I requisiti delle Norme IEC EN 61508 Ed 2: 2010 e IEC EN 61511 Ed. 2: 2016

18 Febbraio 2016

G. Picciolo

Associazione Italiana Strumentisti

ISA Italy Section

Move Forward with Confidence

BUREAU VERITAS

Agenda

- ► The Norm IEC EN 61508 Ed. 2: 2010 – overview
  - Normative & informative requirements
- ► The *new* Norm IEC EN 61511 Ed. 2: 2016 - overview
  - Normative & informative requirements
- Norms relevant clauses in safety-related system design and operation

IEC 61508 Ed. 2 Standard)

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic (E/E/PE) elements that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of application sector standards.

IEC 61508 Ed. 2 Standard)

- International standard and European standard EN 61508 Ed. 2: 2010
- Basic Safety Standard
- Official issue in March 2010 Ed. 2 but already used since 10 years
- 7 volumes
- More than 1000 requirements

IEC 61508 Ed. 2 Standard)

-“Functional Safety of Electrical/Electronic/Programmable

- Electronic Safety-related Systems”

❑ Part 1: General Requirements

❑ Part2 : Requirements for Electrical/ Electronic/Programmable Electronic Safety-related Systems (E/E/PES)

❑ Part 3: Software Requirements

❑ Part 4: Definitions and Abbreviations

❑ Part 5: Examples of Methods for the Determination of SILs

❑ Part 6: Guidelines on the Application of Parts 2 and 3

❑ Part 7: Overview of Techniques and Measures

IEC 61508 Ed. 2 Standard)

- Part 1 - Clause 4
- To conform to the std it shall be demonstrated that the requirements have been satisfied to the required critieria specified (for example safety integrity level) and therefore, for each clause or subclause, all the objectives are met
- Parts 1, 2 , 3 & 4 are normative
- Parts 5, 6 & 7 are informative

PED DIRECTIVE 97/23/CE; EN 764-7

►SAFETY SYSTEMS FOR UNFIRED PRESSURE VESSELS

- § Accessories
- ARTT. 9, 13: DLGS 329: commissioning and periodic tests

  (HIPPS VS PSV, RD)

NORMATIVE CLAUSES: Part 1

- § 5: DOCUMENTATION
- § 6: *FUNCTIONAL SAFETY MANAGEMENT*
- § 7: LIFE CYCLE SAFETY REQUIREMENT
- § 8:FUNCTIONAL SAFETY ASSESSMENT

