Chapter 3

Failures and failure analysis

This document is basically a summary of chapter 3 in the textbook *Reliability of Safety-Critical Systems* by Marvin Rausand.

3.1 States and transitions

Some items only operate in one state, e.g., a cooling pump may always be pumping. Other components operate in two or more states, e.g., a safety valve may be in an open position, or a closed position. For each state the item might have different functions. For example a valve in an open position have two main functions, i.e., keep open and close upon demand. Failing to perform a function is denoted a failure, and more precisely:

☞ *Failure*: The termination of the ability of an item to perform as required

A failure is then an event that occurs in time, whereas a fault is a *state* where the item is not able to perform as required. An error is a "discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition". See Figure 3.1 for an illustration. The Norwegian term for failure is 'svikt'.

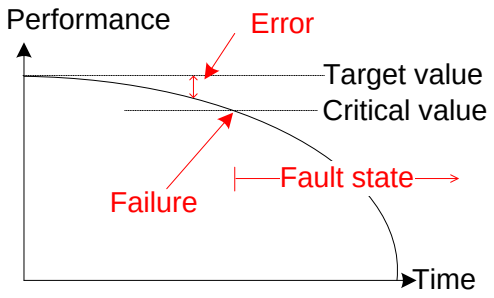

Figure 3.1: Failure and fault

☞ *Fault of an item*: A state of an item, where the item is not able to perform as required. The Norwegian term for fault is 'feil' or 'feiltilstand'.

☞ *Failure mode*: The manner in which a failure occurs, independent of the cause of the failure.

To understand the failure mode concept it is important to have focus on how the failure manifest it self, and not on the cause of the failure.

Example

Consider a shutdown valve that is installed in a gas pipeline feeding a production system. The shutdown valve is a final element of an ESD system, which is performing a SIF. If an emergency occurs in the production system (i.e., the EUC), the valve should close and stop the gas flow. The valve is a hydraulically operated fail-safe gate valve. When an emergency situation is detected in the EUC, an electric signal is sent to the valve control system and the pressure in the valve actuator is bled off. In this example, we consider only the valve. The main failure modes of the valve are:

- *Fail to close on command* (FTC). This failure mode may be caused by a broken spring, blocked return line for the hydraulic fluid, too high friction between the stem and the stem seal, too high friction between the gate and the seats, or by sand, debris, or hydrates in the valve cavity
- *Leakage (through the valve) in closed position* (LCP). This failure mode is mainly caused by corrosion and/or erosion on the gate or the seat. It may also be caused by misalignment between the gate and the seat.
- *Spurious trip* (ST). This failure mode occurs when the valve closes without a closing signal. It is caused by a failure in the hydraulic system or a leakage in the supply line from the control system to the valve.
- *Closing too slowly* (CTS). The process may require the valve to close within a certain time interval (e.g., 10 seconds) after the ESD signal has been given.
- *Fail to open on command* (FTO). When the valve is closed, it may fail to reopen. Possible causes may be leakage in the control line, too high friction between the stem seals and the stem, too high friction between the gate and the seats, and sand, debris, or hydrates in the valve cavity.

The failure rate concept is introduced in Appendix A. Very simplified, we may say that the failure rate, λ, is the frequency of the occurrence of failures:

$$\lambda = \frac{\mathrm{E}[N(t)]}{t} = \frac{\text{Expected number of failures in an interval of length } t}{t} \tag{3.1}$$

The failure rate with respect to failure mode A is often written as λ_{A}.

3.2 Failure causes and mechanism

Failure cause

Definition: Set of circumstances that leads to failure.

The term 'cause' is a difficult term and in our context we distinguish between the "direct" or "proximate" cause and the "root cause", i.e.,:

Proximate cause

Definition: An event that occurred, or a condition that existed immediately before the failure occurred, and, if eliminated or modified, would have prevented the failure

Root cause

Definition: One of multiple factors (events, conditions, or organizational factors) that contributed to or created the proximate cause and subsequent failure and, if eliminated, or modified would have prevented the failure.

Note that the direct or proximate cause on one level in a system hierarchy may be the effect of a failure mode on a lower level. For example the failure proximate failure cause of a pump might be a "bearing failure", where again the failure mode of the bearing is to provide "friction less" rotation of the impeller.

