FAILURE MODES AND EFFECTS ANALYSIS

Introduction

Failure Modes and Effects Analysis (*FMEA*) is a "bottom-up" reliability analysis which considers the failure of component items (the causes) and then examines their effects on the system. Component failure modes are considered systematically, using a set of Guidewords to prompt thought on the possible modes / causes of failure. The failure mode, cause and effect are recorded with the analyst specifying the level of detail required. This method is used to determine the effects of single component or subsystem failures on the overall operation/reliability of a system e.g. supporting reliability documents in a Design Substantiation Report (*DSR*). The study may also include a qualitative assessment of the effect of failure (e.g. catastrophic, critical, major or minor) in order to rank and prioritise failure modes for corrective action. This is called Failure Modes and Effects and Criticality Analysis (*FMECA*) and its primary use is in verifying that single component failure cannot cause catastrophic system failure.

A "Functional FMEA" may be appropriate at the conceptual design stage, where the facility/equipment under consideration is broken down into a number of subsystems. It may not be necessary to know all of the details of the subsystems, e.g. the type, size etc. for a valve, as these requirements are likely to be recommendations from the FMEA output. Therefore a Functional FMEA can be used to apportion reliability targets between subsystems as a basis for more detailed analysis where there is an overall reliability target to be met.

FMEA may be carried out by an individual specialist for the system being studied. A FMEA study is often a precursor to further analysis by quantification methods such as Fault Tree Analysis (*FTA*) or Event Tree Analysis (*ETA*). The output from an FMEA study should therefore be in a form that can readily be carried forward into subsequent analysis.

A FMEA study is not appropriate if internal faults are not known, and it cannot be used to determine the effects of multiple failures. It cannot easily be applied at the early stages of design due to insufficient detail being available on cause and effect.

FTA is the reverse of FMEA in that it is concerned with the identification and analysis of conditions (including component failures) that lead to the occurrence of a defined effect. In contrast to FMEA, it is therefore a "top down" technique.

When considering both techniques the following points may be useful:

- FMEA may be more appropriate than FTA when a large number of distinct system conditions exist which a range of unacceptable consequences.
- Consider using FTA rather than FMEA when there a particular concern about one or just a few system conditions that pose unacceptable consequences. These conditions may have been identified as the system level "effect" using FMEA or some other hazard identification technique.
- FTA is very good at showing how robust a system will be to one or more initiating faults. Thus for systems with high levels of redundancy and/or diversity, or those with majority voting logic, FTA will be more appropriate.
- FMEA is more suited to analysing systems that contain little or no redundancy and does not examine the effects of multiple failures at system level (apart from common cause failures).

- Consider using FMEA when the system contains novel technology and the effects of failure of the components contained within the system need to be explored with insightful judgement.
- Consider using FMEA when there is a need (a) to establish appropriate levels of redundancy within the design of the system, (b) to ensure “fail safe” outputs, (c) to otherwise enhance the design generally.
- FTA enables the fault/failure logic within a system of a particular effect of interest to be represented in diagrammatical form, whereas FMEA records the system effects of each failure cause in tabular format.

In summary, FTA will identify combinations of conditions and component failures that will lead to a single defined adverse effect. FMEA on the other hand considers all single component failures in turn and identifies the range of their effects on the system.

Additional Information & Guidance

- https://www-pub.iaea.org › MTCD › Publications
- https://www.asems.mod.uk/toolkit/fmeafmeca
- IEC 61025 Fault Tree Analysis (FTA) Second Edition December 2006.
- IAEA Nuclear Energy Series No NR-T-3.31 Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for use in Nuclear Power Plant Applications: Appendix ll Failure Analysis Tools and Techniques. Vienna 2020.