Definitions

- A SAFETY-RELATED ***ELEMENT*** IS A PART OF A SAFETY -INSTRUMENTED ***SYSTEM***

Basic SIS structure and subsystem PFDavg/PFH allocation ratio

- Sensor
- Logic Solver
- Final Element

•35 %	•15 %	•50%

- *REF. IEC 61508*

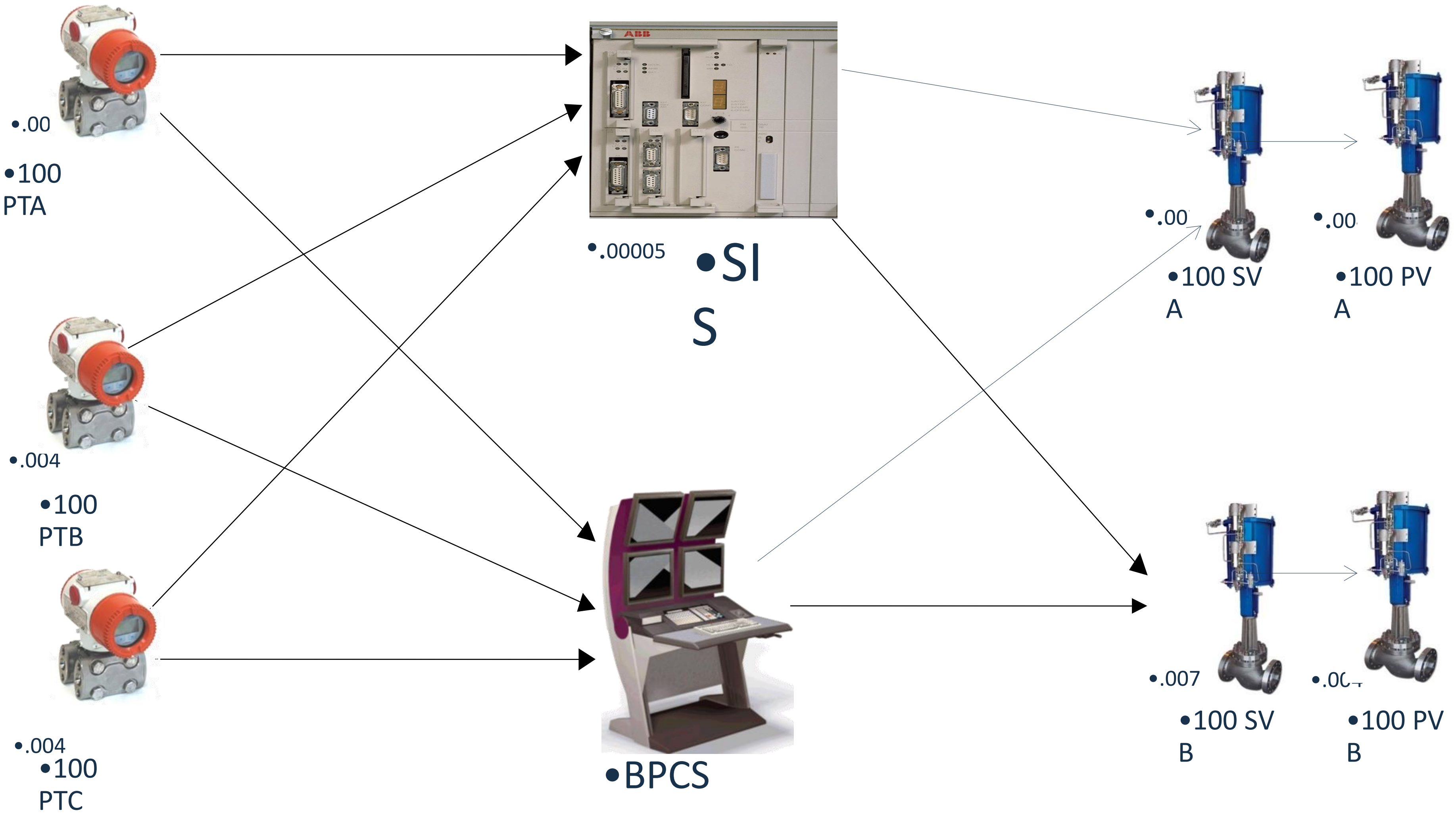
•13 %	•3 %	•84%

- **$PFDavg = PFDavg_{S} + PFDavg_{LS} + PFDavg_{FE}$**

- *VERIFICATO: 200 LOOP*

- **$PFHd = PFH_{S} + PFH_{LS} + PFH_{FE}$**

Bubble Diagram showing the PFDavg of each SIS device

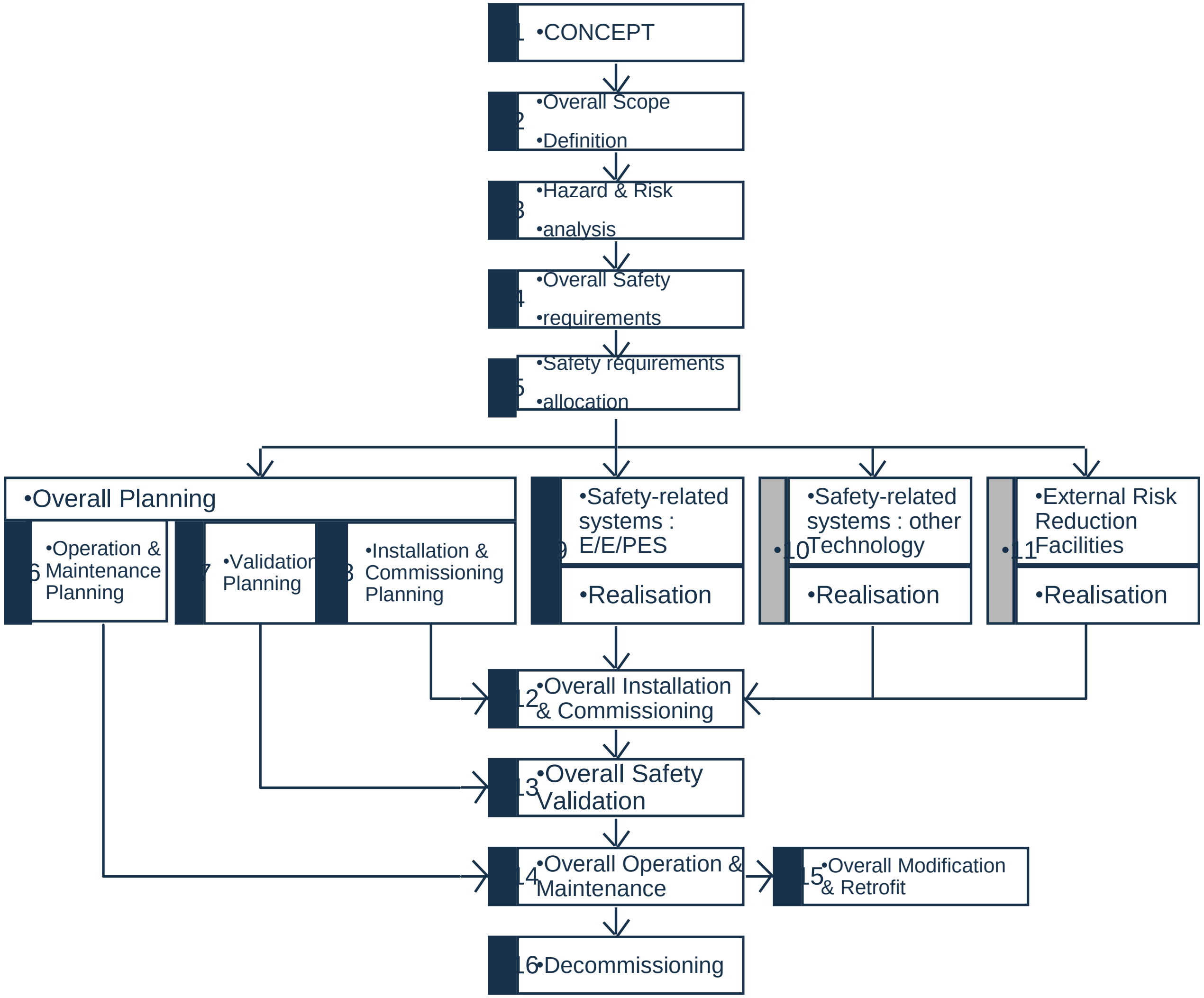


The Norm IEC EN 61508 Ed. 2: 2010 overview: Normative & informative requirements

- The Life Cycle

- SIL

The Life Cycle



1 •CONCEPT

2 •Overall Scope •Definition

3 •Hazard & Risk •analysis

4 •Overall Safety •requirements

5 •Safety requirements •allocation

•Overall Planning

6 •Operation & Maintenance Planning

7 •Validation Planning

8 •Installation & Commissioning Planning

9 •Safety-related systems : E/E/PES •Realisation

•10 •Safety-related systems : other Technology •Realisation

•11 •External Risk Reduction Facilities •Realisation

12 •Overall Installation & Commissioning

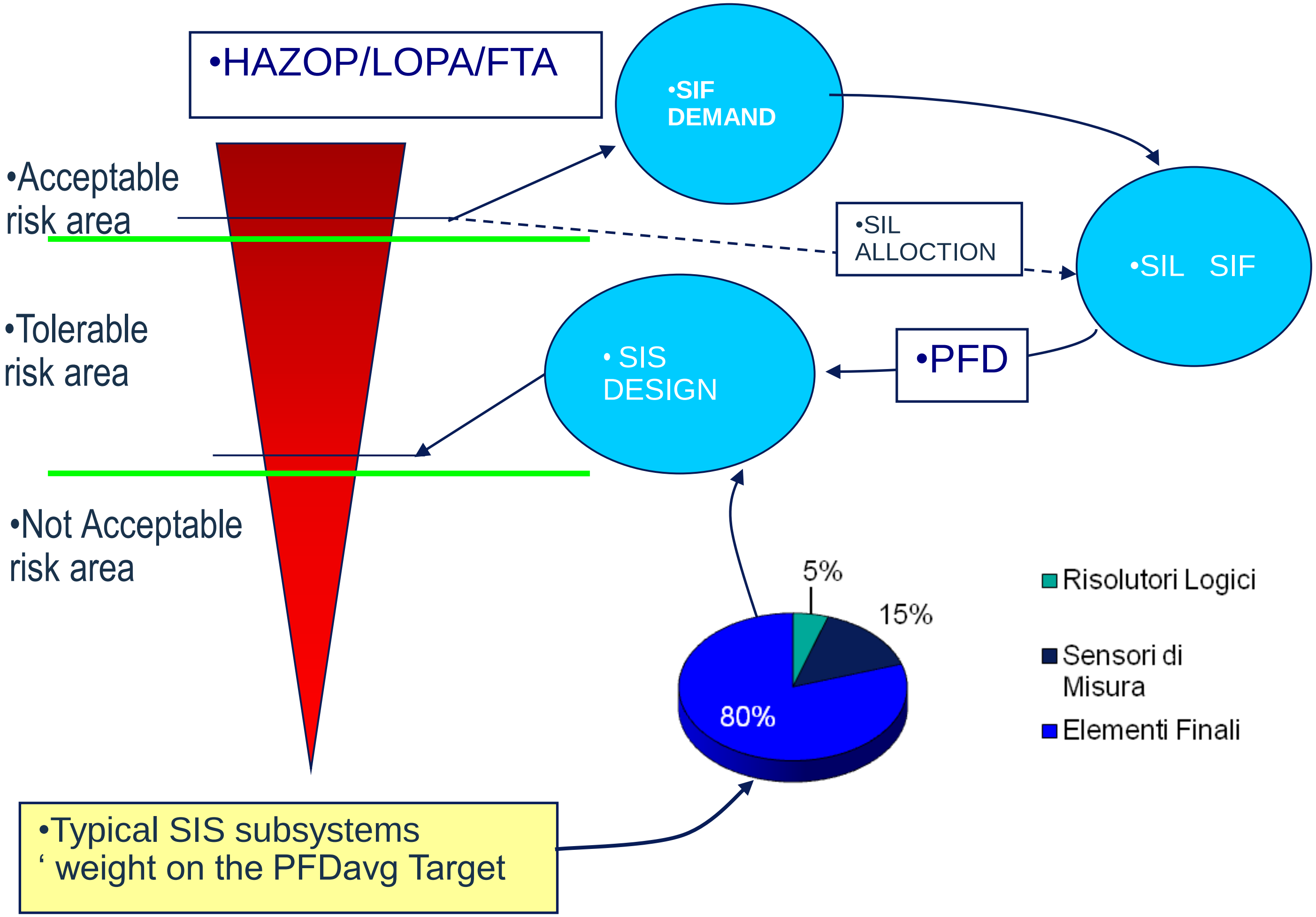
13 •Overall Safety Validation

14 •Overall Operation & Maintenance

15 •Overall Modification & Retrofit

16 •Decommissioning

SIS Assessment Process (SIS)



SIL

- Definition
- Characterization
- Functional safety
  - Failure rates
  - Safety Integrity hardware
  - Capability (systematic integrity)

Functional Safety

Probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time

Safety Function

Function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event.

Safety Integrity Level

Probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time

Target Safety Integrity Levels

Safety Integrity Level (SIL)	Low Demand Mode of Operation (Average probability of failure to perform its design function on demand: PFDavg)	High Demand or continuous Mode of Operation (Probability of *dangerous* failure per hour: PFH)
SIL 4	>=10^{-5} to <10^{-4}	>=10^{-9} to <10^{-8}
SIL 3	>=10^{-4} to <10^{-3}	>=10^{-8} to <10^{-7}
•SIL 2	•>=10^{-3} to <10^{-2}	•>=10^{-7} to <10^{-6}
•SIL 1	•>=10^{-2} to <10^{-1}	•>=10^{-6} to <10^{-5}

Safety Integrity

- In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) that lead to an unsafe state should be included, for example hardware failures, software induced failures and failures due to electrical interference. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the average frequency of failure in the dangerous mode of failure or the probability of a safety-related protection system failing to operate on demand. However, safety integrity also depends on many factors that cannot be accurately quantified but can only be considered qualitatively.

- Safety integrity comprises *hardware* safety integrity and *systematic* safety integrity.

- This definition focuses on the *reliability* (dependability) of the safety-related systems to perform the safety functions .

Safety Integrity

- *Systematic* safety integrity

•Part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure

•NOTE: Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity which usually can).

- *Hardware* safety integrity

•Part of the safety integrity of a safety-related system relating to random hardware failures in a dangerous mode of failure

Dangerous & Safe falures

- **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

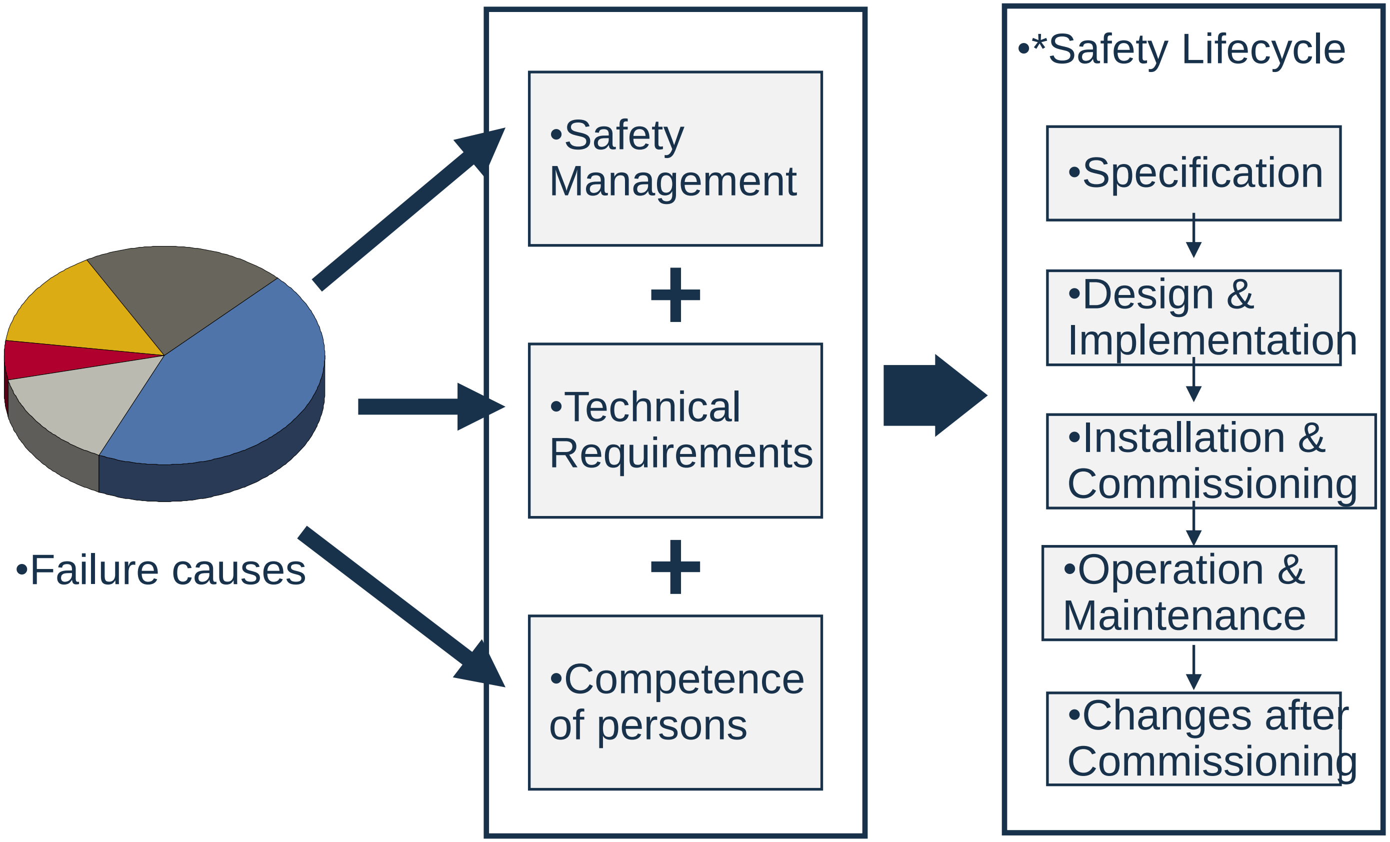
- **Safe failure**

- 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

The Functional Safety Strategy



•* *Simplified view*

Annex A (normative) Techniques and measures for E/E/PE safety-related systems –control of failures during operation

This annex limits the maximum diagnostic coverage that may be claimed for relevant techniques and measures. For each safety integrity level, the annex recommends techniques and measures for controlling random hardware, systematic, environmental and operational failures.

