CHAPTER 8
RELIABILITY AND SAFETY ANALYSIS

Lecture material for TTK 4175 Instrumentation Systems and Safety at the Department of Engineering Cybernetics, Norwegian University of Science and Technology (NTNU).

Author: Professor Mary Ann Lundteigen, Department of Engineering Cybernetics

The essence of a reliability block diagram?
Illustration generated by Microsoft Copilot (powered by OpenAI), July 2025.

The content is updated regularly to improve precision and ensure relevance, which is reflected in the revision number. Please reach out to mary.a.lundteigen@ntnu.no if you have comments or suggestions for improvement.

Rev: 2.0/2026

Revision tracking (most recent)

Rev	Date	Modifications
2.0/26	01.71.2026	Updated after the spring semester of 2025.

Table of Contents

8 Reliability analysis

Reliability is a critical attribute of devices' and systems' performance. It is a type of performance that must be assessed during activities like technology qualification, performance analysis of systems in operation, safety assessments, and the scheduling of maintenance and testing. This chapter introduces basic concepts related to reliability analysis, with a focus on its application to safety-instrumented systems (SIS).

Reliability analysis provides a systematic approach to identifying how systems and devices fail by considering their potential failure modes, estimating failure likelihood, and developing design and operational strategies to mitigate associated risks. This chapter introduces key terminology and failure classifications, explores both qualitative and quantitative analysis methods, and guides the reader through the preparation and execution of reliability assessments. Reliability analysis of SIS focuses on the ability of safety-instrumented functions (SIFs) to perform their required functions when needed, with sufficient fault tolerance and the ability to fail in a manner that ensures or maintains the safe state of the protected system.

Special attention is given to the quantification of Probability of Failure on Demand (PFD) and Probability of Failure per Hour (PFH), the two main reliability performance measures for safety functions proposed by functional safety, like IEC 61508 (2010) and IEC 61511-1 (2016). The chapter also addresses the inclusion of common cause failures (CCFs), the use of reliability data sources, and the importance of updating failure rates based on operational experience. Through this comprehensive overview, readers will gain a foundational understanding of reliability analysis and its critical role in the lifecycle of safety-instrumented systems.

This Chapter has a close link to the following other Chapters: Chapter 6 (SIS), Chapter 9 (Functional Safety), and Chapter 10 (Machinery safety).

8.1 Abbreviations and nomenclature (selected)

CCF	Common cause failures
DC	Diagnostic coverage
DD	Dangerous detected
DU	Dangerous undetected
FTA	Fault tree analysis
IEC	International Electrotechnical Commission
IEV	International Electrotechnical Vocabulary
ISO	International Organization for Standardization
PFD	Average probability of failure on demand
PFH	Probability of having a dangerous failure per hour, alternatively, average frequency of dangerous failures over a given time (measured in hours)
RBD	Reliability block diagram
S	Safe
SFF	Safe failure fraction
SIF	Safety instrumented function
SIS	Safety instrumented system

α	Weigh parameter for updating the failure rate
β	Used with two **totally different** meanings: • Fraction of failure rate (usually DU) that is due to CCFs • Weigh parameter for updating the failure rate (Gamma distribution)
λ	Failure rate (often per hour)
λ_D	Failure rate for dangerous (D) failures
λ_{DU}	Failure rate for dangerous undetected (DU) failures

λ_{DD}	Failure rate for dangerous detected (DD) failures
λ_S	Failure rate for safe (S) failures
λ_{SU}	Failure rate for safe undetected failures
λ_{SD}	Failure rate for safe detected failures
λ_T	Total failure rate
R(t)	Survival probability Pr(T>t)
F(t)	Failure probability – Pr(T≤t)
T	Random variable for time to failure – dependent on the failure distribution
τ	Function test interval
Z(t)	Failure intensity

8.2 Key concepts and terminologies

We will start this chapter by introducing fundamental concepts of reliability, and then the scope of reliability analysis. Note that the term 'system' sometimes refers to a device or several devices, depending on the context. Devices, equipment, components, elements, and items are terms that can sometimes be confusing, as some use them interchangeably while others assign them distinct meanings. Our use of the terms is as follows:

1. **Device:** A self-contained entity that consists of both hardware and software components.
2. **Element:** Often used with the same meaning as a device. For example, final elements are activated devices, such as relays, contactors, and valves, while input elements are sensors, pushbuttons, and switches.
3. **Component:** A part of a device, hardware, or software
4. **Equipment:** Often used with the same meaning as a device but can also cover groups of devices depending on the context, e.g., “equipment group”.
5. **System:** A composition of some of the above-listed entities that serve a specific purpose
6. **Item:** The item generally refers to a device or component that is incorporated into a reliability model.

Reliability analysis is directed to specific functions of the listed entities.

8.2.1 Definition of reliability

A natural starting point is to clarify the meaning of the term **reliability**. While we often use this word in everyday conversation, we may not always consider its precise definition. One of the best sources to use is the online Electrotechnical Vocabulary (IEV), available at https://www.electropedia.org, which defines terms as they are used in international IEC standards.

According to the IEV, reliability is defined as:

> **Reliability**: *The ability (of a function) to perform as required, without failure, for a given time interval, under given conditions.* [IEV ref: 192-01-24]

The key point here is that reliability refers to the capability of a function, meaning a specific task carried out by a system.

A single device or system may perform multiple functions, and the reliability of each function must be assessed individually. According to Rausand and Høyland (2004), these functions can be categorized as follows:

- **Primary function**: This is the main purpose of the system. It defines the core task the system is designed to perform. *Example*: A smoke detector’s primary function is to detect smoke in a room.
- **Auxiliary function(s)**: These are supporting functions that are indirectly necessary for the primary function to operate correctly. *Example*: The power supply interface that ensures the smoke detector remains powered.

- **Information function(s)**: These functions provide information about the system's status. They may include diagnostics, feedback, or configuration data. *Example*: A status LED or a diagnostic signal indicating sensor health.
- **Interfacing function(s)**: These functions enable the system to communicate or interact with other systems. *Example*: A detector with both 4–20 mA and HART communication interfaces.
- **Protective function(s)**: These functions protect the system from damage due to external or internal conditions such as overcurrent, environmental hazards, or mechanical stress. *Example*: An explosion-proof housing for a smoke detector used in hazardous areas (see Chapter 12 on ATEX).
- **Superfluous function(s)**: These are functions that are present in the device but not used in the specific application. Even though they are unused, their potential failure could still impact required functions. *Example*: A wireless interface on a detector that is not currently in use may still pose a risk if it interferes with other functions.

In technical systems, reliability is a subset of dependability, a term that encompasses (beyond reliability) maintainability, maintenance support, performance, safety, and security. In human and organizational systems, the subset of reliability encompasses the study of human error and its associated probability.

The phrase **"**ability to perform" implies that system performance is not guaranteed with absolute certainty. Instead, reliability is typically expressed as a probabilistic measure, for example, the probability that a system will operate without failure over a specified period, or conversely, the probability that it will fail within that time.

This ability to perform depends not only on the system's inherent design and properties but also on the operating conditions. These conditions include factors such as the mode of operation (e.g., startup, normal, or abnormal), environmental exposure, stress levels, and potential human interaction, especially when inappropriate or unintended. All of these can significantly influence the system's actual reliability in practice.

Generally, we may classify the measures of reliability as either:

7. **Probabilities:** Examples include the reliability or survivability function R(t), the failure function F(t), the availability function A(t), and their averages calculated over a given time, such as the average uptime, the average downtime, the average probability of failure on demand (PFD), and the average probability of having a dangerous failure per hour (PFH).
8. **Expected (or mean) lifetime** or **time to failure**: Examples include mean time to failure (MTTF), mean time between failures (MTBF), and remaining useful life (RUL).

8.2.2 Failure terminologies

A key aspect of reliability analysis is understanding **how and why systems fail**. A starting point is to introduce the primary terminology related to failure. The reliability discipline often distinguishes between the following terms:

- **Failure**: *Loss of ability to perform as required.* [IEV 192-03-01]
- **Fault**: *Inability to perform as required, due to an internal state.* [IEV 192-04-01]
- **Error**: *A discrepancy between a computed, observed, or measured value or condition, and the true, specified, or theoretically correct value or condition.* [IEV 192-03-02]

Fig. 1 illustrates how errors, failures, and faults may be related, considering whether they occur at the component level and their impact at the system level. A fault at the component level may occur as a shock, leading to a transition from the normal state to the fault state, or because of an error. Depending on the component's role at the system level, the fault may result in an error or a complete fault.

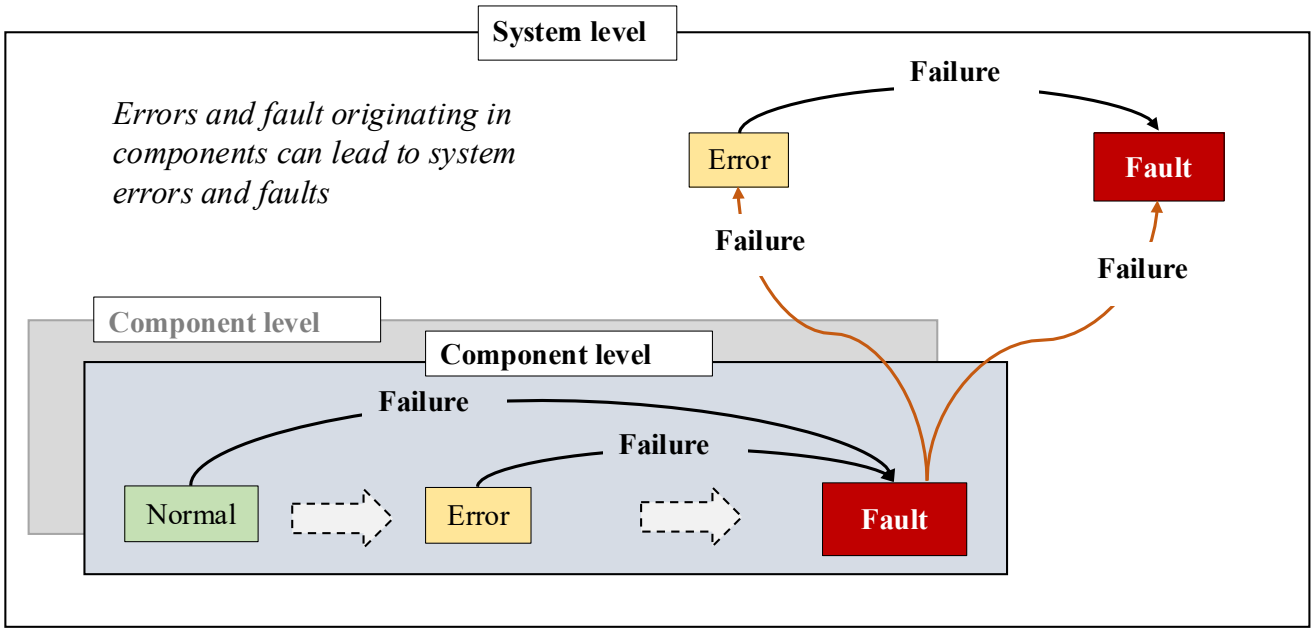


Fig. 1. Relationship between error, failure, and fault (alternative 1)

Fig. 2 shows an alternative way to distinguish between error, fault, and failure, applicable to a continuously operating system, such as a pump. The working state is defined by a target value, or setpoint, with defined upper and lower boundaries. Here, an "error" is the state where the output (blue curve) deviates from the target value without exceeding the specified limits. Another interpretation of error (not shown in Fig. 2) is the difference between the measured output (blue curve) and a real (actual) value (not shown in the figure). Failure occurs when the error exceeds the upper or lower boundary of the working state. The impact can be a fault or a degraded state. The degraded and fault states can be permanent or temporary, as indicated by the blue curve.

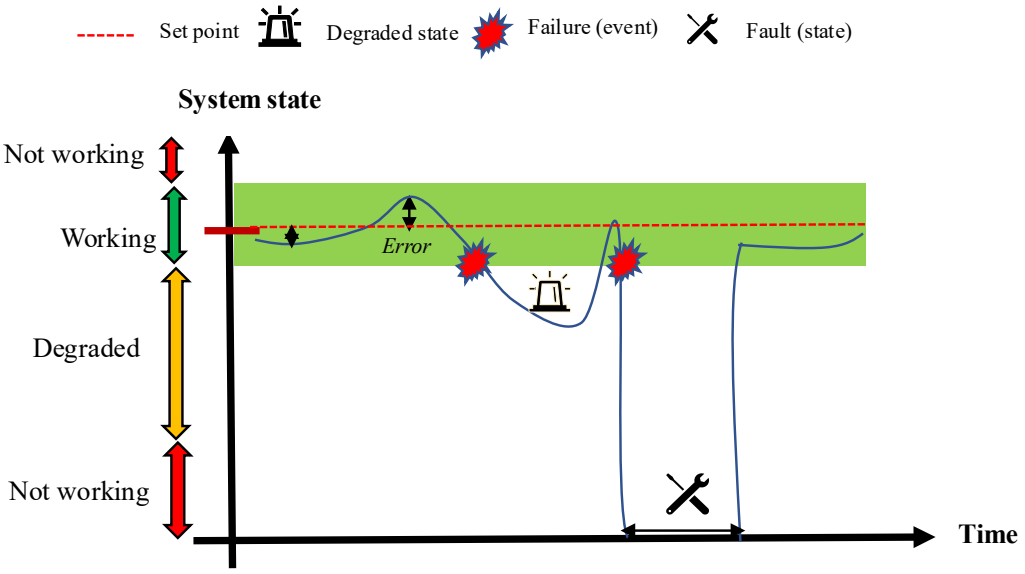


Fig. 2. Relationship error, failure, and fault (alternative 2)

8.2.3 Failure modes and failure causes

Failures can be further analyzed and characterized by examining their **failure modes**, **failure causes**, **failure mechanisms**, and **root causes**, as illustrated in Figure 5. We begin with the concept of a **failure mode**, which is defined as:

> **Failure mode**: *Manner in which failure occurs.* [IEV 192-03-17]

The phrase *"manner in which"* refers to how a failure manifests itself—how it can be observed, interpreted, or explained. In general, typical failure modes include:

- The function is not performed at all
- The function is performed too late or too early
- The function is performed when not required

Failure modes can apply to any function, whether primary, auxiliary, information, interfacing, or protective, depending on the focus of the failure analysis.

A shutdown valve has, for example, failure modes like failure (or fail) to close, delayed operation, premature (spurious) failure, and leakage in the closed position. A pressure transmitter that transmits an analog measurement value can exhibit failure modes, including no measurement, measurement outside the 4-20 mA range, a too-low measurement value, and a too-high measurement value.

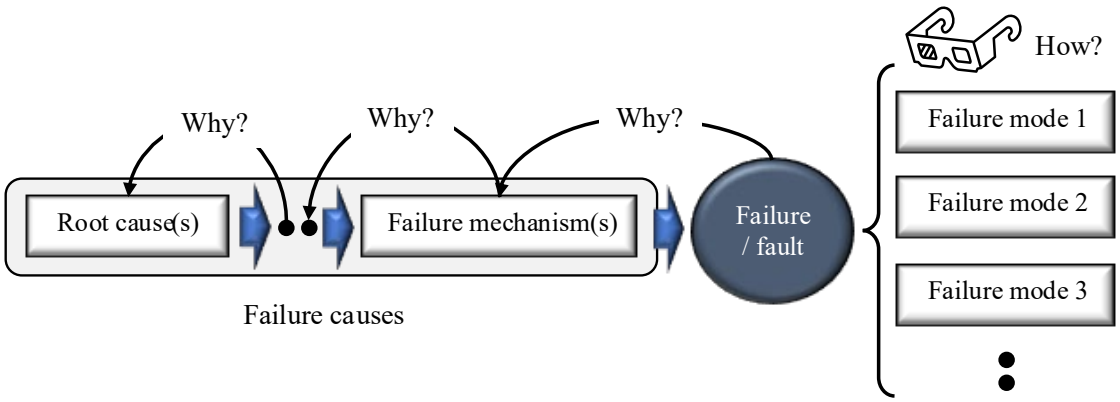


Fig. 3. Relationship between failure terminologies

In reliability analysis, it is not only essential to understand **how** a system can fail, but also to assess the **severity** of failures and identify their **causes**. Without these insights, it becomes difficult to prioritize and implement effective reliability improvements. Fig. 3 illustrates the relationship between the terms failure cause, failure mechanism, and root cause.

Here, a failure cause is defined as:

> **Failure cause**: *Set of circumstances that leads to failure.* [IEV 192-03-11]

Failure causes are often split into failure mechanisms and **root causes**.

> **Failure mechanism**: *Process that leads to failure.* [IEV 192-03-12]

Here, the failure process relates to the physical, chemical, logical (software-related), or a combination of these. Common examples include corrosion, erosion, vibration, incorrect operation, or an improper sequence of actions.

The root cause is the result of an iterative search for the most basic cause of failure:

> **Root cause**: *The underlying cause that led to the fault.*

Root causes may be technical, but they are often human and organizational, such as a lack of training, errors in installation or calibration procedures, incorrect material selection, insufficient environmental protection, wear and tear, inadequate quality assurance, or poor testing practices. While a failure mechanism identifies the immediate technical reason for a failure, the root cause points to deeper systemic issues that, if addressed, can help prevent similar failures in the future, both for the current system and for others with similar characteristics.

8.2.4 Root cause analysis

Understanding the underlying causes of failures is essential for improving system reliability and preventing recurrence. One of the most widely used techniques for this purpose is Root Cause Analysis (RCA). RCA is a structured approach for identifying the root causes of faults, failures, or other undesirable events, enabling corrective actions at the source.

> **Root Cause Analysis**: *A systematic process to find the cause of a fault, failure, or undesired event, so that it can be removed by design, process, or procedure changes.* [IEV 192-12-05]

A root cause analysis method is the Fishbone Diagram, also known as the Ishikawa Diagram (Rausand, 2014).

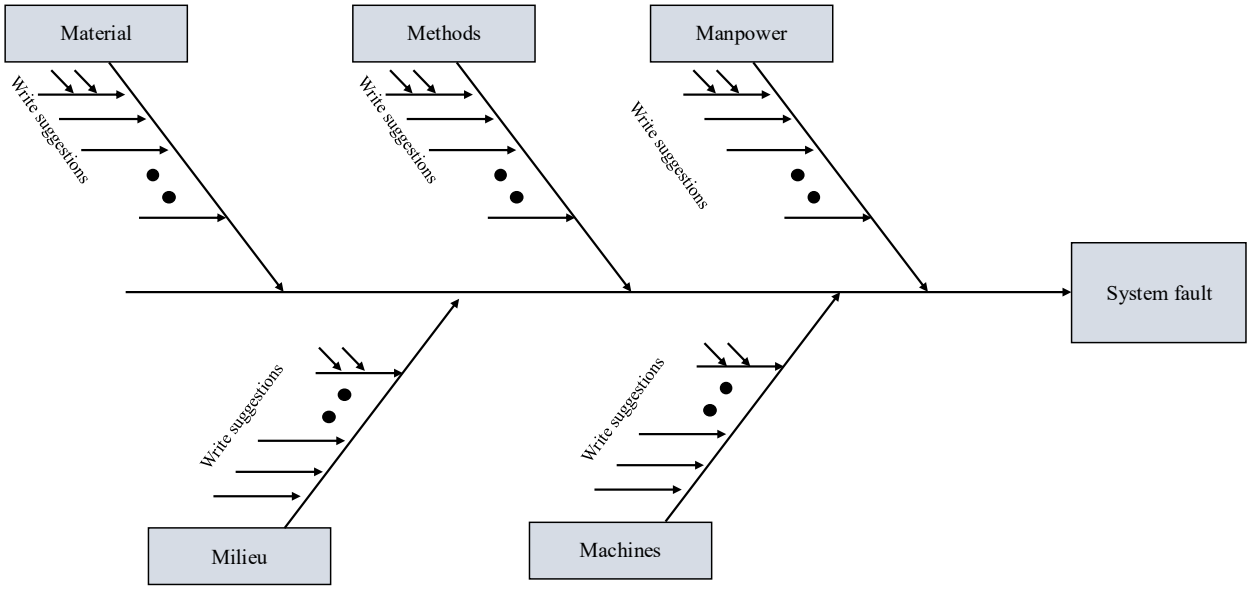


Fig. 4. Fishbone analysis for cause-and-effect analysis

This visual method helps organize potential causes of failure into categories, making it easier to explore contributing factors. The steps for constructing a fishbone diagram are as follows:

1. Identify the system fault or failure under investigation.
2. Draw the diagram shown in Fig. 4, using the "5 Ms" as main branches: Manpower, Methods, Materials, Machinery, and Milieu (environment).
3. Add arrows to each branch to represent contributing factors.

4. Expand with sub-arrows to show more detailed sub-causes under each category.

While the "5 Ms" are a helpful starting point, they can be interpreted broadly to suit different contexts:

- **Manpower**: Personnel involved in operation or maintenance, directly or indirectly.
- **Methods**: Procedures, tools, testing methods, and work practices.
- **Materials**: Physical materials (e.g., device components) and software (e.g., programming languages).
- **Machinery**: Technical components, system parts, interactions, and software algorithms.
- **Milieu**: Environmental conditions such as humidity, temperature, wind, and also external influences like infrastructure or interfacing systems.
- Machines: Technical parts, including system parts, interactions between these, and software algorithms.

The analysis stops when no further information is found. The analysis can also be conducted in a more open-ended manner, meaning identifying causes that may potentially lead to a specific type of system failure.

A root cause analysis is often extended with an impact (or effect) analysis. The analysis of effects can help prioritize the most critical failure causes to target, especially when time, costs, and resources are limited. Failure Modes, Effects, and Criticality Analysis (FMECA) is one such method, which is explained later in this chapter.

8.3 Reliability analysis

Reliability analysis involves a set of steps and methods used to evaluate a system's reliability and to suggest measures to improve it when the requirements are not met. A combination of qualitative and quantitative methods is applied, depending on the purpose and phase of the reliability analysis. There are various ways to visualize this process; one such example is illustrated in Fig. 5.

The content of each step includes the following:

1. **System familiarization:** This step involves collecting information about the system, including its purpose, operational environment, modes of operation, and regulatory requirements. Conduct a functional analysis to identify system functions, and as needed, categorize them into types such as primary or essential functions, supportive functions, informational functions, interface functions, and others. The step also includes determining the reliability requirement that the system function(s) must satisfy.
2. **Graphical representation:** A graphical representation helps visualize system functions and their interactions with other systems. Functional block diagrams and system decomposition are often applied.
3. **Qualitative analysis:** This step involves identifying systematically how system devices may fail. Applicable methods include functional hazards analysis (FHA), failure modes, effects, and criticality analysis (FMECA), as well as variants of FMECA.
4. **Quantitative analysis**: This step involves making a reliability model, identifying the necessary input data for calculating reliability, and interpreting the results. Examples of applicable methods reflecting different types of reliability models are:
   (i) Reliability block diagrams (RBDs),
   (ii) Fault trees (FT)
   (iii) Markov state transition diagrams
   (iv) PetriNets
   (v) Monte Carlo simulations

   The choice of method can be based on what fits best for the type of analysis and the competence and preferences of the persons responsible.

It may be noted that RBDs, Markov state transition diagrams, and fault trees can also be helpful for qualitatively assessing the properties of the functions.

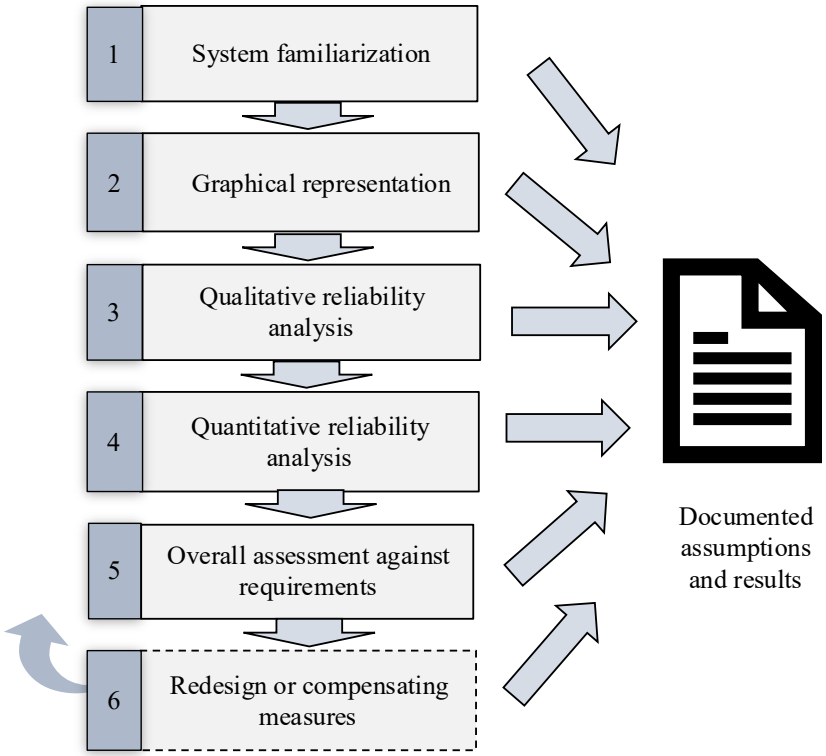


Fig. 5. Reliability analysis process

5. **Overall assessment:** Evaluate the results of the qualitative and quantitative analyses, considering the requirements, validity of assumptions, and contributing factors to uncertainty. Results may be applied in different contexts, such as:
    1. Approving the design before fabrication
    2. As input to maintenance planning, to decide when it is most cost-efficient to schedule the next maintenance.
    3. As input to the evaluation of remaining useful life, to decide whether it is safe to postpone a replacement or not.

    Decisions may need to consider the impact of uncertainty. Probabilities are, in themselves, an expression of uncertainty; however, other measures of uncertainty, such as confidence intervals and sensitivity analyses, may help complement them. For example, to what extent would a change in one specific failure rate, such as switching from a mean value to one with 90% confidence, influence the decisions? Is the confidence bound narrow or wide?

6. **Redesign or compensating measures:** If the qualitative and/or quantitative analyses indicate that the reliability requirements are not met, it may be necessary to redesign the system or modify its operation. Design measures may include adding redundancy, selecting more reliable devices, or increasing diagnostic coverage. The final choice for redesign must balance the added complexity and costs with the reliability gains achieved. Operational adjustments can include more frequent or different types of inspections and repairs, personnel training, or modifications that reduce environmental or operational stresses.

The rest of the chapter continues to introduce concepts and methods relevant to the reliability analysis process. We will focus primarily on quantifying the reliability of safety-instrumented functions (SIFs), which are individual safety functions performed by safety instrumented systems (SIS). Examples of SIS systems are provided in Chapter 6, which is devoted to such systems.

8.4 Failure classification

Failure classification involves grouping failures of similar devices by severity or underlying cause. The classification helps prioritize corrective actions and organize failure statistics. Failure classification can be done in numerous ways, and we are presenting a few of these in the following.

Classification by Lifecycle Phase: Failures are categorized by the phase at which they are introduced or manifested. Examples include:

- Specification failure – Errors or omissions in defining system requirements.
- Design failure – Flaws introduced during the design process.
- Construction failure – Issues arising during system fabrication or assembly.
- Installation failure – Problems encountered during setup or integration.
- Usage failure – Failures occurring during operation or maintenance.

Classification by Root cause: Failures grouped based on broad categories of underlying causes:

- Technical failure – Resulting from hardware, software, or system limitations.
- Human failure (human error) – Caused by mistakes in operation, maintenance, or decision-making.
- Organizational failure – Related to inadequate competence, unclear roles, or insufficient resources.

SIS-specific classification: Classification chosen by international standards on functional safety, such as IEC 61508 (2010) and its process-industry variant IEC 61511-1 (2016). They distinguish between:

- Systematic and random failure (causes)
- Dangerous and safe failure (impacts)

In the following sections, we will focus specifically on these SIS-related failure categories, with emphasis on IEC 61511-1 (2016).

8.4.1 Dangerous vs safe failures

A device may have several failure modes. For example, the failure modes of a valve can include failure to close, failure to open, failure to open spuriously, leakage in the closed position, and delayed operation. Each of these failure modes can be classified as either dangerous or safe when used in a safety system.

IEC 61511-1 (2016) defines a dangerous failure as follows:

5. **Dangerous failure:** Failure which impedes or disables a given safety action of the device.

A dangerous failure is therefore a critical failure and of high importance when determining a safety system's ability to perform its safety actions. The same standard defines a safe failure as:

6. **Safe failure:** Failure which favors (meaning execution) a given safety action, i.e., that results in a spurious activation/operation of the device's safety function so that its safe state is achieved.

Failures of (non-safety-related) functions carried out by a device, such as reopening a fail-close shutdown valve, are sometimes defined as safe failures, even if not strictly in accordance with the definition. In general, safe failures receive limited attention in safety analyses, as their consequences are mainly economic, such as losses from unscheduled shutdowns. One exception is the calculation of the safe failure fraction (SFF), where it is important to incorporate only the "true" failures (those leading to spurious activation). However, some

sources note that safe failures leading to unscheduled plant shutdowns can indirectly affect safety by introducing risks during unexpected stopping and restarting of large facilities. In reliability analyses of SIS functions, the focus is placed on dangerous failures. In contrast, safe failures are considered relevant for production availability assessments, which are not covered in detail in this chapter.

Classification of failure as "dangerous" or "safe" cannot be made generically, meaning without considering the context in which the device is used. Data handbooks and manufacturers' certificates must specify the assumptions under which the failure classification is applied. For example, the failure mode "fail to close" is dangerous if the safety action is to close a valve, but safe if the safety action is to open.

Some failures are safe in the sense that they have no negative impact on safety. For most practical purposes, they are defined as safe failures. However, IEC 61508-4 (2010) has introduced two additional categories to ensure that they are not counted as safe failures for product certification.

