Chapter 3.
Failures and Failure Classification

Mary Ann Lundteigen Marvin Rausand

RAMS Group
Department of Mechanical and Industrial Engineering
NTNU

(Version 0.1)

NTNU – Trondheim
Norwegian University of
Science and Technology

Learning Objectives

The main learning objectives associated with these slides are to:

- To become familiar with key terms and concepts related to failures and failure classification
- To become familiar with different ways of failure classification strategies, using the following sources as basis:
  - IEC 61508 (and IEC 61511)
  - The PDS method
  - OREDA
- To become aware of some typical SIS related failures

The slides include topics from Chapter 3 in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

Outline of Presentation

Definition of Failure

☞ Failure: The termination of the ability of an item to perform a required function. [IEV 191-04-01]

A failure is always related to a required function. The function is often specified together with a performance requirement.[1]
A failure occurs when the function cannot be performed or has a performance that falls outside the performance requirement.

Shutdown valve

According to the performance requirement, the maximum closing time of a shutdown valve shall be no longer than 15 seconds. A failure of the closing function occurs when the closing time exceeds 15 seconds.

[1] Also called a functional requirement

Failure Attributes

A failure is an event that occurs at a specific point in time.

A failure may:

- Develop gradually
- Occur as a sudden event

The failure may sometimes be revealed:

- On demand (i.e., when the function is needed) (“hidden”)
- During a functional test (also “hidden”)
- By monitoring or diagnostics (“evident”)

Fault

☞ Fault: The state of an item characterized by inability to perform a required function [IEV 191-05-01]

While a failure is an event that occurs at a specific point in time, a fault is a state that will last for a shorter or longer period.

When a failure occurs, the item enters the failed state. A failure may occur:

- While running
- While in standby
- Due to demand

Error

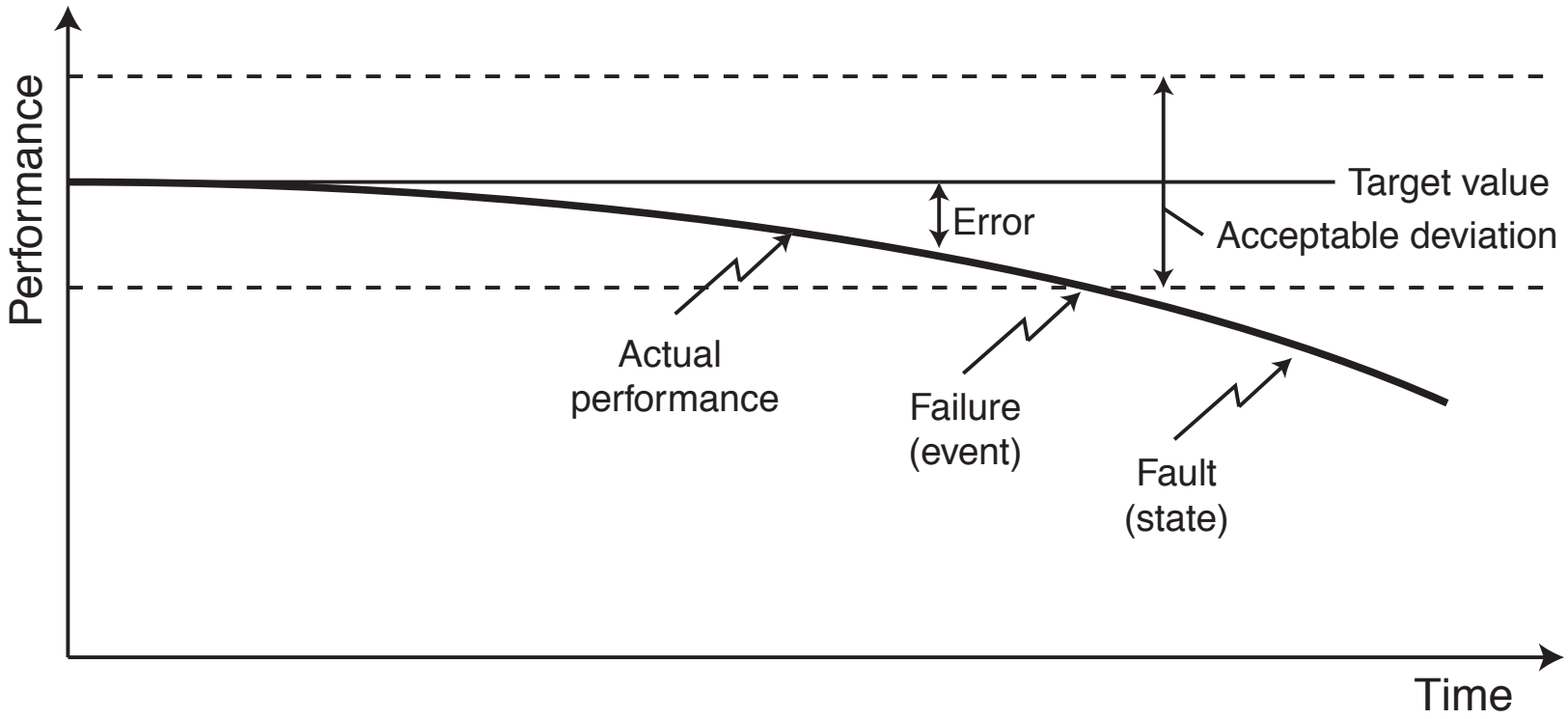
☞ Error: Discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.

