Chapter 10
Reliability of Safety Systems

Marvin Rausand
marvin.rausand@ntnu.no

RAMS Group
Department of Production and Quality Engineering
NTNU

(Version 0.1)

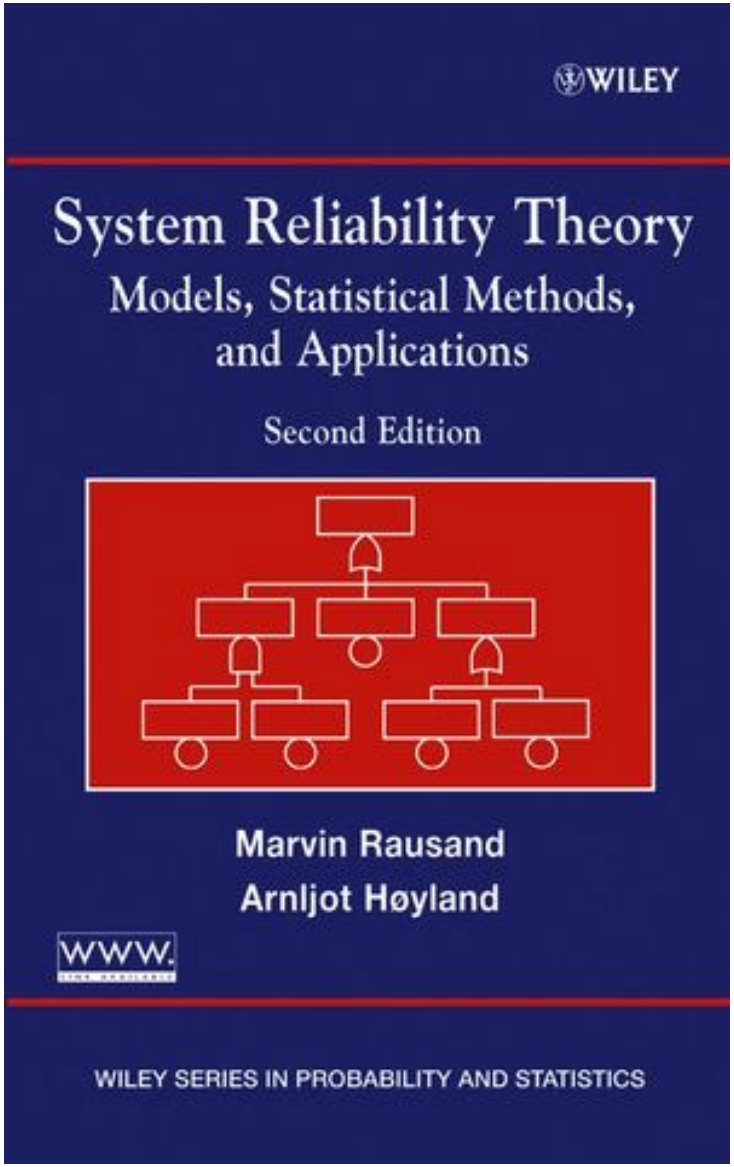
NTNU – Trondheim
Norwegian University of
Science and Technology

Slides related to the book

System Reliability Theory
Models, Statistical Methods, and Applications

Wiley, 2004

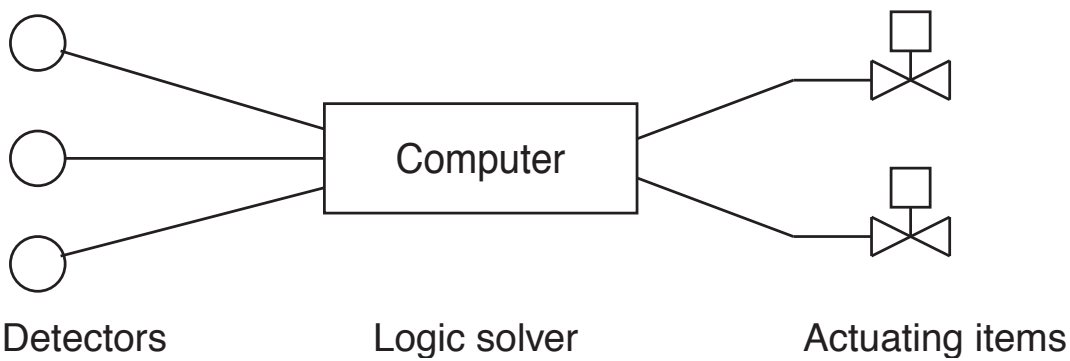
Homepage of the book:
http://www.ntnu.edu/ross/books/srt



What is a safety-instrumented system?