- **No effect failure:** A failure that does not affect the execution of the SIF.
- **No part failure:** A failure that is not directly part of the SIF.

8.4.2 Detected vs undetected failures

Failures that are detected immediately, typically through online diagnostics, can often be corrected quickly or mitigated through compensating measures. However, this would not be the case for many SIS devices, which are passive during normal operation. Failures of such components may be hidden for a longer period, and regularly scheduled tests are necessary to reveal such failures. For the purpose of a more detailed classification of failures, IEC 61511-1 (2016) defines two detection methods:

7. **Detected failure:** A failure relating to hardware and software failures or faults which are not hidden because they announce themselves or are discovered through normal operation or through dedicated detection methods, such as diagnostics.
8.
9. **Undetected failure:** A failure that is hidden as it is not detected by diagnostics.

Safe (S) and particularly dangerous (D) failures are consequently split into detected (D) and undetected (U), leading to the four failure categories: SU, SD, DU, or DD, as shown in Fig. 6. Among these, the DU failure category leads to the longest safety unavailability and, therefore, is the most important when calculating the reliability of safety functions.

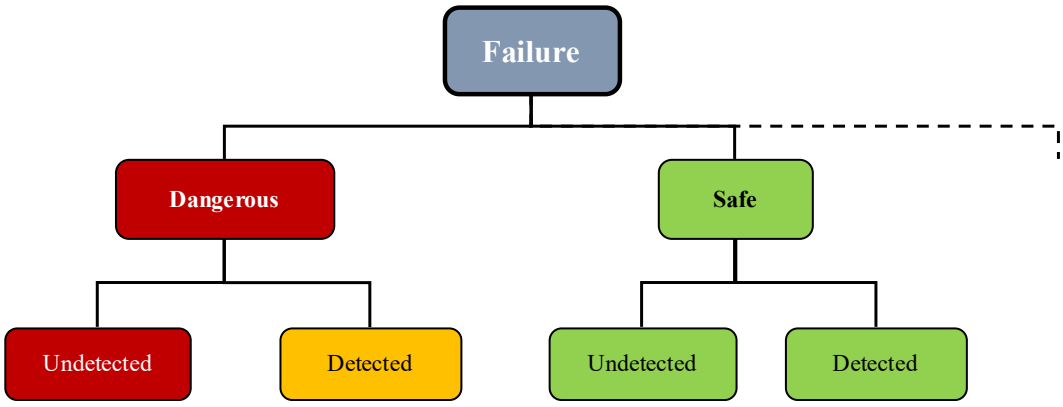


Fig. 6. DU, DD, S, and no part/no effect failures

Fig. 7 illustrates how certain design measures can be introduced to reclassify failures, typically to reduce the number of failure modes being DU:

- A DU failure being reclassified as DD if covered by a new diagnostic capability that is being added

- Examples of how DU or DD failure can be reclassified as SU or SD are:
    - A relay is modified from normally de-energized to a normally energized activation principle. This change ensures that a power loss leads to a safe state rather than a hazardous one.
    - Wire monitoring includes a passive sensor so that it always reads a value larger than zero, instead of providing no reading unless the wire has a fault. By continuously monitoring the integrity of the wiring, faults that would otherwise remain hidden can be detected, thereby improving the overall safety integrity of the system.

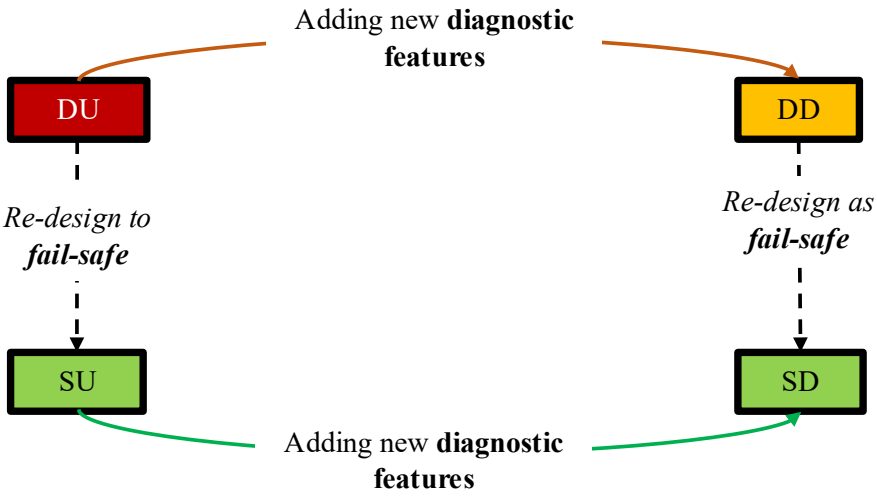


Fig. 7. Measures for the reclassification of failures

8.4.3 Systematic and random failures

While safe and dangerous failures indicate severity, there is no information about *why* the failures occurred. Insight into the causes of failure is also essential, as this information helps determine corrective actions. The functional safety standards have chosen the following two categories: random hardware failures and systematic failures. Here, IEC 61511-1 (2016) defines these as:

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

Examples include failures caused by fatigue, corrosion, or other forms of wear under specified operating and environmental conditions.

11. **Systematic failure:** Failure related to a pre-existing fault, which consistently occurs under conditions, and which can only be eliminated by removing the fault by a modification of the design, manufacturing process, operating procedures, documentation, or other relevant factors.

Examples include design flaws, procedural errors, or software bugs. These failures are typically repeatable and predictable.

The following characteristics are typical; to understand their differences better:

- Random hardware failures are caused by phenomena that cannot be entirely avoided, despite effort.
    - For non-repairable devices, such a failure may mark the end of the device's life.
    - For repairable devices, it defines the time between failures, and follows a statistical distribution, such as the Exponential or Weibull distribution of time to failure.
    - While the occurrence is random, the likelihood and timing can be influenced by:

- Component or device quality and design
- Maintenance and inspection routines
- Environmental and operational stressors

- Systematic failures, in theory, can ideally be entirely avoided—if no mistakes are made when they are corrected. In practice, however, eliminating all systematic faults is extremely difficult. For example:
  - These failures may be unique to a specific situation or repeatable across similar systems.
  - A device may be functioning perfectly but still fail due to a systematic issue.
  - Systematic faults that are perfectly handled do not follow any statistical distribution, as the cause of each fault is removed each time.

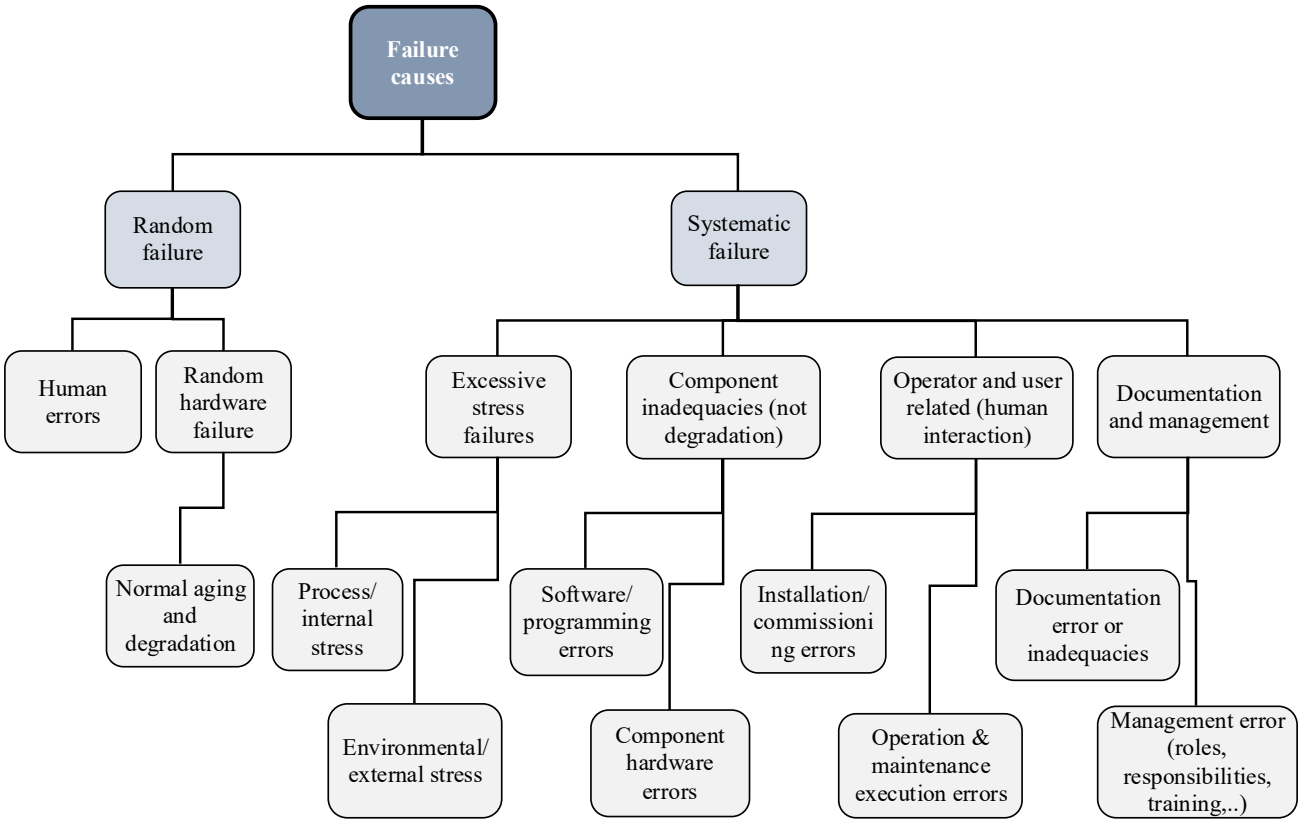


Fig. 8. Classification of random hardware and systematic failures. Adapted from PDS method (2013) and ISO TR 12489 (2013))

Example: A smoke detector installed in the wrong location or of the incorrect type may never detect smoke, even if the device itself is functioning correctly.

In practice, it is common to incorporate both random and systematic faults when estimating failure rates and putting devices into operation. In fact, it may be expected that the most influential contributor is the systematic faults. The reasons being:

- The manufacturer's failure rates exclude systematic faults in their failure rate estimates because they cannot account for environmental and operational influences after the products have been sold. Given that devices are built for high reliability and safety, the failure rates are usually extremely low, particularly for the category of DU failures, where the impact of diagnostics is also accounted for. According to the manufacturer's failure rates, it is extremely unlikely that failures occur randomly.

- Failures found during operation and maintenance can often be attributed to systematic causes, even though some random failures may occur more often than the manufacturer has indicated due to statistical variations in failure times.
- Identifying the underlying cause of failure is not always possible, due to restrictions in available time and resources, meaning that some systematic faults are repaired but not necessarily in a way that prevents them from recurring.
- The practical consequence of not correcting the systematic faults in the ideal gives systematic faults some randomness that justifies their accountability to the failure rate.
- Only systematic faults that can be justified as completely and perfectly handled may be left out of the statistics used to quantify the failure rate.

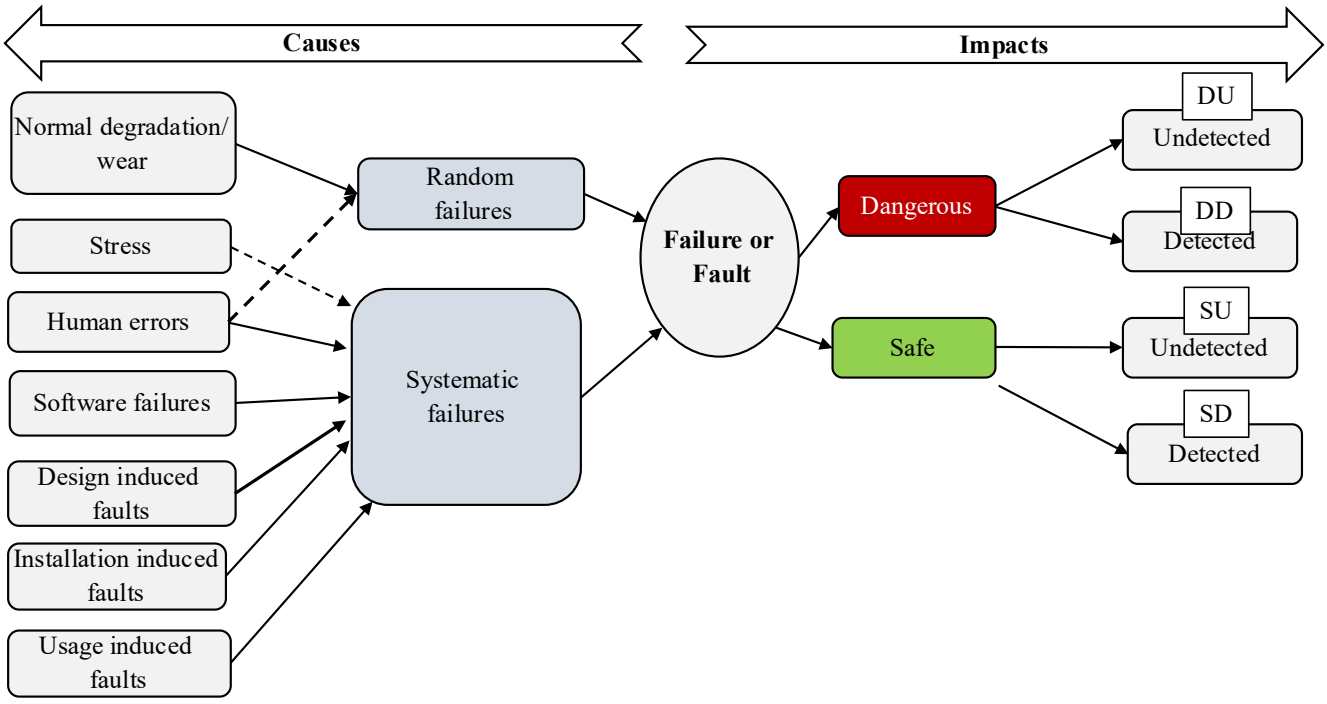


Fig. 9 All failure categories combined

The PDS method handbook (2013) has a nice illustration of random and systematic failure classification, which includes several practical examples of systematic faults reproduced in Fig. 8. Compared to the figure in the PDS handbook, the failure classification of random failures has been extended in line with ISO TR 12489 (2013). The guideline argues that human errors are also unpredictable and recurring, resulting from routine operations and a lack of attention. The criterion for determining whether a human error is systematic or random must be assessed on a case-by-case basis.

To sum up, Fig. 9 illustrates how the classification of failure modes and failure causes relates to each other.

8.4.4 Common cause failures (CCFs)

Up to this point, each failure has been treated as an independent event, occurring without regard to other device failures. Unfortunately, this is not always the case. Devices may be exposed to the same phenomena, and failure events may occur due to a shared cause. This failure category is called common cause failure (CCF). While definitions may vary slightly across standards and industries, a practical and widely accepted interpretation is:

> **CCF:** A failure event involving multiple devices that fail due to a shared cause within a relatively short period.

The phrase “relatively short time interval” is essential. It implies that the failures occur close enough in time to compromise redundancy's effectiveness. For instance, if two redundant valves fail within the same functional test interval, the system may not detect or correct the first failure before the second occurs, undermining the intended fault tolerance.

IEC 61511-1 (2016)has worded the definition slightly differently, but with the same meaning:

> **CCF:** Concurrent failures of different devices, resulting from a single event, where these failures are not the consequences of each other.

An example of a CCF is when two shutdown valves fail to close simultaneously because they are both equipped with the same type of undersized actuator. CCF is an essential and mandatory failure event to include in reliability analyses of safety functions, as explained later in this chapter. Safety standards also require a systematic approach to reduce the contribution of CCFs, and for this purpose, the concepts of root causes and coupling factors are helpful.

8.4.4.1 Root causes vs coupling factors

The concepts of root causes and coupling factors, first introduced by the nuclear industry with NUREG 4780, are beneficial for understanding why a CCF may occur:

12. **Root cause:** The underlying reason for the fault.
13. *Example*: A design flaw or error in the configuration procedure.
14.
15. **Coupling factor:** A characteristic of the design, installation, or operation that explains why a single cause affects multiple devices.
16. Examples:
    - Use of identical components (same model/version)
    - Shared installation environment (e.g., temperature, humidity)
    - Common procedures or personnel for maintenance
    - Similar design principles or software logic

While the root cause identifies the common underlying reason for the failure, the coupling factors explain why the failure affected multiple components simultaneously, rather than just one.

8.4.4.2 Internal vs external CCFs

CCFs are primarily relevant to safety functions that involve redundancy, such as safety-instrumented functions (SIFs) performed by SIS. When CCFs occur within the function itself, due to internal redundancies, they are called internal CCFs, which is the typical meaning of CCFs. There can also be unintended dependencies between different SIFs, even if they are in separate SIS systems. For instance, a PSD function and an ESD function both operate the same shutdown valves. These external CCFs must be considered if such dependencies exist. However, this chapter does not cover external CCFs.

8.4.4.3 Example: CCFs for SIF with redundant subsystems

Fig. 10 illustrates a SIF with two redundant pressure transmitters configured in a 1oo2 voting system, a single PLC controller, and two shutdown valves also in 1oo2 voting. CCFs could affect the pressure transmitters and shutdown valves, but not the controller, since it is a single device.

Examples of root causes and coupling factors for some examples of CCFs that could be experienced are explained in Tab. 1.

Tab. 1. Examples of root causes and coupling factors

CCF example	Root cause	Coupling factors
Both pressure transmitters provided incorrect measurements due to an improper calibration procedure.	Error in calibration procedure.	The same calibration procedure is used for all pressure transmitters.
Both pressure transmitters failed to sense the pipeline pressure due to plugged impulse lines.	Lack of alarm if heat tracing fails, due to incomplete specification.	The same heat-tracing solution for both transmitters.
Both valves failed to close due to water intrusion and icing inside the actuator, resulting from a poor actuator design.	Poor actuator design due to an error in the specification.	The same specification was used for purchasing actuators.
Both valves failed to close due to corrosion that had progressed unchecked because of inadequate maintenance.	Lack of adequate maintenance.	The same (deficient) maintenance procedure was applied to all shutdown valves.

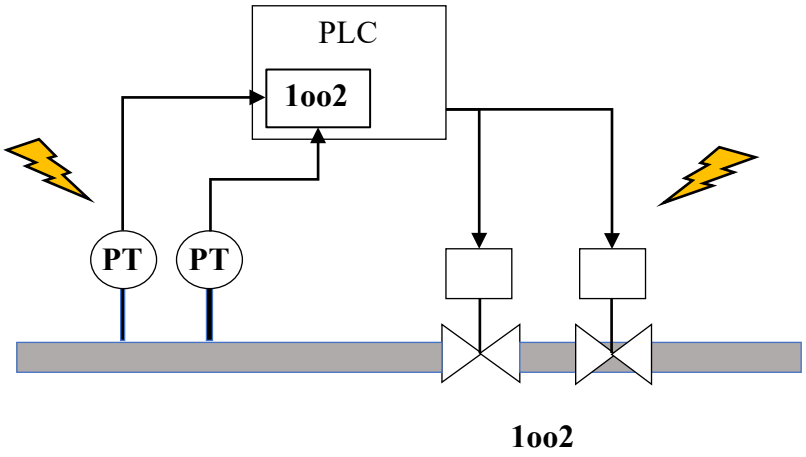


Fig. 10. SIF with redundancy (with the lightning symbol representing a coupling factor)

In summary, Common Cause Failures (CCFs) substantially diminish the effectiveness of redundancy in Safety Instrumented Systems (SIS). While redundancy is intended to improve reliability by providing backup components, CCFs can cause multiple redundant elements to fail simultaneously, undermining the intended safety benefits.

Because of this, CCFs are a critical focus in standards for the design and operation of SIS, such as IEC 61511. These standards impose two key requirements:

- Minimize the likelihood of shared failure causes through careful design, installation, and operational practices.
- Account for the impact of CCFs in reliability calculations, ensuring that the system's safety integrity level (SIL) reflects realistic failure scenarios.

8.4.4.4 Example: CCFs between two independent SIFs

It is often required to have two independent systems for overpressure protection of vessels. Even when two SIFs are designed to be independent, meaning they are realized by two different SIS systems, they may still be vulnerable to Common Cause Failures (CCFs) if they perform similar functions and share specific characteristics. We refer to such CCFs as external, meaning they affect systems that are to operate independently of each other, as opposed to "regular" CCFs that operate internally within systems that apply redundancy.

Fig. 11 assumes that SIF1, implemented in SIS 1, is one of these systems, and that SIF 2, implemented in another SIS (SIS2), or a stand-alone mechanical pressure relief valve implementing a non-SIS safety function (SF), could be the second system. The question is: Which option would be best, given that SIF2 (or SF) must be independent of SIF1?

First note is that, despite realizing SIF 1 and SIF 2 in two different SISs (SIS1 and SIS 2), there are several reasons for vulnerability to CCFs, through the following coupling factors:

- Pressure transmitters of the same or similar type
- The controllers are of the same type (from the same vendor)
- The shutdown valves are of the same type or have the same dimensions
- Testing and maintenance are performed by the same personnel using identical procedures for the same or similar types of equipment

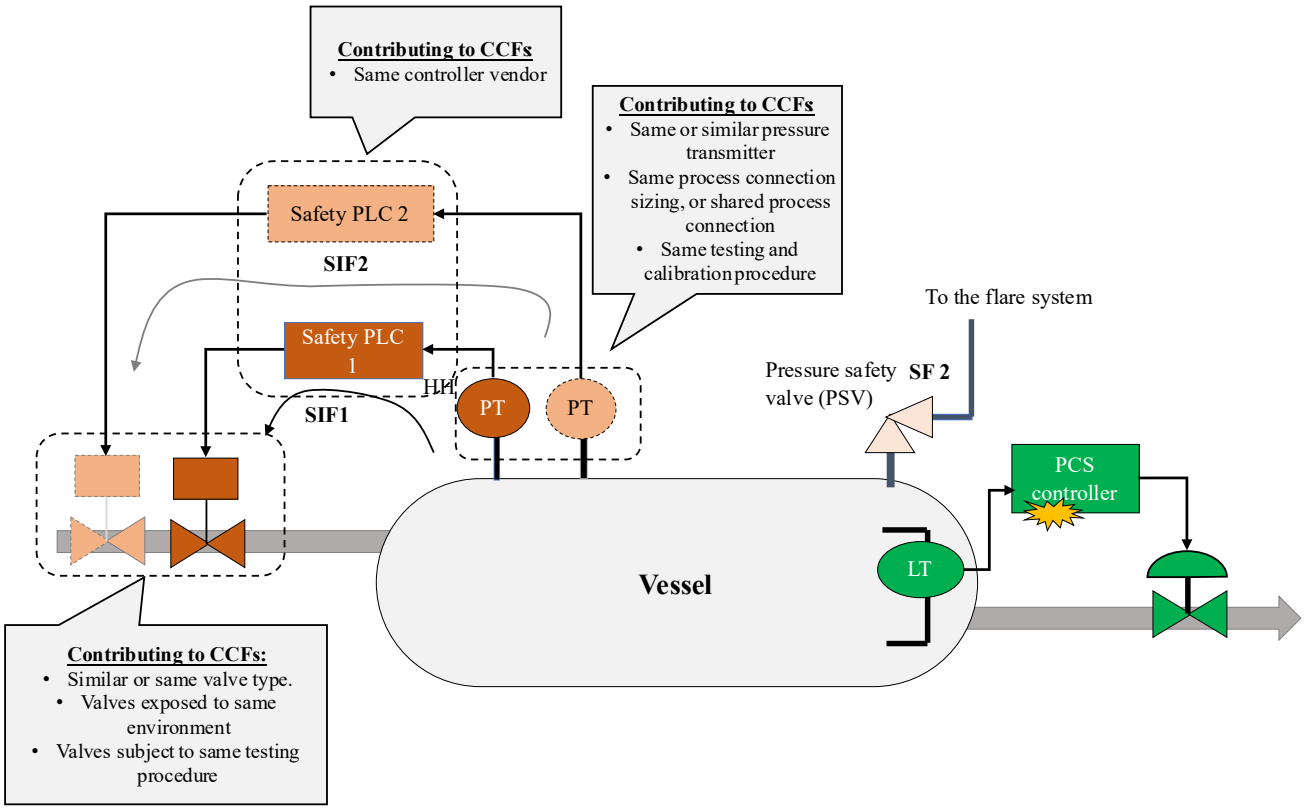


Fig. 11. CCFs between overpressure protection systems

To reduce the risk of external CCFs, one effective strategy is to introduce diversity in the design of the protection layers. In the example shown in Fig. 11. SIF 2 could be replaced with a mechanical pressure relief system, referred to as Safety Function (SF) 2. This system uses a different technology, which is not susceptible to the same failure causes as the original SIF.

By using diverse technologies, such as combining electronic and mechanical systems, the likelihood of a shared failure cause affecting both layers of overpressure protection is reduced. This approach enhances the independence and robustness of overall safety architecture.

8.4.5 Cascading failures

CCFs are one of two types of dependent failures. The other, less relevant to SIS reliability analysis, is cascading Failure (CF). A cascading failure (CF) is best described as a sequence of failures occurring in succession, like a domino effect. For example, NOUREG/CR-6268 defines:

> **Cascading failure (CF):** A cascade failure refers to cases where the failure of A leads to the failure of B, a cascading effect within a design. An example is a valve in the pump suction line that fails to open.

Cascading failures are more common in networks, battery systems, and power grids, where the failure of one component can overload or destabilize others. For example, the IEC Electropedia (IEC glossary) has the related definition related to power generation and transmission:

> **Cascade tripping:** Sequential forced tripping of generation units, transmission units, or both.

SIS systems are more prone to CCFs than CFs because they rely on redundancy rather than on network interactions.

8.5 Identification of system functions and operating environment

A system may, for example, perform many functions, but not all of them are equally obvious and explicitly stated, and some may turn out not to be so relevant for the analysis.

8.5.1 Methods for identifying functions

There are several methods for identifying functions. Functions related to safety may be identified using hazard identification methods, such as preliminary hazard analysis (PHA) and hazards and operability studies (HAZOP), as explained in Rausand and Haugen (2020), or systems-theoretic process analysis (STPA) by Leveson and Thomas (2018). Requirements for consumer products may rely on market analysis combined with structured methods such as quality function deployment (QFD). An even more straightforward approach is to use a checklist of general function categories (or types) and evaluate the extent to which each applies to a specific system. For example, Rausand and Høyland (2004) define the following function categories:

- Essential (or primary) function, which is the function that represents the primary mission of the system.
- Auxiliary functions: Functions indirectly needed to support the essential function.
- Protective functions: Functions dedicated to protecting the system from damage or protecting the environment from damage by the system.
- Information functions: Functions dedicated to informing and providing decision support to humans or the system about technical health, faults, alarms, and the like.
- Interface functions: Functions that are needed to interact with other systems.
- Superfluous functions: Functions that are available but not used. Commercial products often have functional capabilities beyond what is needed for all application areas. Superfluous functions may negatively impact reliability if not identified and managed.

The list helps broaden the scope of functions relevant to and needed by a system beyond its core mission. Applied to a washing machine, we may identify that:

- The essential function of the machine is to wash clothes according to a chosen washing program.
- An auxiliary function to contain water (inside the drum) and discharge the water as requested by the program.
- Protective functions include a door lock that prevents you from opening the door while the drum is active or filled with water and disables the start if the weight of clothes is too high.
- Information functions include the provision of washing status and alarms.

- Interface functions relate to water supply, discharge capacity, power supply, and perhaps wireless connectivity.
- Functions not defined already by the other categories may end up being superfluous functions. However, what is unnecessary is somewhat subjective, depending on the user's needs and interests. For example, some users find the wireless connectivity option uninteresting. Some functions may be superfluous in certain modes of operation but not in others.

Adding more functions increases complexity, even when implemented in software, and the product's reliability may suffer. The product developer must therefore find a suitable balance between the development costs, the risks (and costs) of recalls and upgrades, and what is needed to achieve high customer satisfaction.

8.5.2 Operating environment and modes of operation

Operating conditions and the environment will affect the system's reliability. Some of the impacts are already reflected in the reliability data, while others are not. Factors to consider are:

- Regular environmental conditions, like temperature, humidity, vibration, pressure, dust, and light conditions.
- Abnormal (but to some extent foreseeable) environmental conditions. Like flooding, storms, lightning, falling objects, and exposure from the escalation of nearby accidents.

What systems and functions are important for achieving high reliability may vary depending on the mode of operation. Typical modes of operation are:

- Normal (regular) operation
- Start-up and planned stops
- Abnormal operations, such as hazardous events, require specific actions, like shutting down the facility.
- Maintenance and testing, like work needed for regular testing, dismantling, replacement, and inspections
- Human interaction, i.e., the types of tasks and the systems involved in the interactions with humans.

A reliability analysis must decide which conditions and modes to include. The decision may be more difficult than it seems. A too-narrow boundary can lead to an unrealistic result in the reliability analysis, as important influencing factors are excluded. Having a too-broad boundary increases the complexity of the analysis, and the extended outreach may include factors that are impossible to determine or analyze with confidence. The choice of boundaries should therefore be justified.

8.6 Graphical representation of system functions and composition

Graphical illustrations of system parts and system functions are both valuable and necessary in a reliability analysis. It is beneficial to prepare such representations before applying the specific reliability analysis methods. Also, it serves as a practical communication tool, especially when validating the system against its requirements or actual implementation. Experts may find it easier to provide relevant input if they understand what has been identified so far.

Graphical illustrations can be in terms of:

- System tree, where the focus is to decompose a system into its parts and subparts
- Function tree, where the focus is on identifying key functions and their relationships, without being dependent on their realization
- Hierarchical control diagrams, where the focus is on controller interaction

We will present the first two, as they are more relevant for traditional reliability analysis. Hierarchical control diagrams are more appropriate for identifying emergent, potentially unwanted behavior in software-intensive systems. For example, such diagrams are used in the systems theoretic process analysis (STPA) method, explained in the STPA handbook by Leveson and Thomas (2018) for identifying unsafe control actions and safety constraints.