"Behind" the bearing failure we may find the root cause, e.g., lack of lubrication (grease). To trace root causes we may even go further behind, e.g., lack of maintenance and even deficiency in the maintenance management.

Root Cause Analysis

A systematic root cause analysis is usually a brainstorming process with the following steps:

1. Clearly define the failure or fault
2. Gather data/evidence in terms of:

- When and where did the failure occur?
- What conditions were present prior to the occurrence?
- What controls or barriers could have prevented the occurrence?
- What are the potential causes?
- Which actions can prevent recurrence?

3. Ask why and identify the true root cause associated with the failure
4. Check the logic and eliminate items that are not causes
5. Identify corrective action(s) addressing both proximate and root causes
6. Implement the action(s)
7. Observe the effectiveness of the action(s)
8. If necessary, reexamine the root cause analysis

To find root causes it is recommended to ask "why?" at least five times for each main cause identified, e.g.;

1. Why did the pump fail? -> Cause: Bearing failure
2. Why did the bearing fail? -> Cause: Lack of lubrication
3. Why was the bearing not lubricated? -> Cause: Inadequate maintenance procedures
4. Why was maintenance procedures inadequate? -> Bad maintenance management
5. Why was maintenance management bad? -> To much focus on production rather than a holistic perspective on all support processes, thus failing to recruit RAMS students from NTNU!

The term 'failure mechanism' is more fundamental related to what actually leads to a failure:

☞ *Failure mechanism*: The physical, chemical, or other processes that have lead to a failure Examples of failure mechanisms are:

- Corrosion
- Fatigue
- Cavitation
- Wear

3.3 Classification of Failures Based on Consequence and Detectability

Hardware failures can be classified as:

- *Dangerous* (D) failure. A dangerous failure is a failure that brings the item into a state where it is not able to perform its safety function(s). When the item is in such a state, it is said to have a dangerous (D) fault.
- *Safe* (S) failure. A safe failure is a failure that does not leave the item in a state where it is not able to perform its safety function(s). When the item is in such a state, it is said to have a safe (S) fault.

Dangerous and safe hardware failures/faults may also be categorized as detected or undetected.

- *Detected.* A fault that is detected by automatic diagnostic testing, internal in the item or connected to a logic solver.
- *Undetected.* A fault that is not detected (not diagnosed) by automatic diagnostic testing, internal in the item or connected to a logic solver.

Combining the two principles of categorization yields:

- *Dangerous undetected* (DU) faults. DU-faults are preventing activation on demand and are revealed only by proof testing or when a demand occurs. DU-faults are sometimes called dormant or hidden faults. The DU-faults are of vital importance when calculating the SIF reliability as they are a main contributor to SIF unavailability.
- *Dangerous detected* (DD) faults. DD-faults are detected short time after they occur, by automatic diagnostic testing. The average period of unavailability due to a DD-failure is called the mean time to restoration (MTTR), the mean time elapsing from the DD-failure occurs until the function is restored.
- *Safe undetected* (SU) failures. Non-dangerous failures that are not detected by automatic self-testing.
- *Safe detected* (SD) failures. Non-dangerous failures that are detected by automatic self-testing. In some configurations, early detection of failures may prevent an actual spurious trip of the system.

3.4 Random Hardware Faults vs Systematic Faults

IEC 61508 distinguishes between random hardware failures and systematic faults. The standard also treats software faults, but these may be considered a subclass of the systematic faults.

☞ *Random hardware failure*: Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

A random hardware failure can result in a DD, DU, SD, or SU fault. Three features of a random hardware failure can be deduced from the definition:

- A random hardware failure only applies to the hardware part of an item. 2.
- The failure occurs at a random time, which implies that the time when the failure occurs can be described by a random variable with a probability distribution that may be more or less known.
- The failure of the item results in a physical fault and this fault has to be repaired for the item to be able to function again. A random hardware failure is therefore also called a physical failure.

A systematic failure is defined as follows:

☞ *Systematic failure*. Failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors.

Note that corrective maintenance of a systematic failure without modification will usually not eliminate the failure cause.

3.5 Common-Cause Failures

A common-cause failure (CCF) is sometimes defined as follows:

☞ *Common-cause failure*: Failures of different items, resulting from a single event, where these failures are not consequences of each other

CCFs do not fit entirely into the classification of random hardware failure and systematic faults, but CCFs are often caused by systematic faults. Defense measures against systematic faults may therefore also be efficient means to defend against CCFs.