[IEC 191-05-24].

An error is present when the performance of a function deviates from the target performance (i.e., the theoretically correct performance), but still satisfies the performance requirement. An error will often, but not always, develop into a failure.

Relationship Failure, Fault and Error

A failure may originate from an error. When the failure occurs, the item enters a fault state.



Failure Mode

☞ Failure mode: The way a failure is observed on a failed item. [IEC 191-05-22]

A failure mode is the way in which an item could fail to perform its required function. An item can fail in many different ways – a failure mode is a description of a possible state of the item after it has failed.

Pump

Performance requirement: The pump must provide an output between 100 and 110 liters per minute.
Associated failure modes may be:

- No output
- Too low output
- Too high output
- Too much fluctuation in output

Failure Mode Attributes

Some selected attributes of failure modes:

- A failure mode can have a significant or an insignificant impact on the performance of the component
- A failure mode is a description of how the failure is observed. However, many data sources classify failure causes as failure modes.

How to Classify Failures

Failures may be classified according to their:

- Causes: To avoid future occurrences and make judgments about repair
- Effects: To rank between critical and not so critical failures
- Detectability: To distinguish failures that may be revealed "automatically" (and shortly after their occurrence) and those that may be hidden until special effort is taken, such as proof tests.
- And several other criteria.

Special category:

- Common-cause failures (CCFs)

Failure Classification in IEC 61508

IEC 61508 classify failures according to their:

- Causes:
  - Random (hardware) faults
  - Systematic faults (including software faults)
- Effects:
  - Safe failures
  - Dangerous failures
- Detectability:
  - Detected - revealed by online diagnostics
  - Undetected - revealed by functional tests or upon a real demand for activation

Random Hardware Failures (Faults)

☞ Random hardware failure: Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware. [IEC 61508]

Random hardware failures may be characterized by a failure rate that is either:

- Constant, meaning that the component is in its useful life where impact of aging is negligible
- Non-constant, meaning that the component is subject in the burn-in phase of wear-out phase

Systematic Failures (Faults)

☞ Systematic failure: Failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors[IEC 61508]