NOTE 2 The designations low, medium and high diagnostic coverage are quantified as 60 %, 90 % and 99 % respectively.

7.4.10 Requirements for proven in use elements (Manufacturer)

7.4.10.4 A proven in use safety justification shall be documented, using the information available from 7.4.10.2, that the element supports the required safety function with the required systematic safety integrity. This shall include:

a) the suitability analysis and testing of the element for the intended application;

•b) the demonstration of equivalence between the intended operation and the previous operation experience, including the impact analysis on the differences;

•c) the statistical evidence.

Overview of IEC EN 61508 Ed.2 & IEC EN 61511 Ed.1 Norms – Essential topics

- ►IEC 61508 IS A *BASIC* STANDARD – IT APPLIES TO SAFETY-RELATED ***ELEMENTS*** AND PROVIDES INFORMATION FOR THE WHOLE SAFETY- RELATED SYSTEMS DESIGN AND OPERATION

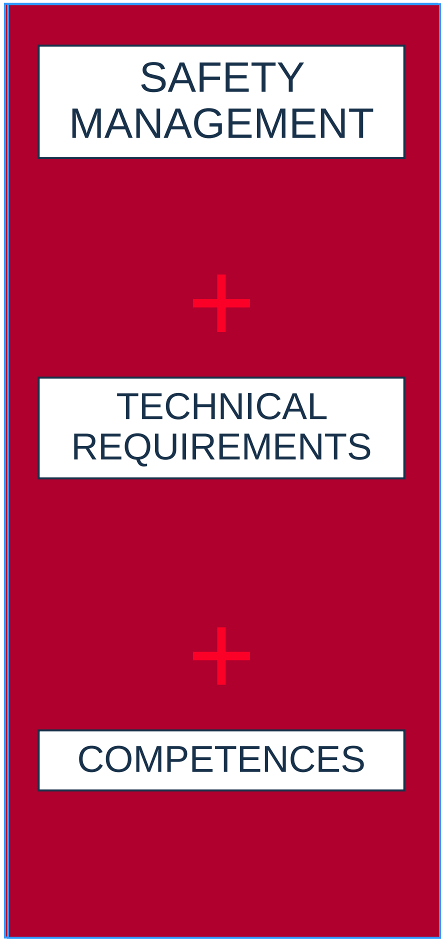
- ►IEC 61511 APPLIES SPECIFICALLY FOR THE DESIGN AND OPERATION OF ***SAFETY INSTRUMENTED SYSTEMS***

Basic Definitions Normative

► § 7.4.4.1.2 - A SUBSYSTEM CAN BE REGARDED AS TYPE “A” IF, FOR THE COMPONENTS REQUIRED TO ACHIEVE THE SAFETY FUNCTION:

- a) THE FAILURE MODE OF ALL CONSTITUENT COMPONENTS ARE WELL DEFINED, AND
- b) THE BEHAVIOUR OF THE SUBSYSTEM UNDER FAULT CONDITIONS CAN BE COMPLETELY DETERMINED; AND
- c) THERE IS SUFFICIENT *DEPENDABLE* FAILURE DATA FROM FIELD EXPERIENCE TO SHOW THAT CLAIMED RATES OF FAILURE FOR DETECTED AND UNDETECTED DANGEROUS FAILURES ARE MET (SEE 7.4.9.3 TO 7.4.9.5)

Gestione della Sicurezza Funzionale



SAFETY MANAGEMENT

+

TECHNICAL REQUIREMENTS

+

COMPETENCES

- ►Functional safety management
- ►Safety life cycle requirements
- ►Verification
- ►Validation

Basic Definitions Normative

- § 7.4.4.1.3 - A SUBSYSTEM CAN BE REGARDED AS TYPE “B” IF, FOR THE COMPONENTS REQUIRED TO ACHIEVE THE SAFETY FUNCTION:

  - a) THE FAILURE MODE OF ALL CONSTITUENT COMPONENTS ARE NOT WELL DEFINED, AND
  - b) THE BEHAVIOUR OF THE SUBSYSTEM UNDER FAULT CONDITIONS CANNOT BE COMPLETELY DETERMINED; AND
  - c) THERE IS NOT SUFFICIENT *DEPENDABLE* FAILURE DATA FROM FIELD EXPERIENCE TO SHOW THAT CLAIMED RATES OF FAILURE FOR DETECTED AND UNDETECTED DANGEROUS FAILURES ARE MET (SEE 7.4.9.3 TO 7.4.9.5)

Basic Definitions Normative

- § 7.4.4.1.2 - A SUBSYSTEM CAN BE REGARDED AS TYPE “A” IF, FOR THE COMPONENTS REQUIRED TO ACHIEVE THE SAFETY FUNCTION:

  - a) THE FAILURE MODE OF ALL CONSTITUENT COMPONENTS ARE WELL DEFINED, AND
  - b) THE BEHAVIOUR OF THE SUBSYSTEM UNDER FAULT CONDITIONS CAN BE COMPLETELY DETERMINED; AND
  - c) THERE IS SUFFICIENT *DEPENDABLE* FAILURE DATA FROM FIELD EXPERIENCE TO SHOW THAT CLAIMED RATES OF FAILURE FOR DETECTED AND UNDETECTED DANGEROUS FAILURES ARE MET (SEE 7.4.9.3 TO 7.4.9.5)

$$\lambda = \lambda S + \lambda U$$

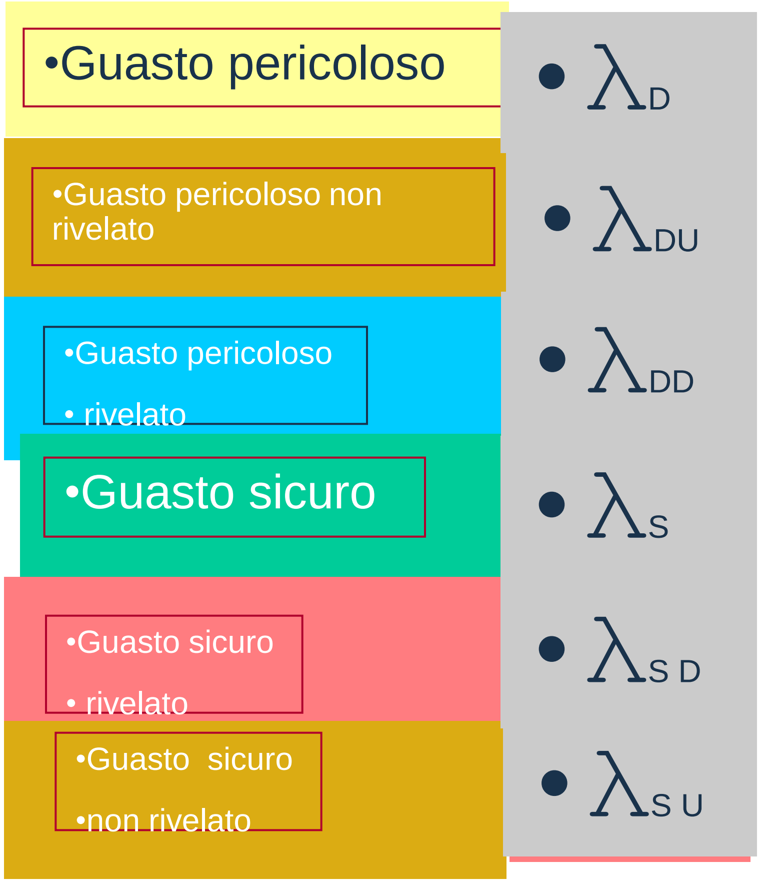
$$\lambda S = \lambda S D + \lambda S U$$

$$\lambda D = \lambda DU + \lambda DD$$

- $DC = \lambda_{DD} / \lambda_{D}$

- DCpst, vi ,cm= $\lambda_{DD, PST,VI, cm} / \lambda_{D}$

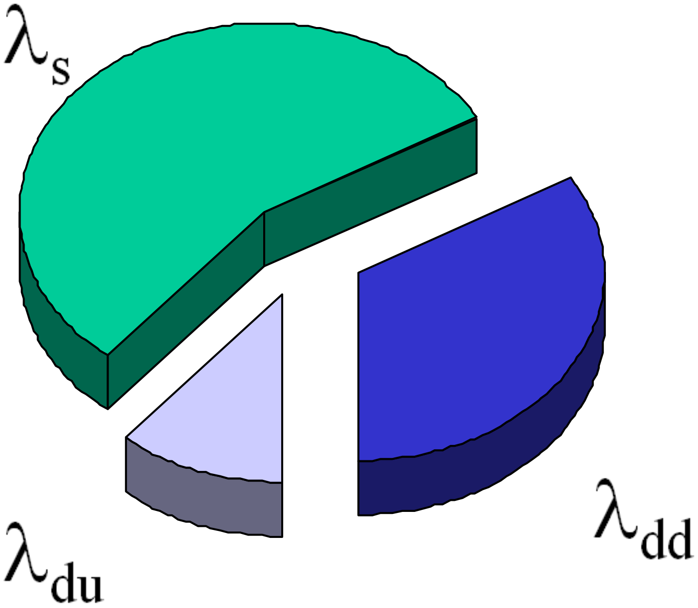
- SFF% = (λ S + λ DD) /λ
- MTTF = 1/ λ_t
- MTTFs = 1/ λ_{SAFE}
- MTTFd = 1/ λDANGEROUS