8.6.1 System tree and function tree

An example of a system tree for a bicycle is shown in Fig. 12. There is no single way to set up the tree, and others may end up with a different type of structure. The level of detail to include depends on the scope and focus of the reliability analysis. Here we see that the analysis stops at level 3 (and 4).

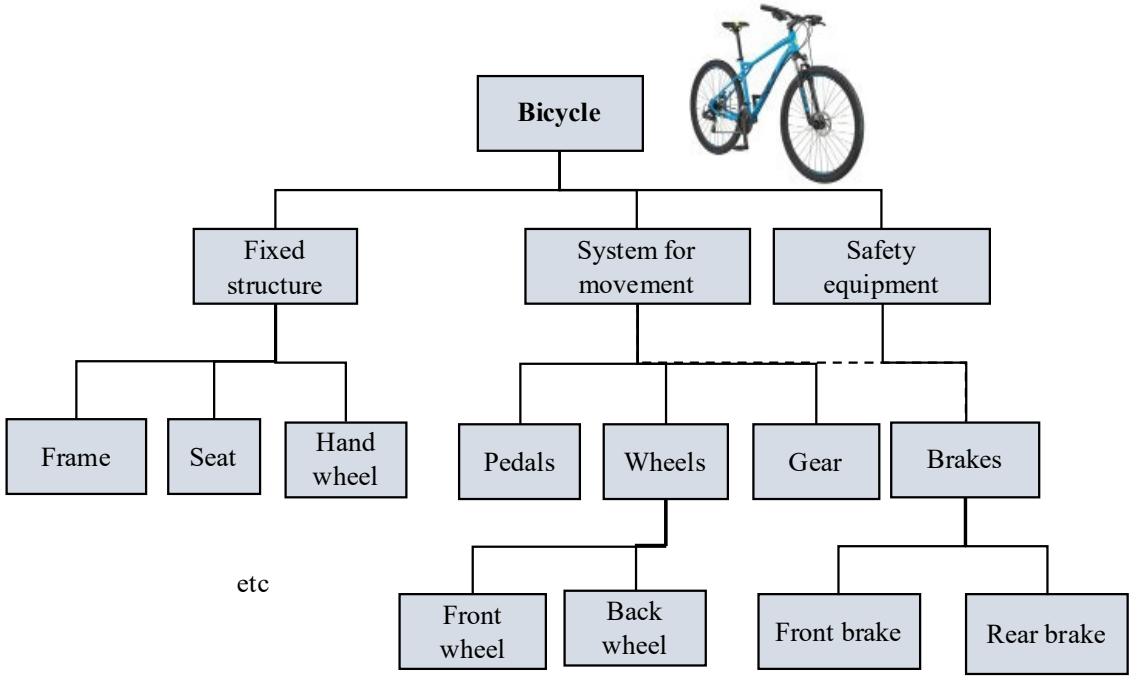


Fig. 12. System tree of a bicycle

A function tree is a hierarchical representation of the system's overall mission, covering the primary function and its related subfunctions. Unlike a system tree, which focuses on physical components, it is not necessary to know how the system is to be implemented.

Fig. 13. Illustrates a function tree inspired by Fig. 12 with focus on the general mission "Transport a person from point A to point B." This primary function can be decomposed into subfunctions such as:

- Provide propulsion
- Maintain balance
- Enable steering
- Allow braking
- Support the rider

Generally, every function and subfunction should be defined in a precise way with at least an (active) verb plus a noun. It appears now that the realization of the functions is not restricted to the bike example in Fig. 12, but opens up for other solutions like a kick scooter, a canoe, or a glider plane.

Focusing on functions is especially useful in the early stages of design, when the physical implementation has not yet been determined. It is also helpful if the plan is to replace one or more parts of an existing system with

new technology. It allows engineers and analysts to explore how alternative solutions and technologies can meet specific functional requirements. Function trees are, therefore, useful tools in innovation projects.

For example, a function tree like the one in Fig. 13 may trigger broader questions about what is essential for the system design:

- Should the goal of transporting two people be maintained, or limited to only one?
- Should the system also be able to carry some goods and have room for storage?
- How flexible should the system be in terms of application areas and skills of the users?
- Would additional gains be achieved if an engine is introduced? Why was the "by own effort" introduced in the first place?

These questions can lead to entirely new design directions, such as:

17. Cargo bikes or electric scooters
18. Autonomous delivery robots
19. Modular transport systems
20. Hybrid personal mobility devices

By focusing on what the system must do, rather than how it is currently done, functioning trees help break away from existing solutions and open the door to innovative alternatives.

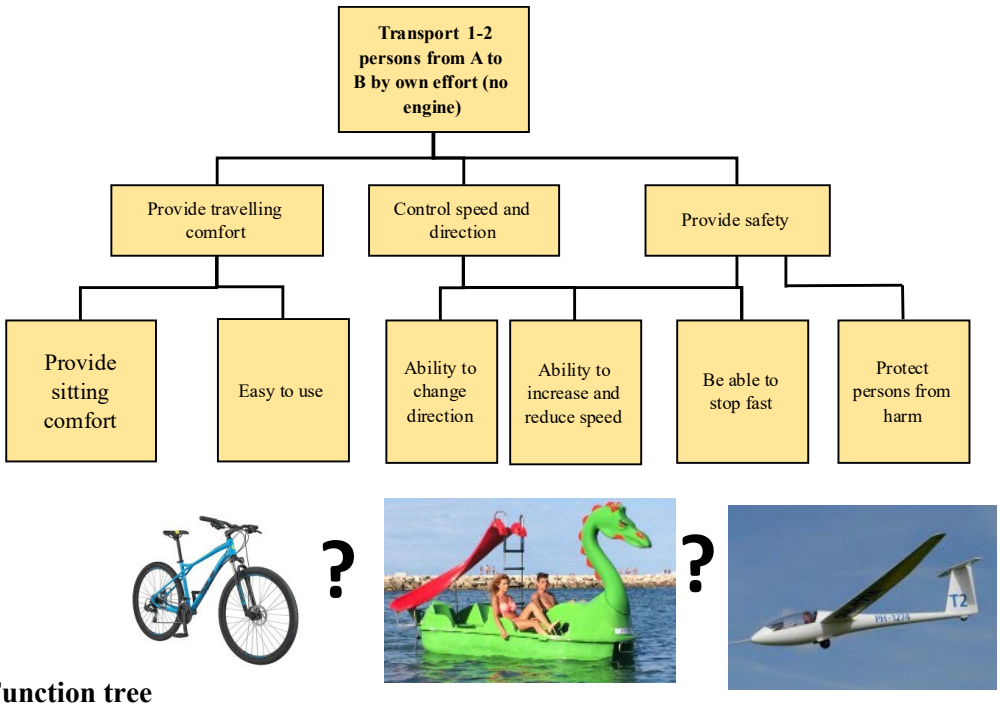


Fig. 13. Function tree

8.6.2 Functional block diagrams

The functional block diagram focuses on how functions relate to each other. The illustration of the functions of a diesel engine in Fig. 14 borrowed from a textbook by Rausand and Høyland (2004) is a good example. We note that the interdependencies among the functions required to start and run the diesel engine are identified, along with their relationships to external systems outside the system boundary.

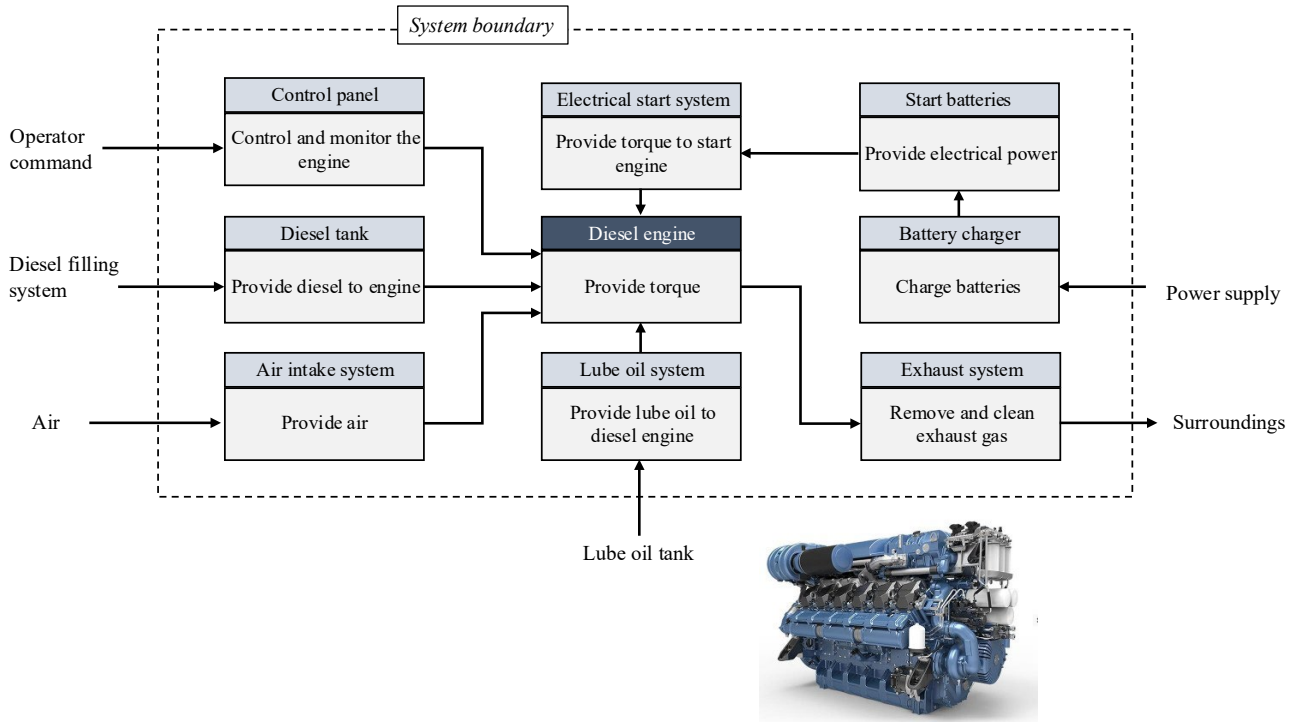


Fig. 14. Functional block diagram (Adopted from Rausand and Høyland (2004))

8.6.3 Hybrid diagrams

A hybrid diagram aims to represent a system as constructed while also making its functions and their interrelationships clearly visible. There are no formal rules for how such diagrams are built, but one applicable rule of thumb is to identify involved devices in a sequence according to the sequence of functions, as shown in Fig. 15 for the operation of an on/off valve. Operating the valve relies on a sensor measurement, which is sent to a central processing unit (CPU) via an intrinsically safe (IS) barrier and an input card. The CPU decides, based on the measurement, whether to send a command via an output card to a solenoid-operated pneumatic valve that either pressurizes or depressurizes the on/off valve to achieve the requested position. The diagram also illustrates where power supplies are added.

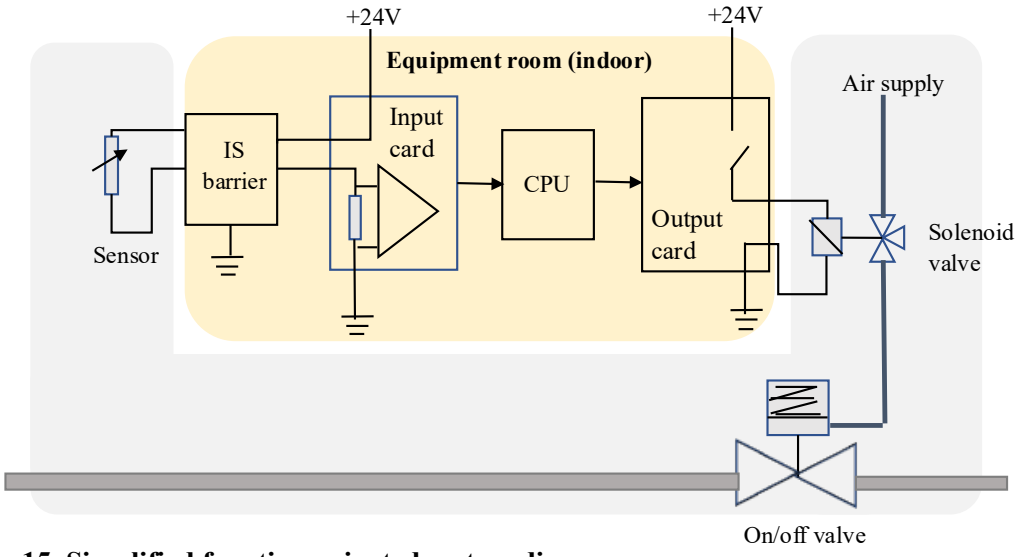


Fig. 15. Simplified function-oriented system diagram

A hybrid diagram should not include all design details; only those relevant to the analysis should be included. Creating this kind of simplified representation serves multiple purposes:

- It identifies components relevant for executing a specific function.
- It identifies reliance on other support systems like power and pressurized air supply.
- It acts as a communication tool for discussions with colleagues, stakeholders, or reviewers, helping confirm whether the system has been correctly interpreted and implemented.

Engineering documents that may be considered as a type of hybrid diagram are:

- Piping and Instrumentation Diagrams (P&IDs)
- Instrument loop diagrams
- Electrical circuit diagrams

For such types of diagrams, formal drawing rules are defined in international and national standards and in company guidelines.

8.7 Methods applied for reliability analysis

Qualitative and quantitative reliability analysis is a structured approach used to identify how a device or system might survive or fail, along with the underlying causes and potential effects of those failures. It plays a critical role in improving system reliability, safety, and maintainability.

This section introduces five commonly used methods in reliability analysis:

- FMECA – Failure Modes, Effects, and *Criticality* Analysis: A systematic technique for identifying failure modes and evaluating their impact and severity.
- FMEDA – Failure Modes, Effects, and *Diagnostic* Analysis: A variant of FMECA that includes diagnostic coverage and is often used in safety-critical applications.
- Fault Tree Analysis (FTA) – A top-down, logic-based method used to analyze the pathways that can lead to a specific system failure.
- Reliability Block Diagram (RBD) – A graphical method for modeling the reliability structure of a system based on the configuration of its components.
- Markov Analysis – A state-based probabilistic method used to model systems with complex dependencies and transitions between operational states.
- Each method offers unique strengths and is suited to different types of systems and analysis goals.

8.7.1 FMECA

FMECA is one of the most widely used methods for systematic failure analysis. Initially developed for military applications, the first formal guideline was published in 1949 under MIL-STD-1629A. Today, FMECA is applied across all industries, and many guidelines have been developed to support its use. An international standard IEC 60812 (2018) has also been devoted to the method and is an important reference. Depending on the sector, FMECA can be referred to as failure mode and effects analysis (FMEA) or failure modes, effects, and detectability analysis (FMEDA). While FMEDA has some distinct features, FMEA and FMECA are, for all purposes, the same method, even if the “C” is missing.

FMECA is most frequently used in the design and product development process, often integrated into quality assurance and verification activities during the early development stages. FMECA was first introduced to identify and assess failures of physical systems (hardware), but over time, variants have been adapted for use with:

- Software programs: Identify possible ways code and coded functions can fail, their impacts, and potential strategies to correct them.
- Manufacturing processes: Identify how faults may be introduced during manufacturing and how to prevent them.
- Logistics and supply chains: Identify bottlenecks and identify strategies to solve these.

FMECA is most commonly conducted as a bottom-up analysis, where each component of the system is assessed individually. Depending on the system's size, the analysis can become quite time-consuming. A top-down analysis may therefore be conducted first, as a screening method, to identify the most critical components or subsystems to assess. For example, a system may comprise some well-known parts and some novel parts, in which case the novel parts might be of most interest.

Our focus here is on physical (hardware) systems, where the main goal of FMECA is to:

- Identify potential failure modes of individual devices
- Analyze their effects on the overall system performance
- Evaluate the criticality of each failure to prioritize mitigation efforts

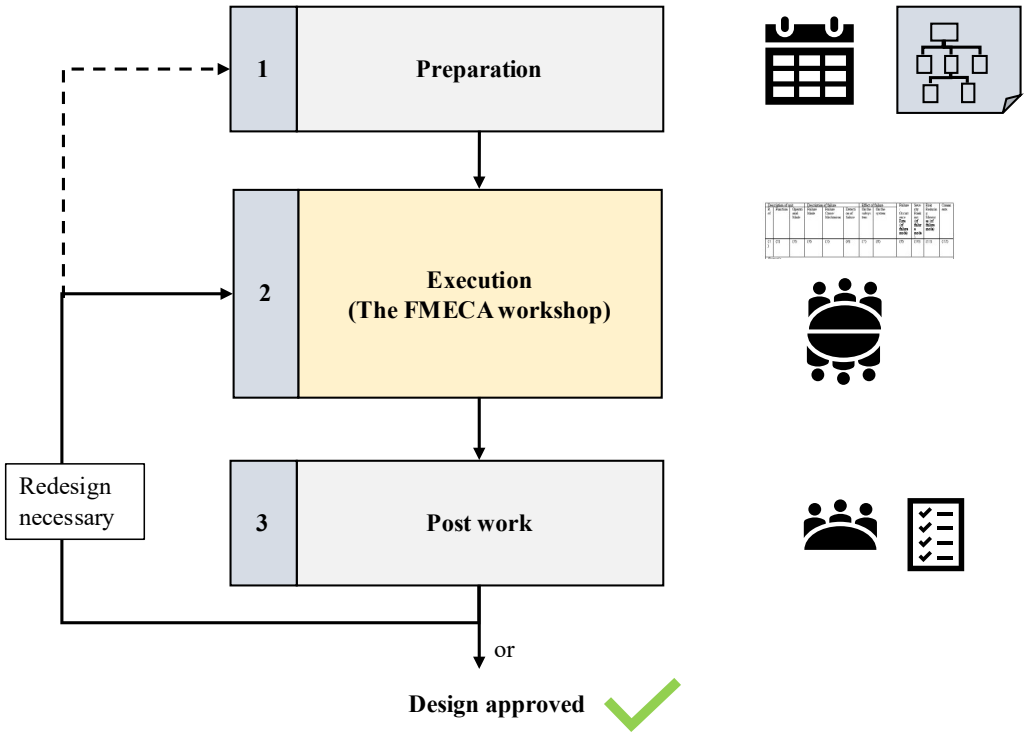


Fig. 16. Steps involved in an FMECA

8.7.1.1 FMECA process

The FMECA process for a bottom-up analysis typically involves the following steps, organized into three stages: preparation, execution, and post-work in Fig. 16.

Preparation: Preparatory work led by an FMECA facilitator

1. Identify system functions and boundaries, often pre-prepared in a list
2. Decompose the system into components or sub-functions, preferably supported with graphical illustrations

3. Make a function list for all components subject to the FMECA analysis
4. Identify who to invite for FMECA workshop and make invitation

Execution: Workshop with experts facilitated by the FMECA facilitator

5. Identify potential failure modes for each component/function
6. Determine the effects of each failure
7. Assess the severity, occurrence, and detectability
8. Calculate a risk priority number (RPN) or criticality index

Post work: Follow-up by those with assigned responsibility for actions

9. Recommend actions to reduce or eliminate high-risk failures
10. Monitor the follow-up

The administrative roles involved in an FMECA are a facilitator, who is responsible for managing all three stages, a scribe, who takes notes during the FMECA execution, and a team of experts that participate in the FMECA workshop.

The results of an FMECA are documented in an FMECA table. This document is critical for the follow-up after the analysis has been completed. There exist several table layout variants, and here we have proposed one shown in Tab. 2 . The table entries are:

1. Reference: An ID or tag number that identifies the device, function, or component.
2. Function: A concise description of the function to perform, including any timing requirements
3. Operational mode: Identification of the specific operation mode considered. Examples include startup, regular operation, phases of operation, abnormal operation, and maintenance. The primary reason for examining various operational modes is that some failures are insignificant in specific modes but critical in others.
4. Failure mode: The way the device can fail
5. Failure causes and mechanisms. The proximate (chemical, physical, software, etc.) causes (failure mechanisms) as well as the underlying explanations (root causes)
6. Fault detection: Whether the failure is notified by an alarm (evident/detected) or not (hidden/undetected).
7. Effect of failure (on subsystem): The effect on the subsystem in which the device is a part.
8. Effect of failure (on the overall system): The effect, considering any other redundant means of performing the same function.
9. Failure rate: The estimated occurrence rate of the type of failure. The rate may be based on expert judgment or on data handbooks. Alternatively, the failure rate can be expressed qualitatively, e.g., unlikely, rarely, often, continuously.
10. Severity: A ranking of the failure severity for the system mission and/or possible damage to humans and the environment.
11. Risk ranking: A calculated ranking of risk, using, for example, what is referred to as the risk priority number (RPN), based on occurrence rate, severity, and, in some cases, also detectability.
12. Risk-reducing measures: Proposed measures to reduce the frequency and/or severity, or a combination. Measures may involve redesigning, modifying the installation, and/or improving or revising procedures for maintenance and testing.
13. Comments: Assumptions can be added along with the people responsible for following up on new risk-reducing measures.

Tab. 2. FMECA table (example)

Description of unit			Description of failure			Effect of failure		Failure/ Occurrence Rate (of failure mode)	Severity Ranking (of failure mode)	Risk ranking (RPN)	Risk Reducing Measure	Comments
Ref	Function	Operational Mode	Failure Mode	Failure causes	Detection of failure	On the subsystem	On the system					
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)

Columns 9 and 10 ask for quantitative information, either in the form of categories (e.g., 1-10 or A to D) or estimated values (like frequencies of a specific type of failure). The choice of values is often based on expert judgment among those participating in the workshop, with input from, e.g., company-internal or external guidelines, user-reported failures from the maintenance system (if available), and generic data handbooks (with reliability data for various types of components). Examples of categories to use for the two columns are shown in Tab. 3.

Tab. 3 Examples of frequency and severity ranking

Frequency ranking			Severity ranking		
Rank	Description	Examples	Rank	Description	Explanation
5	Frequent	≥1/month	1-3	Minor	Failure may result in minor system damage, while causing no harm to people or the environment.
4	Probable	≤1/year	4-6	Major	Failure may result in some, but reversible, injury and/ or harm to the environment.
3	Occasional	≤ 1/10 years	7-9	Critical	Failure may result in irreversible (or very long recovery) harm to people and/ or the environment.
2	Remote	≤ 1/100 years	10	Catastrophic	Failure may result in deaths to people and/or extensive irreversible damage to the environment.
1	Very unlikely	≤1/1000 years			

It is often easier to determine the severity class than the frequency class, considering that identified failure types are rare and may not have been experienced yet. For example, even experts can find it challenging to decide if a failure is 'very unlikely' and 'remote', and the choice is therefore always subject to some uncertainty. A pragmatic distinction of the two terms is:

- Very unlikely: Have never been experienced in the industry sector's history
- Remote: There have been one or two such events over the period the industry has existed, and the events are still considered relevant for the

There are several variants of the FMECA table setup. For example, it is sometimes added columns that are suitable to rank the risk by calculating the risk priority number (RPN). The RPN may be calculated as:

$$RPN = F \times C$$

Here, F is a measure of likelihood, and C is a measure of consequence severity.

Tab. 4. Example of a risk table with acceptance criteria as colors

Severity (consequence)	Frequency/likelihood				
	1	2	3	4	5

10					
7-9					
4-6					
1-3					

RPN is a helpful way of selecting the most important risk reduction measures. The list of proposals can be quite long, and time and budget may call for prioritization. RPN numbers are calculated based on values filled in for frequency and severity (and in some cases, detectability, if included). A higher score means that the risk imposed by a failure is very high, and therefore more critical than another failure with a lower score.

A risk matrix calibrated with acceptable combinations for frequency and severity categories may be applied to put firmer borders for what is acceptable and not. One example of such a risk matrix is shown in Tab. 4. Here, the green cells mean that risk is at a generally acceptable level, and measures listed in the FMECA analysis are not needed for further risk reduction (but there could, of course, be other arguments to implement them). Yellow cells mean that the risk level is conditionally acceptable, meaning that measures must be implemented as long as the cost of the measures does not become disproportionate to the risk reduction they provide. Red cells mean that the risk is unacceptable, and all measures falling into these cells *must* be implemented. The disproportionate principle for the yellow zone can be challenging to understand; one reason is that it must be evaluated and defended on a case-by-case basis. A rule of thumb is that a system designer (or owner) must be willing to spend more money to reduce risk if closer to the red cells than if closer to the green cells. It is also important to consider the effectiveness of measures, so that more effective measures are prioritized over those less effective.

RPN formula can also incorporate a value for the detectability (D) of the fault, considering to what extent, how, and how soon the fault is detected.

$$RPN = S \times O \times D$$

A corresponding column for detection ranking is then added to the FMECA table. The ranking of detectability may be based on, e.g., a 1-5 or 1-10 scale, with some explanation of each value like what was provided in Tab. 3.

8.7.1.2 Case study

Fig. 17 illustrates how a simple pressure transmitter can be assessed using an FMECA process. We assume that a functional block diagram has been created, identifying the transmitter functions, and the inputs, outputs, and interfaces to external systems.

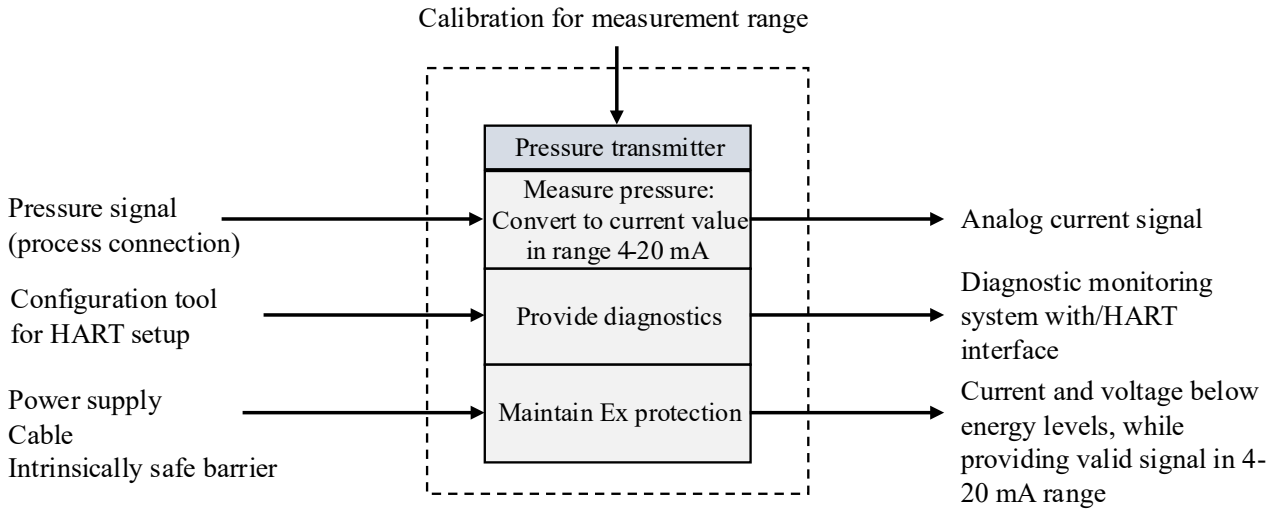


Fig. 17. From system description to a system/functional breakdown

We assume that an FMECA workshop is organized, and that an extract from the information filled into the table is as shown in Tab. 5.

Tab. 5. Extract of information added to an FMECA table

Description of unit			Description of failure			Effect of failure		Failure/ Occurrence Rate (of failure mode)	Severity Ranking (of failure mode)	RPN	Risk Reducing Measures (of failure mode)
Ref	Function	Operational Mode	Failure Mode	Failure Cause/ Mechanism	Detection of failure	Local impact (SIF)	On the protected system (global)				
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
PT	Monitor pressure in the vessel	Process upset leading to an increase in pressure	Providing too low value	Incorrect calibration caused by a maintenance error. Current leakage to earthing system Contamination in the process connection	Hidden/un-detected Hidden/un-detected	The logic solver detects too late or not at all that pressure is too high	Pressure continues to increase. PSV is assumed to open as a secondary barrier.	3	7	21	Add heat tracing for tube. Improve calibration procedure
		High pressure in separator	No measurement provided	Cable breakage (unfortunate cable routing) Totally plugged tube	Evident if cable breakage (monitoring of cable) Hidden if tube is plugged	As above	Pressure continues to increase. PSV is assumed to open as a secondary barrier.	4	3	12	Make sure that the cable monitoring alarm is available in the control room, Add heat tracing to tube.
PT	Provide diagnostic information via HART	(all)	No diagnostic information received	Wrong HART configuration	Evident	Diagnostic data not being notified.	None	4	2	8	HART configuration procedure, HART training
PT	Maintain Ex-ia protection	(all)	Degraded Ex protection (may allow too high energy)	Wrongly dimensioned circuit	Hidden	Possibility igniting gas in the area upon electrical faults.	Fire	2	7	14	Check that the EX circuit dimensioning on a regular basis

8.7.2 FMEDA

FMEDA (Failure Modes, Effects, and Detectability Analysis) is an advanced extension of traditional FMECA (Failure Modes, Effects, and Criticality Analysis), tailored specifically to determine the failure characteristics of individual devices that are to be certified for use with safety-instrumented systems (SIS). The method was first introduced by Goble and Brombacher (1999) and has since been widely applied in industry, particularly by Exida.