A safety-instrumented system (SIS) is a designated system that implements the required safety functions necessary to achieve or maintain a safe state for some equipment (an EUC). A SIS consists of three types of elements:

- Detectors (or sensors)
- Logic solver (e.g., one or more computers)
- Actuating items (e.g., valves, brakes)



Alternative terms

- *Safety-instrumented system (SIS)*; used in IEC 61511 and in the U.S. National Standard ANSI/ISA 84.01
- *Electrical/electronic/programmable electronic (E/E/PE) safety-related system*; used in IEC 61508
- *Instrumented protective system*
- *Programmable electronic system (PES)*
- *Safety-related system (SRS)*
- *Safety shutdown (SSD) system*
- *Emergency shutdown (ESD) system*

Equipment under control

☞ Equipment under control (EUC): Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

☞ EUC control system: System which responds to input signals from the process and/or from an operator and generates output signals causing the EUC to operate in the desired manner. [Also called basic process control system (BPCS)]

☞ EUC risk: Risk arising from the EUC or its interaction with the EUC control system.

[Definitions from IEC 61508-4]

What is functional safety?

☞ Functional safety: is part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.

[Definition from IEC 61508-4]

Requirements to functional safety

Two types of requirements are necessary to achieve functional safety:

1. Safety function requirements: Requirements for the safety functions that have to be performed by the SIS.

2. Safety integrity requirements: Requirements related to the probability that the safety function will perform satisfactorily. These requirements may be derived from a risk assessment of the system.

Safe state

☞ Safe state: A state of the EUC when safety is achieved [IEC 61508-4]

Note

In going from a potentially hazardous condition to the final safe state, the EUC may have to go through a number of intermediate safe states. For some situations a safe state exists only so long as the EUC is continuously controlled. Such continuous control may be for a short or an indefinite period of time.

Layer of protection

☞ Layer of protection (LOP): An independent mechanism that reduces risk by control, prevention, or mitigation. A LOP consists of a grouping of equipment and/or administrative controls that function in concert with other LOPs to control or mitigate risk.

Examples of LOPs are:

- Basic process control system (BPCS) [EUC control system]
- Alarms with defined operator response
- Pressure relief devices
- Safety-instrumented systems (SIS)
- Deluge systems for fire or fume release
- Physical protection (e.g., fire walls)
- Evacuation procedures

A LOP that perform its function with a high degree of reliability may qualify as an *independent protection layer* (IPL).

LOP characteristics

A LOP should have the following characteristics:

- Specificity - A LOP is designed to prevent or mitigate the consequences of one potentially hazardous event. Multiple causes may lead to the same hazardous event, and therefore multiple event scenarios may initiate action by a LOP.
- Independence - A LOP is independent of other LOPs if it can be demonstrated that there is no potential for common cause failures with any other claimed LOPs.
- Dependability - The LOP can be counted on to do what it was designed to do by addressing both random hardware and systematic failures during its design.
- Auditability - A LOP is designed to facilitate regular validation of the protective functions.

Examples of safety-instrumented systems

- Emergency shutdown (ESD) systems in a hazardous chemical process plant
- Automatic train stop (ATS) system in railways
- Guard interlocking and emergency stopping systems for machinery
- Dynamic positioning systems for ships and semisubmersible platform
- Fly-by-wire operations of aircraft flight control surfaces
- Anti-lock brakes on automobiles
- Air-bag systems in automobiles

Main SIS functions

1. When a predefined process demand (deviation) occurs in the EUC, the deviation shall be detected by the SIS sensors, and the required actuating items shall be activated and fulfill their intended functions.
2. The SIS shall not be activated spuriously, that is, without the presence of a predefined process demand (deviation) in the EUC.