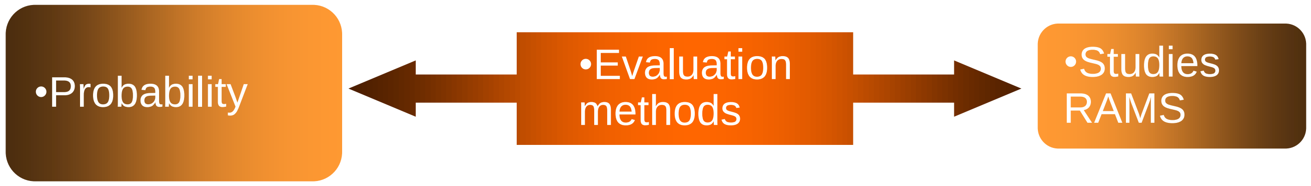
- Guasto pericoloso
- Guasto pericoloso non rivelato
- Guasto pericoloso
- rivelato
- Guasto sicuro
- Guasto sicuro
- rivelato
- Guasto sicuro
- non rivelato

- λ_D
- λ_{DU}
- λ_{DD}
- λ_S
- $\lambda_{S D}$
- $\lambda_{S U}$

FAILURE RATES AND RELATED PARAMETERS (SFF, DC) ARE CONCERNING TO SAFETY REQUIREMENTS SPECIFICATIONS

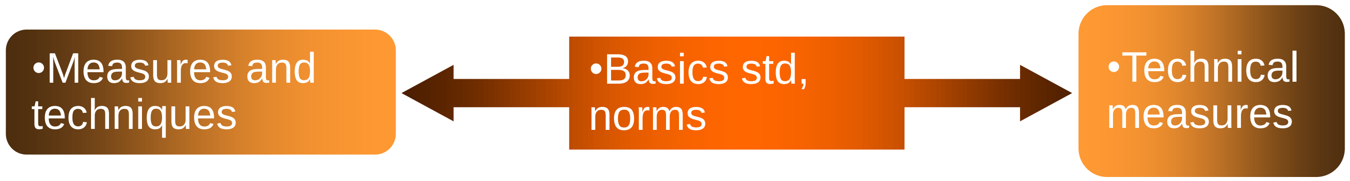


- ⇨ Random failures



- Probability
- Evaluation methods
- Studies RAMS

- ⇨ Systematic failures



- Measures and techniques
- Basics std, norms
- Technical measures

Table 2 - Hardware Safety Integrity

ARCHITECTURAL CONSTRAINTS ON TYPE A SAFETY-RELATED SUBSYSTEMS-HARDWARE FAULT TOLERANCE (EN 61508)

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	SIL4	SIL 4
>= 99%	**SIL 3**	**SIL 4**	SIL 4

Basic Definitions Normative

- § 7.4.4.1.3 - A SUBSYSTEM CAN BE REGARDED AS TYPE “B” IF, FOR THE COMPONENTS REQUIRED TO ACHIEVE THE SAFETY FUNCTION:

a) THE FAILURE MODE OF ALL CONSTITUENT COMPONENTS ARE NOT WELL DEFINED, AND

b) THE BEHAVIOUR OF THE SUBSYSTEM UNDER FAULT CONDITIONS CANNOT BE COMPLETELY DETERMINED; AND

c) THERE IS NOT SUFFICIENT *DEPENDABLE* FAILURE DATA FROM FIELD EXPERIENCE TO SHOW THAT CLAIMED RATES OF FAILURE FOR DETECTED AND UNDETECTED DANGEROUS FAILURES ARE MET (SEE 7.4.9.3 TO 7.4.9.5)

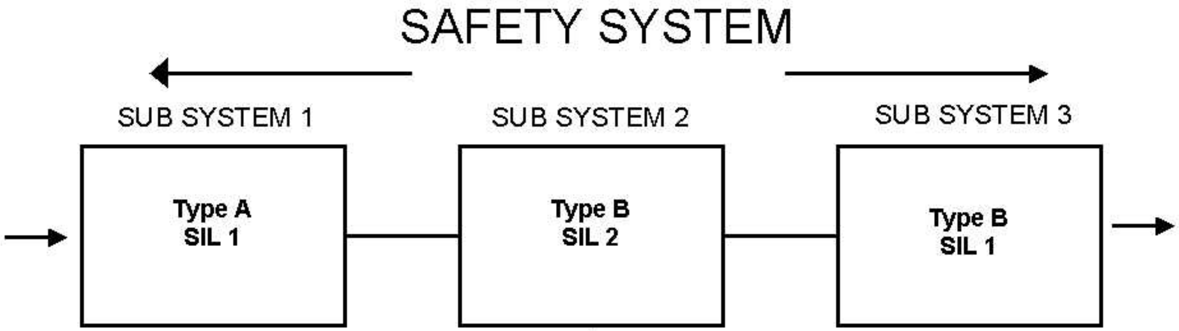
Table 3 - Hardware Safety Integrity

ARCHITECTURAL CONSTRAINTS ON TYPE B SAFETY-RELATED SUBSYSTEMS-HARDWARE FAULT TOLERANCE (EN 61508)

Safe Failure Fraction	0	1	2
•< 60%	•NOT ALLOWED	•SIL 1	•SIL 2
•60%-<90%	•SIL 1	•SIL 2	• SIL 3
•90%-<99%	• SIL 2	• SIL3	• SIL 4
•>= 99%	• SIL 3	• SIL 4	• SIL 4

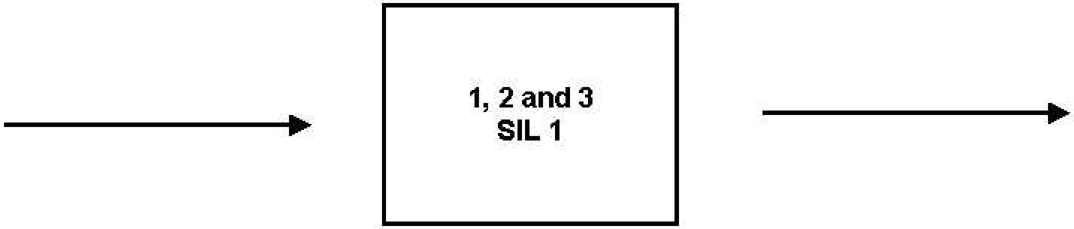
I vincoli architetturali

- Ciascun blocco deve avere la classificazione SIL anche in termini di PFDavg /PFH



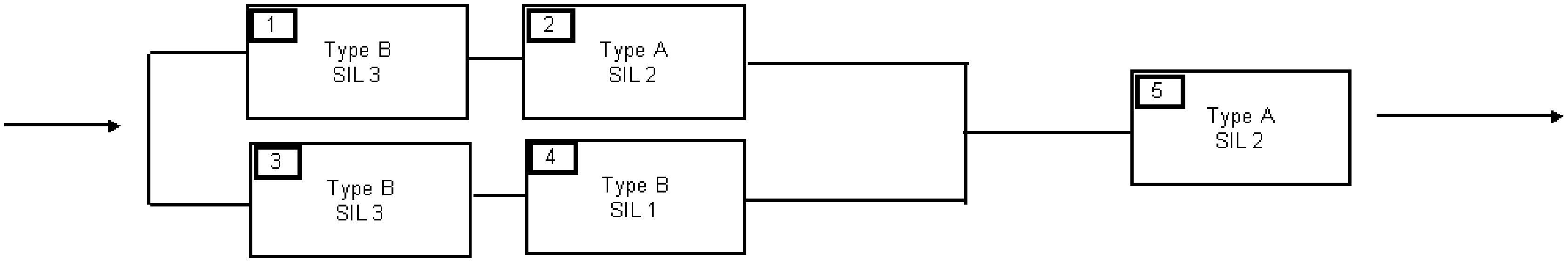
- Il blocco SIL 1 compromette la funzione di sicurezza dle blocco SIL 2