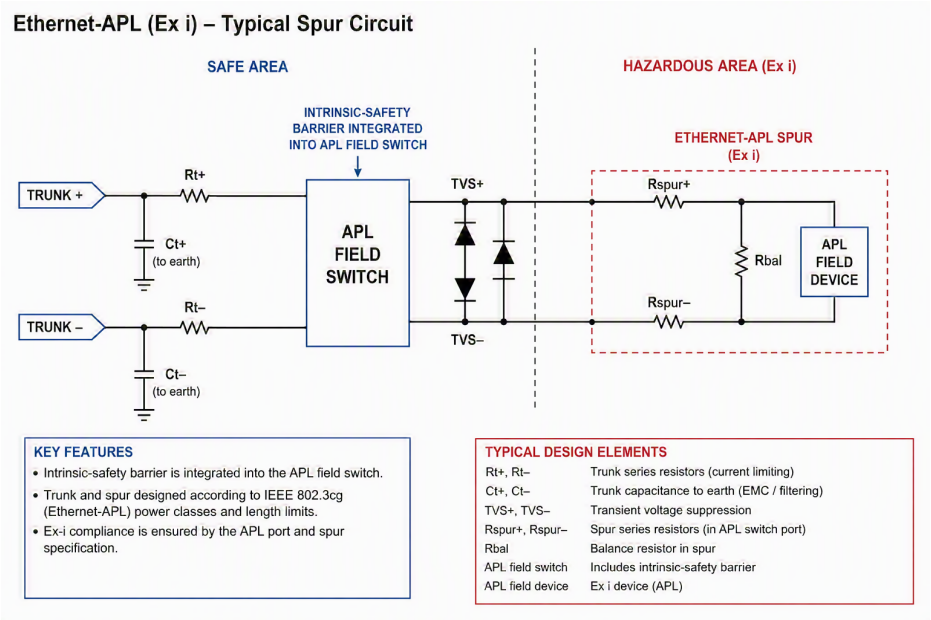


Fig. 18. Ethernet APL circuit diagram subject to an FMEDA (circuit proposed by Copilot)

It introduces a structured classification of failure modes into four categories that are key to safety devices:

- Safe Undetected (SU)
- Safe Detected (SD)
- Dangerous Detected (DD)
- Dangerous Undetected (DU)

FMEDA is organized as a bottom-up analysis of an individual safety device, or part of a safety device. The device is first decomposed into individual sub-parts. The failure modes of each sub-part are assessed individually to determine whether they are safe or dangerous and whether the system can detect them. When Exida is the executor of the analysis, they often apply their own data handbooks that cover many of the most central parts common to safety devices.

The individual analysis of each failure mode for each subpart is aggregated with the results from all other parts, yielding a device-level failure rate for each of the four failure categories.

To illustrate the application of FMEDA, a co-pilot was used to generate an electrical Ethernet APL circuit with an Ethernet APL cable, an Ethernet APL field switch, and a field device with an Ethernet APL interface. Ethernet APL is a two-wire cable that delivers data as well as power, as shown in Fig. 18.

The corresponding FMEDA table, where each failure mode of the components is classified as DU, DD, SU, or SD, is presented in table Tab. 6. The failure rates, expressed per one billion hours (FIT), have been selected by prompting Co-pilot and allocated to the various failure modes, considering criticality (safe or dangerous) and detectability by diagnostics.

$$\lambda_{SD} = \sum_{Column\ 8} \lambda_{i,j}$$
$$\lambda_{SU} = \sum_{Column\ 9} \lambda_{i,j}$$
$$\lambda_{DD} = \sum_{Column10} \lambda_{i,j}$$
$$\lambda_{DU} = \sum_{Column\ 11} \lambda_{i,j}$$

This summation technique, known as the part-count method, assumes that sub-parts contribute equally to the overall circuit failure rate. It does not account for the effects of redundancy or fault tolerance mechanisms within the element, and if these are employed, the resulting failure rates may be somewhat conservative.

The results of an FMEDA can be applied to determine specific reliability parameters often provided with safety devices, such as the diagnostic coverage (DC) and the safe failure fraction (SFF), two parameters required to be calculated by IEC 61508-2 (2010):

$$DC = \frac{\lambda_{DD}}{\lambda_D}$$
$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_{DD} + \lambda_{DU} + \lambda_S}$$

The role of SFF and DC is explained in more detail in Chapter 9 (functional safety). For now, we note that DC can be seen as a conditional probability that a dangerous failure is detected by online (close to continuous) checks, while the SFF is the conditional probability that a failure, being either safe or dangerous, is either detected and quickly repaired (if it is dangerous) or results in a transition to the safe state (if it is safe).

Tab. 6. FMEDA table for an Ethernet APL circuit (Generated by Co-pilot, fictive failure data)

1	2	3	4	5	6	7	8	9	10	11
Name	**Function**	**Failure Mode**	**Effect**	**Crit.**	**λ (FIT)**	**Diagnostics**	**SD (FIT)**	**SU (FIT)**	**DD (FIT)**	**DU (FIT)**
Current limiter	Ex i protection	Open	Spur unavailable	Safe	0.5	Port diagnostics	0.5	0	0	0
Current limiter	Ex i protection	Short	Energy limit exceeded	Dangerous	0.1	Self-test/current monitor	0	0	0.09	0.01
Voltage limiter	Ex i protection	Open	Loss of protection	Dangerous	0.5	Periodic proof test	0	0	0.40	0.10
Voltage limiter	Ex i protection	Short	Port shutdown	Safe	0.1	Voltage monitoring	0.1	0	0	0
TVS	Surge suppression	Open	Reduced immunity	Safe	1	None	0	1	0	0
TVS	Surge suppression	Short	Communication loss	Safe	1	Link monitoring	1	0	0	0
Ethernet PHY	Communication	Silent fail	Communication loss. Assumes fail-safe behavoir.	Safe	20	Link monitoring	20	0	0	0

Ethernet PHY	Communication	Corrupt data	Invalid process data	Dangerous	2	CRC/protocol diagnostics	0	0	2	0
Port voltage monitor	Diagnostics	Failure	Missed fault detection	Dangerous	2	Self-test	0	0	1.98	0.02
Port current monitor	Diagnostics	Failure	Missed overcurrent	Dangerous	2	Self-test	0	0	1.98	0.02
Spur cable	Power/comm.	Open	Communication loss	Safe	5	Link monitoring	5	0	0	0
Spur cable	Power/comm.	Short	Communication loss	Safe	2	Port monitoring	2	0	0	0
Watchdog	Diagnostics	Fail	Reduced diagnostics	Dangerous	1	Online test	0	0	0.99	0.01
				SUM	37.2 FIT	SUM:	28.6	1.00	7.44	0.16
DC (dangerous)	97.9%									
DC(safe)	96.6%									
SFF	96.9%									

8.7.3 Reliability block diagram

A reliability block diagram (RBD) is an intuitive graphical illustration of how individual components contribute to the successful operation of a specific system function.

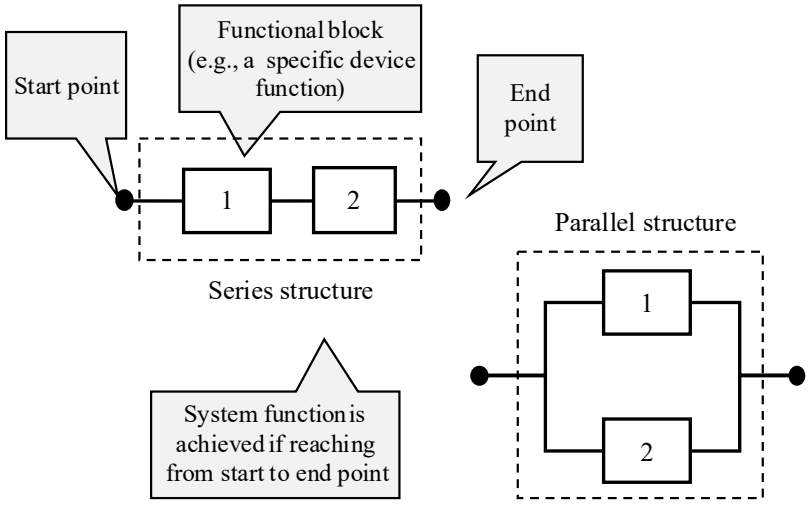


Fig. 19. RBD examples of series and parallel structures

The key elements used in an RBD are:

- Start- and endpoint: Represented by circles, indicating the beginning and end of the system function.
- Functional blocks: Squares, each typically representing a device's function for the analysis. Functional blocks can also have a more abstract meaning, for example, to denote a specific event like "No common cause failure (CCF)" or be events like "no fire present" and "operator responds to alarm".

- Pathways for successful operation: Lines, connecting start- and endpoints with functional blocks organized in series and parallel structures.

Fig. 19 illustrates the two primary RBD structures: series and parallel structures, shown for two functional blocks 1 and 2.

- The series structure is read as follows: The system functions only if both 1 and 2 are functioning. If either 1 or 2 fails, the path from the start to the endpoint is interrupted, and the system fails. This structure represents a 2-out-of-2 voting (2oo2) logic for success: *Both devices must work*.
- The parallel structure is read as follows: The system functions as long as either 1 or 2 is functioning. The system fails only if both 1 and 2 fail. This structure is equivalent to a 1-out-of-2 voting (1oo2) logic for success: *At least one of the two devices must work for successful operation*.

RBDs are typically read from left to right, where each pathway from the start to the endpoint specifies conditions for successful operation. The system function fails if the success path is interrupted by one or more functional blocks that are not performed. The sequence of listed functional blocks is unimportant, as the events represented by the functional blocks are assumed to be entirely independent in the reliability analysis. The pathways do not represent signal transfer between the functional blocks, even though they may seem so at first glance.

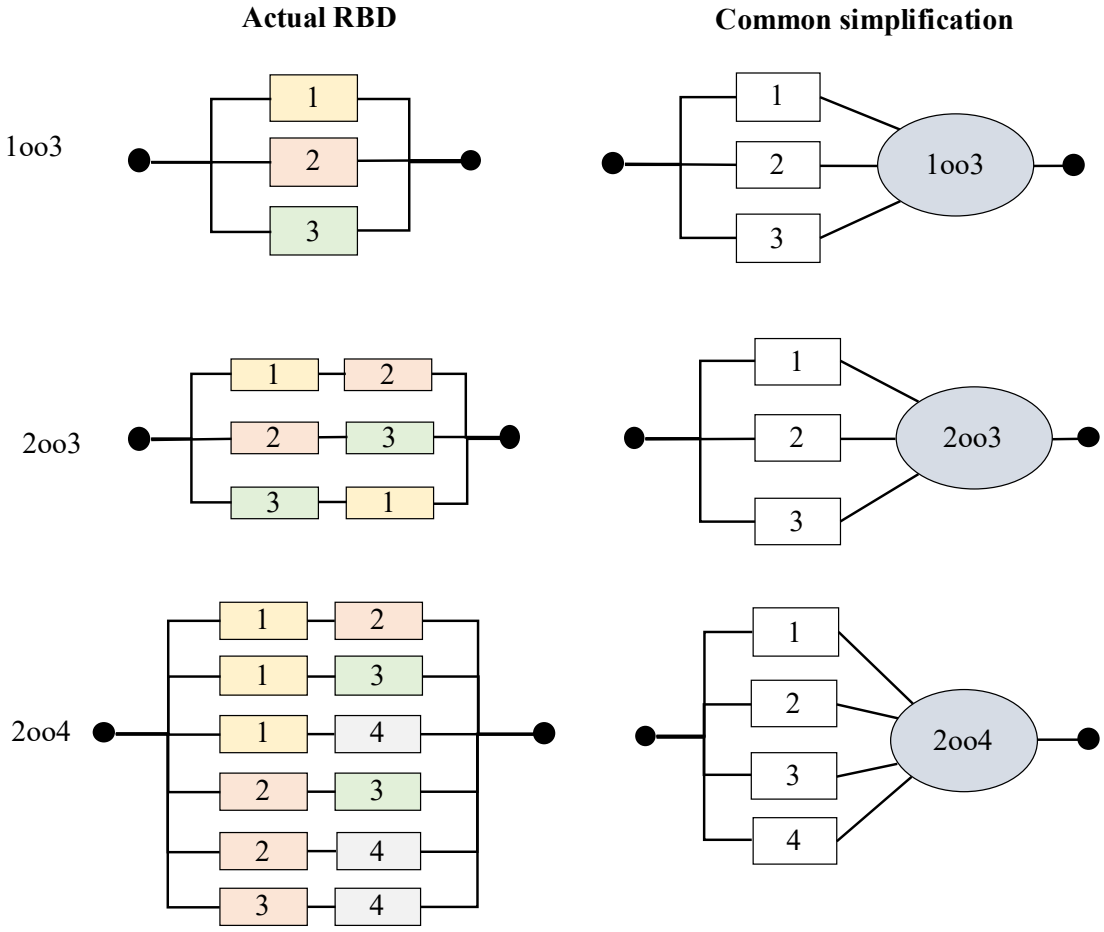


Fig. 20. RBD examples for KooN voted systems with simplified notations

As voting logic becomes more complex, such as 1oo3, 2oo3, and as shown on the left side of Fig. 20, the RBD grows significantly due to the increasing number of combinations that can lead to successful system operation.

For example, a 2oo4 system would require six parallel branches, each representing a unique pair of functioning devices out of the four.

To manage this complexity, a pragmatic simplification is often used:

- All N devices are represented as individual branches in a parallel structure.
- These branches connect to a voting symbol ("circle") that defines the required number of functioning devices (e.g., 2oo4).

This approach maintains clarity while preserving the system's logic. Examples of both complete and simplified RBDs are shown in Fig. 20.

The series and parallel structures shown so far have assumed that any functional block fails independently of the others. However, redundant devices may also fail simultaneously due to shared causes, referred to as common-cause failure (CCF). In this case, a CCF functional block is added to the existing parallel structure, as shown in Fig. 21. With this extension, the RBD states conditions for successful performance when at least one of the devices 1 or 2 functions independently of the other and has not been subject to a CCF. Single points of failure, such as a CCF, increase the probability of failure compared to independent failures. This is the reason for the mandatory inclusion of CCF contributions in reliability models for safety-instrumented functions (SIFs).

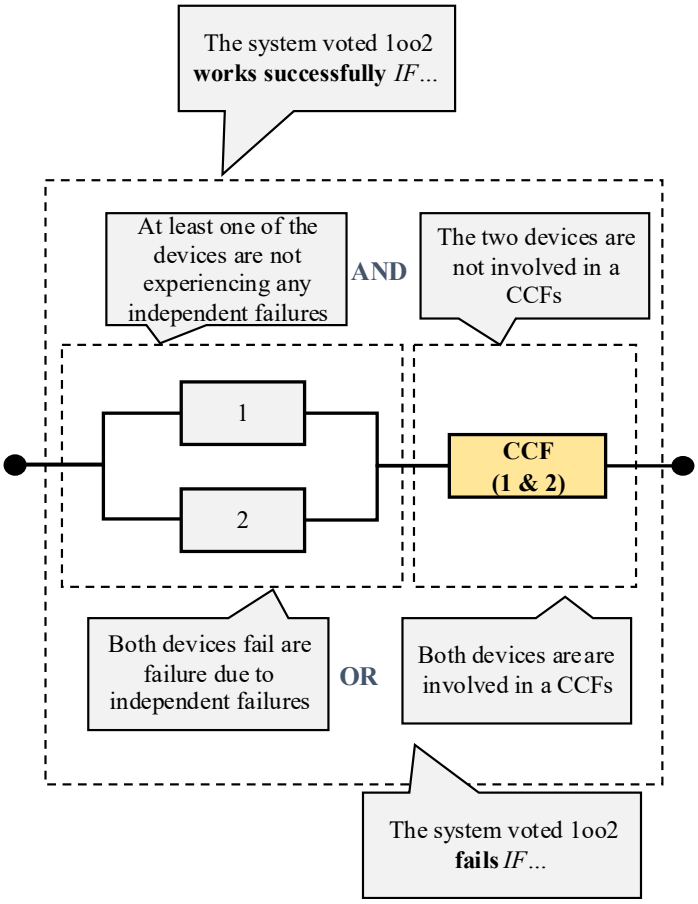


Fig. 21. Adding CCFs to the RBD and how this is interpreted

8.7.4 Fault tree analysis

Fault Tree Analysis (FTA) is a widely used method for analyzing how a system can fail. It was first introduced in 1962 at Bell Telephone Laboratories to assess the reliability of the Minuteman intercontinental missile system.

FTA is a graphical modeling technique that illustrates the logical relationships between a system-level failure (top event) and the contributing lower-level events (such as component failures) in a tree-like structure. Since the analysis begins with the top-level failure and works downward to identify causes, FTA is considered a top-down approach.

According to Rausand and Høyland (2004), FTA involves the following main steps:

1. Define the system, including its boundaries and the specific failure or loss scenario at the system level.
2. Construct the fault tree, mapping out the logical connections between events.
3. Identify minimal cut sets, which are the smallest combinations of basic events that can lead to the top event.
4. Perform qualitative analysis, reviewing and validating the structure and logic of the fault tree, including verification of minimal cutsets reflecting how the system is actually working and failing.
5. Conduct quantitative analysis, assigning probabilities to events to calculate the likelihood of the top event.

A fault tree models events as binary: an event (failure) is either present or absent. From step 5, this binary model is extended with a probabilistic analysis by assigning probabilities or failure rates related to the events.

8.7.4.1 TOP Event definition and fault tree construction

The Top Event is the starting point of an FTA and represents a system-level failure or loss being analyzed. Effort should be put into how the Top Event is worded, as this influences the scope of the analysis. A well-defined Top Event should answer the following questions:

- What is the system to be assessed? (object)
- What is the system failure or loss? (failure)
- Under what circumstance(s)? (when)

Example Top Events:

- *The washing machine [object] fails to discharge water [failure] at the end of the washing program [when].*
- *The train [object] leaves the train station without permission (failure) while the red signal is lighted (when)*

The analysis proceeds downward to identify causes, such as events and faults that may lead to the Top Event. The main components of a fault tree include:

1. Basic Events (BE)
   These are the lowest-level failure causes, typically at the component level, where no further decomposition is performed. Basic events can also include human errors or external influences.
2. Logic Gates
   These define the logical relationships between events. Common gates include:
   - AND: All input events must occur for the output to occur.
   - OR: Any input event can cause the output.
   - KooN (k-out-of-n): The output occurs if *k* out of *n* inputs fail (used here in the context of *failure*).

- XOR: The output occurs if exactly one input occurs.

3. Transfer Symbols (Transfer-In and Transfer-Out)
   These are used to link different parts of a fault tree, especially when the tree spans multiple pages or is modularized. Transfer symbols help maintain clarity and manageability in large or complex systems.

The KooN gate in FTA can be confusing, particularly for analyses of SIS systems where voting is often applied. In contrast to the KooN voting of an SIF subsystem that identifies conditions for successful performance, the KooN gate in a fault tree provides conditions for failure. For example, a 1oo3-voted subsystem means that at least one of three devices must function for the subsystem to operate. If modeled in a fault tree, we would need to select the 3oo3 gate, as the condition for failure of this subsystem is that all three devices fail.

Several commercial tools are available for constructing fault trees and performing both qualitative and quantitative analyses (steps 3–5). The graphical symbols used in FTA are illustrated in Fig. 22.

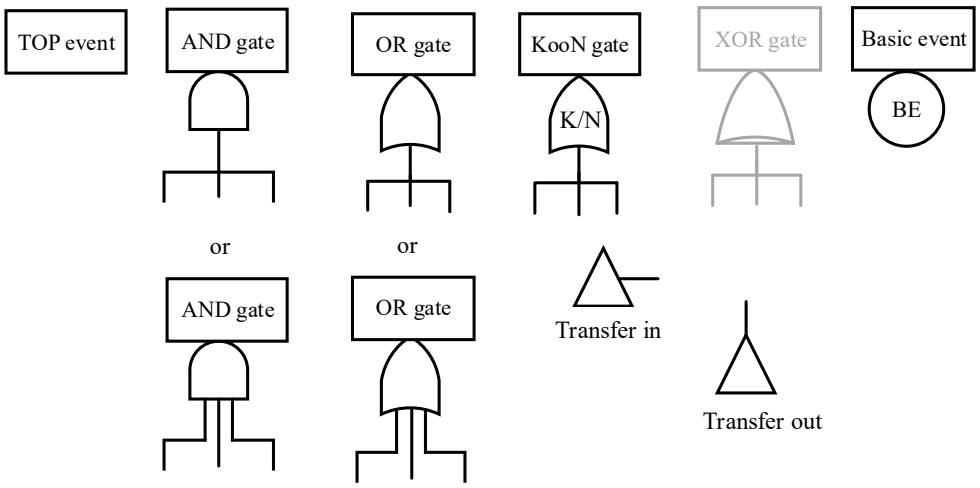


Fig. 22. FTA graphical symbols

A firewater pump system, illustrated in Fig. 23, consists of two pumps that are fed from a common water source. The same engine powers both pumps.

When the pressure in the supply lines drops suddenly, for example, due to the activation of a dry sprinkler system (such as when a heat-sensitive bulb melts), a normally closed valve is designed to open automatically, allowing water to flow into the system.

The corresponding fault tree, shown to the right of the figure, models the potential causes of system failure. While the structure of the tree can vary, it must always preserve the correct logical relationships between events. Even when analyzing the same system, multiple fault tree layouts may result. This variation is not an issue if the conditions and events leading to the Top Event are accurately and logically represented.

8.7.4.2 Find minimal cut sets

Identifying minimal cut sets (MCS) is one of the most valuable steps of an FTA, as they provide useful information both qualitatively and quantitatively.

MCSs are a subset of cut sets, where a cut set is a combination of basic events that, if they all occur, will lead to the Top Event (system failure). A cut set is considered minimal, i.e., an MCS, if it contains the smallest possible number of basic events that are necessary to cause the Top Event. In other words, an MCS is a cut set from which no basic event can be removed while preserving its status as a cut set. The order of a cut set (and of an MCS) is the number of basic events it contains.

Cut sets and MCSs can be identified manually if the fault tree is quite small. However, for larger and more complex trees, automated algorithms are typically required. These algorithms are implemented in most commercial fault tree analysis tools.

Tab. 7 lists all cut sets in relation to the pump system in Fig. 23. Here, cut sets marked with an asterisk (*) are the MCSs. For example, [VF] is an MCS, whereas [VF, PTF] is not because the basic event PTF can be removed without losing status as a cut set. We observe that no minimal cut sets have an order higher than 2 in our example. Naturally, any cut set of order 1 is minimal.

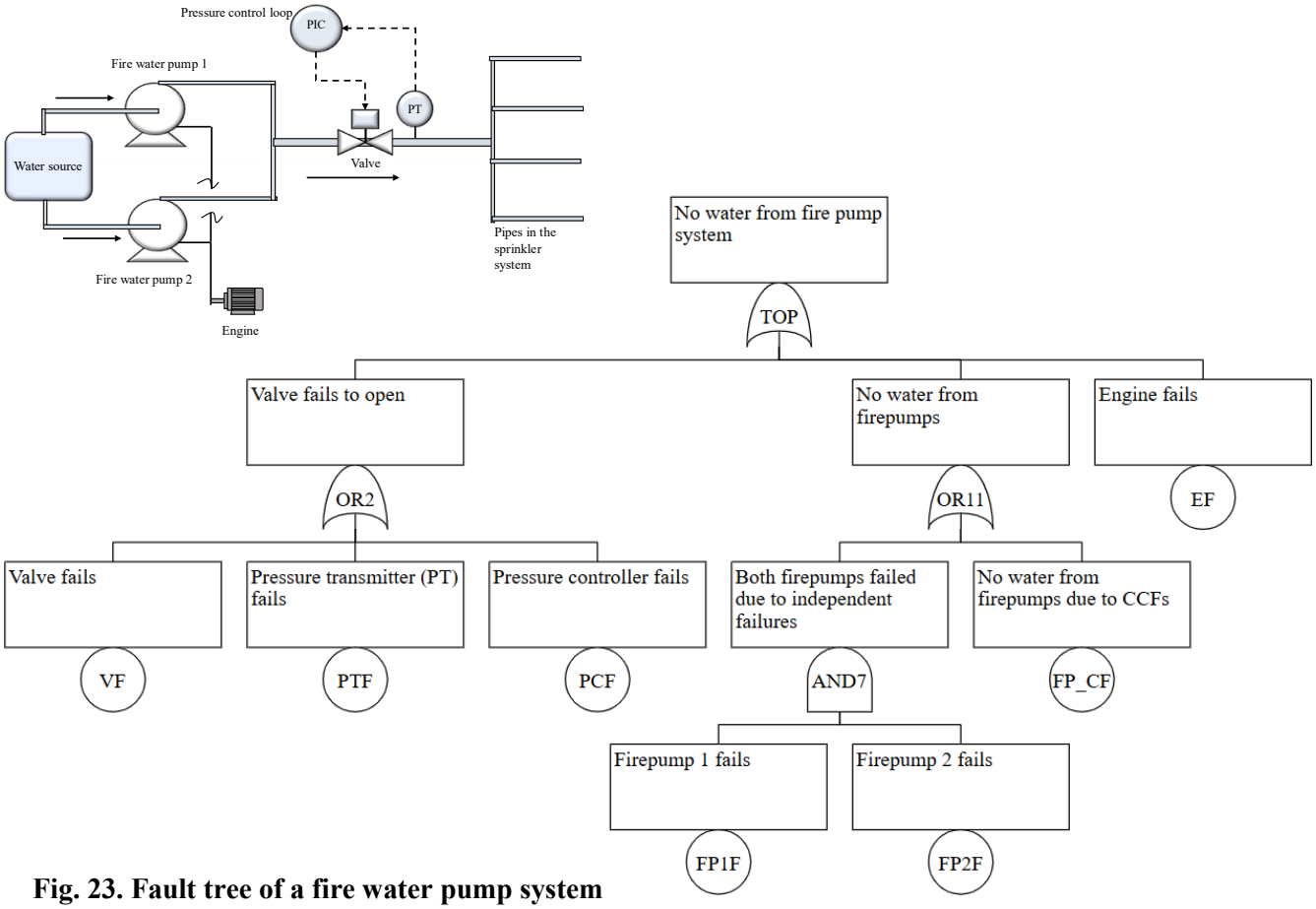


Fig. 23. Fault tree of a fire water pump system

Tab. 7. Cutsets and MCSs for the pump system

Order	Cut sets /**Minimal cut sets***
1	**[VF]*, [EF]*, [PFT]*, [PCF]*, [FP_CCF]***
2	[EF,VF], **[FP1F,FP2F]*,** [VF,PTF], [VF,PCF],[PTF,PCF], [EF,PTF], [EF,PCF], [FP_CCF, EF], etc.
3	[VF,PTF,PCF], [VF,FP1F,FP2F], [VF,PTF,EF], etc.
4	[VF,PTF,PCF,EF], [VF,PTF,FP1F, FP2F], etc.
5	[VF,PTF,PCF,FP1F,FP2F], etc.
6	[VF, PFT, PCF, FP1F, FWP2, EF]

8.7.4.3 Determining MCS with the MOCUS algorithm

Several algorithms are available in the literature for automatically generating lists of cut sets and minimal cut sets. One of the most widely used is the MOCUS algorithm, developed by Fussell and Vesely (1972). Their original example is illustrated in Fig. 24 and further explained in Rausand and Høyland (2004).

The MOCUS algorithm systematically identifies cut sets using a structured top-down approach by decomposing **AND** and **OR** gates. The process works as follows:

1. List inputs to OR gates vertically
2. List inputs to AND gates horizontally
3. Continue decomposing inputs to OR and AND gates in the same manner until only basic events remain. When fully developed, all cut sets are listed vertically.
4. Select minimal cut sets (marked with *)
   The automation of this process is not explained here, so we do it manually:

   (i) Cut sets of order 1 (single basic event) are minimal by default.

   (ii) Higher-order cut sets must be evaluated one by one to determine if they are minimal by checking if one or more basic events can be removed without losing the status as a cut set.

   (iii) Orders larger than 4 are sometimes used as a cutoff limit for when development of MCSs stops (as their occurrence becomes very unlikely).

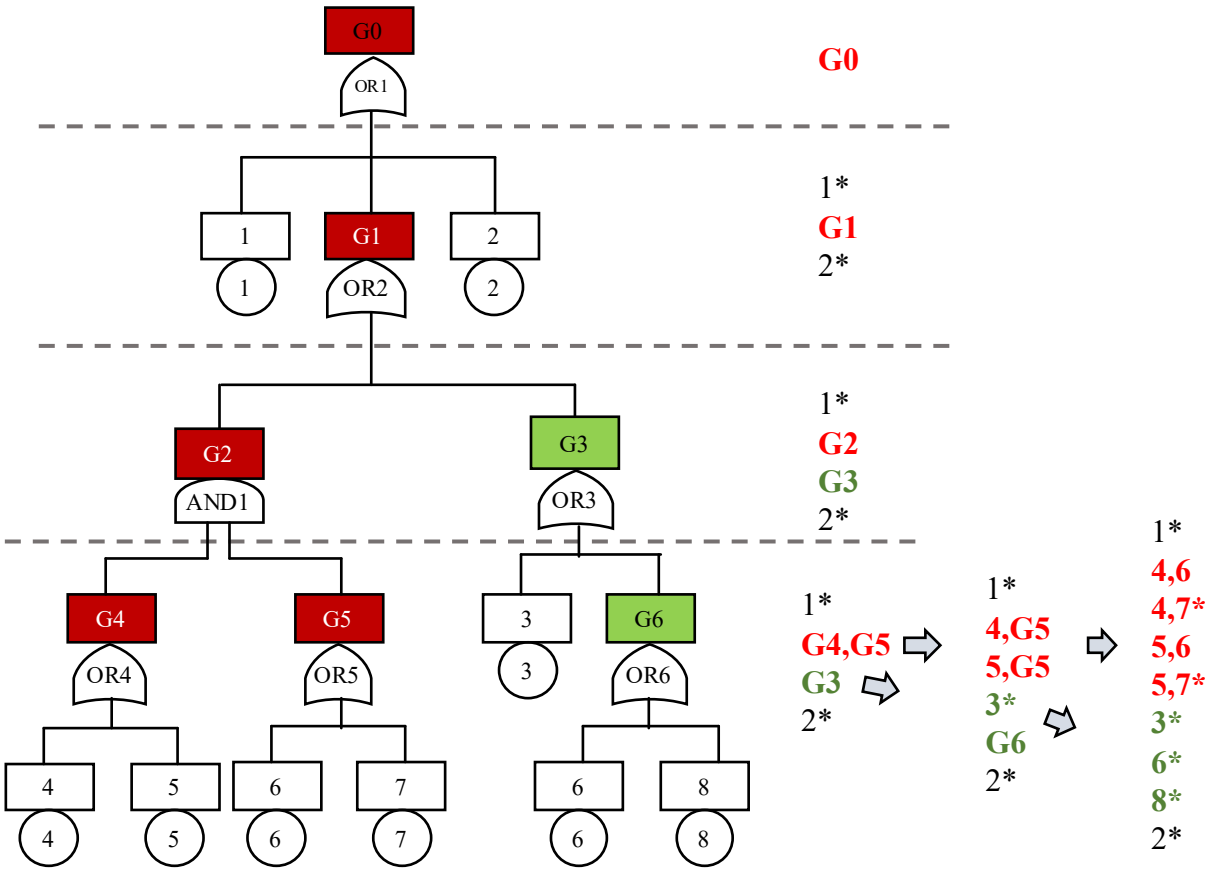


Fig. 24. MOCUS algorithm, adapted from Rausand and Høyland (2004)

A helpful program for FTA is the open-source program at https://jvatn.folk.ntnu.no/eLearning/FTA/. It is best to run this program in a private window (CTRL-Shift-N) and, if there are problems with updating the model, erase "cached images and files" (via CTRL-Shift-Del).