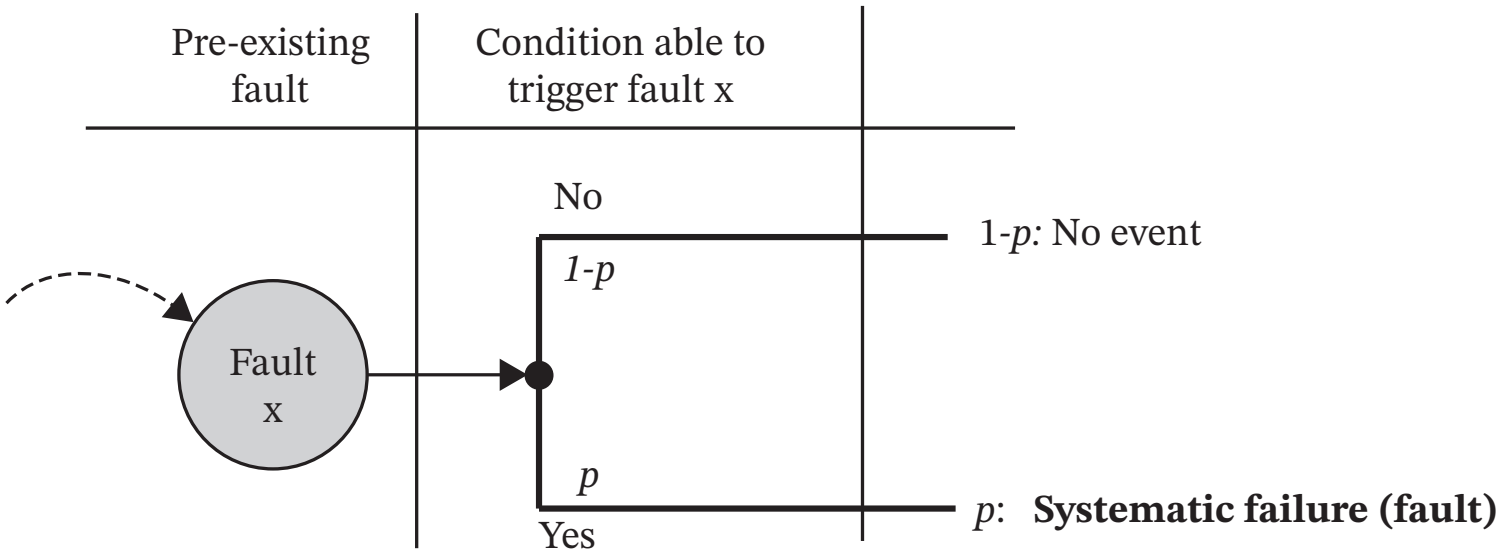
Systematic faults (non-physical causes):

- Systematic fault will always be repeated when triggering condition is available
- Systematic faults may be introduced in any lifecycle phase
- If properly corrected, the failure will in theory never re-appear

Systematic Failures (Faults)

The concept of systematic faults can be difficult to comprehend.

ISO TR 12489 has suggested useful illustration of what is a systematic failure:



Adapted from ISO TR 12489

Systematic Failures (Faults)

The illustration indicates that:

- It is necessary that an error or mistake has been made by someone. This could occur in any lifecycle phase.
- Once introduced, it remains there often undiscovered
- The mistake is NOT sufficient to cause a failure of the item, but triggers a fault of the item upon certain conditions
- The systematic fault will persistently occur as long as this condition *is* present and the mistake or error has not been corrected
- Even if a system has been found to be free of systematic faults under some conditions, it may have systematic faults under other conditions
- Most systematic faults are deterministic events. However, if the occurrence of the triggering condition is random, it is possible to also argue that the occurence of systematic faults is random

Safe Failure

IEC 61508 defines a safe failure as follows:

☞ Safe failure: Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or

b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.

A safe failure can result in loss of production or service, but not the loss of safety.

Dangerous Failure

IEC 61508 defines a dangerous failure as follows:

☞ Dangerous failure: Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or

b) decreases the probability that the safety function operates correctly when required

A dangerous failure may result in loss of safety.

Detected and Undetected Faults

IEC 61508 distinguishes between detected and undetected failures. The most precise definition is, however, identified in ISO TR 12489:

- Detected: Failure which is immediately evident to operation and maintenance personnel as soon as it occurs. A typical example is failures reported as diagnostic faults or alarms.

- Undetected: Failure which is not immediately evident to operations and maintenance personnel. A typical example is a failure that is hidden until the component is asked to carry out its function.