Failure definitions

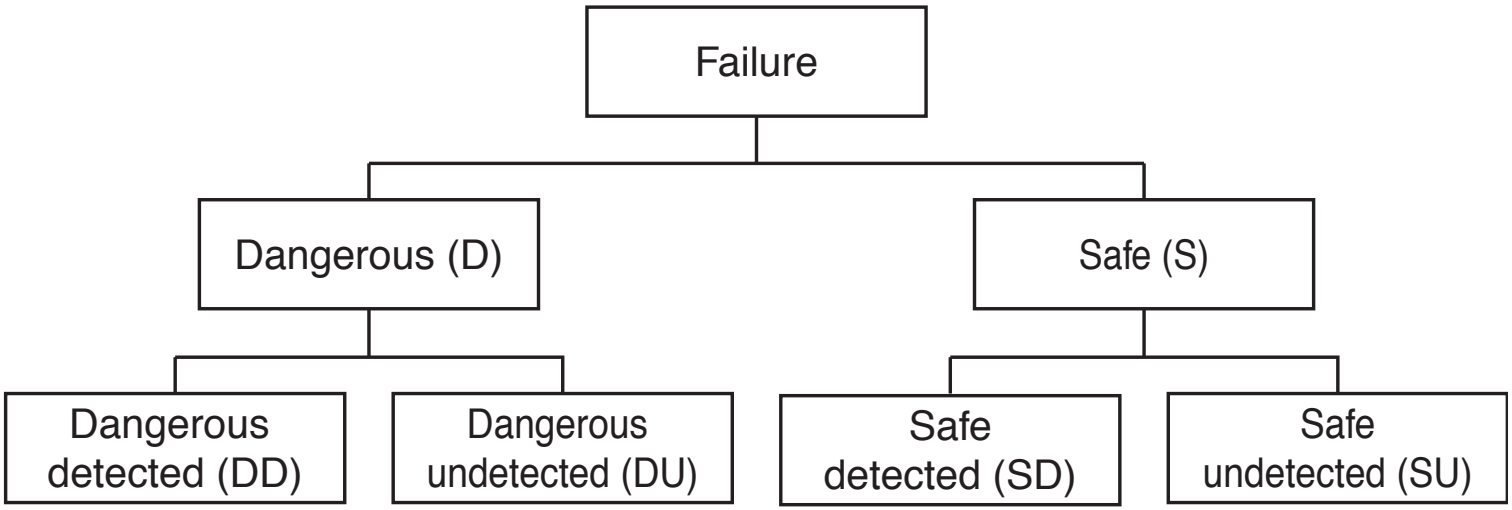
- Dangerous failure - has the potential to put the SIS in a hazardous or fail-to-function state.
- Safe failure - does not have the potential to put the SIS in a hazardous or fail-to-function state.

A detected failure is a failure that is detected by the diagnostic tests or through normal operation.

Failure classification – 1

SIS failures may be classified as:

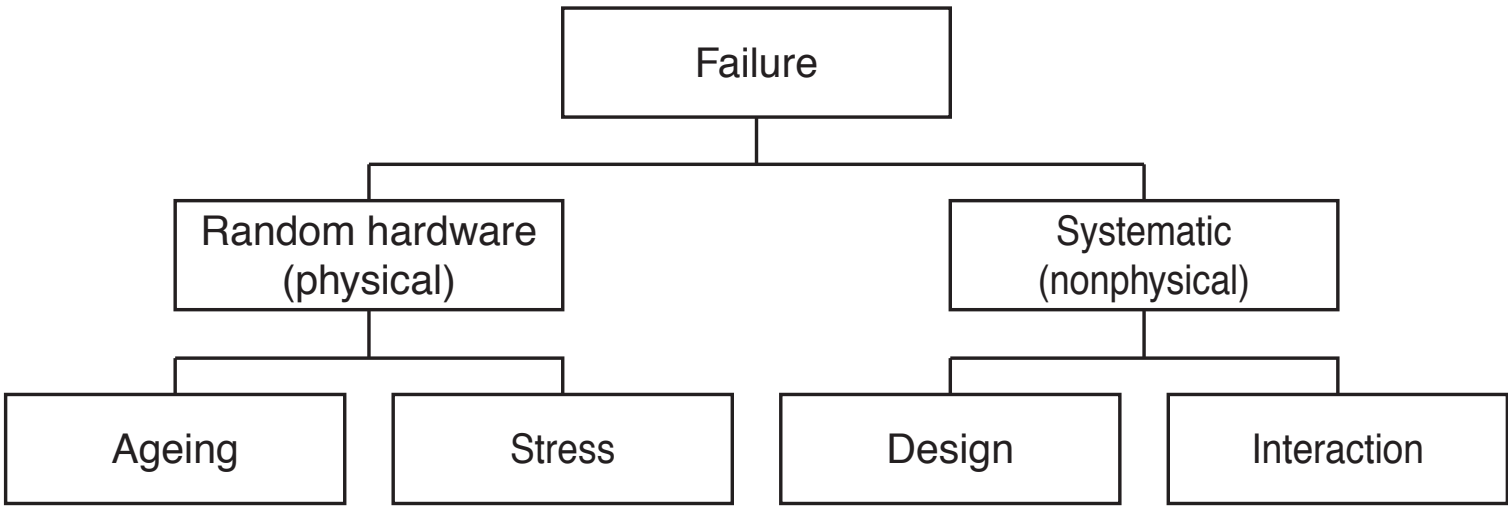
- Dangerous (D) failures
  - Dangerous undetected (DU) failures
  - Dangerous detected (DD) failures
- Safe (S) failures
  - Safe undetected (SU) failures
  - Safe detected (SD) failures