There are also commercial tools that provide trial versions. For example, the GRIF-WORKSHOP offers trial versions that support fault tree modeling, minimal cut set extraction, and both qualitative and quantitative analysis. You can explore the tool here: GRIF-WORKSHOP Boolean Package – Tree Module.

8.7.5 Comparison between RBD and FTA

RBD and FTA are, in principle, two similar methods with shared and distinct attributes, as explained in the following sections.

21. RBD and FTA are both binary analyses, meaning that only two states are considered: Functioning and failure.
22. RBD is success-oriented, while FTA is failure-oriented.
23. A fault tree model can always be converted to an RBD and vice versa.

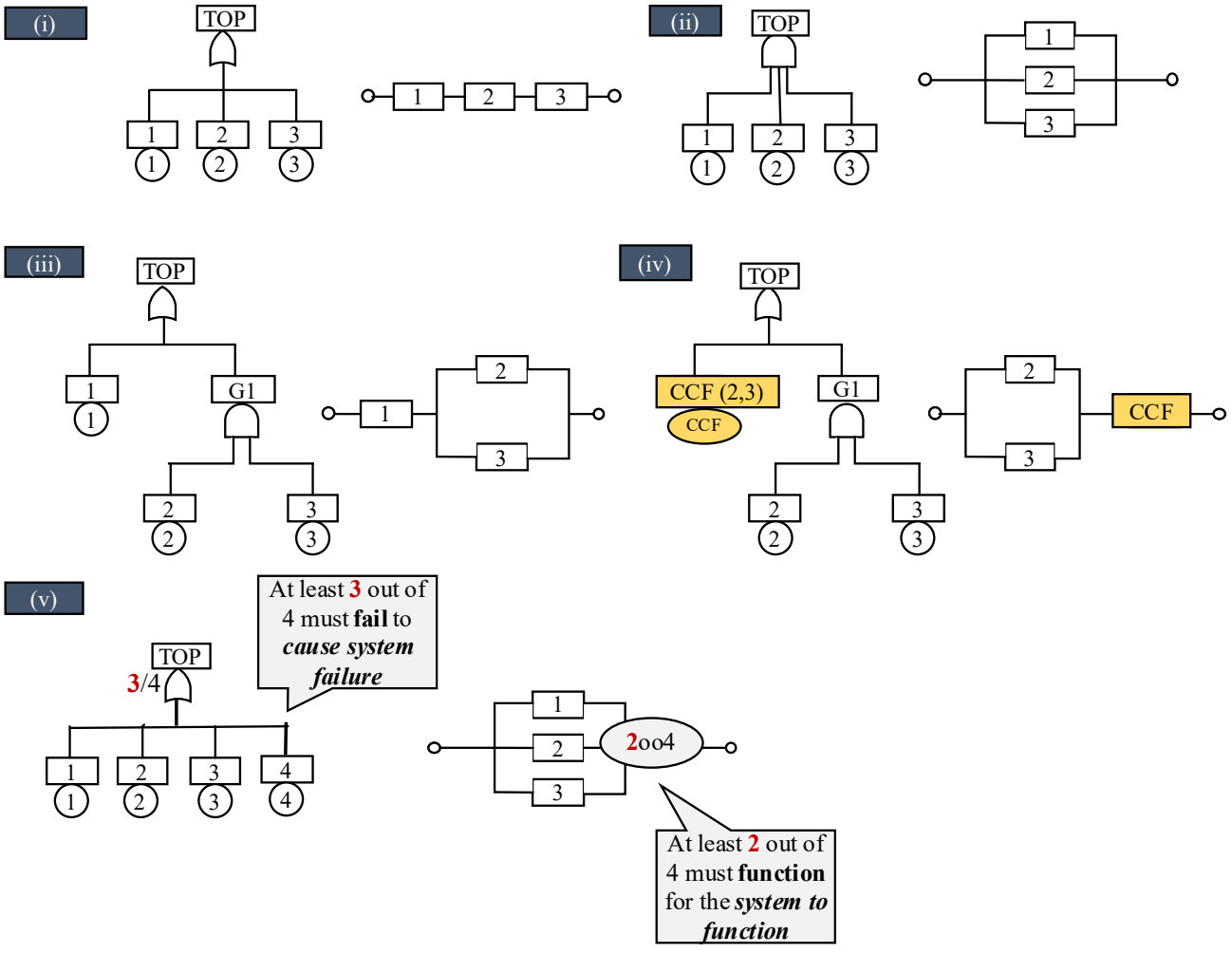


Fig. 25. Relationship Fault trees and RBDs

Examples of conversion from a fault tree to an RBD are illustrated in Fig. 25. It includes:

(i) From OR gate to a series structure

(ii) From AND gate to a parallel structure

(iii) From a combination of OR and AND gate to a hybrid series and parallel structure

(iv) As (iii), but with CCFs included

Since an RBD can always be converted to a fault tree and vice versa, it may seem unimportant which method is selected. However, the difference in mindset (success-oriented versus failure-oriented) is likely to affect what is eventually covered in the chosen model. For example, a fault tree, as a starting point, often leads to more events being included than starting with an RBD.

One explanation might be that the FTA explicitly incorporates the analysis's goal into the Top Event, thereby increasing awareness of the precise context for the reliability analysis. Another explanation is that one tends to iterate more (downwards in the fault tree) when considering explicit failure causes, as well as external influences and latent conditions that may have an impact.

A fault tree analysis may also reveal faults in other systems that are not directly related to the system's assessed function. For example, an RBD may identify the battery, ignition system, motor starter, and fuel system to enable the car to start. In contrast, a fault tree has the same types of events as a fault tree, plus additional ones relevant to how the TOP event is formulated, such as the driver being locked out due to a missing or disabled key.

8.7.6 Markov analysis

Markov analysis combines a graphical state-oriented modeling approach (Markov model) with quantitative analysis. Unlike RBD and FTA, it enables the representation of system states beyond just functioning and failure, such as degraded and in standby. A Markov model can also incorporate different repair strategies to restore the system to a functioning state. Markov analysis can be used to quantify the same reliability measures as with RBD and FTA related to the functioning and failure of system function, in addition to probabilities and frequencies of either being or entering other modeled states.

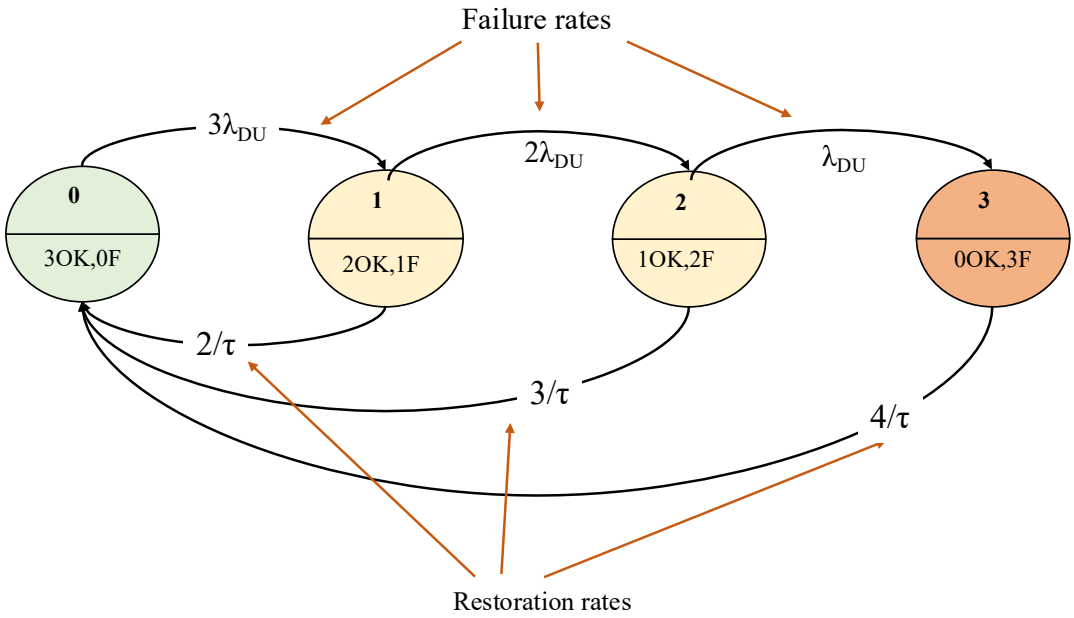


Fig. 26. Markov diagram for a system of three components

A concise and accessible introduction to Markov analysis is provided in Rausand and Høyland (2004). Here, we highlight a few key aspects of the method. For example, the key assumption in Markov modeling is that all transitions follow an exponential distribution, meaning the transition rates are constant. It means that the process

is memoryless in the sense that whether a transition from a state occurs depends only on the probability of being in that state and the transition rates out of it.

Tab. 8 lists the four distinct states, 0 to 3, of a system of three devices. The states are added in a Markov model as circles with applicable transitions as arrows, as shown in Fig. 26. We have assumed that we focus on DU failures. he transitions are identified with constant transition rates, here using λ_{DU} for failure rates and μ for restoration (or repair) rates. The model assumes that it is always possible to regain a fully functioning (all OK) state, meaning that the diagram can be used to determine steady-state probabilities. In our case, the main restoration time is influenced by the mean downtime of the system if the DU failure(s) is/are present. Without such a possibility (of return), one of the states becomes an absorbing state, i.e., a state where the system ends up, e.g., in a failed state.

Tab. 8. System states

State	State description
0	The devices are functioning (3OK)
1	Two devices are functioning, one has failed (2OK, 1F)
2	One part is functioning, two have failed (1OK, 2F)
3	All three devices have failed (0OK,3F)

The probability of being in a state is determined by setting up the transition matrix and applying the Markov equation. The equations assume that the Markovian property is fulfilled, meaning that all failure rates are constant because transitions are independent of what happened before the system leaves the state.

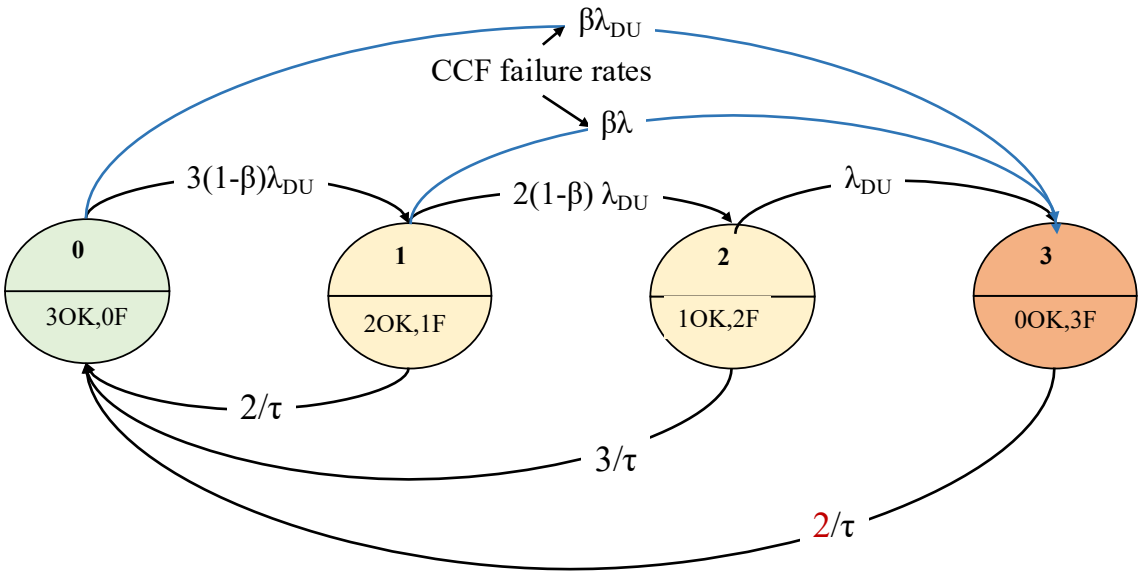


Fig. 27. Markov diagram with three components, also identifying CCFs

In the analysis of safety functions, it is required to include the contribution of CCFs. The way this is done in a Markov diagram is shown in Fig. 27:

- Additional transitions are made from states where two or more components can fail to the state where all components have failed.
- CCF failure rates are added, and the corresponding failure rates for independent failures are corrected accordingly, following, e.g., the standard beta factor model.

A Markov state diagram may also model states representing applicable failure categories of a device. The example, Fig. 28 illustrates failure categories typical for safety devices.

So far, this Chapter does not include quantitative analysis using Markov equations. The topic is well explained in Rausand and Høyland (2004) and Rausand (2014).

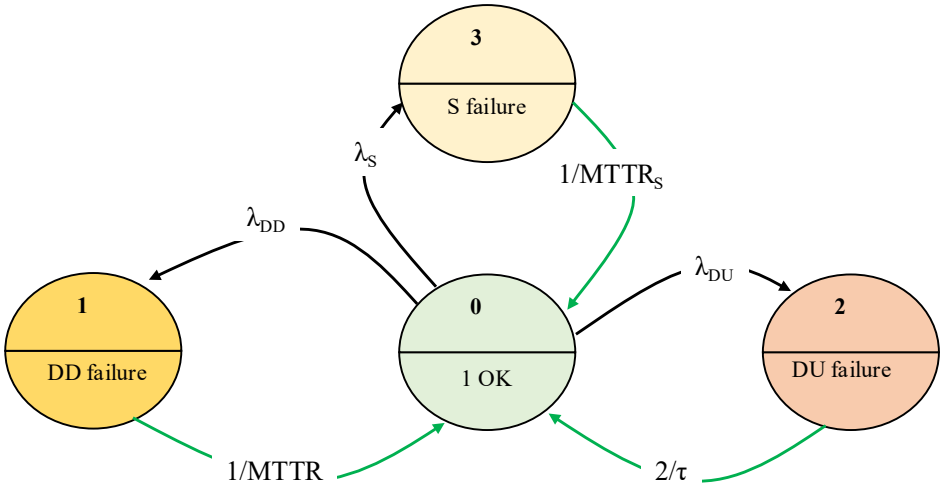


Fig. 28. Markov diagram for one component with 4 states

8.8 Quantitative reliability analysis

There are several options for probabilistic and frequency-based measures used to express system reliability. For a more comprehensive treatment of reliability theory, refer to Rausand and Høyland (2004). In this section, we will provide a brief overview of selected key concepts that form the foundation for quantifying the reliability of safety instrumented functions (SIFs).

8.8.1 The reliability function R(t) and failure function F(t)

A common starting point in reliability analysis is to define the reliability function R(t), also known as the survival function, or its inverse, the failure function F(t). The reliability function is mathematically expressed as the probability that the system or component will survive beyond time t, where T is a random variable representing the time at which the device fails:

$$R(t)=\Pr(T>t)$$

The use of capital T indicates that time to failure is not a fixed value but a stochastic (random) variable that follows a probability distribution (e.g., exponential, Weibull, or normal distribution), depending on the nature of the system and failure behavior. In this chapter, we will primarily apply the exponential distribution.

8.8.2 Determine reliability and failure function based on RBDs

Previously, we introduced the reliability function and the failure function for individual components. Now, we extend these concepts to series and parallel system structures, and we provide examples for subsystems with two devices. The process involves three main steps:

Step 1. Develop the structure function (we choose to base it on RBDs):

We begin by defining a structure function $\Phi(X(t))$, where $X(t)$ is a vector representing the state of each component at time *t*. For simplicity, consider a system with two components, with states denoted by $X_1(t)$ and $X_2(t)$. Each component can be in one of two states:

- 1: functioning
- 0: failed

In a series system, the entire system functions only if both components are functioning. The structure function is:

$$\Phi(\mathbf{X}(t)) = X_1(t) \cdot X_2(t)$$

In a parallel system, the system functions if at least one component is functioning. The structure function is:

$$\Phi(\mathbf{X}(t)) = 1 - (1 - X_1(t))(1 - X_2(t)) = \max(X_1(t), X_2(t))$$

If both components fail (i.e., X1(t)=X2(t)=0), the system also fails.

Step 2. Convert the structure function to a reliability function:

Since the future state of each component is uncertain, we introduce probability distributions for their states over time.
Let:

- $R_1(t)$ = probability that component 1 is functioning at time *t*
- $R_2(t)$ = probability that component 2 is functioning at time *t*
- $R_s(t)$ = probability that the system is functioning at time *t*

Using the structure functions:

$$R_s(t) = R_1(t) \cdot R_2(t)$$

For the parallel structure, the reliability function becomes:

$$R_s(t) = 1 - (1 - R_1(t))(1 - R_2(t)) = R_1(t) + R_2(t) - R_1(t) \cdot R_2(t)$$

24.

or more complex systems, the structure function must be simplified before converting to a reliability function. See Rausand and Høyland (2004) for detailed methods.

Step 3. Select an applicable probability distribution:

Assume that the time to failure for each component follows an exponential distribution: $R_i(t) = e^{-\lambda_i t}$ for i=1,2.

For the series structure, we get:

$$R_s(t) = e^{-\lambda_1 t} \cdot e^{-\lambda_2 t} = e^{-(\lambda_1 + \lambda_2)t}$$

For the parallel structure, we get:

$$R_s(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}$$

If the components are identical (i.e., $\lambda_1=\lambda_2=\lambda$), the equations simplify to:

$$R_s(t) = e^{-2\lambda t} \text{ (for series structure)}$$

$$R_s(t) = 2e^{-\lambda t} - e^{-2\lambda t} \text{ (for parallel structure)}$$

Let's calculate the reliability after 500 hours, assuming a failure rate of: $\lambda_1 = \lambda_2 = \lambda = 1E-4$ per hour. We get:

$$R_s(500) = e^{-2 \cdot E-4 \cdot 500} = 0.904 \text{ (series structure)}$$

$$R_s(500) = 2e^{-1E-4 \cdot 500} - e^{-2 \cdot 1E-4 \cdot 500} = 0.976 \text{ (parallel structure)}$$

As expected, the parallel structure is more reliable than the series structure.

The failure function, denoted F(t), represents the probability that a system has failed by time *t*. It is directly related to the reliability function R(t):

F(t)=1−R(t) and (of course) $F(t)=1-R(t)$

For the series and parallel structure of two identical components failing independently, we get:

Series structure:

$$F_s(t) = 1 - e^{-2\lambda t}$$

Parallel structure:

$$F_s(t) = 1 - 2e^{-\lambda t} + e^{-2\lambda t}$$

8.8.3 Determine failure function based on minimal cut sets

Failure functions can also be derived from minimal cut sets (MCSs) identified in a fault tree analysis (FTA). Following the terminology in Rausand and Høyland (2004):

- Let $q_i(t)$ be the probability that component *i* has failed by time *t*. This is the probability of a basic event occurring in the fault tree
- Let $Q_0(t)$ be the probability that the system is in the failed state. This is the probability of the TOP event occurring.
- Let $Q_j(t)$ be the probability that the minimal cut set j causes system failure.

Recall that a minimal cut set is the smallest combination of component failures that causes system failure. If a minimal cut set C_j contains components that must all fail for the cut set to occur, then:

$$\breve{Q}_j(t) = \prod_{i \in C_j} q_i(t)$$

The **upper bound approximation** assumes that any one of the *k* minimal cut sets can independently cause system failure, analogous to a parallel structure in terms of failure.

$$Q_0(t) \le 1 - \prod_{j=1}^{k} (1 - \breve{Q}_j(t)) \approx 1 - \prod_{j=1}^{k} (1 - \breve{Q}_j(t))$$

Assuming exponentially distributed time to failure and identical components, the failure probability for each functional element is:

$$q_1(t) = q_2(t) = 1 - e^{-\lambda t}$$

The series structure implies that any failure (of the two) leads to a system failure, resulting in two minimal cut sets [1], [2]:

$$\breve{Q}_1(t) = 1 - e^{-\lambda t}, \breve{Q}_2(t) = 1 - e^{-\lambda t}$$

$$Q_0(t) \approx 1 - \prod_{j=1}^{2} (1 - \breve{Q}_j(t))$$

$$Q_0(t) \approx 1 - (e^{-\lambda t})^2 = 1 - e^{-2\lambda t}$$

This matches the failure function for a series system: F(t) = 1 - R(t). The parallel structure requires that both components fail, meaning one minimal cut set: [1, 2]:

$$\breve{Q}_1(t) = \prod_{i=1}^{2} q_i(t) = (1 - e^{-\lambda t})^2$$

$$Q_0(t) \approx 1 - \prod_{j=1}^{1} (1 - \breve{Q}_j(t))$$

$$Q_0(t) \approx 1 - (1 - (1 - e^{-\lambda t})^2) = 1 - 2e^{-\lambda t} + e^{-2\lambda t}$$

Again, this matches the failure function for a parallel system: F(t) = 1 - R(t).

8.8.4 The failure density function f(t)

F(t) and R(t) are determined from a probability density function f(t), defined as:

$$f(t) = \frac{d}{dt} F(t) = -\frac{d}{dt} R(t)$$

The formula expresses the likelihood that the item will fail within a very short time interval, meaning it represents a probability per unit of time. If we assume that the time to failure of a device is exponentially distributed with parameter λ (lambda), then:

$$f(t) = \lambda \cdot e^{-\lambda t}$$

Later, we will introduce the parameter λ as the failure rate of a device; however, in the context of the probability density function, it has a vaguer meaning. At time t = 0, when the failure density is equal to λ, it is evident that the parameter is also a measure per time unit. Then, as t goes to infinity, f(t) approaches 0, because of the assumptions underlying the exponential distribution: As time goes by, it becomes less likely to experience a failure, meaning that the failure has probably already occurred.

F(t) expresses how the failure probability accumulates over the same period t, meaning:

$$F(t) = \int_0^t f(u)du = \lambda e^{-\lambda t} du = 1 - e^{-\lambda t}$$

The reliability function follows from the relationship that F(t)+R(t)=1 at any time t, meaning that if not failed, it must have survived:

$$R(t) = 1 - F(t) = e^{-\lambda t}$$

With these formulas, we can calculate the probability of an item surviving a specific time t, for example, 500 hours, and the probability of failing before a time t (e.g., 500 hours), assuming we have a reasonable estimate of λ . For example, with $\lambda = 1E-4$:

$$R(500) = e^{-1E-4 \cdot 500} = 0.95$$

$$F(500) = 1 - e^{-1E-4 \cdot 500} = 0.05$$

This means there is a 99.5% chance the item survives 500 hours, and a 0.5% chance it fails before then.

8.8.5 Failure intensity function z(t)

The failure intensity function, denoted z(t), is a conditional probability of failure per time unit. It is calculated as the probability that an item will fail in the following short time interval, given that it has survived up to time t. It is defined as:

$$z(t) = \frac{\frac{dF(t)}{dt}}{R(t)} = \frac{f(t)}{R(t)}$$

In other words, z(t) is the conditional rate towards a device failure, knowing that the device survived until t. For this reason, z(t) is referred to as the force of mortality (FOM), and this term has, according to Rausand and Høyland (2004), been introduced to avoid confusion with the rate of occurrence of failures (ROCOF). FOM applies to non-repairable devices, while ROCOF applies to repairable ones.

Assuming that the time to failure follows an exponential distribution, z(t) becomes:

$$z(t) = \frac{\lambda \cdot e^{-\lambda t}}{e^{-\lambda t}} = \lambda$$

With the exponential distribution, the failure intensity becomes a constant value, i.e., time independent. This assumption may apply to some types of technical devices, but not to humans: The constant value would indicate that the probability of a specific human dying in an upcoming period has nothing to do with their age.

8.8.6 Mean time to failure (MTTF)

The Mean Time to Failure (MTTF) represents the expected (average) time until a device fails, excluding any repair or replacement. In this context, the MTTF is the point in time at which the device is taken out of service or replaced by a new one. Mathematically, MTTF is defined as:

$$MTTF = E(T) = \int_0^\infty t \cdot f(t)dt = \int_0^\infty R(t)dt$$

The latter part of the equation is not straightforward to understand, but the explanation is provided in Rausand and Høyland (2004).

Assuming the time to failure of a single device follows an exponential distribution with failure rate λ, the MTTF becomes:

$$MTTF = \int_0^\infty R(t)dt = \int_0^\infty e^{-\lambda t}dt = \frac{1}{\lambda}$$

If we assume that $\lambda = 1E-4$ per hour, MTTF becomes 10,000 hours, which is slightly more than one year.

For redundant structures, it is often easier to first determine F(t) to derive R(t). For example, a subsystem of two devices voted 1oo2, $F(t) = (1-e^{-\lambda t})^2 = 1-2e^{-\lambda t}+e^{-2\lambda t}$. Then $R(t) = 2e^{-\lambda t}-e^{-2\lambda t}$. The corresponding MTTF becomes:

$$MTTF = \int_0^\infty R(t)dt = \int_0^\infty 2e^{-\lambda t}-e^{-2\lambda t}dt = \frac{2}{\lambda}-\frac{1}{2\lambda} = \frac{3}{2\lambda}$$

Assume that the items are identical with $\lambda = 1E-4$ per hour. By inserting this failure rate into the equations, we get MTTF = 5000 hours for a series structure and for the parallel structure MTTF= 15000 hours. As expected, the parallel system has a significantly higher MTTF than the series system, due to its redundancy.

If the two devices are not identical, but represented by two different failure rates, MTTF becomes:

$$MTTF = \int_0^\infty e^{\lambda_1 t}+e^{\lambda_2 t}-e^{-(\lambda_1+\lambda_2)t}dt = \frac{1}{\lambda_1}+\frac{1}{\lambda_2}-\frac{1}{\lambda_1+\lambda_2}$$

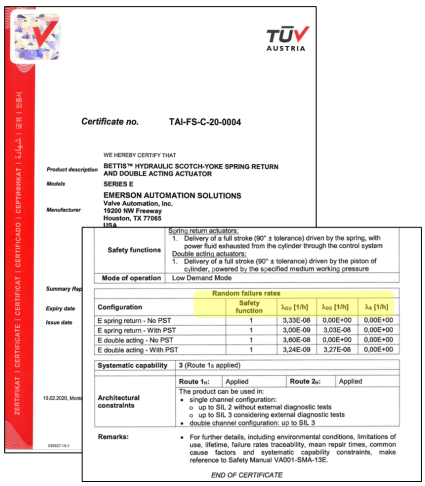
8.8.7 Rate of occurrence of failure (the device failure rate)

The rate of occurrence of failures (ROCOF) is what we define as the failure rate of devices. In its simplest form, ROCOF is defined as:

$$ROCOF = \frac{E(N(t))}{t}$$

Where:

- E[N(t)] is the expected number of failures over an interval t
- t is the interval of observation



TÜV AUSTRIA

Certificate no. TAI-FS-C-20-0004

WE HEREBY CERTIFY THAT

Product description: BETTIS™ HYDRAULIC SCOTCH-YOKE SPRING RETURN AND DOUBLE ACTING ACTUATOR

Models: SERIES E

Manufacturer: EMERSON AUTOMATION SOLUTIONS, Valve Automation, Inc., 19200 NW Freeway, Houston, TX 77065, USA

Safety functions:
Spring return actuators:
1. Delivery of a full stroke (90° ± tolerance) driven by the spring, with power fluid exhausted from the cylinder through the control system
Double acting actuators:
1. Delivery of a full stroke (90° ± tolerance) driven by the piston of cylinder, powered by the specified medium working pressure

Mode of operation: Low Demand Mode

Random failure rates

Configuration	Safety function	λ_{DU} [1/h]	λ_{DD} [1/h]	λ_{S} [1/h]
E spring return - No PST	1	3,33E-08	0,00E+00	0,00E+00
E spring return - With PST	1	3,00E-09	3,03E-08	0,00E+00
E double acting - No PST	1	3,60E-08	0,00E+00	0,00E+00
E double acting - With PST	1	3,24E-09	3,27E-08	0,00E+00

Systematic capability: 3 (Route 1_S applied)

Route 1_H:	Applied	Route 2_H:	Applied

Architectural constraints: The product can be used in:
- single channel configuration:
  - up to SIL 2 without external diagnostic tests
  - up to SIL 3 considering external diagnostic tests
- double channel configuration: up to SIL 3

Remarks:
- For further details, including environmental conditions, limitations of use, lifetime, failure rates traceability, mean repair times, common cause factors and systematic capability constraints, make reference to Safety Manual VA001-SMA-13E.