Detected and Undetected Faults

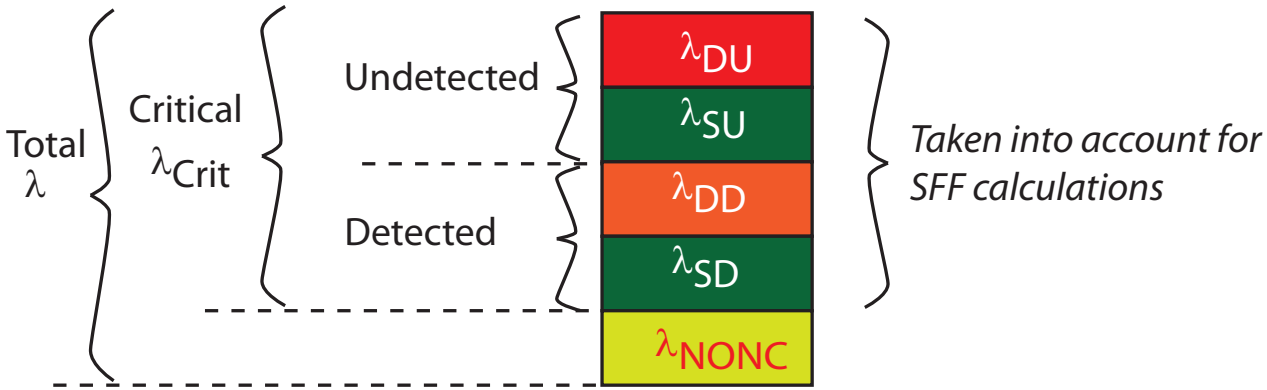
The classification of detected and undetected is used with safe and dangerous failures. Some examples include:

- Safe undetected (SU): A spurious (untimely) activation of a component when not demanded
- Safe detected (SD): A non-critical alarm raised by the component
- Dangerous detected (DD): A critical diagnostic alarm reported by the component, which will, as long as it is not corrected prevent the safety function from being executed
- Dangerous undetected (DU): A critical dangerous failure which is not reported and remains hidden until the next test or demanded activation of the safety function