- Il blocco risultante è SIL 1



I vincoli architetturali

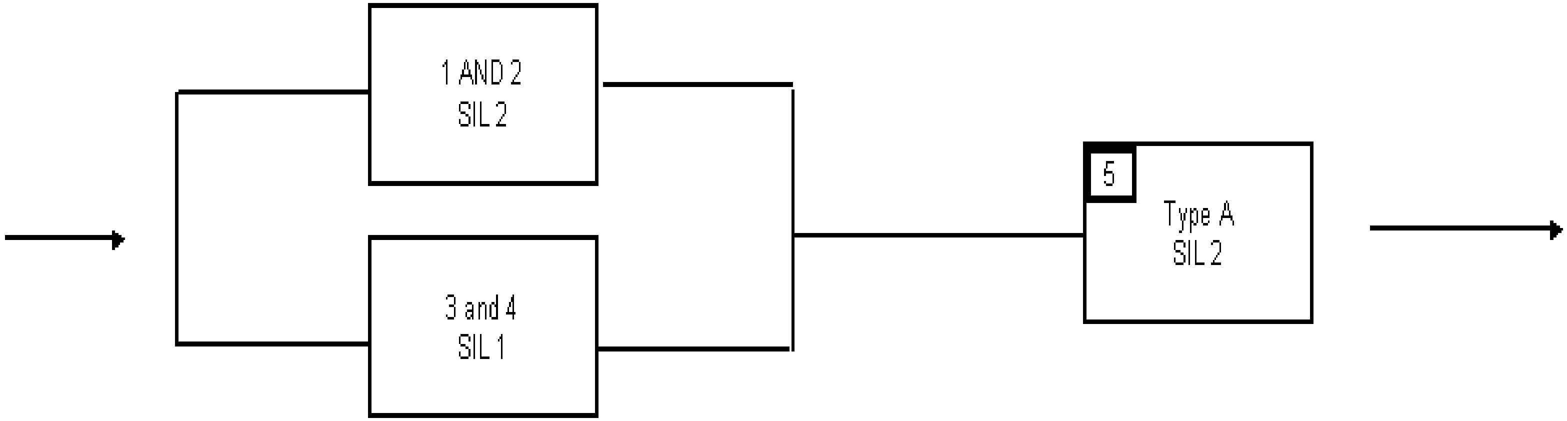
- Consideriamo il seguente sistema



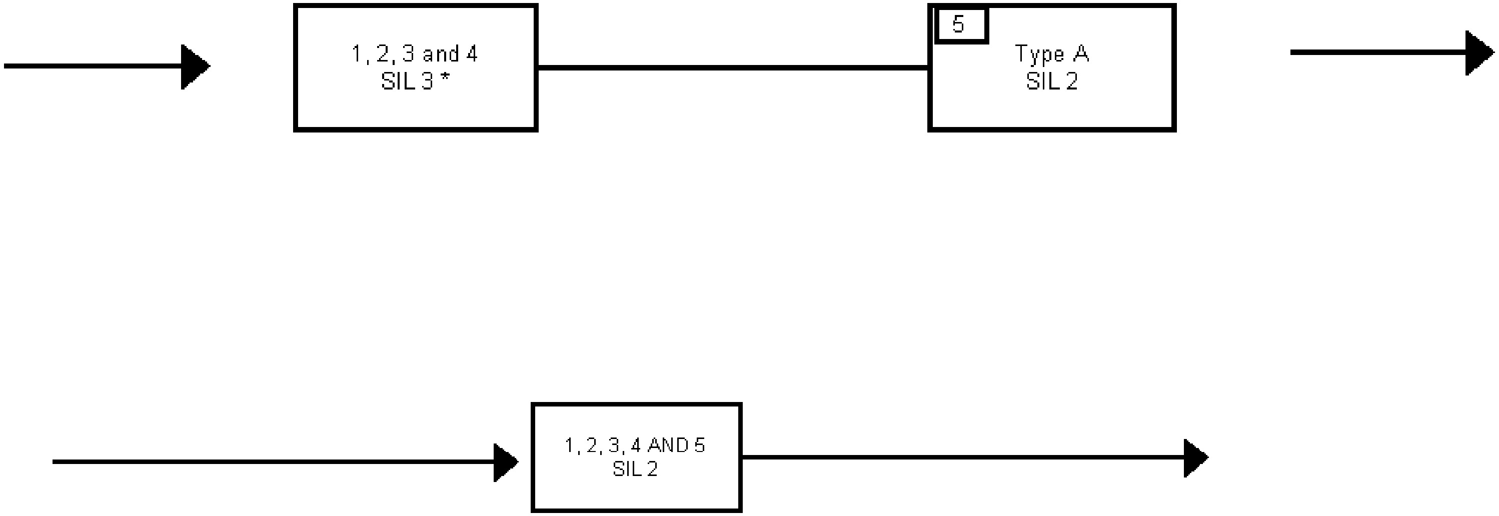
I vincoli architetturali

- I due blocchi serie possono essere semplificati in un blocco ciascuno

- Per i blocchi in parallelo dobbiamo considerare la tolleranza al guasto di ciascun blocco

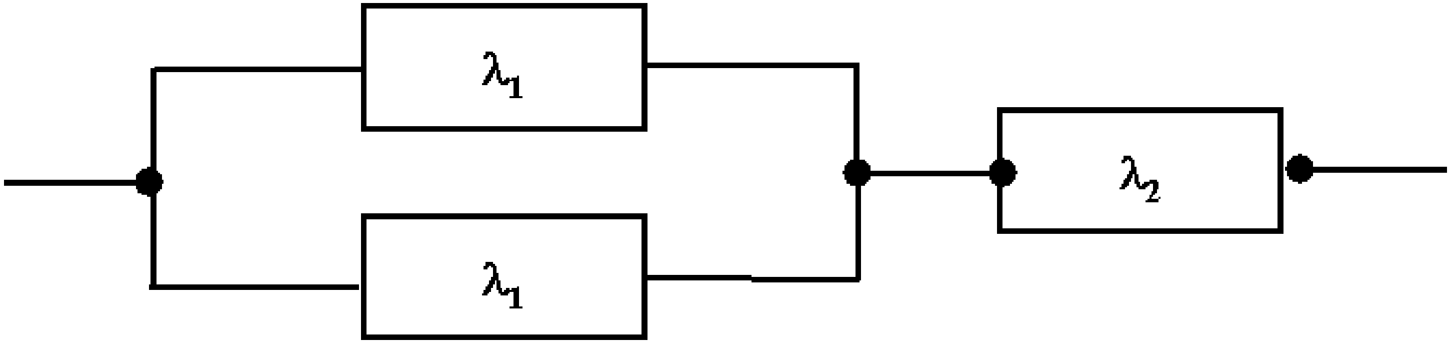


I vincoli architetturali



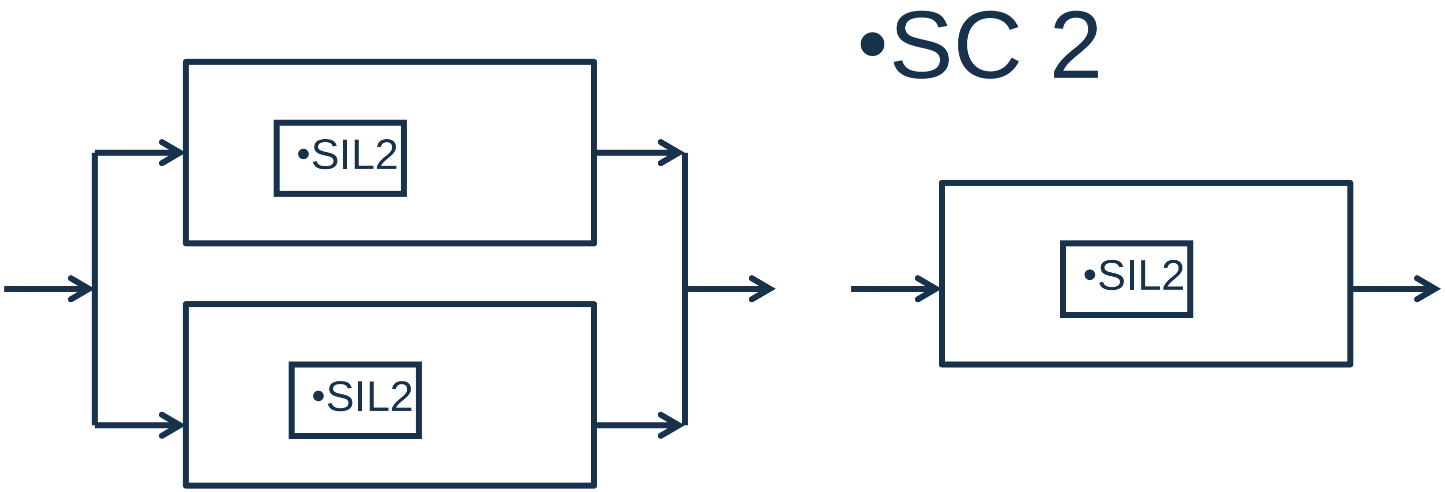
I Guasti di modo comune

- E’ possibile che uno o più canali ridondanti possano guastarsi per un guasto comune



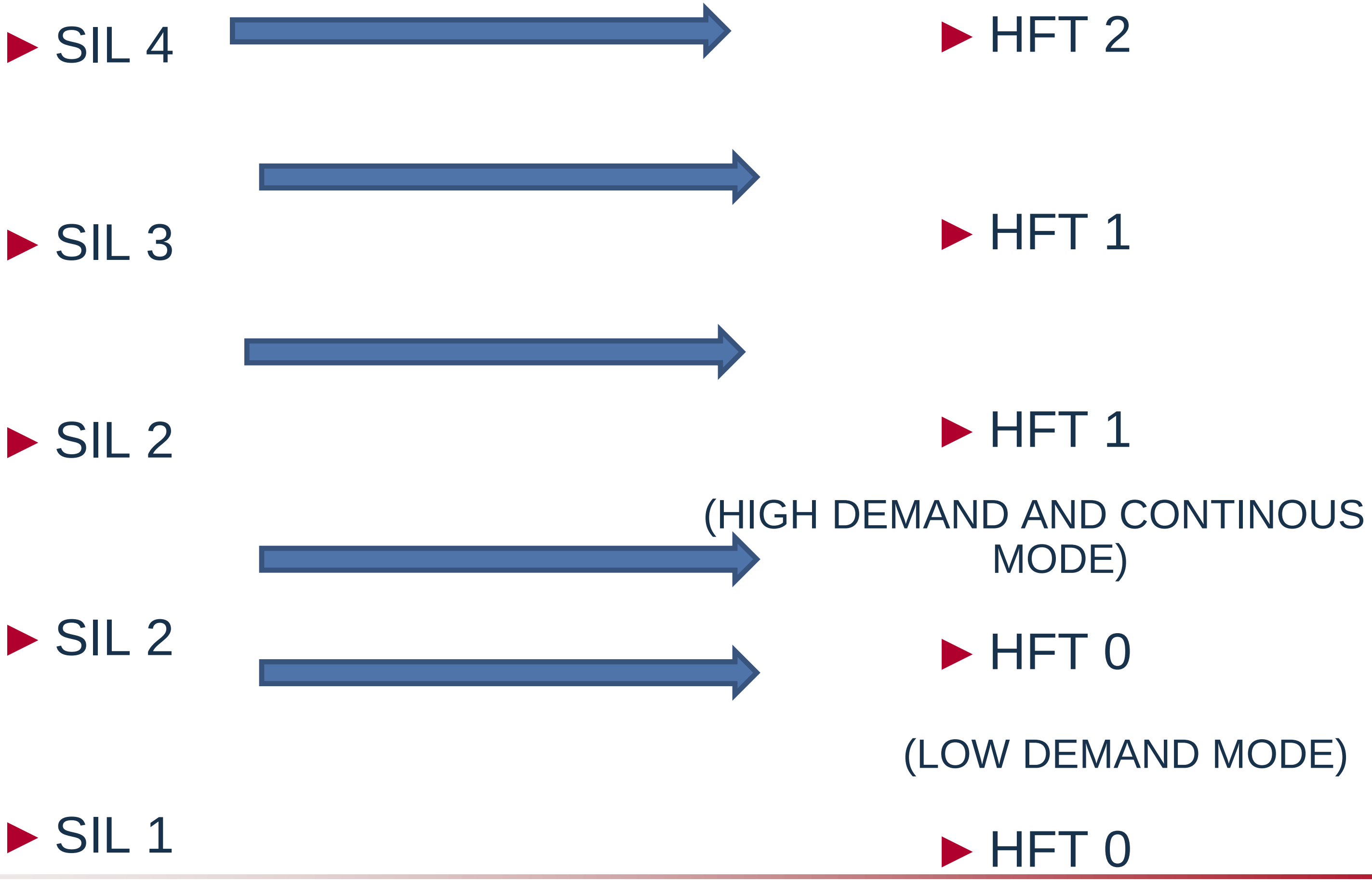
- In questa situazione la ridondanza non è efficace
- Il fattore di guasto di modo comune, indicato con ß, è particolarmente critico per i canali ridondanti identici.