END OF CERTIFICATE

Fig. 29. Example of failure rate notation in a component certificate

When analyzing a homogeneous group of items (i.e., identical or sufficiently similar), the failure process can be modeled as a Homogeneous Poisson Process (HPP) if:

- Each item's time to failure is exponentially distributed
- The repair or restoration time is negligible (i.e., the item is quickly returned to service, where what is quickly enough is evaluated in the context it is used)

Under these assumptions, the probability of experiencing *n* faults during the period is:

$$\Pr(N(t) = n) = \frac{(\lambda t)^n}{n!} e^{-\lambda t}$$

The expected number of faults over the same period becomes:

$$E(N(t)) = \sum_{n=0}^{\infty} n \cdot P(N(t) = n) = \lambda t$$

Thus, the ROCOF simplifies to:

$$ROCOF = \frac{E(N(t))}{t} = \lambda$$

It is this λ that is the failure rate of repairable components, whereas λ calculated from MTTF is the failure rate of a non-repairable component. However, by assuming the mean time to repair (MTTR) is negligible relative to

MTTF, then MTBF≈MTTF. In this case, the formulas for MTTF also apply to the relationship between MTBF and MTFF, i.e., that for a single component, we get the relationship:

$$\lambda = \frac{1}{MTBF}$$

Reliability data handbooks may provide MTBF or λ, and in either case, the other can be calculated with the given relationship.

Remark: We have just learnt that ROCOF becomes constant when the HPP process applies. However, in reliability analyses of safety-instrumented systems (SIS), we will later learn that a specific category of safety-critical failures, named dangerous undetected (DU), is not detected during regular operation and remains hidden until the next scheduled test is performed. As a result, it seems that the requirement for negligible restoration time is violated. However, in this case, it is claimed that the mean time to a DU failure is so long (in the range of 1/1E-6 hours or even lower values) that a restoration at the next test interval (e.g., after one year) is still fast enough. This example illustrates that what is considered a negligible restoration time is context dependent.

The failure rates provided by manufacturer documentation, like the ones shown in Fig. 29 are therefore ROCOF and calculated for a failure process assumed to be HPP even for DU failures.

8.8.8 Mean time between failures (MTBF) and availability (A)

The mean time between failures (MTBF) represents the average time between successive failures for a repairable device. It incorporates the time until the device(s) fail and the time required to restore them:

$$MTBF = MTTF + MTTR$$

Here:

- MTTF is the mean time to failure
- MTTR is the mean time to repair or restoration, where restoration also incorporates the time it takes to detect the failure

We can also estimate the MTBF as shown in Fig. 30**,** considering actual experienced survival (time to failure – TTR) and down times (time to repair – TTR).

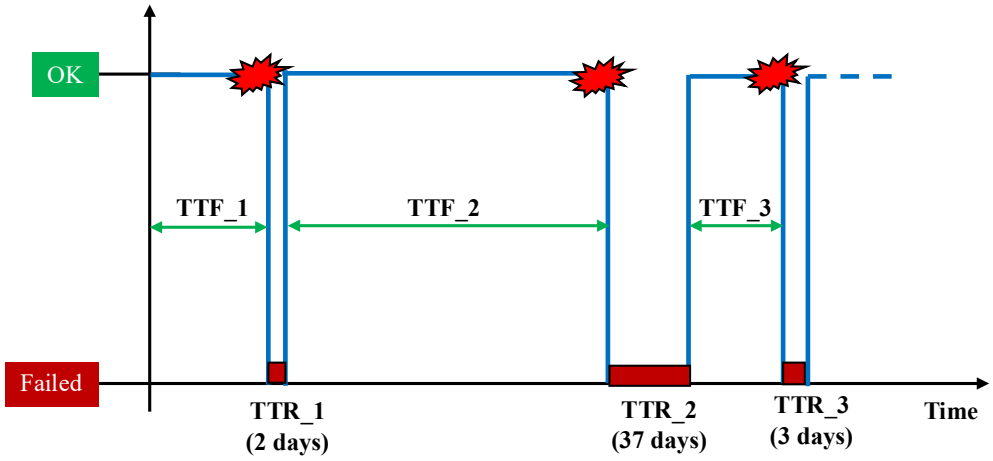


Fig. 30. Example data for calculating MTBF and MTTR

Fig. 30 has provided some example values of TTFs and TTRs: During the period of interest, three periods were recorded for time to failure (TTF) of TTF1 = 3 years, TTF2 = 4 years, and TTF3 =1 year.

MTTF is the mean (or average) value of the three TTFs, i.e.,

$$MTTF = \frac{3+5+1}{3} = 3 \text{ years}$$

Likewise, the average mean time to restoration (or repair) MTTR is the mean value of the three TTRs, i.e.,

$$MTTR = \frac{2+37+4}{3} = 14.3 \text{ days or } 0.039 \text{ years.}$$

It means that the MTBF becomes:

$$MTBF = MTTF + MTTR = 3 + 0.039 = 3.0039 \text{ (years)}$$

The average availability (A = availability) is the mean time the system is operational and is a function of MTTF and MTTR:

$$A = \frac{MTTF}{MTTF + MTTR} = \frac{MTTF}{MTBF}$$

With the calculated MTBF and MTTR, the A becomes 87%.

$$A = \frac{3}{3.039} \approx 87\%$$

The corresponding unavailability, i.e., $\overline{A}$:

$$\overline{A} = 1 - A = \frac{MTTR}{MTBF} = \frac{0.039}{3.039} \approx 13\%$$

When MTTR << MTTF, we can assume that $MTBF \approx MTTF$. The following simplification therefore applies for the unavailability:

$$\overline{A} = 1 - A \approx \frac{0.039}{3} \approx 13\% \text{ (and similar for the availability).}$$

8.8.9 Bathtub curve

The failure rate over the lifetime of devices is often explained with the bathtub curve (illustrated in Fig. 31), even if variants exist. The curve is typically divided into three distinct phases:

- Phase 1: Infant mortality phase, where the failure rate is initially high due to manufacturing defects, installation issues, or early-life weaknesses. This phase ends when the manufacturer (or user) has identified and removed those that relate to quality and misuse issues.
- Phase 2: Useful life period, where the failure is approximately constant. If the device fails during this period, we assume perfect repair or replacement so that the device's state remains as good as new.
- Phase 3: Wear-out phase, where the wear has reached a level where the failure rate increases. In this phase, repairs and maintenance are less effective, and the state achieved is no more than “as good as before.” A replacement of the device is required when its performance is seriously affected or when the time in use exceeds the manufacturer's recommendation.

Throughout all phases, it is essential to recognize that the failure rate is uncertain due to imperfect knowledge. A mean value of the failure rate can therefore be complemented with information about the confidence or credibility intervals. Regularly recalculating failure rates as new data become available is also an important activity.

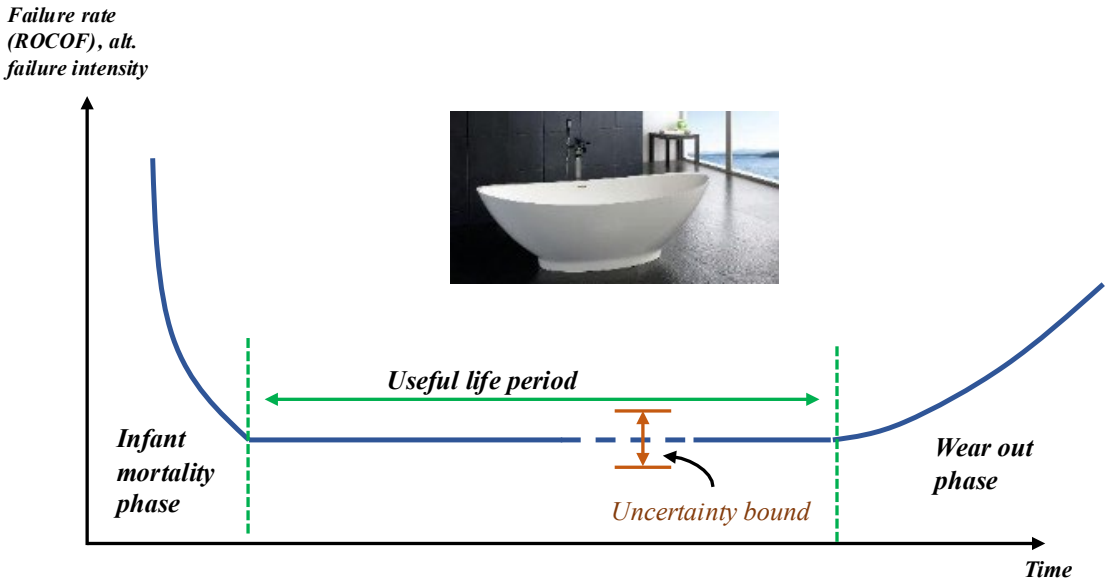


Fig. 31. Bathtub curve for failure rate

8.9 Choice of reliability measure for SIFs

Two different reliability measures are suggested for SIFs, based on how often the SIFs are demanded, meaning required to respond to real hazardous events:

- Average probability of failure on demand (PFD): Applies to SIFs operating in low-demand mode, meaning one or fewer demands per year.
- Average probability of having a dangerous failure per hour (PFH), also called dangerous failure frequency (per hour): Applies to SIFs operating in the high-demand or continuous mode of operation. Here, high-demand mode means more than one demand per year, and continuous mode means that the demands are part of regular operations.

In this chapter, there is slightly more focus on PFD than PFH, as PFD is more common for SIFs in the process industry.

8.9.1 What is the PFD?

The PFD is defined as the average probability that SIF, or a SIF subsystem, is in a dangerous failed state during the time interval from 0 to τ:

$$PFD = \frac{1}{\tau}\int_0^{\tau} F(t)dt = 1 - \frac{1}{\tau}\int_0^{\tau} R(t)dt$$

Where:

- **F(t)** is the time-dependent probability that the system has failed dangerously at time *t*.
- **R(t)** is the time-dependent probability that the system has survived dangerous failures up to time t.
- **τ** is the regular test interval (i.e., the time between periodic proof tests).

Given that SIF devices are repairable systems, this measure also represents the fraction of time during which the SIF or its subsystem is unavailable due to dangerous failures. Dangerous failures can be classified as dangerous detected (DD) or dangerous undetected (DU), and both contribute to PFD, but not equally. A dangerous failure to be detected by diagnostics online within a short time after the fault was introduced by diagnostics, and if the failure is repaired and the device restored within a few hours, the influence on the SIF

availability is negligible. In contrast, a DU failure is, by definition, not detected automatically and immediately and remains hidden until the next regular test (or real demand). The period during which a DU failure remains hidden can range from months to years, depending on the test interval. The unavailability due to DU failures is therefore a dominating contributor to PFD, whereas DD failures can often (under the given conditions above) be neglected. Consequently, assuming for now that SIF consists of one device with exponentially distributed time to (a DU) failure, the PFD becomes:

$$PFD = \frac{1}{\tau}\int_0^{\tau} 1 - e^{-\lambda_{DU} t}\, dt = 1 - \frac{1}{\tau}\int_0^{\tau} e^{-\lambda_{DU} t}\, dt$$

Here,

- $F(t) = 1 - e^{-\lambda_{DU}\, t}$ is the failure probability as a function of time for a single device exposed to an exponentially distributed time-to-failure.
- $R(t) = e^{-\lambda_{DU}\, t}$ is the corresponding reliability (or survival) function.
- λ_{DU} is the DU failure rate.
- The proof test interval τ is on the order of months to a few years (e.g., 1 year = 8760 hours).

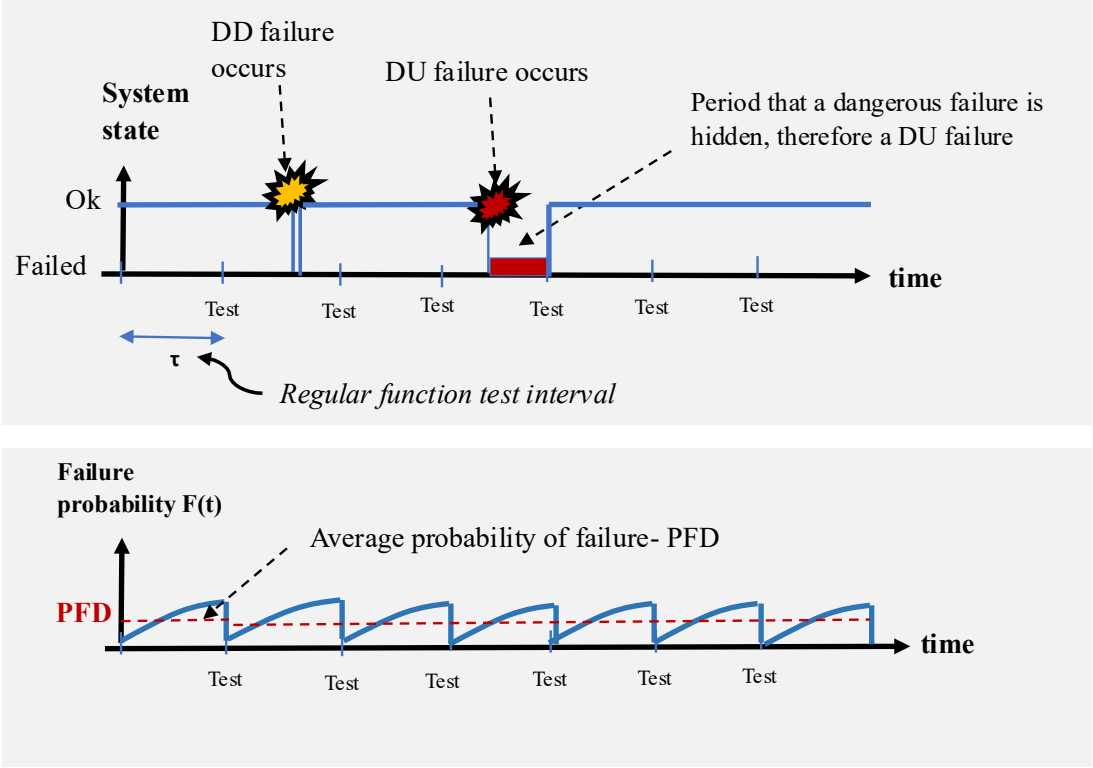


Fig. 32. Interpretation of PFD

The PFD can be interpreted as follows, with support in the illustrations in Fig. 32.

- The upper part of the figure shows a timeline where low-demand SIF is subject to regular testing. For simplicity, we consider a period during which the test intervals are equal.

- At some point between tests, a DU failure may occur. If a demand happens after the failure but before the next test, the SIF will not perform its intended function. If there is no demand, the DU failure remains hidden until the next scheduled test.

The lower part of the figure shows the probabilistic behavior of the system over time:

- At the start of each test interval (and immediately after each test), the system is assumed to be fully functional, meaning F(t)=0.
- As time progresses, the probability of a DU failure increases, causing F(t) to rise.
- Just before the next test, F(t) reaches its maximum value for that interval.
- After the test, any detected failures are repaired, and the system is restored to an "as good as new" condition, resetting F(t) to zero.

This behavior assumes:

- Exponentially distributed time to failure
- Over time, considering that the devices are being perfectly repaired and put back into operation, the occurrence of failures follows a homogeneous Poisson process

Because the test intervals are assumed to be equal and the failure rate is constant, the pattern of F(t) repeats identically in each interval. Therefore, the average value of F(t) over one interval is representative of all intervals. This average value of F(t) over the interval of the proof test is what we define as the PFD.

The PFD must be recalculated if the test interval is changed or the DU failure rate takes a new value.

8.9.2 PFD of a single device

Recall that the PFD can be calculated using either the reliability function R(t) or the failure function F(t). As explained in Rausand (2014), it is often more practical to perform calculations with F(t) as the formulas are easier to derive.

Consider a single device with a constant DU failure rate λ_{DU}. Recall that the failure function becomes:

$$F(t) = 1 - e^{-\lambda_{DU} t}$$

In many practical cases:

- The failure rate λ_{DU} is on the order of 1E-6 per hour.
- The proof test interval τ is on the order of months to a few years (e.g., 1 year = 8760 hours).

Given these conditions, the product λ_{DU} and τ are typically much less than 0.1, allowing us to use the approximation:

$$F(t) \approx \lambda_{DU} \cdot t$$

This simplifies the PFD calculation significantly. The average PFD over the interval $[0,\tau]$ becomes:

$$PFD = \frac{1}{\tau}\int_0^{\tau} F(t)dt = \frac{1}{\tau}\int_0^{\tau} 1 - e^{\lambda_{DU} t}dt \approx \frac{1}{\tau}\int_0^{\tau} \lambda_{DU} t dt \approx \frac{\lambda_{DU}\tau}{2}$$

Why is $\lambda_{DU} \cdot \tau$ often less than 0.1? This is because DU failure rates are typically in the range of 1E-6/hour, and test intervals are several months to one or two years. For example, the product of λ_{DU} =1E-6 and τ = 8760 (one year) is 0.00876.

8.9.3 PFD for series and parallel structure

We will now show how to determine PFD formulas for series and parallel structures involving two identical and independent devices. Here, "independent" means that the devices fail independently of each other. For now, we exclude the contribution of CCFs.

Series structure

For a series structure of devices, the system fails if any one of the devices fails. Assuming a constant failure rate λ_{DU} for a series structure of N components, we get:

$$F(t) = 1 - e^{-N \cdot \lambda_{DU} t} \approx N \cdot \lambda_{DU} t$$

Then, PFD becomes:

$$PFD = N \cdot \frac{\lambda_{DU} \tau}{2} = \frac{N \cdot \lambda_{DU} \tau}{2}$$

In case of two devices in series, the PFD becomes:

$$PFD = 2 \cdot \frac{\lambda_{DU} \tau}{2} = \lambda_{DU} \tau$$

$$\begin{aligned} PFD_{SIF} &= 1 - (1 - PFD_{IE})(1 - PFD_{LS})(1 - PFD_{LS}) \\ &\approx PFD_{IE} + PFD_{LS} + PFD_{LS} \text{ when } \mathrm{PFD}_i \leq 0.1 \end{aligned}$$

Parallel structure

In a parallel configuration of N devices, considering that any failure of a device results in system failure, then F(T) becomes:

$$F(t) = (1 - e^{-\lambda_{DU} t})^N \approx (\lambda_{DU} t)^N$$

Then PFD becomes:

$$PFD = \frac{1}{\tau} \int_0^{\tau} (\lambda_{DU} t)^N \, dt = \frac{(\lambda_{DU} \tau)^N}{N+1}$$

For a parallel system of two devices, voted 1oo2, we get:

$$F(t) = (1 - e^{-\lambda_{DU} t})^2 \approx (\lambda_{DU} t)^2$$

The average PFD becomes:

$$PFD = \frac{1}{\tau} \int_0^{\tau} (\lambda_{DU} t)^2 \, dt = \frac{(\lambda_{DU} \tau)^2}{3}$$

Similarly, we can derive simplified PFD formulas for more complex K-out-of-N (KooN) architectures. These are systems where the function is successful if at least K out of N components are operational. The general KooN formula is:

$$PFD = \frac{1}{\tau}\int_0^{\tau}\binom{n}{n-k+1}Q_{MCS}\,dt = \binom{n}{n-k+1}\frac{1}{\tau}\int_0^{\tau}(\lambda_{DU}t)^{n-k+1}\,dt$$

$$= \binom{n}{N-k+1}\frac{1}{\tau}\frac{\lambda_{DU}^{N-k+1}\tau^{N-k+2}}{N-k+2}$$

$$= \binom{N}{N-k+1}\frac{(\lambda_{DU}\tau)^{N-k+1}}{N-k+2}$$

(1)

The general formula for PFD of a KooN voted system of identical and independent devices subject to DU failures is therefore:

$$PFD = \binom{n}{n-k+1}\frac{(\lambda_{DU}\tau)^{n-k+1}}{n-k+2} \qquad (2)$$

The same formula (2) can also be derived directly from considering minimal cutsets introduced in fault tree analysis (FTA) using the upper bound approximation:

- A kooN system or identical or similar devices fail if N-k+1 failures occur
- The total number of combinations of faults, M, is $\binom{n}{n-k+1}$
- Each minimal cutset will consist of N-k+1 basic events. The probability of a minimal cutset occurring *i* is $Q_i(t)$ and will be the same for all minimal cutsets; therefore, it is named $Q_{MCS}(t)$*:*

$$Q_i(t) = Q_{MCS}(t) = \left(1-e^{-\lambda_{DU}t}\right)^{n-k+1} \approx (\lambda_{DU}t)^{n-k+1}$$

PFD can be calculated as:

$$PFD = \frac{1}{\tau}\int_0^{\tau}\binom{n}{n-k+1}Q_{MCS}\,dt = \binom{n}{n-k+1}\frac{1}{\tau}\int_0^{\tau}(\lambda_{DU}t)^{n-k+1}\,dt$$

$$= \binom{n}{N-k+1}\frac{1}{\tau}\frac{\lambda_{DU}^{n-k+1}\tau^{N-k+2}}{n-k+2}$$

$$= \binom{n}{n-k+1}\frac{(\lambda_{DU}\tau)^{n-k+1}}{n-k+2}$$

The formulas derived are summarized in Tab. 9, and are here referred to as simplified formulas.

Tab. 9. Simplified PFD formulas for kooN voted systems of identical devices

k/n	1	2	3	4
1	$\frac{\lambda_{DU}\tau}{2}$	$\frac{(\lambda_{DU}\tau)^2}{3}$	$\frac{(\lambda_{DU}\tau)^3}{4}$	$\frac{(\lambda_{DU}\tau)^4}{5}$

2	--	$\lambda_{DU}\tau$	$(\lambda_{DU}\tau)^2$	$(\lambda_{DU}\tau)^3$
3	--	--	$\frac{3(\lambda_{DU}\tau)^2}{2}$	$2(\lambda_{DU}\tau)^2$
4	--	--	--	$2\lambda_{DU}\tau$

It is also possible to calculate the PFD for systems where the devices are not identical, that is, they have different failure rates. In a 1oo2 configuration, the system fails only if both devices fail. If the two devices have failure rates, $\lambda_{DU,1}$ and $\lambda_{DU,2}$ the failure function becomes:

$$F(t) = (1-e^{-\lambda_{DU,1}t})(1-e^{-\lambda_{DU,2}t}) \approx \lambda_{DU,1} \cdot \lambda_{DU,2} \cdot t^2$$

The PFD becomes:

$$PFD = \frac{1}{\tau}\int_0^{\tau} \lambda_{DU,1}\lambda_{DU,1} \cdot t^2 dt = \frac{\lambda_{DU,1}\lambda_{DU,1}\tau^2}{3}$$

8.9.4 Calculating the PFD of a complete SIF

A SIF typically consists of three subsystems, as illustrated in Fig. 33:

1. Sensor subsystem (e.g., sensors or other initiators)
2. Logic solver subsystem
3. Final element subsystem (e.g., actuated valves or relays)

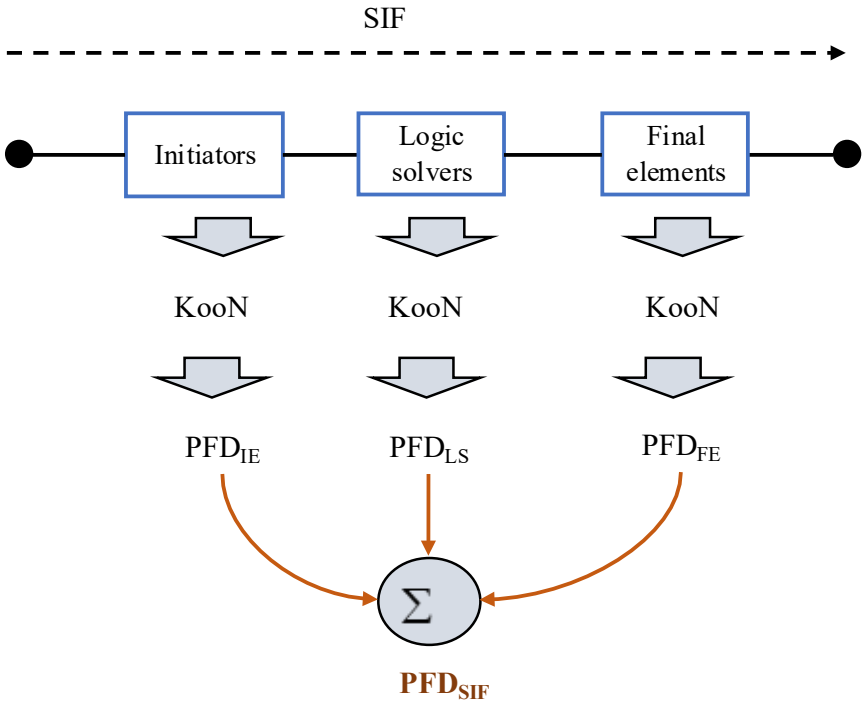


Fig. 33. How to calculate PFD of a SIF

Each of these subsystems may have its own K-out-of-N (KooN) voting configuration, and the corresponding PFD is calculated using the relevant formulas provided in Tab. 9. As the subsystems are totally independent of each other, the overall PFD of the SIF becomes:

$$PFD_{SIF} = 1-(1-PFD_{IE})(1-PFD_{LS})(1-PFD_{LS})$$

In practice, the overall PFD of the SIF can often be approximated as the sum of the PFDs of its three subsystems, if the values of the PFD are small, typically 0.1 or less. This means that PFD of the SIF becomes

$$PFD_{SIF} \approx PFD_{IE} + PFD_{LS} + PFD_{LS} \tag{3}$$

A value less than 0.1 is reasonable to expect, as it is the highest permitted value to be in the range of a safety integrity level (SIL), explained in the next section with Tab. 10.

Consider a SIF composed of the following subsystems:

- Three sensors: S1, S2, S3, configured in a 2oo3 voting arrangement
- One logic solver: L1
- Two final elements (valves): V1 and V2, configured in a 1oo2 voting arrangement

The corresponding RBD is shown in Fig. 34.

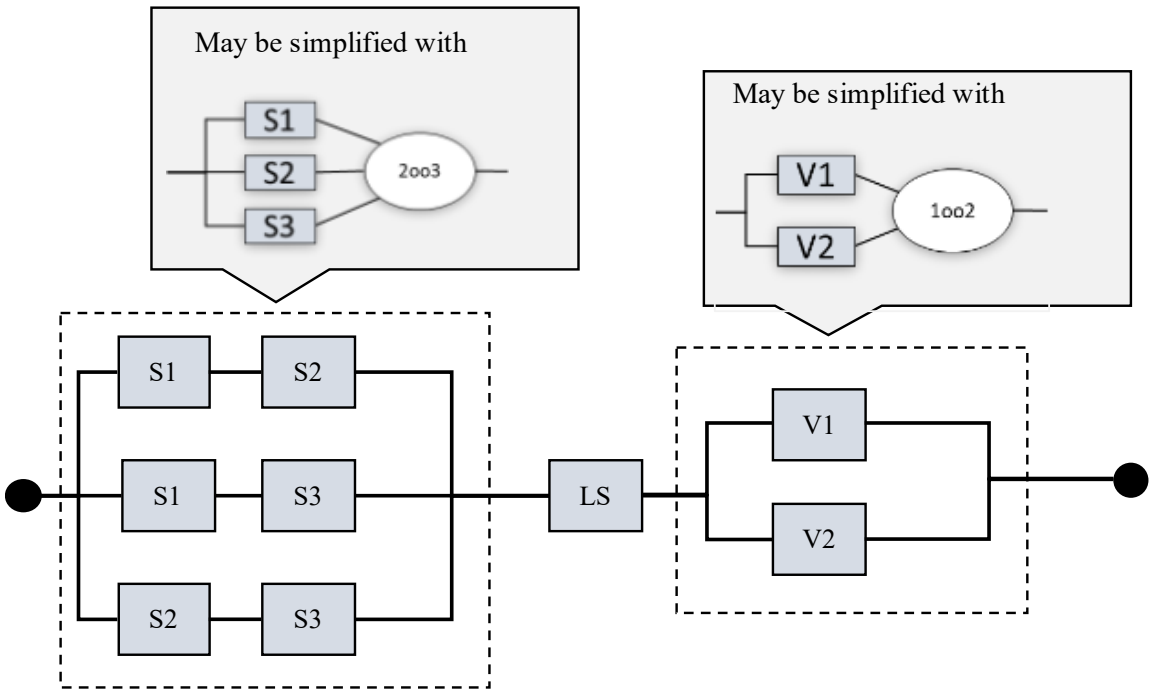


Fig. 34. RBD for en SIF

Using the applicable formulas from Tab. 9, the total PFD of the SIF becomes:

$$PFD = (\lambda_{DU,S}\tau)^2 + \frac{\lambda_{DU,L}\tau}{2} + \frac{(\lambda_{DU,V}\tau)^2}{3}$$

The formula assumes that the test interval is the same for all three subsystems. This is a common and practical assumption during the design phase of a SIF. However, in actual operation, the test intervals may vary between subsystems depending on maintenance strategies and operational constraints.

Calculation example: Assume that $\tau = 8760$ Hours (one year), and the failure rate for sensors is $\lambda_{DU,S} = 1E-6$ Per hour, for the logic solver, it is $\lambda_{DU,L} = 1E-7$ per hour, and for the valves it is $\lambda_{DU,V} = 3E-6$ Per hour. By inserting the values, we get PFD of the SIF equal to:

$$PFD_{SIF} = 7.67E-5 + 4.38E-4 + 2.30E-4 \approx 7.45E-4$$

The value of the PFD is within the SIL 2 level, as is explained in the following section.

8.9.5 Safety integrity level (SIL)

The purpose of calculating the PFD of SIF is to compare the result with the permitted range of the safety integrity level (SIL) requirement. SIL and its implications for the design of an SIF are explained in Chapter 9 on functional safety.

Functional safety standards define four Safety Integrity Levels (SILs), SIL 1 to SIL 4, each corresponding to a specific range of acceptable PFD and PFH values, as shown in Tab. 10. Here, PFH is the Probability of Dangerous Failure per Hour, or also referred to as the dangerous failure rate, a topic we will address later.