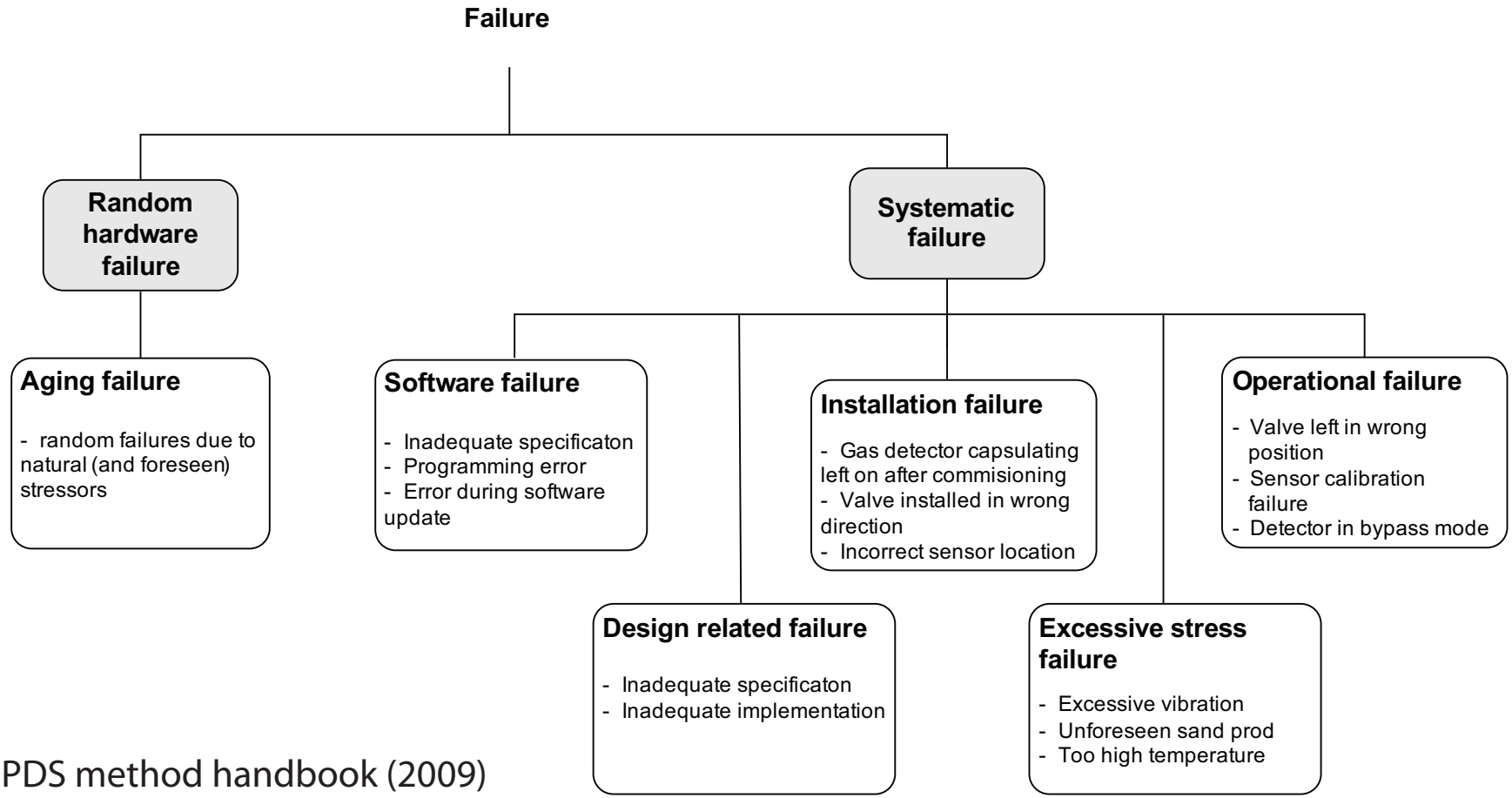
Failure Classification in PDS Method

The PDS method (www.sintef.no/pds) distinguishes between:

- Critical failures
  - Dangerous failures: detected and undetected
  - Safe detected and safe undetected (spurious) failures
- Non-critical failures



Failure Classification in PDS Method



Source: PDS method handbook (2009)

Examples of Systematic Faults as Defined by PDS Method

Systematic faults may be:

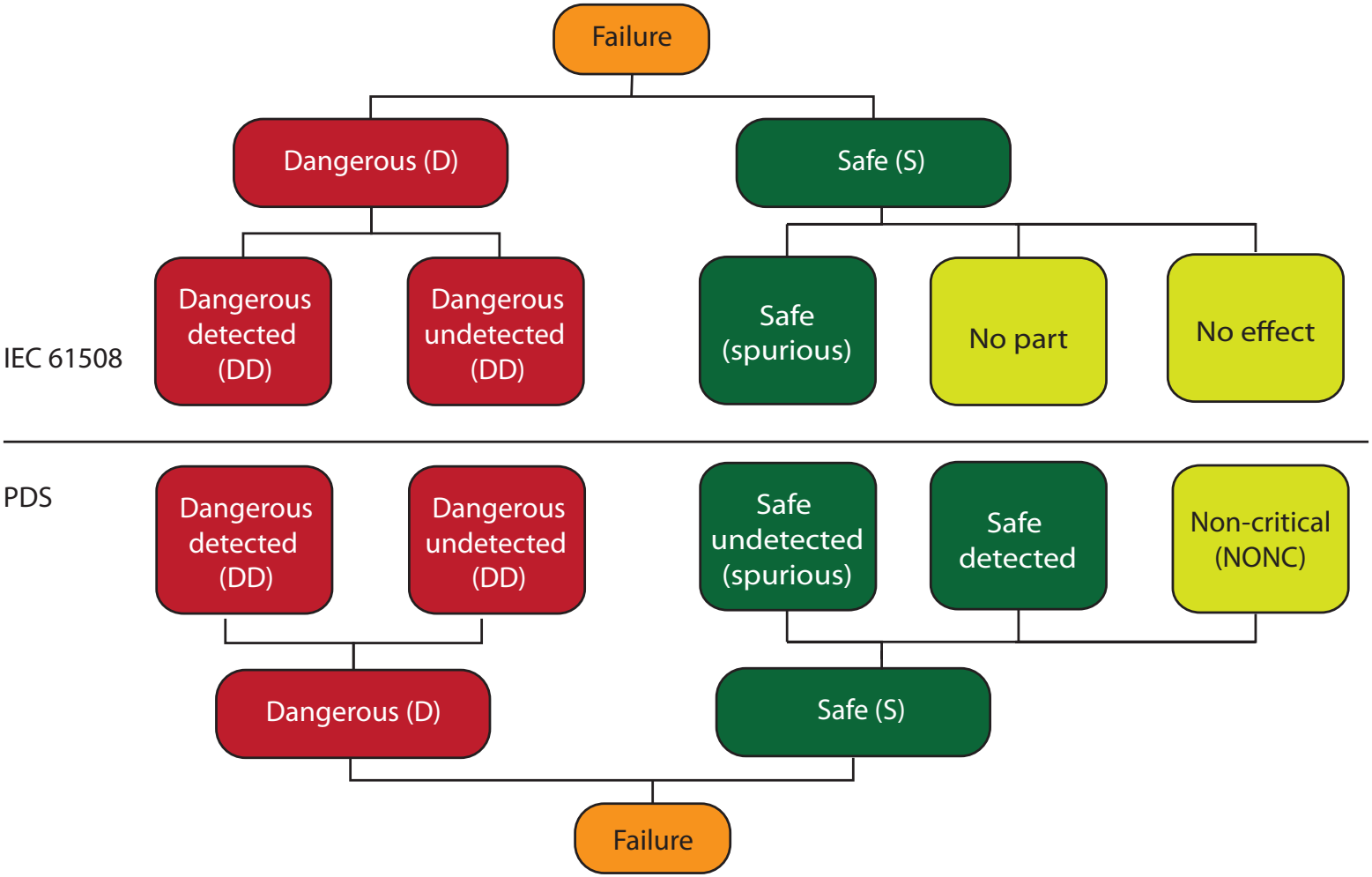
- Software faults:
  Programming errors, compilation errors, inadequate testing, unforeseen application conditions, change of system parameters, etc.
- Design related faults:
  Faults (other than software faults) introduced during the design phase of the equipment. It may be a fault in the system specification itself, a fault in the manufacturing process and/or in the quality assurance of the item.
- Installation faults:
  Faults introduced during the last phases prior to operation, i.e., during installation or commissioning. If detected, such faults are typically removed during the first months of operation and such faults are therefore often excluded from data bases.