Systematic Capability (SC)



- La “Systematic capabilty” 2 vincola il livello SIL level nelle architetture di canali identici
- In questa situazione la ridondanza non è efficace

TIPO “B” DC ≥ 0.6



- SIL 4
- SIL 3
- SIL 2
- SIL 2
- SIL 1

- HFT 2
- HFT 1
- HFT 1

(HIGH DEMAND AND CONTINOUS MODE)

- HFT 0

(LOW DEMAND MODE)

- HFT 0

PART 2, Hardware fault TOLEERANCE: Route 2H § 7.4.4.3.2

For type A elements only, if it is determined that by following the HFT requirements specified in 7.4.4.3.1, for the situation where an HFT greater than 0 is required, it would introduce additional failures and lead to a decrease in the overall safety of the EUC, then a safer alternative architecture with reduced HFT may be implemented. In such a case this shall be justified and documented. The justification shall provide evidence that:

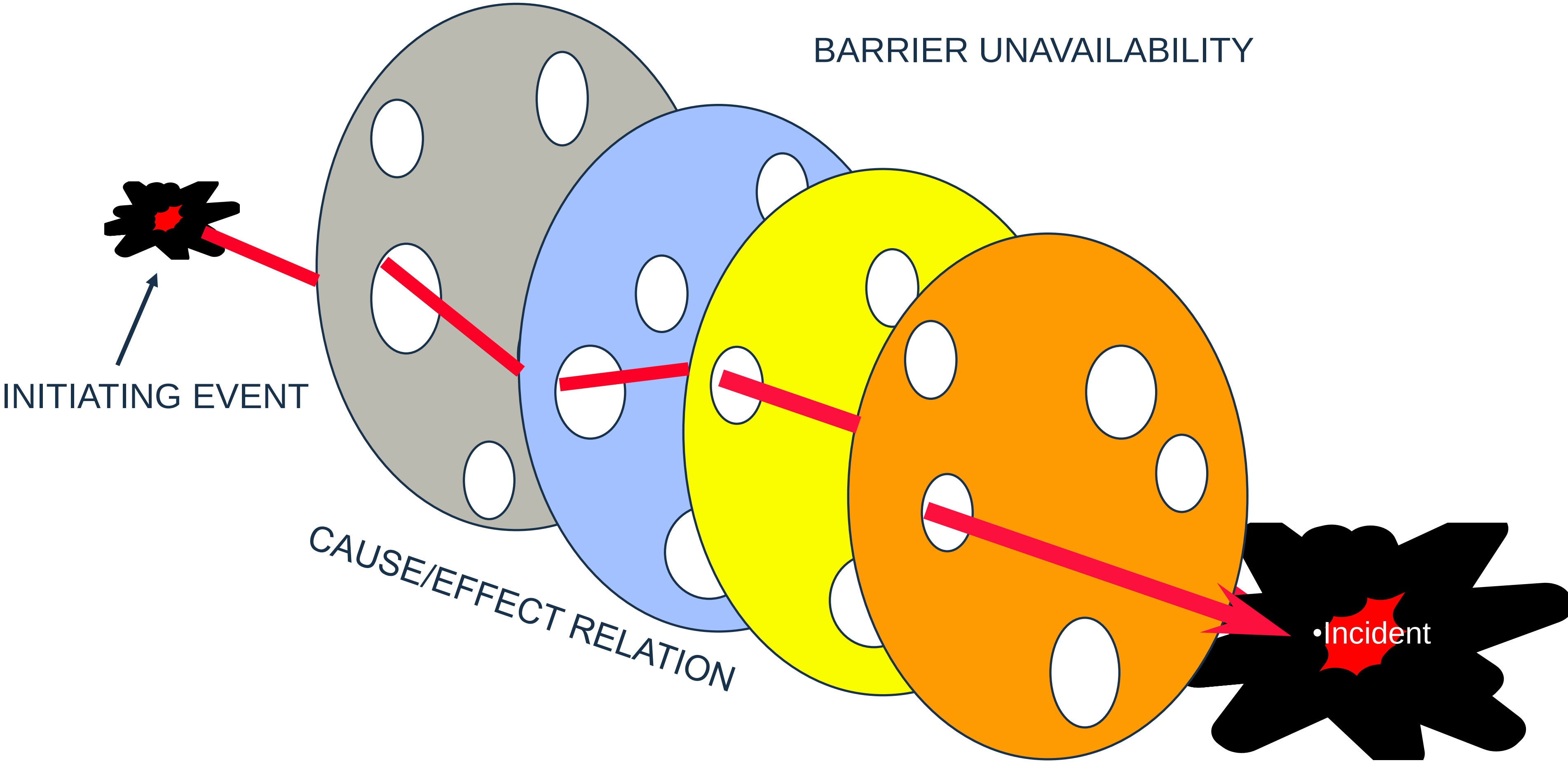
a) compliance with the HFT requirements specified in 7.4.4.3.1 would introduce additional

- failures and lead to a decrease in the overall safety of the EUC; and

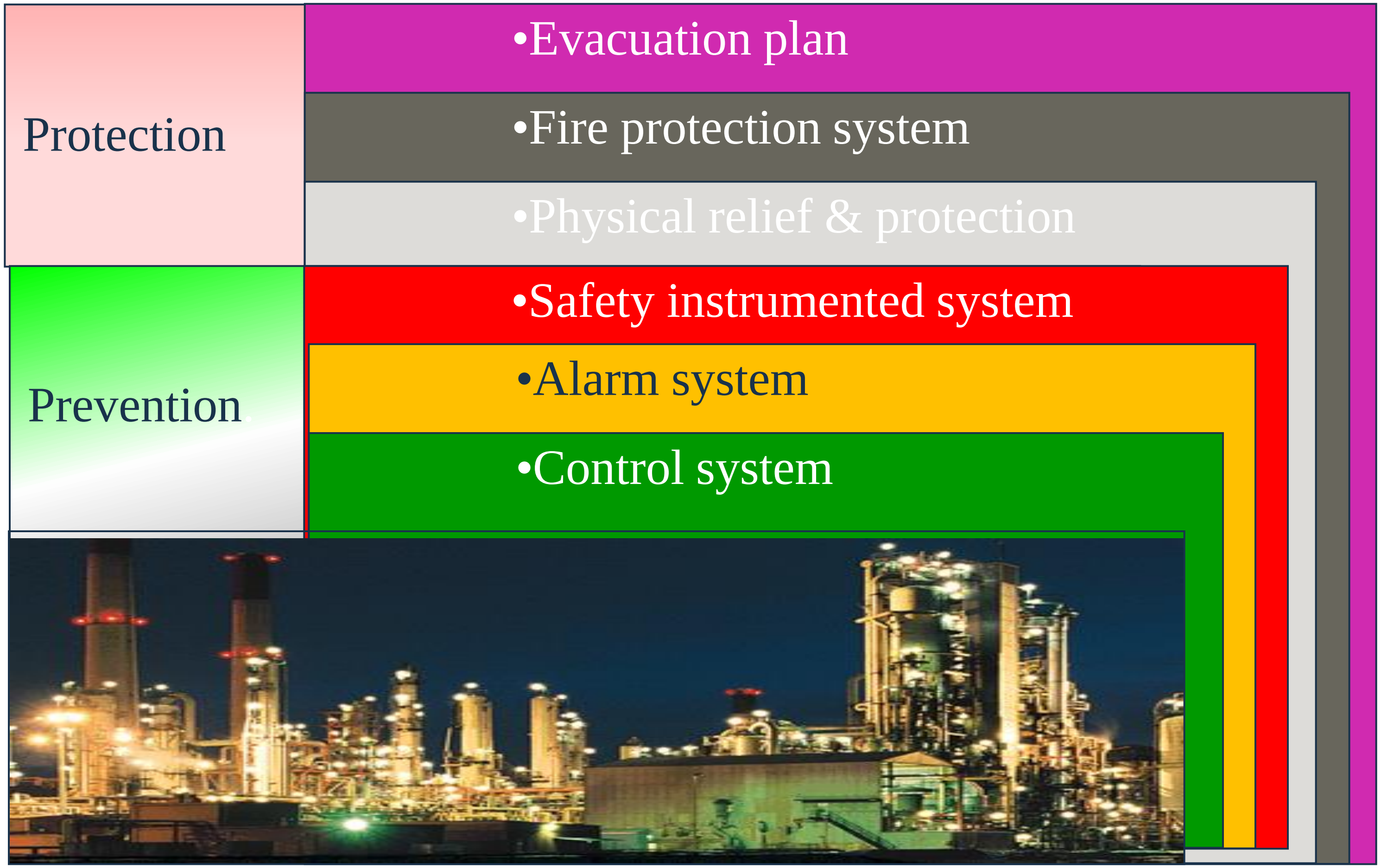
b) if the HFT is reduced to zero, the failure modes, identified in the element performing the

- safety function, can be excluded because the dangerous failure rate(s) of the identified
- failure mode(s) are very low compared to the target failure measure for the safety function
- under consideration (see 7.4.4.1.1 c)). That is, the sum of the dangerous failure
- Frequencies of all serial elements, on which fault exclusion is being claimed, should not
- exceed 1 % of the target failure measure. Furthermore the applicability of fault exclusions
- shall be justified considering the potential for systematic faults

INDEPENDENT PROTECTION LAYER CONCEPT



The Process Plant protection layers



Protection

- Evacuation plan
- Fire protection system
- Physical relief & protection

Prevention

- Safety instrumented system
- Alarm system
- Control system

Application Differences

A.1 Application Differences:

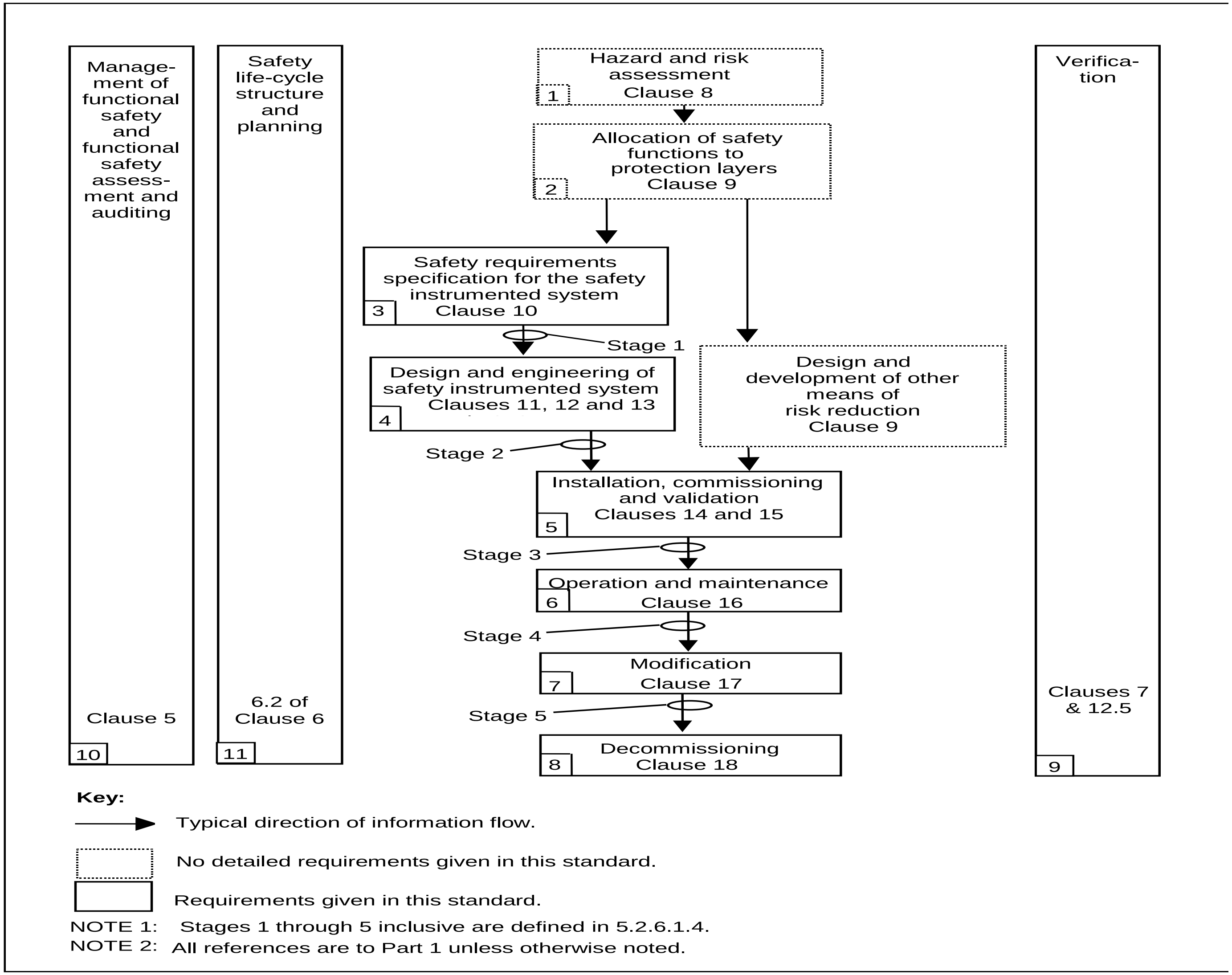
- IEC61511 relates solely to the process sector, while IEC61508 relates to all industrial sectors (e.g., machinery, process, medical, rail).

- IEC61511 addresses the process sector owner/user applications, while IEC61508 addresses the manufacturers' design requirements for the E/E/PE elements and related equipment requirements necessary to achieve the SIL claim limit assigned to each E/E/PE element and related equipment.

- IEC61511 does not address software, while IEC61508 does address software (i.e., full variability programming) utilized in SIS elements and equipment.

IEC61511 addresses application programming (i.e., limited variability languages and fixed variability language) utilized in the process sector applications.

IEC 61511 LIFECYCLE


Management of functional safety and functional safety assessment and auditing
Clause 5
10
Safety life-cycle structure and planning
6.2 of Clause 6
11
Hazard and risk assessment
Clause 8
1
Allocation of safety functions to protection layers
Clause 9
2
Safety requirements specification for the safety instrumented system
Clause 10
3
Stage 1
Design and engineering of safety instrumented system
Clauses 11, 12 and 13
4
Design and development of other means of risk reduction
Clause 9
Stage 2
Installation, commissioning and validation
Clauses 14 and 15
5
Stage 3
Operation and maintenance
Clause 16
6
Stage 4
Modification
Clause 17
7
Stage 5
Decommissioning
Clause 18
8
Verification
Clauses 7 & 12.5
9

Key:

→ Typical direction of information flow.

⬚ No detailed requirements given in this standard.

□ Requirements given in this standard.

NOTE 1: Stages 1 through 5 inclusive are defined in 5.2.6.1.4.

NOTE 2: All references are to Part 1 unless otherwise noted.

What’s new in IEC 61511 Ed. 2

- DEFINITIONS
- SIL4
- HARDWARE FAULT TOLERANCE RULES
- BCPS/CONTROL SYSTEM
- APPLICATION SOFTWARE
- SAFETY MANUAL

Definitions

- SAFETY INTEGRITY = DEPENDABILITY (J. C, Laprie, 1989)
  - dependability is a measure of a system's availability, reliability, and its maintainability. This may also encompass mechanisms designed to increase and maintain the dependability of a system.
- DIAGNOSTIC COVERAGE
  - FRACTION OF DANGEROUS FAILURES
- FAULT EXCLUSION (REF. EN 13 849) – ROUTE 2H, § 7.4.4.3.2
- PRIOR USE = PROVEN IN USE

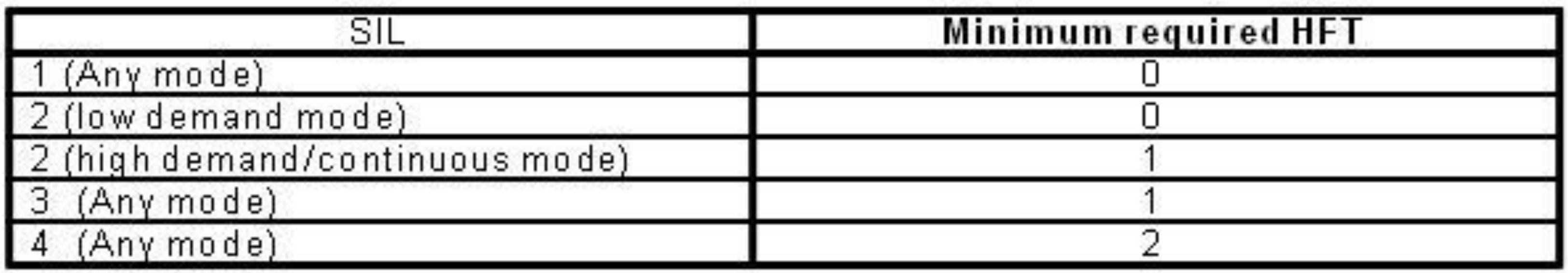
Improvements

- APPLICATION PROGRAM SIS SAFETY LIFE CYCLE REQUIREMENTS
- SECURITY RISK ASSSESSMENT (SIS VULNERABILITY) OBLIGATION WITH OWNER
- SAFETY REQUIREMENTS SPECIFICATION EXTENSION
  - PROCESS OPERATING MODES
  - EXTREMES OF ENVIRONMENTAL CONDITIONS DURING SHPPING SORAGE, INSTALLTION AND EPERATION
- HARDWARE FAULT TOLERANCE
- ROUTE 2H
- § 11.4.6, § 11.4.7, § 11.4.8, § 11.4.9

IEC 61511 – Minimum hardware fault tolerance						
Table 5 – PE logic solvers					Table 6 – other devices	
SIL	**Minimum hardware fault tolerance**				**SIL**	**Minimum hardware fault tolerance**
	SFF< 60%	**SFF 60% to 90%**	**SFF >90%**			
1	**1**	**0**	**0**		**1**	**0**
2	**2**	**1**	**0**		**2**	**1**
3	**3**	**2**	**1**		**3**	**2**
4	**see IEC 61508**				**4**	**see IEC 61508**

Table 3 from IEC 61508 – Architectural constraints on Type B			
Safe Failure Fraction	**Hardware fault tolerance**		
	0	**1**	**2**
<60%	**Not Allowed**	**SIL1**	**SIL2**
60% to <90%	**SIL1**	**SIL2**	**SIL3**
90% to <99%	**SIL2**	**SIL3**	**SIL4**
≥99%	**SIL3**	**SIL4**	**SIL4**

TABLE 6 - § 11.4.6



SIL	Minimum required HFT
1 (Any mode)	0
2 (low demand mode)	0
2 (high demand/continuous mode)	1
3 (Any mode)	1
4 (Any mode)	2

11.4.6 If the minimum HFT as specified in Table 6, would result in decreased overall process safety then the HFT may be reduced. This shall be justified and documented. The justification shall provide evidence that the proposed architecture is suitable for its intended purpose and meets the safety integrity requirements.

SIL 4

General requirements

11.5.2.1 Components and subsystems selected for use as part of a safety instrumented system for SIL 1 to SIL 4 applications shall either be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate, or else they shall be in accordance with 11.4 and 11.5.3 to 11.5.6, as appropriate.