Tab. 10. SIL table in IEC 61508

SIL	Allowed failure probability (PFD) when low demand	Allowed failure rate of dangerous failures per hour (PFH) when high/continuous demand
4	1E-5 ≤ PFD < 1E-4	1E-9≤ PFH < 1E-8
3	1E-4 ≤ PFD < 1E-3	1E-8 ≤ PFH < 1E-7
2	1E-3 ≤ PFD < 1E-2	1E-7 ≤ PFH < 1E-6
1	1E-2 ≤ PFD < 1E-1	1E-6 ≤ PFH < 1E-5

These ranges were likely established by the international committee responsible for developing IEC 61508 (2010). While the exact rationale is not publicly documented, the following considerations likely influenced the definitions:

1. What is the lowest acceptable reliability for a safety function?

To be considered a safety function, the system must meet a minimum reliability threshold. This means:

- PFD must be no greater than 0.1 (or 1E-1), implying that, on average, no more than one dangerous failure is allowed per 10 demands.
- Alternatively, for continuous or high-demand modes, PFH must be no greater than 1E-5 per hour, which corresponds to approximately one dangerous failure every 10 years.

2. What is the highest reliability that can realistically be claimed?

There are practical limits to how reliable a system can be, even when designed for safety:

- It is generally not feasible to claim a PFD lower than 1E-5, meaning the system would fail dangerously less than once every 100,000 demands.

- In low-demand applications, it would also be difficult to collect sufficient statistical evidence to support such a low failure rate.

3. What are reasonable intervals between levels?

To provide a structured and scalable framework, each SIL level spans a range of reliability values that differ by a factor of 10. A logarithmic scale:

- Makes a clear differentiation between levels
- Recognizes uncertainty in data and assumptions (of a factor of 10)
- Range is narrower for lower SIL than higher SIL levels, relating to the max and min values of PFD and PFH

8.10 Inclusion of CCFs

A commonly used assumption in reliability analysis is that a device being part of a redundant (kooN) architecture can fail in one out of two ways:

1. Independently (of all other devices failing), or
2. Due to a CCF, where the device and at least one more device fail at the same time due to shared cause.

To model this behavior mathematically, we divide the total failure rate of a device into two parts, $\lambda^{(i)}$ as the independent failure rate and $\lambda^{(c)}$ as the CCF failure rate:

$$\lambda = \lambda^{(i)} + \lambda^{(c)}$$

One of the most widely used models for modeling the fraction of independent failures relative to the CCF ones is the standard beta factor model.

8.10.1 The standard beta factor model

The standard beta factor model introduces a parameter β as the proportion of failure rate where the device is involved in a CCF:

$$\lambda^{(i)} = (1-\beta)\lambda$$

$$\lambda^{(c)} = \beta\lambda$$

Where:

- λ is the total failure rate of the device
- β is the beta factor, representing the proportion of failures caused by a common cause

Consequently,

$$\lambda = (1-\beta)\lambda + \beta\lambda$$

We often focus on λ_{DU} failures, even if the same concept applies also to DD and safe failures, even if the corresponding values of β will be different. Typical values for β for DU failures range from 1% to 10%. While this may seem small, the impact of CCFs on system reliability can be significant, often exceeding the contribution from independent failures, especially in redundant systems.

To incorporate the standard beta factor model into an RBD, each subsystem with redundant devices is expanded to include a virtual “CCF block” (yellow), as shown in Fig. 35. This block represents a binary event:

- No CCF: the system behaves as expected
- CCF occurs: all redundant devices in the subsystem fail simultaneously

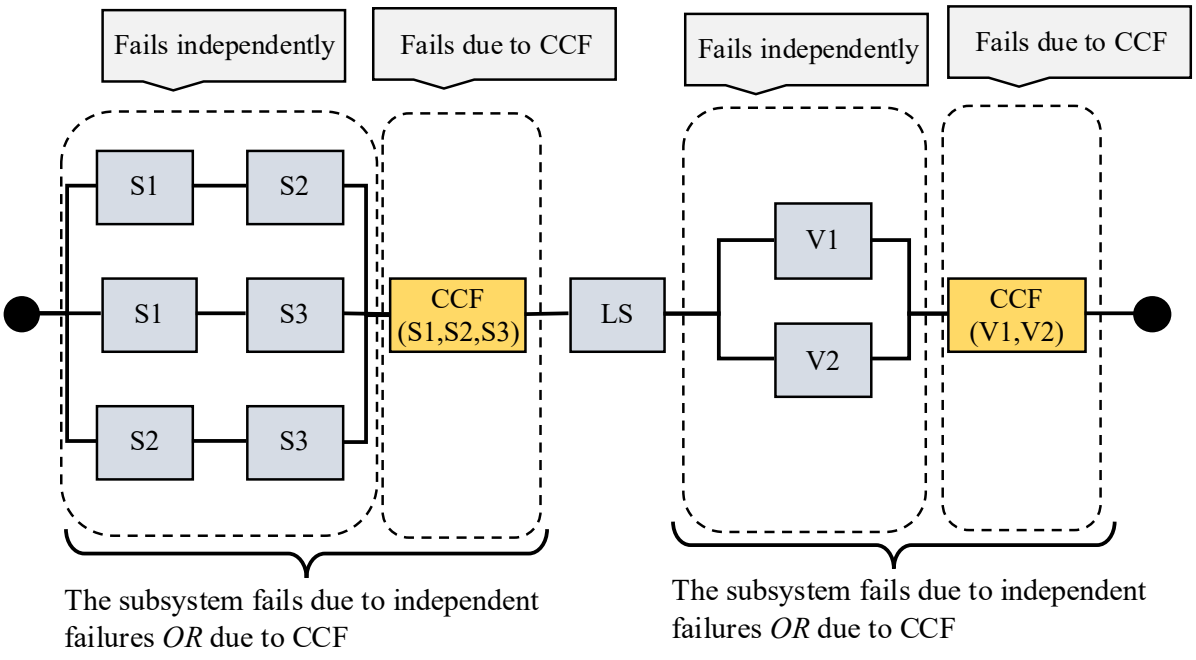


Fig. 35. RBD of a SIF with CCF

A fundamental assumption of the standard beta factor model is that all components of a subsystem are part of the CCF, though this is not always the case.

When calculating the PFD, we perform the following two steps for each subsystem with redundancy:

- The virtual CCF block is treated as a 1oo1 system with DU failure rate by β
- The independent DU failure rate is multiplied by (1-β)

For the RBD in Fig. 35, the total PFD becomes:

$$PFD_{SIF} = ((1-\beta_S)\lambda_{DU,S}\tau)^2 + \frac{\beta_S\lambda_{DU,S}\tau}{2} + \frac{\lambda_{DU,L}\tau}{2} + \frac{((1-\beta_V)\lambda_{DU,V}\tau)^2}{3} + \frac{\beta_V\lambda_{DU,V}\tau}{2}$$

Here, the PFD for the CCF parts is shown in red, and the modifications to the independent failure rate for the corresponding subsystems are shown in blue. We notice that the logic solver has no CCF contribution, as it is a single system.

Calculation example:

Assume that $\tau = 8760$ and that $\lambda_{DU,S} = 1E-6$ per hour, $\beta_S = 5\%$, $\lambda_{DU,L} = 1E-7$ per hour, and $\lambda_{DU,V} = 3E-6$ per hour, and $\beta_V = 10\%$.

Then:

$$PFD_{SIF} = [6.93E-5 + 2.19E-4] + 4.38E-4 + [1.86E-4 + 1.31E-3] = 2.22E-3$$

By incorporating CCFs into the PFD calculation, we observe that the total PFD approximately doubles compared to the value calculated without considering CCFs.

Despite this increase, the SIF remains within the SIL 2 range, meeting the required reliability criteria.

8.10.2 How do you decide on the value of beta?

The value of the beta factor (β), used to model the impact of CCFs, can often be found in a product's certification documents or in reliability data handbooks. These values are often determined or retrieved from the following sources:

- Reliability data handbooks
- Checklists

Reliability data handbooks:

It is not straightforward to determine the β-values, as CCFs are rare events. Therefore, the values are often based on a combination of qualitative analyses, including expert judgment from manufacturers and those with operational experience, and quantitative analyses of operational data.

This approach has been used for the data proposed in the PDS data handbook. A previous (draft) version of the PDS Data Handbook (2009), focusing on reliability data for typical SIS devices, proposed β-values as shown in Tab. 11.

Tab. 11 PDS data handbook values (based on draft version, 2009)

Component group	Component	β	Comment/source
Input devices	Pressure switch	0.06	Updated SINTEF estimates based on former values and additional knowledge from operational reviews.
	Proximity switch	0.06	
	Process transmitter	0.06	
	Fire/gas detectors	0.07	
	ESD push button	0.04	
Control logic units	Standard industrial PLC	0.07	SINTEF estimates are based on additional judgments.
	Programmable safety system	0.05	
	Hardwired safety system	0.03	
Final elements	ESV/XV incl. Xmas tree valves (main valve + actuator)	0.05	Updated SINTEF estimates based on former values and additional knowledge from operational reviews.
	HIPPS valve	0.05	
	Blowdown valves (main valve + actuator)	0.05	
	Pilot valves on same valve	0.10	
	Pilot valves on different valves	0.05	
	Control valves	0.05	
	Pressure relief valve, PSV	0.05	β value for (redundant) PSVs on the same equipment/vessel. For PSVs on different equipment, a value of 0.03 is suggested.
	Deluge valve	0.05	
	Fire damper	0.05	
	Relay	0.05	

Checklists:

Checklists serve as a useful alternative to data handbooks, especially for new or custom devices without existing operational data or field experience. Various checklists can be found in industry guidelines and standards; for example,

- EC 61508-6 (2010): Generic CCF checklist
- IEC 62061 (2021): Checklist targeting machinery systems and related protective devices

These checklists often involve a systematic evaluation of the applicable:

- Root causes of CCFs
- Coupling factors (e.g., environmental, design, or procedural similarities)

Tab. 12 shows an example of a checklist adopted from IEC 62061. The user evaluates to what extent the answer is yes or no for a series of structured questions. If yes, the suggested score applies, while no (or partially no) gives a score of 0. A relationship between the summed score and β values is proposed. A column has been added to the table to illustrate its application.

Tab. 12. CCF checklist (adopted from IEC 62061)

Item	Score	Yes/No
Separation/segregation		
Are SCS signal cables for individual channels routed separately from those for other channels at all positions? For example: • Signal cables for the individual channels are separate from other channels at all positions or sufficiently shielded (connected to protective earth) • Short circuit detection provided • Sufficient clearances and creepage distances on printed-circuit boards	5	5
Where information encoding/decoding is used, is it sufficient to detect signal transmission errors?	10	0
Are SCS signals and power cables/sources separate at all positions, or are they sufficiently shielded (i.e., no interference from any other electrical system to the SCS signals)?	5	5
If subsystem elements can contribute to a CCF, are they provided as physically separate devices in their local enclosures?	5	5
Diversity/redundancy		
Does the subsystem employ different technologies, for example, one electronic or programmable electronic and the other an electromechanical relay or a hydraulic valve?	8	0
Does the subsystem employ elements that use different physical principles (e.g. sensing elements at a guard door that use mechanical and magnetic sensing techniques)?	10	10
Does the subsystem employ elements with temporal differences in functional operation and/or failure modes?	10	0
Do the subsystem elements have a diagnostic test interval of ≤1 min?	10	10
Complexity/design/application		
Is cross-connection between channels of the subsystem prevented, except for diagnostic testing?	2	2

Assessment/analysis		
Has an analysis been conducted to identify sources of common-cause failure, and have predetermined sources of common-cause failure been eliminated by design? For example, over voltage, over temperature, over pressure etc.	9	**9**
Are field failures analyzed and fed back into the design?	9	**9**
Competence/training		
Do subsystem designers understand the causes and consequences of common-cause failures?	4	**4**
Environmental control		
Are the subsystem elements likely to always operate within the range of temperature, humidity, corrosion, dust, vibration, etc., over which they have been tested, without external environmental control?	9	**9**
Is the subsystem immune to adverse influences from electromagnetic interference?	9	**9**
	SUM:	**77**
From score to β-values:	β:	**2%**

Overall score	Common cause failure factor (β)
≤ 35	10 % (0,1)
36 to 65	5 % (0,05)
66 to 85	2 % (0,02)
86 to 100	1 % (0,01)

8.10.3 PDS method for inclusion of CCFs

As already mentioned, the standard beta factor model assumes that all redundant devices fail simultaneously in a CCF event. While this assumption is reasonable for systems with two devices, it becomes increasingly conservative for systems with three or more devices. In many cases, depending on what is the shared cause, it is more likely that a CCF may affect only a subset of the redundant devices, such as two out of three, rather than all of them.

To address this, the PDS method handbook (2013) has introduced an alternative to the standard beta factor model by applying a correction factor to β, denoted CMooN. This factor adjusts the contribution of CCFs based on the system's voting configuration.

- The PDS method uses the term MooN (equivalent to KooN) to describe voting architectures.
- The baseline is a 1oo2 system, for which $C_{MooN} = 1$.
- For other configurations (e.g., 2oo3, 1oo3), the model uses a multiple beta factor approach to reflect the likelihood of different CCF scenarios.

This approach assumes that in systems with more than two devices, CCFs can involve combinations of two or more devices, up to the total number of devices in the subsystem.

Example: Three-Device Sensor Subsystem: Consider a subsystem with three sensors: S1, S2, and S3. Possible CCF scenarios include:

- Double failures: (S1, S2), (S2, S3), (S1, S3)
- Tripple failure: (S1, S2, S3)

The system's vulnerability to CCFs depends on its voting logic:

- A 1oo3 system only fails if all three devices fail, making it less sensitive to CCFs.
- A 2oo3 system fails if any two or more devices fail, making it more vulnerable to CCFs.

The CMooN values provided in Tab. 13 reflect these differences and are used to scale the beta factor accordingly.

Tab. 13. C_{MooN} values (PDS method)

M/N	2	3	4	5	6
1	C_{1oo2}=1.0	C_{1oo3}=0.5	C_{1oo4}=0.3	C_{1oo5}=0.2	C_{1oo6}=0.15
2		C_{2oo3}=2.0	C_{2oo4}=1.1	C_{2oo5}=0.8	C_{2oo6}=0.6
3			C_{3oo4}=2.8	C_{3oo5}=1.6	C_{3oo6}=1.2
4				C_{4oo5}=3.6	C_{4oo6}=1.9
5					C_{5oo6}=4.5

When incorporating the CMooN factor into the Common Cause Failure (CCF) portion of the PFD formulas, a corresponding correction should ideally also be applied to the independent failure rate. However, unlike the simple (1−β) adjustment used in the standard beta factor model, this correction becomes mathematically complex in the PDS method.

To maintain practicality, the PDS method takes a pragmatic approach: it omits the correction factor for independent failures altogether. This simplification is justified because:

- The worst-case value of (1−β) is typically around 90%.
- Omitting the correction results in a slightly higher PFD, which is conservative and acceptable from a safety perspective.

The modified formula for PFD of the SIF becomes:

$$PFD_{SIF} = (\lambda_{DU,S}\tau)^2 + \frac{C_{2oo3}\beta_S\lambda_{DU,Ss}\tau}{2} + \frac{\lambda_{DU,L}\tau}{2} + \frac{(\lambda_{DU,V}\tau)^2}{3} + \frac{C_{1oo2}\beta_V\lambda_{DU,V}\tau}{2}$$

The result shows a slight increase in the total PFD, primarily due to the higher contribution from CCFs in the 2oo3 sensor subsystem.

Using the same data as earlier and the values of C_{MooN}, we get:

$$PFD_{SIF} = [7.67E-5 + 4.27E-4] + 4.38E-4 + [2.30E-4 + 1.31E-3] = 2.49E-3$$

The PFD of the SIF increases slightly due to the additional contribution from Common Cause Failures (CCFs) in the 2oo3 sensor subsystem.

8.10.4 Other contributors to PFD

While this discussion has focused on the primary contributors to the **PFD**, several additional factors can influence the total PFD of a SIF. These are briefly mentioned below:

Impact of Proof Test Coverage (PTC): In practice, regular proof tests—also referred to as function tests—may not detect all dangerous undetected (DU) failures. Several factors contribute to this limitation:

- Multiple Sub-Tests:
  A complete proof test may comprise several individual function tests. For example, in the case of valves:
  - A closure test may verify the valve's response time.
  - A leakage test may be conducted separately to ensure the valve remains tight in the closed position.

- Limitations Due to Test Conditions:
  Even when all sub-tests are performed, some faults may remain undetected because test conditions do not fully replicate real demand conditions. For instance:
  - While individual shutdown valves can be tested, it may not be feasible to simulate a simultaneous plant-wide shutdown.
  - As a result, the combined demand on shared systems—such as hydraulic or pneumatic actuators—is not tested, potentially masking failures that would only appear under full-load conditions.

These limitations highlight the importance of understanding PTC and recognizing that even well-designed tests may leave a portion of DU failures undetected.

- In such cases, the PFD formulas can be extended to include the impact of PTC. The PTC expresses the % of dangerous faults detected by the proof test and the remaining fraction that remains hidden til a renewal or replacement takes place.
- For example, with a PTC of 85% to 95%, the remaining 5–15% of DU failures would remain hidden until a full proof test is performed.

Impact of Partial Testing: Partial testing targets specific failure modes and can be performed more frequently than complete proof tests. This approach is beneficial for devices such as on/off valves, where complete testing may be disruptive to operations:

- For example, while a full closure test of a valve might require a complete process shutdown, a partial stroke test—such as moving the valve to 20% of its range—can be performed with minimal or no process disturbance.
- This type of test can detect certain dangerous undetected (DU) failure modes, such as a valve that fails to begin closing when demanded.

PFD formulas can be extended to account for the effects of partial testing:

- Partial tests reduce the PFD by identifying specific failure modes earlier, thereby shortening the average time a failure remains undetected.
- However, partial tests do not replace complete proof tests. They must be modeled separately in the reliability analysis to accurately reflect their limited coverage.

The effectiveness of partial testing is typically expressed through a Partial Test Coverage (PTC) factor, which quantifies the proportion of DU failures that the partial test can detect.

8.10.5 IEC 61508 formulas

IEC 61508 introduces a set of formulas derived from Markov analysis and related approximations. One key advantage of using Markov analysis is its ability to model a broader range of system states, including the impact of devices with detected dangerous (DD) failures.

The core strategy in IEC 61508 is to express the PFD as the average proportion of downtime at a given point in time, typically calculated over the first test interval. This approach applies to all subsystems, regardless of the voting configuration used.

The general formula used is:

$$PFD = \lambda_D \cdot t_{GE}$$

Here,

- λ_D is the total dangerous failure rate of the subsystem.
- t_{GE} is the mean average downtime associated with D failures.

Let's consider a 1oo1 (one-out-of-one) system. A failure in this configuration can result from either:

- A DD (Detected Dangerous) failure, or
- A DU (Undetected Dangerous) failure.

It is assumed that a single device cannot simultaneously experience both a DD and a DU failure.

- For DU failures, the system is unavailable on average for a fraction of time given by:

$$\frac{\tau}{2} + MRT$$

Here,

  - τ is the function test interval.
  - MRT is the mean repair time.

- For DD failures, the failure is detected immediately and restored within the Mean Time to Restoration (MTTR).

The t_{GE} is the weighted downtime caused by DU and DD failures, determined as:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Fig. 36 illustrates how the mentioned terms contribute to PFD using a reliability block diagram. Compared with previous PFD calculations, we now have a new contributor: the λDD failure rate. If this rate is set to zero, we are back to the formulas of PFD in Tab. 9.

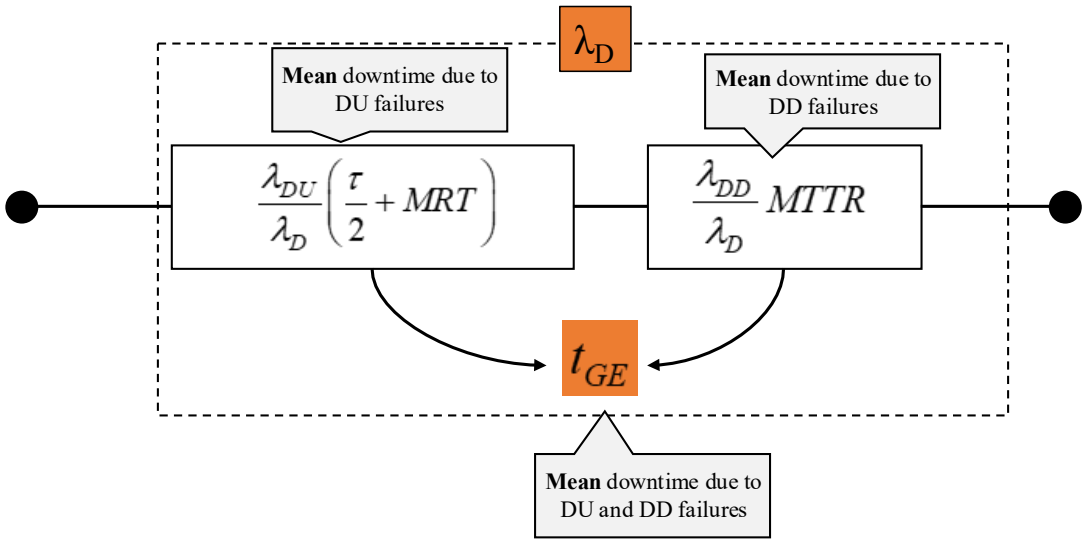


Fig. 36. A 1oo1 system (adopted from IEC 61508)

The PFD of a subsystem voted 1oo1 then becomes:

$$PFD^{1oo1} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Consider a single sensor that is tested once per year with $T_1 = 8760$ (hours). We assume that the DU failure rate is 1E-6/hour, and the DD failure rate is 3E-6/hour. We presume that MRT = MTTR = 8 hours, that is, a bit less than a working day or a shift. The PFD becomes:

$$\begin{aligned} PFD^{1oo1} &= \lambda_D \left[\frac{\lambda_{DU,S}}{\lambda_{D,S}} \left[\frac{T_1}{2} + MRT \right] + \frac{\lambda_{DD,S}}{\lambda_{D,S}} MTTR \right] \\ &= 4E-6\left[0.25 \cdot [4388] + 0.75 \cdot 8 \right] \\ &= 4.39E-3 + 2.4E-5 \\ &= 4.41E-3 \end{aligned}$$

If calculated using PFD formulas in Tab. 9, the PFD becomes 4.38E-3. As we see, the differences are negligible, but the calculation effort is larger. The main reason for the similarity in results is that the downtime from DD failures is insignificant compared to DU failures.

IEC 61508-6 offers formulas only for a limited set of voted configurations. However, the author and I have derived the KooN formulas shown in Tab. 14. Note that some notations might differ slightly from those used in IEC 61508.

Tab. 14. IEC 61508 formulas

Voting	IEC 61508 formula
1oo1	$PFD^{1oo1} = \lambda_D \cdot t_{CE}$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$
2oo2	$PFD^{2oo2} = 2\lambda_D t_{CE}$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$
1oo2	$PFD^{1oo2} = 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left[\frac{T_1}{2} + MRT\right]$ $t_{ce} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{3} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$
1oo3	$PFD^{1oo3} = 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^3 t_{CE} t_{GE1} t_{GE2} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left[\frac{T_1}{2} + MRT\right]$ $t_{ce} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE1} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{3} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE2} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{4} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$

2oo3	$PFD^{2oo3} = 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left[\frac{T_1}{2} + MRT\right]$ $t_{ce} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{3} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$
1oo4	$PFD^{1oo4} = 24[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^4 t_{CE} t_{GE1} t_{GE2} t_{GE3} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left[\frac{T_1}{2} + MRT\right]$ $t_{ce} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE1} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{3} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE2} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{4} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE2} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{5} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$
2oo4	$PFD^{2oo4} = 24[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^3 t_{CE} t_{GE1} t_{GE2} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left[\frac{T_1}{2} + MRT\right]$ $t_{ce} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE1} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{3} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE2} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{4} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$

Tab. 15 compares the results obtained using two different approaches:

- Simplified PFD formulas (from Tab. 9), which consider only *dangerous undetected (DU)* failures.
- IEC 61508 formulas (from Tab. 14) which also account for *dangerous detected (DD)* failures.

In this comparison, we assume the DD failure rate is 10 times that of the DU failure rate. However, the values for CCFs, with $\beta = \beta_D$ and the mean repair time (MRT = MTTR), are kept the same in both cases.

Tab. 15 Comparing results using formulas in Tab. 9 and Tab. 14

Parameter	Value	Denomination
λ_{DU}	1.00E-06	Per hour
λ_{DD}	1.00E-05	Per hour
Tau	8760	Hours
β	5 %	
MRT	8	Hours
MTTR	8	Hours
β_D	5 %	

	Independent failures only (no CCFs)		Independent failures and CCFs	
Voting	**PFD simplified formulas (Tab. 9)**	**PFD IEC 61508 formulas (Tab. 14)**	**PFD simplified formulas (Tab. 9)**	**PFD IEC 61508 formulas (Tab. 14)**
1oo1	4.38E-3	4.47E-3	4.38E-3	4.47E-3
1oo2	2.56E-5	2.69E-5	2.42E-4	2.45E-4
2oo3	7.67E-5	8.06E-5	2.88E-4	2.96E-4
1oo3	1.68E-7	1.84E-7	2.19E-4	2.24E-4
2oo4	6.72E-7	7.35E-7	2.20E-4	2.24E-4
1oo4	1.18E-9	1.35E-9	2.19E-4	2.23E-4

The comparison highlights that DU failures are the dominant contributors to the overall PFD, which makes the use of simplified formulas generally sufficient for most evaluations. Although the IEC 61508 formulas account for both DU and DD failures, the influence of DD failures is relatively minor in most configurations. This is particularly evident in non-redundant architectures, such as 1oo1, and when common cause failures (CCFs) are considered, where the results from both methods are very similar.

Even in redundant systems, simplified formulas offer a close approximation, making them a practical choice for quick assessments. However, in scenarios where DD failures have long restoration times, such as when access to the equipment is restricted, their impact becomes more significant and must be taken into consideration. For instance, equipment installed in subsea environments may require weeks or even months to retrieve and replace. Unless effective compensating measures are available, the contribution of DD failures cannot be omitted from the analysis.

8.11 PFH for high-demand SIFs

The probability of having a dangerous failure per hour (PFH) is a reliability measure applied in IEC 61508 (2010) and IEC 61511-1 (2016) for SIFs operating in the high-demand or continuous mode. It expresses the frequency of SIF failures due to dangerous failures, measured in units per hour. To what extent the SIF failure results in loss of safety of the plant it protects depends on whether the SIF is a last-in-line barrier or an intermediate one.

8.11.1 Simplified formulas

Rausand (2014) provides a good explanation for how the PFH formula is derived. In simple words, it is the average (or mean) number of dangerous failures estimated or experienced over an interval T measured in hours, i.e.,

$$PFH = \frac{E[N(T)]}{T} \quad (4)$$

Here, T is the interval for which PFH is calculated, and E[N(t)] is the expected number (N) of dangerous failures during T (measured in hours). There is no clear definition of how long T can be, but two requirements apply for the further development of the formula:

- The interval should not be so long that more than one dangerous failure of SIF is expected. A dangerous failure occurs if one of the subsystems voted kooN has experienced N-k+1 dangerous failures.
- At the end of the interval, it is expected that all dangerous failures are corrected, including the hidden (undetected) ones, so that the state of SIF is as good as new.

The further development of the formula relies on the following assumptions:

1. Subsystems comprise identical devices: The KooN system comprises identical or very similar devices with the same failure rates.

2. Failure process is HPP: With the assumption that all dangerous failures are restored to their original (as-good-as-new) state at regular intervals (T), the failure probability F(t) follows an exponential distribution. Consequently, the failure process is treated as a Homogeneous Poisson Process (HPP). F(T) can be derived by using rules for the failure function or the survival function of series and parallel structures. The most straightforward approach is to derive F(T) for each minimal cutset.
3. E(N(T)) can be replaced by F(T): If the length of T is decided so that no more than one dangerous failure of the koon system is expected, we may assume that:

$$E(N(T)) \approx \Pr(N(T) \le 1) = 0 \cdot \Pr(N(T) = 0) + 1 \cdot \Pr(N(T) = 1) = \Pr(t < T) = F(T)$$

4. Dangerous Detected (DD) failures can be excluded: While DD failures generally have a negligible impact on PFD, the situation is different for PFH. There may not be enough time to correct a DD failure before the next demand. DD failures can be excluded only if the SIF is forced to enter a safe state, even in the presence of DD faults. Otherwise, DD failures should be treated as Dangerous Undetected (DU) failures. IEC 61508 suggests formulas that include DD and DU failures for specific voted configurations.

The formula then becomes, having used the approximation that $1-e^{-\lambda_{DU}T} \approx \lambda_{DU}T$ when $\lambda_{DU} \cdot T \le 0.1$:

$$PFH^{koon} = \frac{F_{koon}(T)}{T} = \frac{\binom{n}{n-k+1}\left(\lambda_{DU}T\right)^{n-k+1}}{T} = \binom{n}{n-k+1}\lambda_{DU}^{n-k+1}T^{n-k} \quad (5)$$

CCFs are added in the same way as for low-demand systems, by adding a new functional block. The corresponding PFH formula becomes:

$$PFH^{koon} = \binom{n}{n-k+1}\left((1-\beta)\lambda_{DU}\right)^{n-k+1}T^{n-k} + \beta\lambda_{DU}$$

8.11.2 PFH formulas in IEC 61508

Appendix B3.3 in IEC 61508-6 (2010) provides formulas for calculating PFH that account for both DU and DD failures. Similar formulations are also presented in IEC 62061 (2021) , which is specific to machinery safety.

A future extension of this chapter may include a detailed presentation of these formulas along with a comparative analysis of results. However, under the common assumption that DD failures must cause the Safety Instrumented Function (SIF) to transition to a safe state, their contribution to the overall PFH is expected to be minimal.

