ▪ Rectifier Failure ▪ EMI Filter Failure

FMECA Column Definitions

The following provides a typical definition for a sample of columns used in a FMECA. MIL-STD-1629. This military specification should be referred to understand each column used and their full definition.

Element Name	Element Description
SEQUENCE NUMBER	A serial number or other reference designation identification number for each failure
ITEM NAME/ FUNCTION	This can be a type of hardware (Electronic Module, Relay, Mechanical Valve etc.) or a function (e.g. Electrical Distribution Function)
FAILURE MODE	All probable failure modes for each item/ function under analysis.
FAILURE EFFECT	The consequences of each assumed failure mode on item operation, function or status are identified in the FMECA sheets. Failure effects can focus on the specific block diagram element which is affected by the failure under consideration. The failure under consideration may impact the several indenture levels, from Local Effects, Next Higher Level Effects and End Effects, as described below.
LOCAL EFFECT	This is normally limited to the effects on the item exhibiting the specific failure mode, for example, an Electrical relay failure mode maybe "Coil fails open circuit", Local effect would be "Unable to Energize Relay"
NEXT HIGHER LEVEL EFFECTS	The effects of the failure as it would been seen at the Next Higher Level (within the system/ equipment structure) would be noted in this column. In the example of the failure mode of the relay, had it been unable to energize, the effect at the Next Higher Level maybe "Loss of 28Vdc to the Motor Starter Circuit Breaker"
END EFFECTS	Evaluate and define the total effect an assumed failure has on the operation, function, availability or status of the system (or equipment). Once again using the relay failure mode example this loss of the Motor Starter Capability at the system level would, cause the loss of an electric motor. HOW CRITICAL IS THE ELECTRIC MOTOR OPERATIONS. If the motor was be used for a Lathe in a factory, it maybe not so critical. If the Motor was be used in the guidance (steering) function of a remote robotic manipulating arm then it could be more critical or severe.
SEVERITY CLASSIFICATION	A severity classification category assigned to each failure mode depending upon its effects of an equipment and/or system operation. The severity classification are consistent between MIL-STD-1629 and MIL-STD-882, and are listed below **Category I – Catastrophic:** A failure which may cause death or weapon system loss (i.e. aircraft, tank, missile, ship, etc.) **Category II – Critical:** A failure which may cause severe injury, major property damage, or major system damage which will result in a mission loss.

Element Name	Element Description
	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 availability or mission degradation. **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. It should be noted that although the definitions of each severity classification category tend to be heavily biased to a military application, they could also be adapted to address commercial concerns, for example: • the loss of an commercial airliner; • the failure of an railway signaling system, resulting in a train collision or even; or • the failure resulting in the severe damage to a production plant, resulting in a prolonged plant shutdown and loss of production revenues can all have their own profound impact
FAILURE DETECTION METHOD	A description of the methods by which occurrence of the failure mode is detected by the operator. The failure detection means, such as visual or audible warning devices, automatic sensing devices, sensing instrumentation or none will be identified.
FAILURE ISOLATION	A description of the procedure that would allow the operator (and maintainer) to isolate the malfunction or failure. The operator may be interested to isolate to a functional level, so that he/she may implement Operational Actions, such as shutting down the offended component within a system. This action may include the switching to a system's redundant element. On the other hand the maintainer would be interested in isolating the failure to the element that would allow for a corrective maintenance action to be implemented. This may be to the offending Line Replacement Unit (or assembly).
REMARKS	Any amplifying remarks pertaining to and clarifying any other column in the worksheet line shall be noted. Notes regarding recommendations for design improvements shall be recorded and further amplified in the FMECA report.