Examples of Systematic Faults

Systematic faults may be (continued):

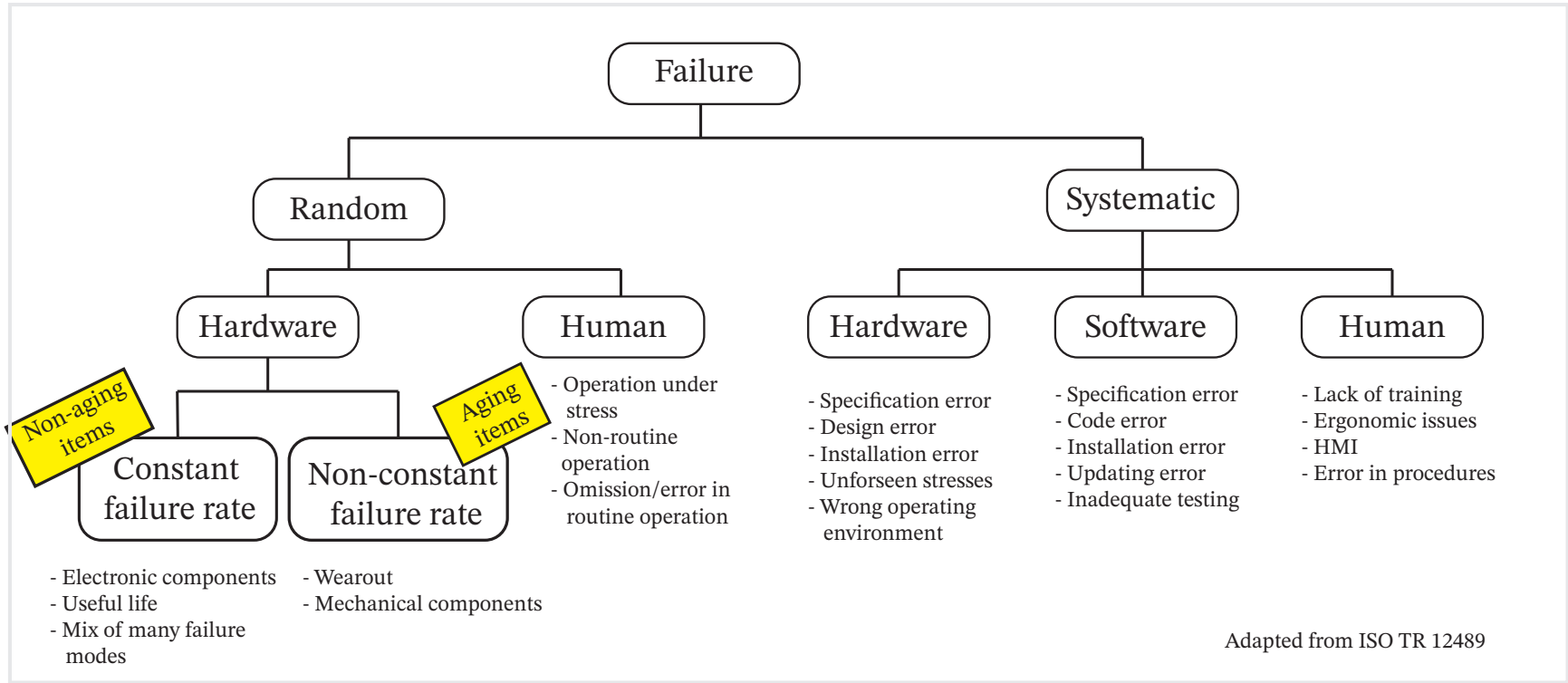
- Excessive stress:
  Failures that occur from stresses beyond the design specification are placed upon the component. The excessive stresses may be caused either by external causes or by internal influences from the medium.
- Operational errors:
  Initiated by human errors during operation or maintenance/testing