8.12 Reliability data source

All failure rates and other reliability data calculated from statistical analyses are associated with uncertainty. An extensive statistical base, combined with a structured process for data quality assurance, may reduce uncertainty. Examples of questions to ask to evaluate sources of uncertainty are:

1. Is the assumption about constant failure rates reasonable?
2. Are the data sources relevant for your application domain?
3. Are data quite or otherwise not so applicable considering the type of equipment considered?
4. Are reliability data from manufacturers and field experience consistent, and what are the possible explanations?

We are addressing each of these questions below.

8.12.1 Is a constant failure rate reasonable?

Constant failure rates are often considered a reasonable assumption for electronic and programmable electronic systems, given their predictable behavior over time. However, electromechanical and mechanical systems are more susceptible to mechanical degradation and may experience an increasing failure rate when their useful life has ended.

Despite this, the PFD formulas often still assume a constant failure rate for these systems. Although devices may experience an increasing failure rate over time, we may consider it constant over a shorter observation period and repeat the analysis at regular intervals. In this way, the effects of degradation are indirectly accounted for by recognizing that the failure rate may increase from one observation period to the next. For regularly maintained systems, the failure rate can also decrease over time.

When failure rates are regularly updated using real-world operational data, degradation effects are inherently accounted for in the recalculated values.

A complete overhaul or replacement is assumed to be triggered when degradation becomes a dominant factor, meaning that the failure rate continues to increase despite maintenance efforts.

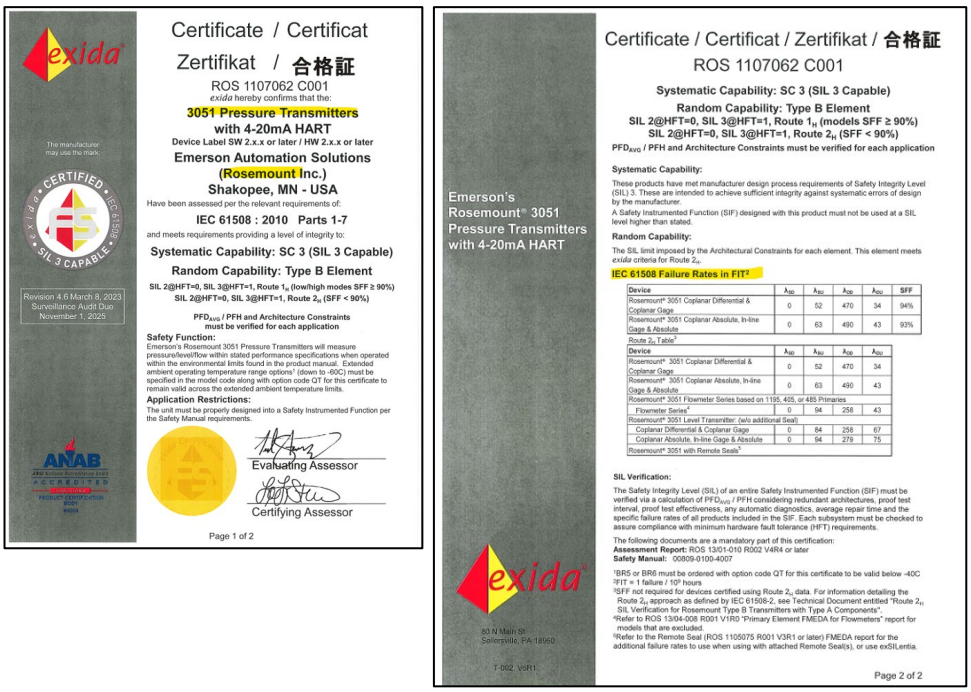

Certificate / Certificat
Zertifikat / 合格証
ROS 1107062 C001
exida hereby confirms that the:
3051 Pressure Transmitters
with 4-20mA HART
Device Label SW 2.x.x or later / HW 2.x.x or later
Emerson Automation Solutions
(Rosemount Inc.)
Shakopee, MN - USA
Have been assessed per the relevant requirements of:
IEC 61508 : 2010 Parts 1-7
and meets requirements providing a level of integrity to:
Systematic Capability: SC 3 (SIL 3 Capable)
Random Capability: Type B Element
SIL 2@HFT=0, SIL 3@HFT=1, Route 1H (low/high modes SFF ≥ 90%)
SIL 2@HFT=0, SIL 3@HFT=1, Route 2H (SFF < 90%)
PFDAVG / PFH and Architecture Constraints must be verified for each application
Safety Function:
Emerson's Rosemount 3051 Pressure Transmitters will measure pressure/level/flow within stated performance specifications when operated within the environmental limits found in the product manual. Extended ambient operating temperature range options[1] (down to -60C) must be specified in the model code along with option code QT for this certificate to remain valid across the extended ambient temperature limits.
Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.
Evaluating Assessor
Certifying Assessor
Page 1 of 2
Certificate / Certificat / Zertifikat / 合格証
ROS 1107062 C001
Systematic Capability: SC 3 (SIL 3 Capable)
Random Capability: Type B Element
SIL 2@HFT=0, SIL 3@HFT=1, Route 1H (models SFF ≥ 90%)
SIL 2@HFT=0, SIL 3@HFT=1, Route 2H (SFF < 90%)
PFDAVG / PFH and Architecture Constraints must be verified for each application
Emerson's Rosemount® 3051 Pressure Transmitters with 4-20mA HART
Systematic Capability:
These products have met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.
Random Capability:
The SIL limit imposed by the Architectural Constraints for each element. This element meets exida criteria for Route 2H.
IEC 61508 Failure Rates in FIT[2]
SIL Verification:
The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFDAVG / PFH considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.
The following documents are a mandatory part of this certification:
Assessment Report: ROS 13/01-010 R002 V4R4 or later
Safety Manual: 00809-0100-4007
[1]BR5 or BR6 must be ordered with option code QT for this certificate to be valid below -40C
[2]FIT = 1 failure / 10[9] hours
[3]SFF not required for devices certified using Route 2H data. For information detailing the Route 2H approach as defined by IEC 61508-2, see Technical Document entitled "Route 2H SIL Verification for Rosemount Type B Transmitters with Type A Components".
[4]Refer to ROS 13/04-008 R001 V1R0 "Primary Element FMEDA for Flowmeters" report for models that are excluded.
[5]Refer to the Remote Seal (ROS 1105075 R001 V3R1 or later) FMEDA report for the additional failure rates to use when using with attached Remote Seal(s), or use exSILentia.
Page 2 of 2

Fig. 37. Rosemount transmitter reliability data (Emerson)

8.12.2 What are the relevant data sources?

There are several recognized sources for obtaining reliability data, such as failure rates, CCF fractions like β, and diagnostic coverage (DC) values, all of which are essential for reliability and safety analyses:

1. Manufacturer data: Datasheets or certificates provided by equipment manufacturers. These often include failure rates based on internal testing or field experience.
2. Generic (industry) data sources: Generic data for typical devices and systems within an industry domain, incorporating operational experience. Examples include the PDS Data handbook, the Exida Safety Equipment Reliability Handbook, or the OREDA (Offshore Reliability Data).

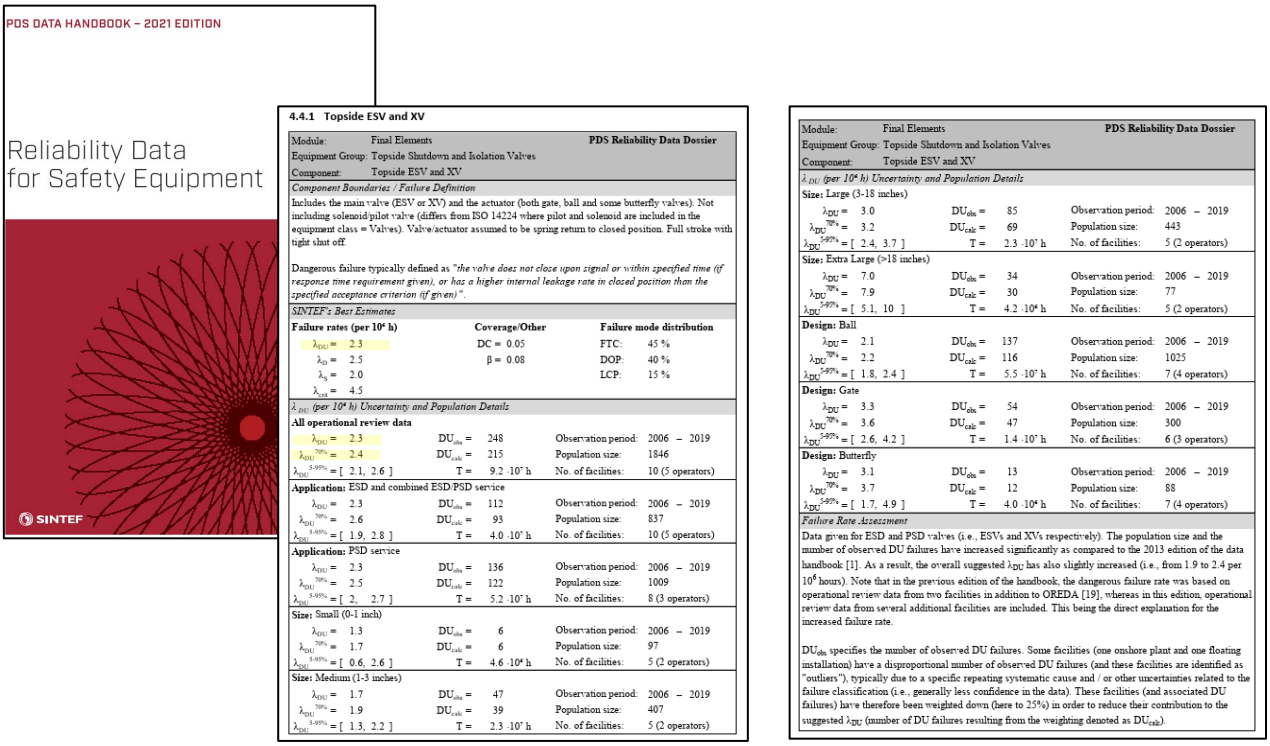
3. Failure analysis methods: Bottom-up analyses, such as FMECA (Failure Modes, Effects, and Criticality Analysis) or FMEDA (Failure Modes, Effects, and Diagnostic Analysis), or standards like MIL-HDBK-217F, can be used to estimate failure rates through component-level analysis.
4. Operational experience: Failure data collected from an organization's own operational experience or usage history. This is often the most relevant and accurate source for specific applications.

An example of reliability data provided by a manufacturer is shown in Fig. 37, with Emerson's product Rosemount 3051 pressure transmitter. The transmitter is certified for use in safety systems, and the failure rates are split into DU, DD, SU, and SD, as well as the safe failure fraction (SFF). The certificate indicates that different configurations and variants of the product may have varying failure rates. In addition, the unit of measure chosen is failure in time, which means the number of failures per billion hours FITs (1E-9 per hour).

Data handbooks provide reliability data not specific to a product type, but rather for a group of similar devices, such as level transmitters in general or those that employ a specific measurement principle. These values are typically derived from laboratory testing or by aggregating real-world operational data collected from multiple facilities within a specific industrial sector.

One such example is the PDS data handbook (2022) , also presented at https://pds-forum.com/pds-data-handbook. The handbook includes reliability data for devices typical of safety applications, derived from operational experience across several petroleum-sector companies. Fig. 38 illustrates how data is presented in a data dossier for a shutdown valve (named ESV and XV) used in topside (not subsea) offshore facilities. For example:

- A brief explanation of the data set, and what is meant by a dangerous failure.
- Failure rates are provided for dangerous and safe failures, including diagnostic coverage and β for CCFs.
- The distribution for dangerous failure modes
- Examples of sample sets (population, observation period, and applications) used as input


PDS DATA HANDBOOK – 2021 EDITION

Reliability Data for Safety Equipment

SINTEF

4.4.1 Topside ESV and XV

Module: Final Elements — PDS Reliability Data Dossier
Equipment Group: Topside Shutdown and Isolation Valves
Component: Topside ESV and XV

Component Boundaries / Failure Definition

Includes the main valve (ESV or XV) and the actuator (both gate, ball and some butterfly valves). Not including solenoid/pilot valve (differs from ISO 14224 where pilot and solenoid are included in the equipment class = Valves). Valve/actuator assumed to be spring return to closed position. Full stroke with tight shut off.

Dangerous failure typically defined as *"the valve does not close upon signal or within specified time (if response time requirement given), or has a higher internal leakage rate in closed position than the specified acceptance criterion (if given)"*.

SINTEF's Best Estimates

Failure rates (per 10^6 h)	Coverage/Other	Failure mode distribution
λ_{DU} = 2.3	DC = 0.05	FTC: 45 %
λ_D = 2.5	β = 0.08	DOP: 40 %
λ_S = 2.0		LCP: 15 %
λ_{crit} = 4.5		

λ_{DU} (per 10^6 h) Uncertainty and Population Details

All operational review data			
λ_{DU} = 2.3	DU_{obs} = 248	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ = 2.4	DU_{calc} = 215	Population size:	1846
$\lambda_{DU}^{5-95\%}$ = [2.1, 2.6]	T = 9.2 ·10⁷ h	No. of facilities:	10 (5 operators)
Application: ESD and combined ESD/PSD service			
λ_{DU} = 2.3	DU_{obs} = 112	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ = 2.6	DU_{calc} = 93	Population size:	837
$\lambda_{DU}^{5-95\%}$ = [1.9, 2.8]	T = 4.0 ·10⁷ h	No. of facilities:	10 (5 operators)
Application: PSD service			
λ_{DU} = 2.3	DU_{obs} = 136	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ = 2.5	DU_{calc} = 122	Population size:	1009
$\lambda_{DU}^{5-95\%}$ = [2, 2.7]	T = 5.2 ·10⁷ h	No. of facilities:	8 (3 operators)
Size: Small (0-1 inch)			
λ_{DU} = 1.3	DU_{obs} = 6	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ = 1.7	DU_{calc} = 6	Population size:	97
$\lambda_{DU}^{5-95\%}$ = [0.6, 2.6]	T = 4.6 ·10⁶ h	No. of facilities:	5 (2 operators)
Size: Medium (1-3 inches)			
λ_{DU} = 1.7	DU_{obs} = 47	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ = 1.9	DU_{calc} = 39	Population size:	407
$\lambda_{DU}^{5-95\%}$ = [1.3, 2.2]	T = 2.3 ·10⁷ h	No. of facilities:	5 (2 operators)

Module: Final Elements — PDS Reliability Data Dossier
Equipment Group: Topside Shutdown and Isolation Valves
Component: Topside ESV and XV

λ_{DU} (per 10^6 h) Uncertainty and Population Details

Size: Large (3-18 inches)			
λ_{DU} = 3.0	DU_{obs} = 85	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ = 3.2	DU_{calc} = 69	Population size:	443
$\lambda_{DU}^{5-95\%}$ = [2.4, 3.7]	T = 2.3 ·10⁷ h	No. of facilities:	5 (2 operators)
Size: Extra Large (>18 inches)			
λ_{DU} = 7.0	DU_{obs} = 34	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ = 7.9	DU_{calc} = 30	Population size:	77
$\lambda_{DU}^{5-95\%}$ = [5.1, 10]	T = 4.2 ·10⁶ h	No. of facilities:	5 (2 operators)
Design: Ball			
λ_{DU} = 2.1	DU_{obs} = 137	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ = 2.2	DU_{calc} = 116	Population size:	1025
$\lambda_{DU}^{5-95\%}$ = [1.8, 2.4]	T = 5.5 ·10⁷ h	No. of facilities:	7 (4 operators)
Design: Gate			
λ_{DU} = 3.3	DU_{obs} = 54	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ = 3.6	DU_{calc} = 47	Population size:	300
$\lambda_{DU}^{5-95\%}$ = [2.6, 4.2]	T = 1.4 ·10⁷ h	No. of facilities:	6 (3 operators)
Design: Butterfly			
λ_{DU} = 3.1	DU_{obs} = 13	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ = 3.7	DU_{calc} = 12	Population size:	88
$\lambda_{DU}^{5-95\%}$ = [1.7, 4.9]	T = 4.0 ·10⁶ h	No. of facilities:	7 (4 operators)

Failure Rate Assessment

Data given for ESD and PSD valves (i.e., ESVs and XVs respectively). The population size and the number of observed DU failures have increased significantly as compared to the 2013 edition of the data handbook [1]. As a result, the overall suggested λ_{DU} has also slightly increased (i.e., from 1.9 to 2.4 per 10^6 hours). Note that in the previous edition of the handbook, the dangerous failure rate was based on operational review data from two facilities in addition to OREDA [19], whereas in this edition, operational review data from several additional facilities are included. This being the direct explanation for the increased failure rate.

DU_{obs} specifies the number of observed DU failures. Some facilities (one onshore plant and one floating installation) have a disproportional number of observed DU failures (and these facilities are identified as "outliers"), typically due to a specific repeating systematic cause and / or other uncertainties related to the failure classification (i.e., generally less confidence in the data). These facilities (and associated DU failures) have therefore been weighted down (here to 25%) in order to reduce their contribution to the suggested λ_{DU} (number of DU failures resulting from the weighting denoted as DU_{calc}).

Fig. 38. Extract from the PDS reliability handbook (Open sample shown for shutdown valves)

The failure rate with the notation "crit" is the sum of dangerous failures and safety failures that lead to system downtime, and is a failure category also used by OREDA, the extensive database of reliability data in the petroleum sector, which is not limited to safety applications. For more information about OREDA, please visit https://oreda.com/.

Examples of other relevant data handbooks for devices and systems used in safety applications include those by Exida, a consultancy and certification body specializing in safety products. For more information, visit https://silsafedata.com/.

8.12.3 Data handbooks vs manufacturer data

Manufacturer data for a specific product and generic data for similar component types often differ, sometimes by factors of 10 to 100. For example, in Fig. 39, we notice that:

- The manufacturer suggests DU failure rates in the range from 32E-9/hour to 41E-9/hour (1 FIT = 1E-9/hour) for the pressure transmitter of type Rosemount 3051, which corresponds to 0.032E-6/hour to 0.041E-6/hour.
- The generic DU failure rate for pressure transmitters in the PDS data handbook, not specific to Rosemount, is 2.0E-6/hour for a generic (average) pressure transmitter.

The generic DU failure rate is 48 to 63 times higher than the manufacturer's suggested rate for their device. However, there are (good) reasons why they are different, and they therefore serve various purposes:

- Manufacturers' reliability data are based on internal analysis, testing, and some feedback. However, end-user feedback is often sparse and occurs after the guarantee period (which is often much shorter than the system's life).
- Manufacturers often exclude failures that relate to installation and usage.

The manufacturers' failure rates are therefore applicable when comparing products. At the same time, generic data may be more appropriate if the purpose is to determine the reliability to be expected in operation. Generic failure rates, combined with the user's own experience of failures, can be used to assess the system's reliability.

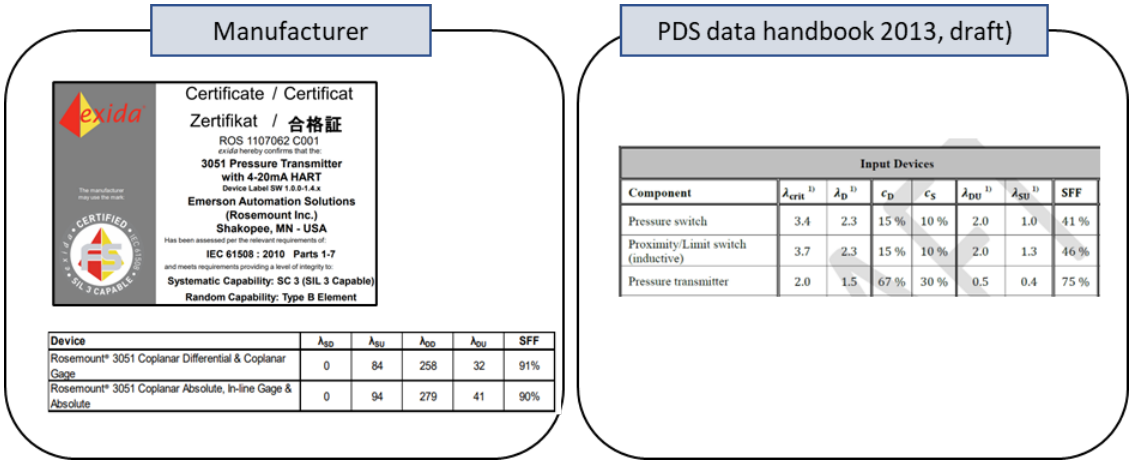


Fig. 39. Manufacturer vs PDS handbook data

The webpage by **FunctionalsafetyEngineer.com** has made a nice overview of many reliability data sources along with some discussion about which ones to use. See: https://functionalsafetyengineer.com/failure-data-rates-sis-sil/

8.13 Calculating updated failure rates using operational experience

There are generally two approaches to calculating failure rates from operational experience. We will refer to these approaches as the maximum-likelihood and Bayesian approaches, which are explained separately below. The starting point is that we have observed X DU failures (X_{DU}) over an observation period T for a group of N components, yielding an aggregated observation period of NT. When the time to a DU failure is assumed to be exponentially distributed (i.e., with a constant failure rate), the occurrence of failures follows a homogeneous Poisson process.

8.13.1.1 Maximum likelihood approach

The mean (or expected) occurrence of DU failures, which we refer to as the maximum likelihood value, when following a Homogeneous Poisson distribution, is:

$$\hat{\lambda}_{DU} = \frac{X_{DU}}{N \cdot T} \quad (6)$$

Along with this value, we may calculate the confidence interval:

$$\left[\frac{Z_{1-\varepsilon/2,2X_{DU}}}{2NT}, \frac{Z_{\varepsilon/2,2(X_{DU}+1)}}{2NT} \right]$$

Here, 1-ε is the confidence interval and $Z_{p,v}$ the surrogate number of the observed data within the Chi-square probability p and v degrees of freedom. If XDU = 0, the confidence interval is referred to as one-sided:

$$\left[0, \frac{Z_{\varepsilon/2,2(X_{DU}+1)}}{2NT} \right] \text{(one-sided upper bound)}$$

Standards, like IEC 61511 (part 1, section 11.5.9), instead suggest that failure rates used in SIL calculations are determined from the upper statistical confidence limit of at least 70%, rather than from the mean (maximum-likelihood) estimate. However, to avoid being overly conservative, the datasets must be sufficiently extensive and not limited to a single observation period. The 70% value is therefore more applicable when calculated for an aggregated dataset and used as input to generic data handbooks, as shown in Fig. 38.

8.13.1.2 **Bayesian approach:**

The core idea of the Bayesian approach is to combine prior knowledge of the DU failure rate (from design data or a previous operational period) with new observations, namely, the number of failures in the most recent period.

- A suitable distribution for the DU failure rate is the Gamma distribution with parameters α and β, i.e., $\Gamma(\alpha, \beta)$.
- When the new observations (occurrences of DU failures, i.e., X_{DU} over a period of NT) follow a Poisson process (i.e., the individual time-to-failure is exponentially distributed the posterior distribution remains Gamma-distributed, but now with parameters $\alpha + X_{DU}$ and $\beta + NT$, i.e., $\Gamma(\alpha + X_{DU}, \beta + NT)$. See, e.g., chapter 13 in Rausand and Høyland (2004) for further explanation.
- To determine parameters α and β of the prior distribution, we need to decide on a suitable mean and standard deviation because the following applies to the distribution:

$$E(\Lambda) = \frac{\alpha}{\beta}$$

$$Var = \frac{\alpha}{\beta^2} \text{ or } SD^2 = \frac{\alpha}{\beta^2}$$

25.

26. Here, we may assume that $E(\Lambda)$ is equal to a mean value suggested by the manufacturer or a data handbook, here denoted $\lambda_{DU,init}$. For the standard deviation, we may assume that we recognize that the proposed mean is subject to some uncertainty, expressed by a corresponding (worst-case) value $\lambda_{DU,cons}$. The choice of conservative failure DU failure rate can, for example, be a value calculated at 70% (one-sided) confidence, as suggested in IEC 61508-2 and IEC 61511-1, to compensate for uncertainty. The PDS data handbook includes, for example, both the 70% upper confidence value and the 90% confidence interval, along with the mean values. In the lack of conservative value estimates, it is proposed to use $2 \cdot \lambda_{DU,init}$. With $E(\Lambda) = \lambda_{DU,init}$ and $SD = \lambda_{DU,cons} - \lambda_{DU,init} = \sqrt{Var}$, we get the following prior values of α and β:

$$\beta = \frac{\lambda_{DU,init}}{\left(\lambda_{DU,cons} - \lambda_{DU,init}\right)^2}$$

$$\alpha = \beta \cdot \lambda_{DU,init}$$

Note that this β (of the Gamma distribution) has nothing to do with CCF's β.

- Then calculate the new updated DU failure rate using the values found for α and β and the information about the new failures that arrived during the aggregated period NT.

$$\hat{\lambda}_{DU} = \frac{\alpha + X_{DU}}{\beta + \mathrm{N} \cdot T} \quad (7)$$

An uncertainty bound can also be calculated for the Bayesian estimate for the failure rate, but in this case the name credibility interval is used instead of confidence interval.

Example:
Assume that a 1 DU fault has been found within an equipment group with 35 on/off valves over a period of 3 years. One year equals 8760 hours. We will now apply and compare the two approaches for updating the DU failure rate.

Approach: Maximum likelihood estimate

We can then calculate the following failure rate based on the formula, where only faults reported in the observation period is used:

$$\hat{\lambda}_{DU} = \frac{x_{DU}}{\mathrm{N} \cdot T} = \frac{1}{35 \cdot 3 \cdot 8760} \approx 1.1E-6 \text{ (per hour)}$$

If the upper bound value with 70% confidence level is chosen as an alternative to the mean value, as suggested in e.g., IEC 61511, the chosen value becomes:

$$\frac{Z_{30\%/2,2(1+1)}}{2 \cdot 35 \cdot 3 \cdot 8760} = 3.67\text{E-6 (per hour)}$$

However, the 70% upper bound is typically calculated when merging larger value sets rather than for a single period. For such a small sample set, it would be overly conservative, potentially leading to more frequent function testing than needed.

Note: The Excel function CHISQ.INV.RT has been used to calculate Z-values.

Approach: Bayesian update

With this approach, we need to determine the prior values of the Gamma distribution (α,β). For this purpose, we need to determine an initially assumed (or previously applied from a previous observation period) DU failure rate, along with our confidence in this value, expressed as a worst-case (conservative) estimate. Here, we suggest using a manufacturer failure rate, λDU, init = 2.0E-6 failures/hour, and a generic failure rate from a data handbook as the (more) conservative failure rate, λDU, cons = 3.0E-6 failures/hour. This gives:

$$\beta = \frac{2.0E-6}{\left(3.0E-6-2.0E-6\right)^2} \approx 2.0E6 \text{ (hours)}$$

$$\alpha = 2.0E6 \cdot 2.0E-6 \approx 4 \text{ (faults)}$$

Combined with the new data, the estimated failure rate becomes:

$$\hat{\lambda}_{DU} = \frac{4 + x_{DU}}{2.47E6+\mathrm{N} \cdot T} = \frac{4+1}{2.0E6 + 35 \cdot 3 \cdot 8760} \approx 1.71E-6 \text{ (per hour)}$$

The Bayesian failure rate is slightly higher than the failure rate estimated from observations in the period alone. This is reasonable since the manufacturer also suggested a higher failure rate than 1.1E-6 per hour.

The updated DU failure rate is an important input to PFD recalculations during the operational phase. If the PFD exceeds the permitted PFD value (PFD requirement) or the SIL requirement, it is necessary to reduce the regular test interval. Likewise, an extension of the regular test interval may be permitted if the updated PFD is below the required level.

The SINTEF guideline by Håbrekke et al. (2023) provides more insights into SIL follow-up activities, including various strategies for updating the failure rates.

8.14 Bibliography

Fussell, J. B., & Vesely, W. E. (1972). A new methodology for obtaining cut sets for fault trees. *Trans. Amer. Nucl. Soc*, *15*, 262–263.

Goble, W. M., & Brombacher, A. C. (1999). Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems. *Reliability Engineering & System Safety*, *66*(2), 145–148.

Håbrekke, S., Hauge, S., & Lundteigen, M. A. (2023). *Guideline for follow-up of safety instrumented systems (SIS) in the operational phase. An APOS project report*. SINTEF.

IEC 60812. (2018). *Failure modes and effects analysis (FMEA and FMECA)*. International Electrotechnical Commission.

IEC 61508. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems (Seven parts)*. International Electrotechnical Commission.

IEC 61508-2. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety related systems*. International Electrotechnical Commission.

IEC 61508-4. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*. International Electrotechnical Commission.

IEC 61508-6. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3* International Electrotechnical Commission.

IEC 61511-1. (2016). *Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements*. International Electrotechnical Commission.

IEC 62061. (2021). *Safety of machinery - Functional safety of safety-related control systems*. International Electrotechnical Commission.

IEC glossary. *IEC Electropedia: The World's Online Electrotechnical Vocabulary (webpage)*. International Electrotechnical Commission. Retrieved 15.05.24 from https://www.electropedia.org/

ISO TR 12489. (2013). *Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems*. International Organization for Standardization.

Leveson, N., & Thomas, J. (2018). *STPA handbook*. COPYRIGHT © 2018 BY NANCY LEVESON AND JOHN THOMAS.

PDS data handbook. (2022). *Reliability Data for Safety Equipment*. SINTEF.

PDS method handbook. (2013). *PDS Method Handbook: Reliability Prediction Method for Safety Instrumented Systems*. SINTEF.

Rausand, M. (2014). *Reliability of Safety-Critical Systems: Theory and Applications*. Wiley.

Rausand, M., & Høyland, A. (2004). *System Reliability Theory – Models, Statistical Methods, and Applications*. Wiley.