Criticality Analysis

The purpose of the Criticality Analysis is to rank each failure mode as identified in the FMEA, according to each failure mode's severity classification and its probability of occurrence. MIL-STD-1629 is an excellent data source for the implementation of a Criticality Analysis. The result of the Criticality Analysis will leads itself to the development of a Criticality Matrix. The failure mode criticality number for each specific failure mode (**Cm**) is calculated as follows:

$$\boldsymbol{C_m = \beta . \alpha . \lambda_p . t}$$

Where:

$\boldsymbol{C_m}$= Failure Mode Criticality Number
$\boldsymbol{\beta}$= Condition Probability of Failure Effect
$\boldsymbol{\alpha}$= Failure Mode Ratio
$\boldsymbol{\lambda_p}$= Part Failure Rate: e.g. Failures Per Million Hours (fpmh)
$\boldsymbol{t}$= Mission Phase Duration e.g. operational 20 hours

The criticality number of each assembly (or system) is calculated per each severity category. This criticality number is the sum of the specific failure mode criticality numbers related to the particular severity category:

$$\boldsymbol{C_r = \sum_{n-1}^{j} (\beta . \alpha . \lambda_p . t)\, n}$$

$$\boldsymbol{n=1,2,3 \ldots j}$$

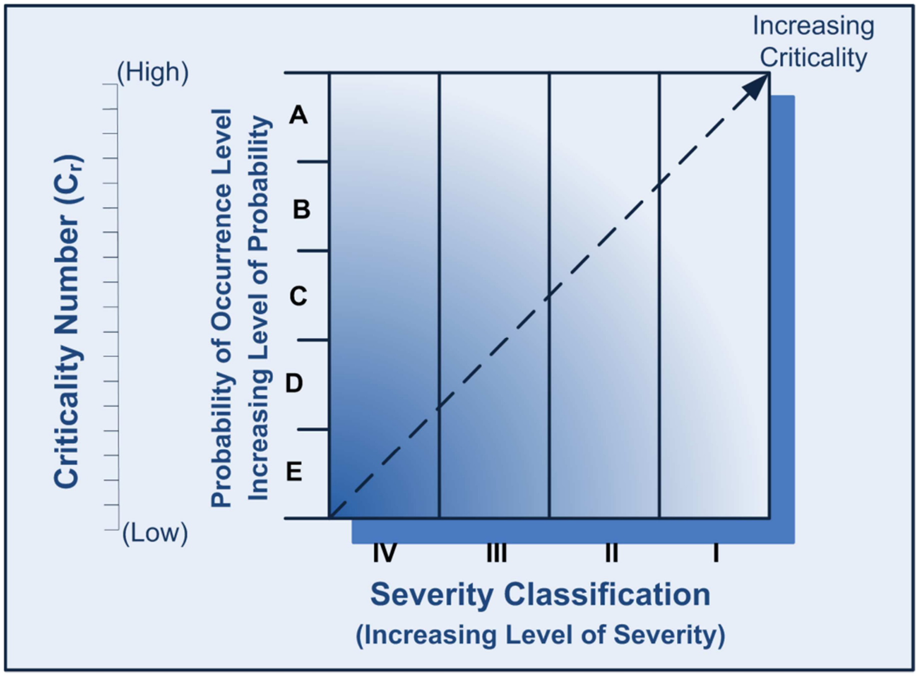
Where: m - number of failure modes at the particular severity category

Where:

$\boldsymbol{C_r}$= Criticality Number for the Item
$\boldsymbol{n}$= The failure modes in the items that fall under a particular criticality classification.
$\boldsymbol{j}$= Last failure mode in the item under the criticality classification.

Criticality Matrix

The resulting FMECA analysis will enable a criticality matrix to be constructed. The criticality matrix displays the distribution of all the failure mode criticality numbers according to the severity category and referring to the criticality scale.


Increasing Criticality
(High)
(Low)
Criticality Number (C_r)
Probability of Occurrence Level
Increasing Level of Probability
A
B
C
D
E
IV
III
II
I
Severity Classification
(Increasing Level of Severity)

In accordance with Mil-Std-1629 the scale is divided into five levels:

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 mission period.

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 mission period.

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 mission period.

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 mission period.

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 mission period.