PDS method vs. in IEC 61508



Failure Classification in ISO TR 12849

ISO TR 12489 adds to the category random failures, to capture that some systematic faults (induced by human errors) can be regarded as random.



Other Classification in Oil and Gas Sector

OREDA data handbooks, and the most important standard on failure classification in oil and gas industry, ISO 12224, classifies failures according to:

- Critical failure:
  A failure of an item that causes immediate cessation of its ability to perform a required function. In this case, "its ability" comprises two elements:
  - Loss of ability to function on demand (safety-related)
  - Loss of ability to maintain production (production-availability related)

  This means that critical failures usually include what IEC 61508 defines as DU, DD, and SU failures.
- Degraded failure:
  A partial failure where the item has a degraded performance, but is still able to perform i's essential functions
- Incipient failure:
  Also a partial failure, but its degradation is barely noticable and can be regarded as a very early symptom of a degradation under development

Common Cause Failures (CCFs)

A common cause failure (CCF) is of particular interest and concern for safety-critical systems, since it may violate the effects of redundancy.

IEC 61508 defines a CCF as follows:

☞ CCF: Failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure

A CCF is a sub-category of dependent failures. The category of dependent failures include CCFs as well as cascading failures.

A replicated systematic failure will under similar (triggering) conditions result in a CCF. Defending against systematic faults is therefore an efficient way to defend against CCFs also.

What Failures to Include in Failure Rates

Manufacturers' perspective:

- Failure rates reported by manufacturers include primarily the effects of random hardware failures assuming that the items are in their useful life period. They can argue that their systems are free from systematic faults by having applied measures to prevent, detect, and correct relevant tools, methods, and procedures.

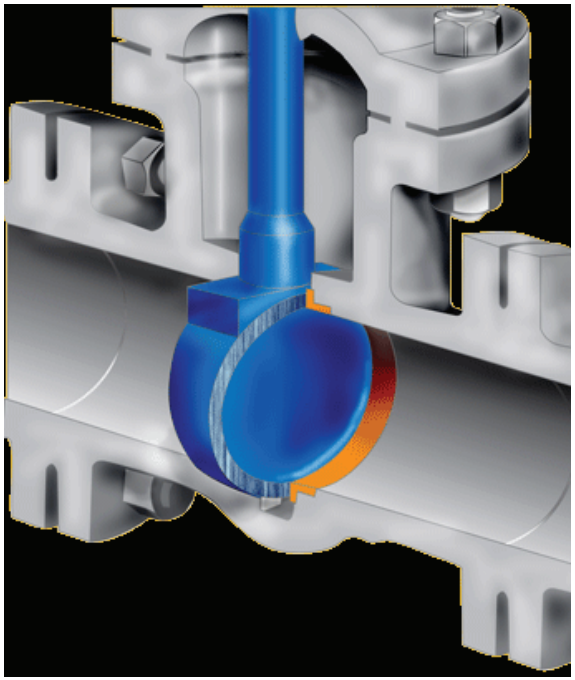
End users' perspective:

- Failure rates experienced by end user include a mixture of failures:
  - Some are random hardware failures from the useful life period
  - Some are random hardware failures in the wear-out life period
  - Some are systematic failures occurring only once (because they are properly corrected)
  - Some are systematic failures re-occurring (because they have NOT been properly corrected)

In practice, we find that:

- Failure rates experienced operation is often higher than what manufacturers suggest
- Failure rates are often calculated under the assumption of constant failure rate, even if this assumption is not (fully) true

Example: Failure Classification According to IEC 61508



www.franklinvalve.com

Typical failure mode	Classification
Fail to close (FTC)	DU
Leakage in closed position (LCP)	DU
Premature (spurious) closure (PC)	SU
Fail to open (FTO)	SU
Leakage to environment (LTE)	SD

Remark: Valves have usually limited diagnostic features, as opposed to sensors/transmitters and logic solvers.