Failure classification – 2

Failures may also be classified according to the cause of the failure:

- Random hardware failures
  - Aging failures
  - Stress failures
- Systematic failures
  - Design failures
  - Interaction failures



Systematic failures

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

Examples of systematic failure causes include:

- Human errors in safety requirements specification, design, manufacture, installation and operation of hardware
- Human errors in design and/or implementation of software

Failure classification – 3

SIS failures may be categorized according to the time of their origin:

1. Failures caused by faults originating *before or during system installation* (e.g., software specification and program faults, hardware manufacturing faults and incorrect selection of components)
2. Failures caused by faults or human errors originating *after system installation* (e.g., random hardware failures, and failures caused by incorrect use)

Failure rates

The following failure rates are used in the quantitative analyses:

Failure Rate	Type of Failure
λ_S	Safe failures
λ_{SD}	Safe detectable failures
λ_{SU}	Safe undetectable failures
λ_D	Dangerous failures
λ_{DD}	Dangerous detectable failures
λ_{DU}	Dangerous undetectable failures

Safe failure fraction

The safe failure fraction (SFF) is the fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure.

$$\mathrm{SFF} = \frac{\sum \lambda_{\mathrm{S}} + \sum \lambda_{\mathrm{DD}}}{\sum \lambda_{\mathrm{S}} + \sum \lambda_{\mathrm{D}}}$$

where the sum is taken over all relevant items.

The SFF may alternatively be defined as the conditional probability that a failure is either a safe failure or a detected dangerous failure (when we know that a failure has occurred).

FMEDA

A Failure Modes, Effects and Diagnostic Analysis (FMEDA) is an extension of a traditional FMECA to identify online diagnostic techniques.

Id.	Component	Function	Failure mode	Failure causes	Failure effects	Criticality	Failure rate λ	Detectable (yes/no)	Diagnostic (descr.)	Mode D/S	λ^{DU}	λ^{DD}	λ^{SD}	λ^{SU}	Remarks

Causes of dangerous failures

Dangerous failures may arise from:

- Incorrect specification of the system, hardware or software
- Omissions in the safety requirements specification (e.g., failure to develop all relevant safety functions during different modes of operation)
- Random hardware failure mechanisms
- Systematic hardware failure mechanisms
- Software errors
- Common cause failures
- Human error
- Environmental influences (e.g., electromagnetic, temperature, mechanical phenomena)
- Supply system voltage disturbances (e.g., loss of supply, reduced voltages)

Diagnostic testing

There are two main diagnostic testing techniques:

1. *Reference* diagnostic can be carried out with a single circuit and is based on specific characteristics of the SIS, like voltage, currents, signal timing, signal sequence, and temperature.
2. *Comparison* diagnostic compares data between two or more SIS units. If a failure occurs in the circuitry, processor or memory of one SIS unit, there will be differences between the data tables in that unit when compared to another unit.

Diagnostic coverage – 1

Diagnostic coverage (DC) is defined as the ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic tests. Diagnostic coverage does not include any faults detected by proof tests. [IEC 61511-1]

$$\mathrm{DC} = \frac{\sum \lambda_{\mathrm{DD}}}{\sum \lambda_{\mathrm{D}}}$$

The DC may also be interpreted as the conditional probability that a failure will be detected by diagnostic testing (when a failure occurs).

Note

Diagnostic coverage may exist for the whole or parts of a SIS. For example, diagnostic coverage may exist for sensors and/or logic system and/or final elements.

Diagnostic coverage – 2

For some applications it is necessary to distinguish between the diagnostic coverage for dangerous and safe failures.

Let:

DC_D = the diagnostic coverage for *dangerous* failures

DC_S = the diagnostic coverage for *safe* failures

[Based on Goble and Brombacher 1999]

Proof testing

A proof test is a test performed to reveal undetected faults in a safety-instrumented system so that, if necessary, the system can be restored to its designed functionality.

A generic standard

IEC 61508 "Functional safety of electrical/ electronic/ programmable electronic (E/E/PE) safety-related systems" is a generic standard that applies to all safety-related systems using electrical, electronic, and programmable electronic devices irrespective of the application sector.

Examples of application sectors within the scope are:

- Process industries (emergency shutdown systems, fire and gas detection systems)
- Manufacturing industries (industrial robots, machine tools)
- Transportation (automatic train stop systems, braking systems)
- Medical (electro-mechanical apparatus)

Objectives of IEC 61508

- To facilitate the development of application sector standards such as
  - IEC 61511 - for the process industry sector
  - IEC 62061 - for machinery systems
- To enable the development of E/E/PE safety-related systems where application sector international standards do not exist.

