Appendix C

Failure Modes, Effects, and Criticality Analysis

C.1 Introduction

Failure Mode and Effects Analysis (FMEA) was one of the first systematic techniques for failure analysis. It was developed by reliability engineers in the late 1950's to determine problems that could arise from malfunctions of military systems. A Failure Mode and Effects Analysis is often the first step in a systems reliability study. It involves reviewing as many components, assemblies and subsystems as possible to identify possible failure modes and the causes and effects of such failures. For each component, the failure modes and their resulting effects on the rest of the system are written onto a specific FMEA form. There are numerous variations of such forms. An example of an FMEA form is shown below.

A Failure Mode and Effects Analysis is mainly a qualitative analysis, which is usually carried out during the design stage of a system. The purpose is then to identify design areas where improvements are needed to meet the reliability requirements. The Failure Mode and Effect Analysis can be carried out either by starting at the component level and expanding upwards (the "bottom up" approach), or from the system level downwards (the "top down" approach). The component level to which the analysis should be conducted is often a problem to define. It is often necessary to make compromises since the workload could be tremendous even for a system of moderate size. It is, how¬ever, a general rule to expand the analysis down to a level at which failure rate estimates are available or can be obtained. Most Failure Mode and Effects Analyses are carried out according to the "bottom-up" approach. One may, however, for some particular systems save a considerable amount of effort by adopting the "top down" approach. With this approach, the analysis is carried out in two or more stages. The first stage is an analysis on the functional block diagram level. The possible failure modes and failure effects of each functional block are identified based on knowledge of the block's required function, or from experience on similar equipment. One then proceeds to the next stage, where the components within each functional block are analysed. If a functional block has no failure modes which are critical, then no further analysis of that block needs to be performed. By this screening, it is possible to save time and effort. A weakness of this “top down” approach lies in the fact that it is not possible to ensure that all failure modes of a functional block have been identified.

An FMEA becomes a Failure Modes, Effects and Criticality Analysis (FMECA) if practicalities or priorities are assigned to the failure mode effects.

More detailed information on how to conduct a Failure Mode and Effects Analysis (and an FMECA) may be found in:

- MIL-STD 1629 “Procedures for performing a failure mode and effect analysis”
- IEC 60812 “Procedures for failure mode and effect analysis (FMEA)”
- SAE ARP 5580 “Recommended failure modes and effects analysis (FMEA) practices for non-automobile applications”
- SAE J1739 “Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) and Effects Analysis for Machinery (Machinery FMEA)”

C.2 FMECA procedure

1. FMECA prerequisites
2. System structure analysis
3. Failure analysis and preparation of FMECA worksheets
4. Team review
5. Corrective actions

Important aspects of FMECA prerequisites are:

1. Define the system to be analysed in terms of (a) System boundaries (which parts should be included and which should not), (b) Main system missions and functions (incl. functional requirements), and (c) Operational and environmental conditions to be considered
2. Collect available information that describes the system to be analysed; including drawings, specifications, schematics, component lists, interface information, functional descriptions, and so on

3. Collect information about previous and similar designs from internal and external sources; including FRACAS (Failure reporting, analysis, and corrective action system) interviews with design personnel, operations and maintenance personnel, component suppliers, and so on.

Various methods for the system structure analysis exist. An SADT analysis may be a good starting point.

A suitable FMECA worksheet for the analysis has to be decided. In many cases the client (customer) will have requirements to the worksheet format - for example to fit into his maintenance management system. A sample FMECA worksheet covering the most relevant columns is given in Figure **??**.

FMECA

System: Performed by:
Subsystem: Date:
Function: Page:

DESCRIPTION OF UNIT			DESCRIPTION OF FAILURE			EFFECT OF FAILURE			FAILURE RATE	CRITICALITY	CORRECTIVE ACTION	REMARKS
IDENTI - FICATION	OPERATIONAL MODE	FUNCTION	FAILURE MODE	FAILURE MECHANISM	HOW TO DETECT	LOCAL	SYSTEM	OPERAT . STATUS				

Figure C.1: Relevant columns in an FMECA form.

