Table of Contents

1. FMEA/FMECA

Summary:
Failure modes and effects analysis (FMEA) is a reliability evaluation technique to determine the effect of system and equipment failures. This qualitative technique helps identify failure potential in a design or process i.e. to foresee failure before it actually happens. A FMECA is an analytical quantitative technique which ranks failure modes according to their probability and consequences.

1.1. FMEA/FMECA

1.1.1. A description of the technique, including its purpose

1.1.1.1.

Failure modes and effects analysis (FMEA) was one of the first systematic techniques for failure analysis. It was developed in the United States military (Military Procedure MIL-P-1629, titled ‘Procedures for Performing a Failure Modes, Effects and Criticality Analysis’, November 9, 1949) as a reliability evaluation technique to determine the effect of system and equipment failures. Failures were classified according to their impact on mission success and personnel, equipment and safety. In the 1960’s it was used by the aerospace industry and NASA during the Apollo program. More and more industries - notably the automotive industry - have seen the benefits to be gained by using FMEAs to complement their design processes.

1.1.1.2.

This qualitative technique helps identify failure potential in a design or process i.e. to foresee failure before it actually happens. This is done defining the system which is under consideration to ensure system boundaries are established and then by following a procedure which helps to identify design features or process operations that could fail. The procedure requires the following essential questions to be asked:

1.1.1.3.

- How can each component fail?
- What might cause these modes of failure?
- What could the effects be if these failures did occur?
- How serious are these failure modes?
- How is each failure mode detected?
- What are the safeguards in place to protect against accidents resulting from the failure mode?

1.1.1.4.

As an aid in structuring the analysis and ensuring a systematic approach, results are recorded in a tabular format. Several different forms are in use, and the form design can be tailored-made to suit the particular requirements of a study. Examples of forms can be found in BS5760 [1], HSE Marine Risk Assessment Report [1] and Def Stan 00-40 Part 1 [1].

1.1.1.5.

The FMEA analysis can be extended if necessary by characterising the likelihood, severity and resulting levels of risk of failures. FMEAs that incorporate this criticality analysis (CA) are known as FMECAs. A FMECA is an analytical quantitative technique which ranks failure modes according to their probability and consequences (i.e. the resulting effect of the failure mode on the system, mission and personnel). It is referred to as a “bottom-up approach” as it starts by identifying the potential failure modes of a component and analysing their effects on the whole system. It can be quite complex depending how the user drives the technique.

1.1.1.6.

It is important to note that the FMECA does not provide a model by which system reliability can be quantified. Hence, if the objective is to estimate the probability of events, a technique which results in a logic model of the failure mechanisms must be employed, typically a fault tree and/or an event tree.

1.1.1.7.

A FMEA or FMECA can be conducted on either a component or a functional level. A functional FMEA/FMECA

only covers hardware aspects but a functional FMEA/FMECA can cover all aspects of a system. For either approach the general principle remains the same.

1.1.2. When it might be used

1.1.2.1.

FMEA is applicable for any well-defined system but is primarily used for reviews of mechanical and electrical systems. It can be used in many situations, for example, to assess the design of a product in terms of what could go wrong in manufacturing and in service as a result of the weakness in design. It can also be used to analyse failures in the manufacturing process itself and during service. It is effective for collecting information needed to troubleshoot system problems and improving maintenance and reliability of plant and equipment (defining and optimising) as it focuses directly and individually on equipment failure modes.

1.1.2.2.

The FMECA technique is best suited for detailed analysis of system hardware, and should preferably be carried out by the designer in parallel with system development. This will not only speed up the analysis itself, but also force the design team to think systematically about the failure characteristics of the system. The primary use of the FMECA is in verifying that single component failures cannot cause catastrophic system failure.

1.1.2.3.

There are a number of areas today in which the use of FMECA has become mandatory to demonstrate system reliability. Examples of such requirements are in classification of Dynamically Positioned (DP) vessels and in a number of US military applications for which MIL-STD documents apply.

1.1.3. Advantages, disadvantages and limitations to the defence sector or the particular domain

1.1.3.1.

Advantages

- It is widely-used and well-understood, and easy to understand and interpret
- It can be performed by a single analyst, or more if required
- Qualitative data about the causes and effects can be incorporated into the analysis
- It is systematic and comprehensive, and should identify hazards with an electrical or mechanical basis
- The level of detail incorporated can be varied to suit the analysis
- It identifies safety-critical equipment where a single failure would be critical for the system
- Even though the technique can be quite time consuming it can lead to a thorough understanding of the system being considered

1.1.3.2.