IEC 61508 has seven parts

IEC 61508 has seven parts:

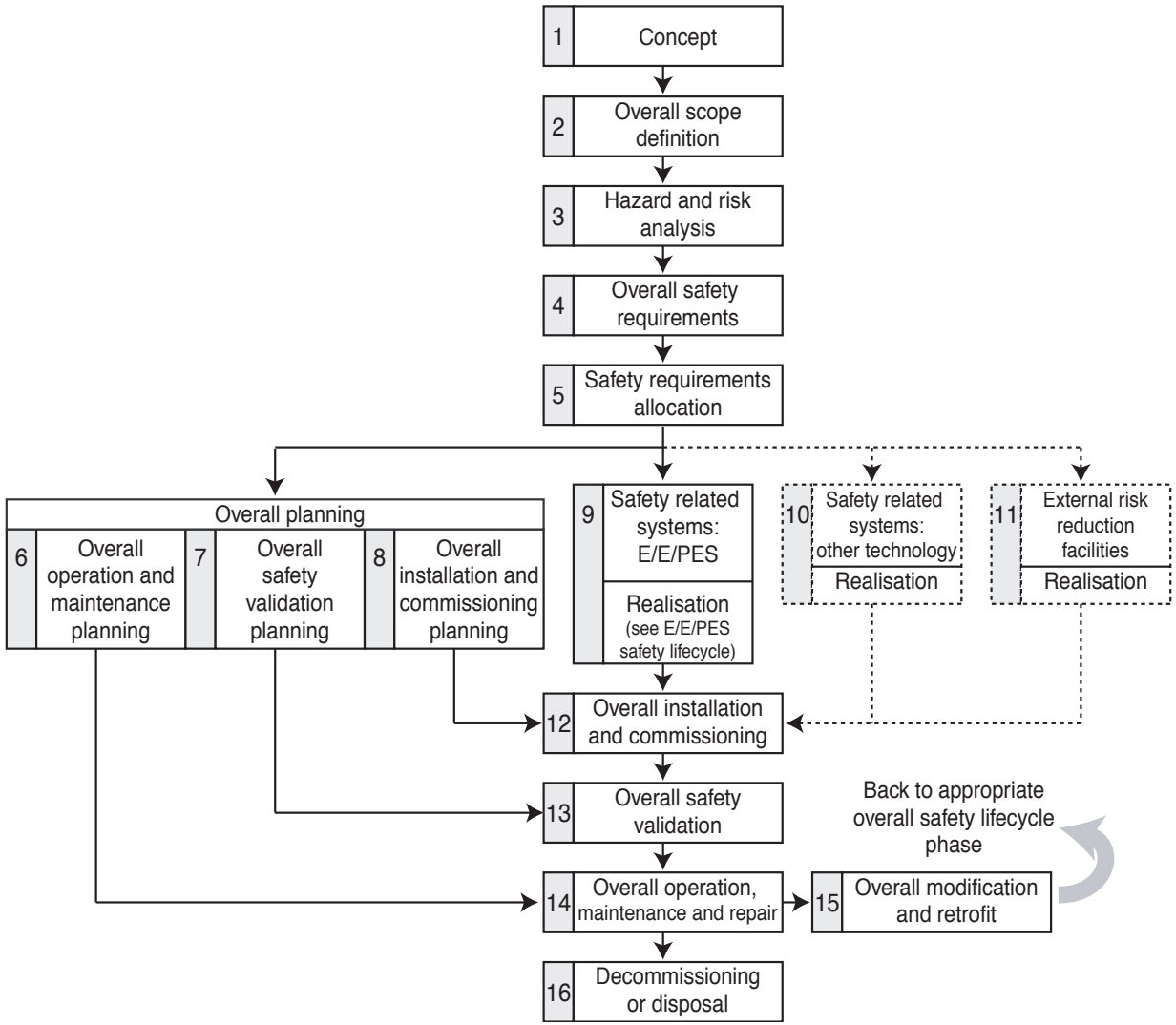
1. General requirements
2. Requirements for E/E/PE safety-related systems
3. Software requirements
4. Definitions and abbreviations
5. Examples of methods for determination of safety integrity levels
6. Guidelines on the application of IEC 61508-2 and IEC 61508-3
7. Overview of techniques and measures