C.3 Columns in the FMECA form

Please refer to the listed references to get a comprehensive discussion of the various columns in an FMECA form. In the following we highlight some important aspects.

C.3.1 Operational mode

Example of operational modes are: idle, standby, and running. Operational modes for an air plane include, for example, taxi, take-off, climb, cruise, descent, approach, flare-out, and roll. Also note that operational mode at the system level is not the same as operational mode at the component level.

C.3.2 Failure mechanisms and failure causes

Failure mechanisms relates to physical, chemical or other processes that deteriorates the entity, and leads to a failure The term "failure cause" is often used in two different ways:

- Proximate cause, e.g., failure on a lower level in the system hierarchy such as a defect bearing in a pump

- Root cause, for example bad maintenance, inadequate design etc.

Figure ?? illustrates the relation between function, failure mode, failure cause and failure mechanism:

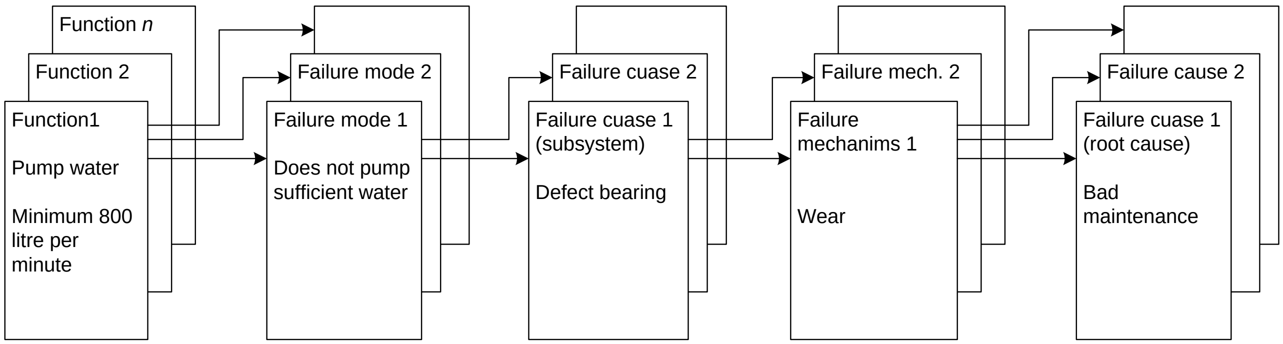

Figure C.2: Relation between function, failure mode, failure cause and failure mechanism

C.3.3 Hidden versus evident failures

We often distinguish between hidden and evident failures. The term “hidden” often relates to entities that is not continuously demanded. For example the SIFA valve on a train (bleed of the air pressure by activation) is a hidden function, and a failure will not be detected automatically. The term “evident” relates to entities that are continuously demanded, and a failure will most likely be detected immediately. Note that the same SIFA-valve will also have a evident function (“not bleed of air pressure under normal operation”) because an unintended activation immediately will be detected (breaks are activated).

C.4 Example of FMECA form

Figure ?? shows an example FMECA form for a bike.

FMECA

System: Bike
Subsystem: Traction
Function: Convert pedal force from the rider to wheel torque

Performed by: Jørn
Date: Some date
Page: 1

DESCRIPTION OF UNIT			DESCRIPTION OF FAILURE			EFFECT OF FAILURE			FAILURE RATE	CRITICALITY	CORRECTIVE ACTION	REMARKS
IDENTI - FICATION	OPERATIONAL MODE	FUNCTION	FAILURE MODE	FAILURE MECHANISM	HOW TO DETECT	LOCAL	SYSTEM	OPERAT . STATUS				
Chain	Running	Convert torque from crank to gear	Not converting Uneven movement	Fatigue	Inspection	No gear torque	Bike is not moving	Can't reach lecture today	Low	High	Bring chain lock	

Figure C.3: Example FMECA for a bike