Disadvantages

- The technique adopts a bottom-up approach and if conducting a component level FMEA or FMECA this can be boring and repetitive
- The benefit gained is dependent upon the experience of the analyst or, under Def Stan 00-40 Part 1 [1], the group.
- It requires a hierarchical system drawing as the basis for the analysis, which the analyst usually has to develop before the FMEA process can start
- It is optimised for mechanical and electrical equipment, and does not apply easily to Human Factor Integration, procedures or process equipment
- It is difficult for the technique to cover multiple failures as equipment failures are generally analysed one by one therefore important combinations of equipment failures may be overlooked
- Most accidents have a significant human or external influence contribution and these are not a usual failure mode with FMEA
- More than one FMEA may be required for a system with multiple modes of operation
- Due to its wide use there can be temptation to read across data from ARM or ILS projects where, for example, the fault-tree technique has been used. As a consequence, the safety perspective can be lost as human error has been excluded and the focus has been solely on determining faults and on not on more far-reaching safety issues
- Perhaps the worst drawback of the technique is that all component failures are examined and documented, including those, which do not have any significant consequences.
- For large systems, especially those with a fair degree of redundancy built into them, the amount of unnecessary documentation is a major disadvantage. Hence, the FMECA should primarily be used by designers of reasonably simple systems. It should however be noted that the concept of the FMECA form can be quite useful in other contexts, e.g. when reviewing an operation rather than a hardware

system. Then the use of a form similar to the FMECA can provide a useful way of documenting the analysis. Suitable columns in the form could for example include; operation, deviation, consequence, correcting or reversing action, etc.

1.1.4. Sources of additional information, such as Standards, textbooks and web-sites

1.1.4.1.

Def Stan 00-40 Part 1: Reliability and maintainability. [1]

BS 5760: Part 5 Reliability of Systems, Equipment and Components: Part 5 Guide to Failure Modes, Effects and Criticality Analysis. [1]

HSE Website - Marine Risk Assessment, Offshore Technology Report 2001/063 [1]

IET - Health and Safety Briefing 26a - Quantified risk assessment techniques – Part 1 (failure modes and effects analysis – FMEA) [1].

1.1.5. A simple example of an FMEA/FMECA

1.1.5.1.

An example extract from an FMEA of a ballast system is shown below. This can be found in the HSE Marine Risk Assessment Report. The column headings are based on the US Military Standard Mil Std 1629A, but with modifications to suit the particular application. For example, the failure mode and cause columns are combined. The criticality of each failure is ranked as minor, incipient, degraded or critical.

1.1.5.2.

Filling ballast tanks under gravity							
Ref	**System/Equip Failure**	**Cause**	**Effect**	**Detection**	**Mitigation / Compensation / System Response / Safeguards**	**Overall assessment**	**Overall criticality**
1BF	Sea Chest	1. Blocked	Tanks do not full. Reduced stability, change of heel/trim increased hull stresses	• Valve position indicators. • Ballast tank level radar/sounding system. • If severe, angle of heel/trim.	i. Clean chest with steam ii. Redundancy 3 other sea chests	In a worst case where failure was not acted upon quickly then a degraded state could arise where the ballasting operation of several tanks could be affected	D
1BF	Sea Chest	2. Loss of sea chest grid integrity	Ingress of foreign bodies possible blockage of control valves and suction piping. Tanks do not fill. Build up of debris in system. Reduced stability, change of heel/trim increased hull stresses.	• Valve position indicators. • Ballast tank level radar/sounding system. • If severe, angle of heel/trim.	i. Clean chest with steam ii. Redundancy 3 other sea chests	In a worst case where failure was not acted upon quickly then a degraded state could arise where the ballasting operation of several tanks could be affected	D
				• Valve position	i. Clean chest	Overall	

2BF	Sea Chest	1. Partial Blockage	Reduced filling rate.	indicator. • Ballast tank level radar/sounding system.	with steam ii. Redundancy 3 other sea chests	effect considered incipient due to detection ability and redundancy	I
3BF	Sea Chest	1. Leak at sea chest	Loss of ballast control in affected tank. Change of heel/trim.	• Valve position indicator. • Ballast tank level radar/sounding system.	i. Continuously pumped to maintain correct level. ii. Isolate with sea chest blanks. iii. Equalises to exterior sea height in affected tank.	Loss of control in a tank is considered as degraded	D

1.1.6. Additional comments (e.g. Computer tools available, related techniques, different names)

1.1.6.1.

Failure Modes and Effects and Criticality Analysis (FMECA) is an analytical QRA technique, used by ARM and ILS systems engineers, most commonly and effectively at the late design, test and manufacture stage of a project. It requires the breakdown of the system into individual components and the identification of possible failure modes or malfunctions of each component, (such as too much flow through a valve). Referred to as a bottom up approach, it starts by identifying the potential failure modes of a component and analysing their potential effects on the whole system. Numerical levels can be assigned to the likelihood of the failure and the severity or consequence of the failure.

1.1.6.2.

Note: It is important to recognise that FMEA/FMECA Standards have different approaches to criticality. Failure mode severity classes 1 – 5 for Standards MIL1629A and ARP926A go from Class 1 being the most severe (e.g. loss of life) to Class 5 being less severe (i.e. no effect), whereas BS 5760 [1] deals with criticality in the opposite direction where Class 5 is the most severe.

1.1.6.3.

Software:

Isograph,

Reliasoft,

Microsoft Excel.

1.2. Version Control

1.2.1. Version 2.3 to 3.0 Uplift

Source URL: https://www.asems.mod.uk/toolkit/fmeafmeca

Links
[1] https://www.asems.mod.uk/ExtReferences