Overall safety lifecycle – 1

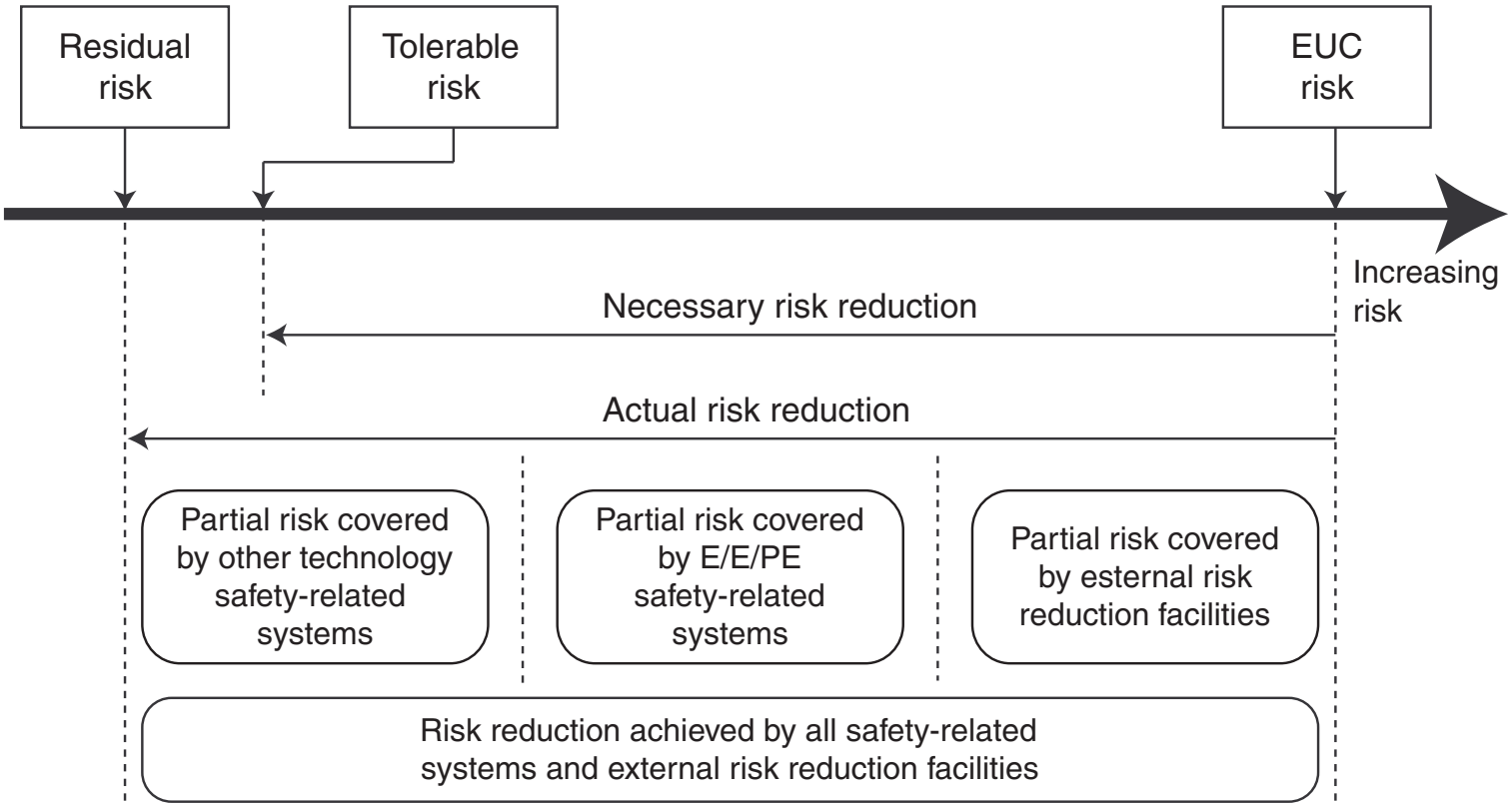
IEC 61508 introduces the concept of an Overall Safety Lifecycle (see next frame) to ensure that all activities necessary to achieve the required safety integrity level are performed. For each phase the standard specifies:

- The objectives to be achieved
- The requirements to meet the objective
- The scope of each phase
- The required inputs to the phase
- The deliverables required for each phase