3.6 OREDA Failure Classification System

OREDA is a data source for equipment used in offshore oil and gas production activities. Several OREDA handbooks with generic data have been published, and now the OREDA public data is available through the web (www.oreda.com). The ISO 14224 standard is based on the work carried out in the OREDA project. In OREDA failure causes are classified as either design-related, fabrication/installation-related, operation/maintenance-related, or miscellaneous (not identified or covered by the other categories). Failure effects are split into critical, degraded, and incipient:

- *Critical failure*: A critical failure is defined as a failure of an item that causes an immediate cessation of its ability to perform a required function. In this context, the term "required function" comprises two elements: The ability to activate on demand and the ability to maintain production when safe (no demands). This failure category therefore includes failures that may prevent the execution of a SIF as well as unintended (spurious) activation failures.

- *Degraded failure*: A degraded failure is a partial failure, which means that the item has a degraded performance but that it is still able to perform its essential function. A hydraulic leakage in an actuator for a fail-safe (close) valve may, for example, lead to spurious closure of the valve, but will not, while in open position, prevent the valve from closing on demand.

- *Incipient failure*: An incipient failure is also a partial failure, but its degradation is barely noticeable. An incipient failure is more like a symptom that the item may soon get a degraded failure if no corrective action is taken.

3.7 Failure Modes, Effects, and Criticality Analysis

A Failure Modes, Effects, and Criticality Analysis (FMECA) is a structured, bottom-up technique used to assess the effects on a system of each potential component failure. The FMECA is performed by analysing each component within the system to identify how it might fail (failure mode) and what could be the consequences of such a failure on the system (failure effect). The analysis is usually documented in a specific FMECA worksheet. The FMECA procedure is discussed in Appendix C

The objectives of an FMECA are to:

(a) Identify how each of the system components can conceivably fail (i.e., what are the failure modes?).

(b) Determine the causes of these failure modes.

(c) Identify the effects each failure mode can have on the rest of the system.

(d) Describe how the failure modes can be detected.

(e) Determine how often each failure mode occurs.

(f) Determine how serious the various failure modes are.

(g) Assess the risk related to each failure mode.

(h) Identify risk-reducing actions/features that may be relevant. FMECA is mainly used in the design phase of a SIS to identify and analyze poten-tial failures.

The analysis is qualitative but may have some quantitative elements that include specifying the failure rate of the failure modes and a ranking of the severity of the failure effects. FMECA can also be used in later phases of the life cycle of the SIS. The objective is then to identify parts of the system that should be improved to meet certain safety requirements, or as input to test and maintenance planning.

3.8 Failure Modes, Effects, and Diagnostic Analysis

A Failure Modes, Effects, and Diagnostic Analysis (FMEDA) is an extension of an FMECA that is tailor-made for a SIS. The FMEDA worksheet has additional columns that cover the following:

- Each failure mode is classified as either dangerous or safe.
- The diagnostics related to each failure mode are identified and described. -
- The detectability of each failure mode by online diagnostics is assessed. A number 1 is entered to indicate detectability. A number 0 is entered if the failure mode is not detectable.
- System specific failure rates related to the various categories are estimated, that is, λ_{DU}, λ_{DD}, λ_{SU} and λ_{SU}. Special spreadsheet programs have been developed for this purpose.
- Diagnostic and proof test coverage. The FMEDA worksheet therefore provides traceable failure rates and failure mode distributions as a basis for calculations of PFD_{avg}, PFH, and SFF.

The inputs to and the outputs from an FMEDA are shown in Figure 3.2.

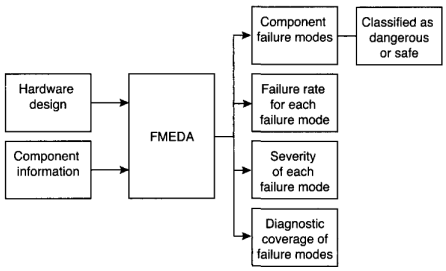

Figure 3.2: FMEDA inputs and outputs (Rausand, 2014)

Bibliography

Rausand, M. (2014). *Reliability of Safety-Critical Systems*. Wiley Series in Probability and Statistics. Wiley.