FMEDA - a variant of FMECA

An *Failure modes, Effects, and Diagnostic Analysis* (FMEDA) is an extension of an FMECA that is tailored-made for a SIS.

- FMEDA as a method was developed by the company Exida
- Is in principle, very similar to an FMECA, and a FMECA-like table is used
- Focus is placed on (and columns in the table are allocated to) the classification of each failure mode into DU, DD, SU or SD
- Failiure rates can be estimated for each failure category with basis in the classification and the overall failure rate of the item
- Also proof test coverage may be considered
- The approach can supplement manufacturers calculations of failure rates, and specific measures like the safe failure fraction (SFF) and diagnostic coverage factor (DC)

More information is available from the book “Safety instrumented systems verification”, by William M. Goble and Harry Cheddie.

The FMEDA Process

A description to follow soon.

FMEDA Example

Table 1
FMEDA (failure modes, effects and diagnostic analysis) for high diagnostic PLC AC input circuit (failure per billion hours)

1 Name	2 Code	3 Function	4 Mode	5 Cause	6 Effect	7 Criticallty λ	8	9 Remarks	10 Det.	11 Diagnostics	12 Mode	13 SD	14 SU	15 DD	16 DU
R1-10K	4555-10	Input	Short		Threshold shift	Safe	0.125		0		1	0	0.13	0	0
		Threshold	Open	solder open	Open circuit	Safe	0.5		1	Lose input pulse	1	0.5	0	0	0
			Drift low			Safe	0.01	none until too low	0		1	0	0.01	0	0
			Drift high			Safe	0.01	none until too high	1	Lose input pulse	1	0.01	0	0	0
R2100K	4555-100	Current limit	Short		Short input	Safe	0.125		1		1	0.13	0	0	0
			Open	solder open		Safe	0.5		1	loss input pulse		0	0	0.5	0
			Drift low			Safe	0.01	none until too low	0		1	0	0.01	0	0
			Drift high			Safe	0.01	none until too high	1	Lose input pulse	1	0.01	0	0	0
D1	4200-7	Voltage drop	Short	surge	Over voltage	Safe	2		1	Lose input pulse	1	2	0	0	0
			Open		Open circuit	Safe	5		1	Lose input pulse	1	5	0	0	0
D2	4200-7	Voltage drop	Short	surge	Overvoltage	Safe	2		1	Lose input pulse	1	2	0	0	0
			Open		Open circuit	Safe	5		1	Lose input pulse	1	5	0	0	0
OC1	4805-25	Isolate	led dim	wear	No light	Safe	28		1	Comp. mismatch	1	28	0	0	0
			Tran. Short	internal short	Read logic 1	Dang.	10		1	Comp. mismatch	0	0	0	10	0
			Tran. Open		Read logic 0	Safe	3		1	Comp. mismatch	1	6	0	0	0
OC2	4805-25	Isolate	led dim	wear	No light	Safe	28		1	Comp. mismatch	1	28	0	0	0
			Tran. Short	internal short	Read logic 1	Dang.	10		1	Comp. mismatch	0	0	0	10	0
			Tran. Open		Read logic 0	Safe	6		1	Comp. mismatch	1	6	0	0	0
OC1/OC2			Cross	channel short	Same signal	Dang.	0.01		0		0	0	0	0	0.01
R3-100K	4555-100	Filter	Short		Lose filter	Safe	0.125			0	1	0	0.13	0	0

W.M. Goble, A.C. Brombacher / Reliability Engineering a

Reference: Goble, W.M. and Brombacher, A. Using a failure modes, effects and diagnosis analysis (FMEDA) to mesure diagnostic coverage in programmable electronic systems. DOI:10.1016/S0951-8320(99)00031-9 (Journal of Reliability Engineering and System Safety)

The failure rates (SD, SU, DD, and DU are summarized for all failure modes.