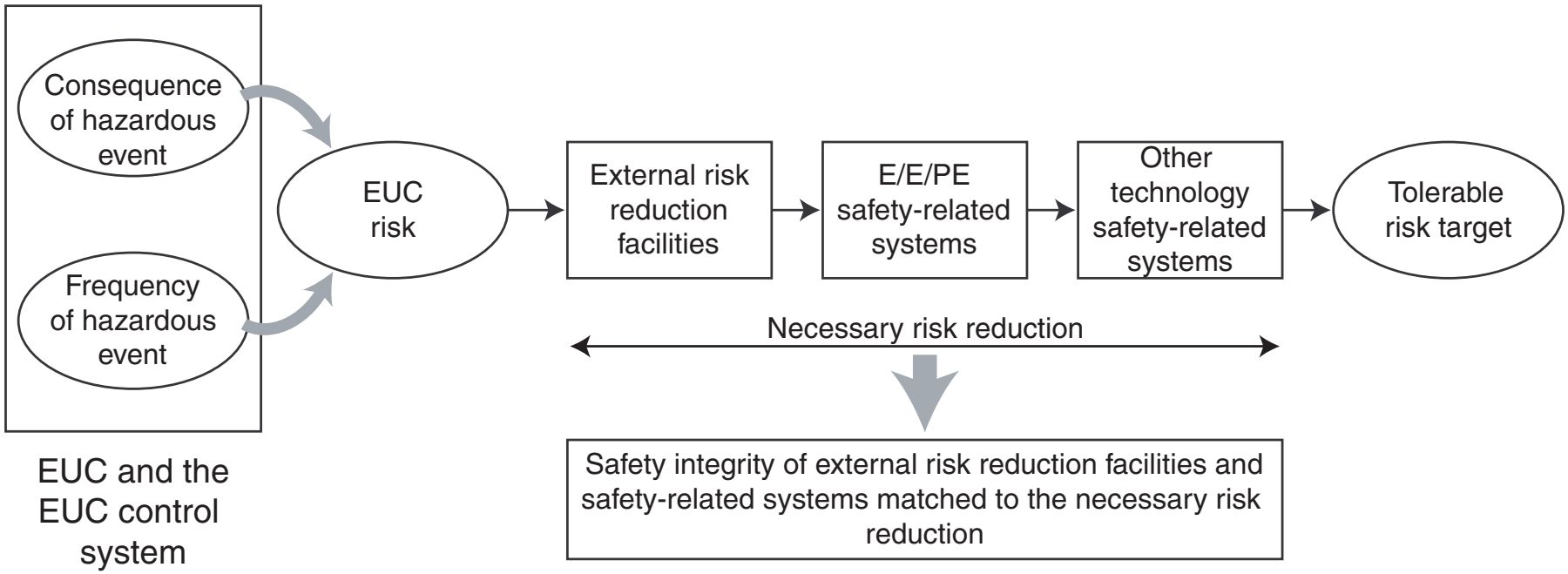
Overall safety lifecycle – 2



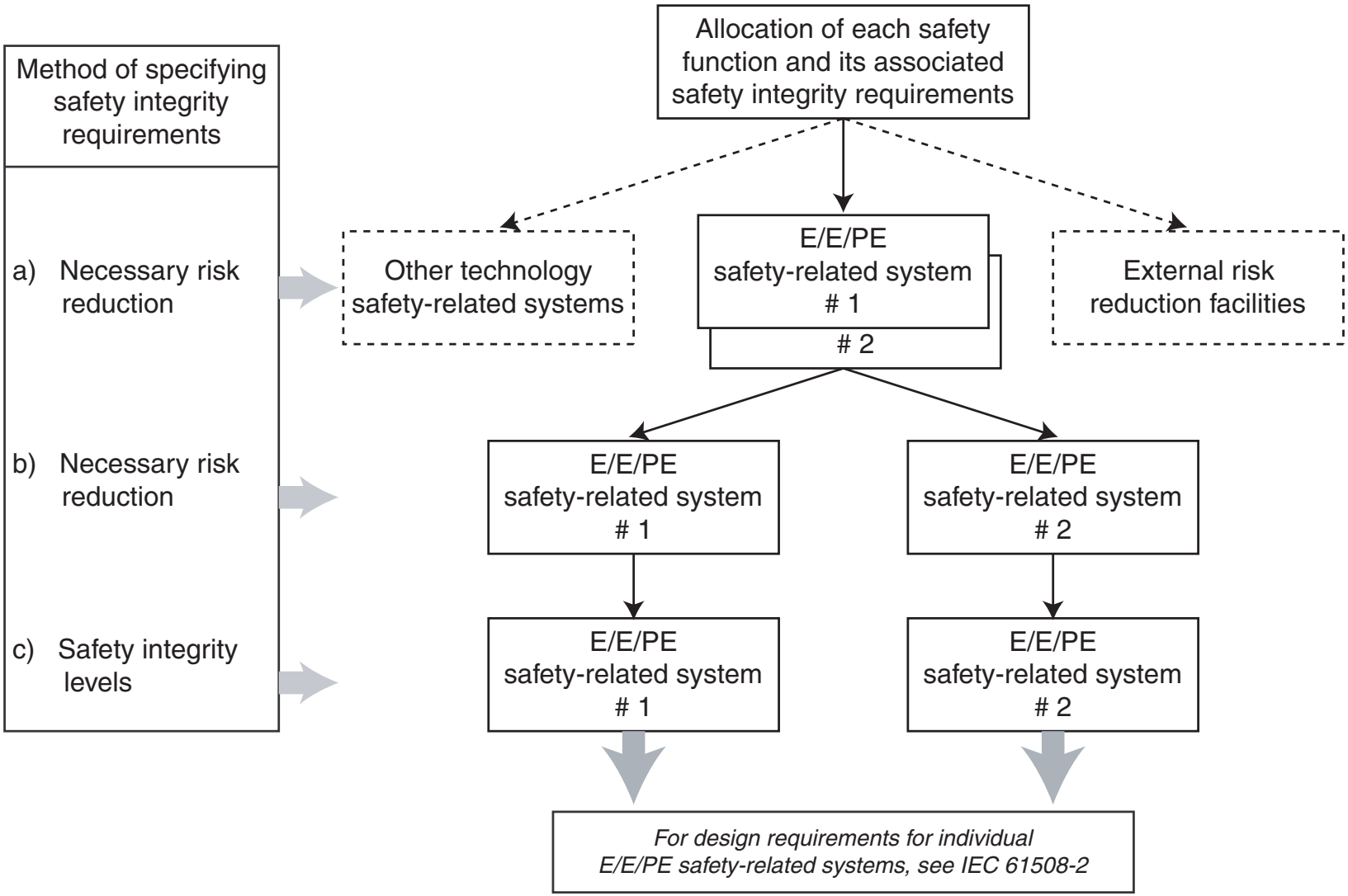
Risk reduction: General concepts



Risk and safety integrity concepts



Allocation of safety requirements



Safety integrity level – 1

☞ Safety integrity: The probability that a SIS will satisfactorily perform the required safety functions under all the stated conditions within a stated period of time.

☞ Safety integrity level (SIL): A discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the SIS, where SIL 4 is the highest level and SIL 1 is the lowest level.

Safety-instrumented function

IEC 61508 details the requirements necessary to achieve each safety integrity level. A safety function that is implemented by a SIS is often called a safety-instrumented function (SIF).

A SIS will usually implement more than one SIF. If the safety integrity requirements for these SIFs differ, the requirements applicable to the highest relevant SIL shall apply for the entire SIS, unless there is sufficient independence of implementation between the various SIFs.

Safety integrity level – 2

Safety Integrity Level (SIL)	Low Demand Mode of Operation[a] (Aver. probability of failure to perform its design function on demand)	High Demand Mode or Continuous Mode of Operation[b] (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

a) Low demand mode means that the frequency of demands for operation of the SIS is not greater than once per year, and not greater than twice the proof-test frequency.

b) High demand mode means that the frequency of demands for operation of the SIS is greater than once per year or greater than twice the proof-test frequency.

Architectural constraints – 1

The IEC 61508 architectural constraints on *low complexity* subsystems are given by:

	Hardware fault tolerance		
Safe failure fraction	0	1	2
$< 60\%$	SIL 1	SIL 2	SIL 3
$60\% - 90\%$	SIL 2	SIL 3	SIL 4
$90\% - 99\%$	SIL 3	SIL 4	SIL 4
$\geq 99\%$	SIL 3	SIL 4	SIL 4

Architectural constraints – 2

The IEC 61508 architectural constraints on *complex* subsystems are given by:

	Hardware fault tolerance		
Safe failure fraction	0	1	2
$< 60\%$	N/A	SIL 1	SIL 2
$60\% - 90\%$	SIL 1	SIL 2	SIL 3
$90\% - 99\%$	SIL 2	SIL 3	SIL 4
$\geq 99\%$	SIL 3	SIL 4	SIL 4

N/A means “Not allowed”

Architectural constraints – 3

The architectural constraints (AC) are those constraints that are imposed by IEC 61508-2 to limit the SIL that can be claimed for any safety function on the basis of its hardware fault tolerance and its safe failure fraction (SFF). They require a subsystem to have a minimum level of redundancy based on its SFF to insure the required hardware fault tolerance. For a device with a low SFF, redundancy may be required.

Risk reduction factor

A Risk Reduction Factor (RRF) is a measure of how much protection is afforded to the system by application of a specific solution (e.g., installing a high reliability temperature transmitter)