11.5.2.2

For an SIS implementing a SIL 4 functions then the following shall apply:

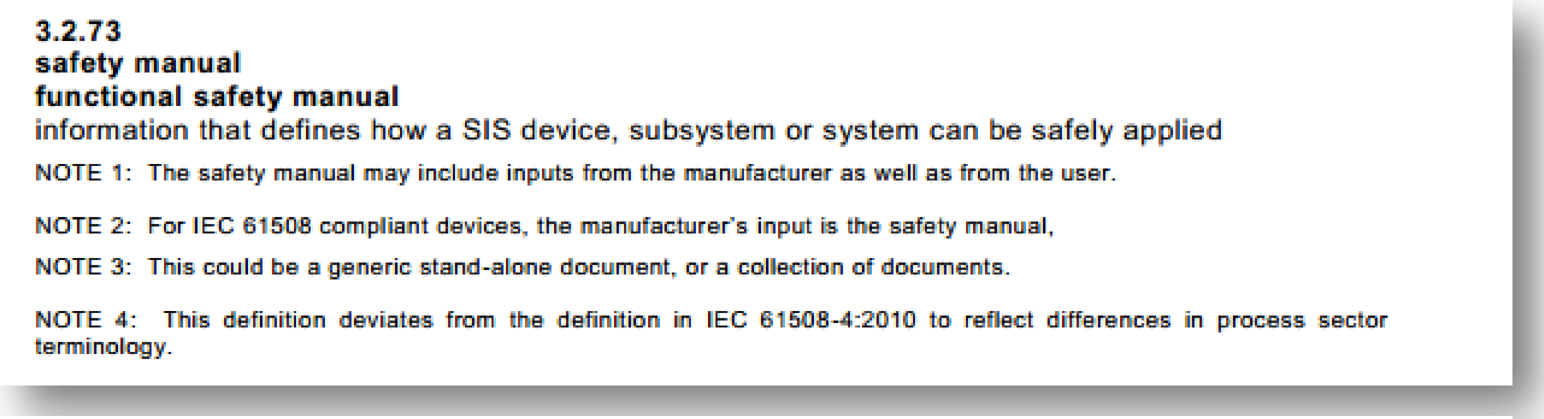
a) All system elements shall be proven by prior use in safety applications

b) hard wired non programmable elements shall be used

The Safety Manual (IEC 761508-2, ANNEX D)

- D1. The purpose of the safety manual for compliant items is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of this standard.
- D.2.2 For every function, the safety manual shall contain:
- ………..
- d) the failure modes of the diagnostics, internal to the compliant item (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the diagnostics to detect failures of the function;
- i) for those failure modes, in respect of a specified function, that are capable of being detected by external diagnostics, sufficient information shall be provided to facilitate the development of an external diagnostics capability. The information shall include details of failure modes and for those failure modes the failure rates.

What is stated in IEC 61511-1



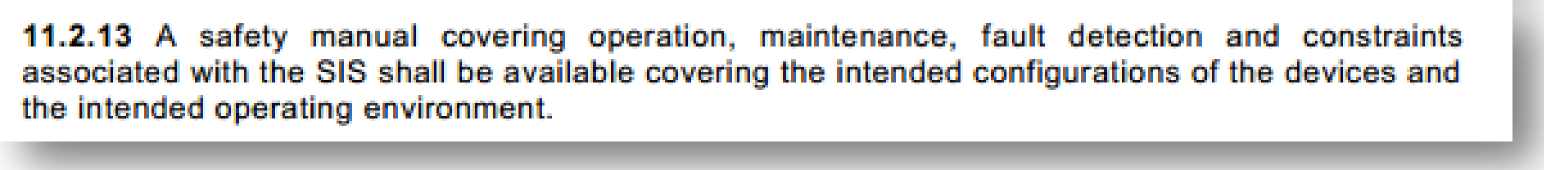
3.2.73
safety manual
functional safety manual
information that defines how a SIS device, subsystem or system can be safely applied

NOTE 1: The safety manual may include inputs from the manufacturer as well as from the user.

NOTE 2: For IEC 61508 compliant devices, the manufacturer's input is the safety manual,

NOTE 3: This could be a generic stand-alone document, or a collection of documents.

NOTE 4: This definition deviates from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

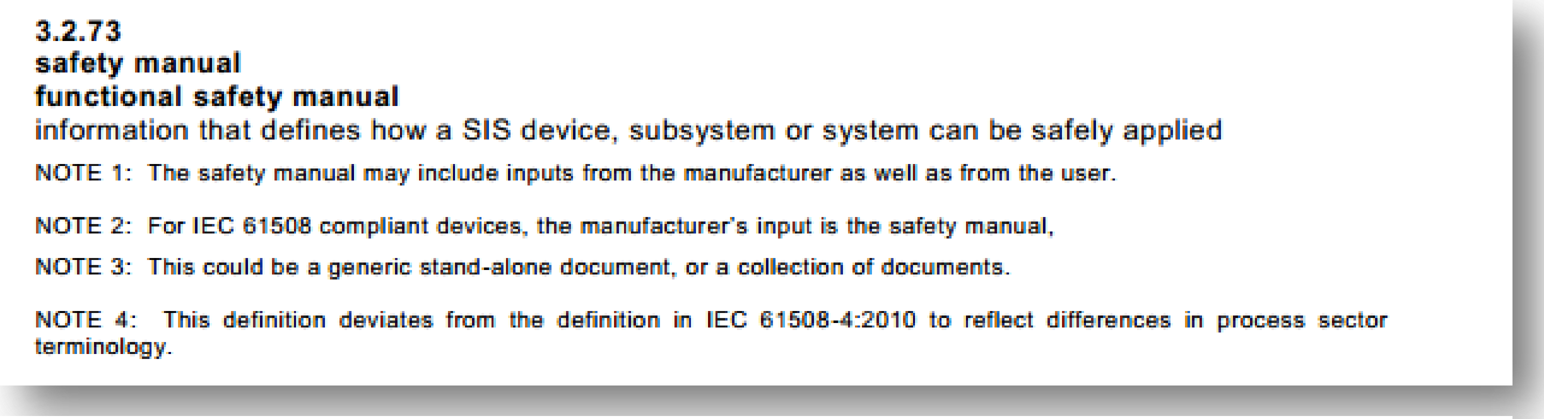


11.2.13 A safety manual covering operation, maintenance, fault detection and constraints associated with the SIS shall be available covering the intended configurations of the devices and the intended operating environment.

•SM per IEC 61511:

- is the responsibility of end user
- Is not made generic, but for a specific installation/application
- comprises input from SMs per IEC 61508 (for IEC 61508 compliant items) plus other input needed to document safe use of prior use components and/or logic solvers and SIS loops.

What is stated in IEC 61511-1



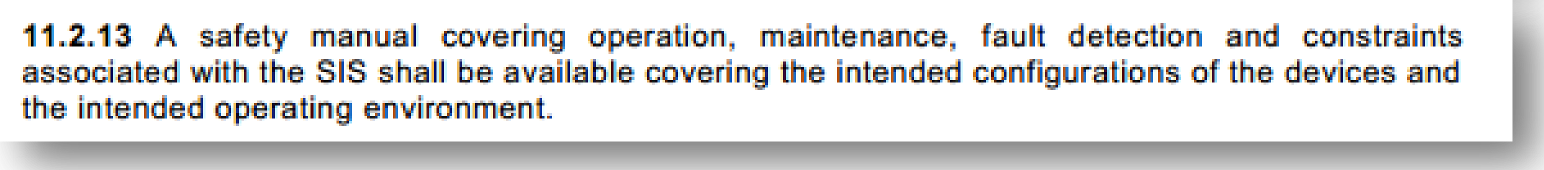
3.2.73
safety manual
functional safety manual
information that defines how a SIS device, subsystem or system can be safely applied

NOTE 1: The safety manual may include inputs from the manufacturer as well as from the user.

NOTE 2: For IEC 61508 compliant devices, the manufacturer's input is the safety manual,

NOTE 3: This could be a generic stand-alone document, or a collection of documents.

NOTE 4: This definition deviates from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.



11.2.13 A safety manual covering operation, maintenance, fault detection and constraints associated with the SIS shall be available covering the intended configurations of the devices and the intended operating environment.

But is not this type of information already provided in other documents provided by many manufacturers and system integrators?

What is stated in IEC 61511-2

IEC 61511-2 says:

The purpose of the safety manual is to document all the necessary information related to how a device, SIS subsystem, or system can be **safely applied**.[A.11.2.13]

Proposed content (A.11.2.13):

- Description and topology
- Revision and constraints (AP, HW, FW)
- Operational description, incl. fail-safe operation
- Assumptions related to operation, maintenance, and testing
- Restrictions safety functions (e.g. configuration settings)
- Failure modes and rates
- Other reliability data (DC, MTTR, test intervals)

•A.11.2.13 bullet list may be improved. Duplicated points

What is stated in IEC 61511-2

Some of this information is beyond “can be safely applied“?

Covered by other documents, such as SM per IEC 61508 if existing?

Proposed content (A.11.2.13):

- ► Description and topology
- ► Revision and constraints (AP, HW, FW)
- ► Operational description, incl. fail-safe operation
- ► Assumptions related to operation, maintenance, and testing
- ► Restrictions safety functions (e.g. configuration settings)
- ► Failure modes and rates
- ► Other reliability data (DC, MTTR, test intervals)

•A.11.2.13 bullet list may be improved. Duplicated points

Points for discussion

Produced by whom?

- End users involvement and responsibility. Allocated to system integrator/engineering during project execution, but what about operational phase?

Produced when:

- During design phase
- Must be provided for non-compliant items
- Must be provided for plant-specific considerations: application program, proof testing of subsystems and whole loop

Purpose?

- What is necessary to demonstrate “can be safety applied”?
- Focus on compliance to safe design requirements, or the application (operation, maintenance and modifications)?
- Example: *How to carry out proof tests (beyond function testing)*

Relation to other documents:

- Manufacturer & system integrators input is SM per IEC 61508 and “Operation and maintenance manual+”

Points for discussion

What type of
safety manual?

"Device". Low-complexity, non E/E/PE

IEC 61508 SM only

Or IEC 61511 SM for prior use

"Logic solver with application program"

IEC 61508 SM

IEC 61511 SM to cover application program & interface

"VSD drive"

IEC 61508 SM (if existing)

IEC 61511 SM to cover installation-specific issues

"Device": E/E/PE

IEC 61508 SM only

Points for discussion

Safety manual for device (field devices):

- Per 61508 OR
- Per IEC 61511

Safety manual a subsystem (e.g. logic solver):

- Safety manual per 61508 for generic typicals
- Safety manual per IEC 61511 for application program and plant specific considerations
- Can be covered by “updating” the operation and maintenance manual?

Safety manual for a whole SIS system:

- Non-existing
- SRS gives references to all SMs and compliance reports

Safety manual in GL070

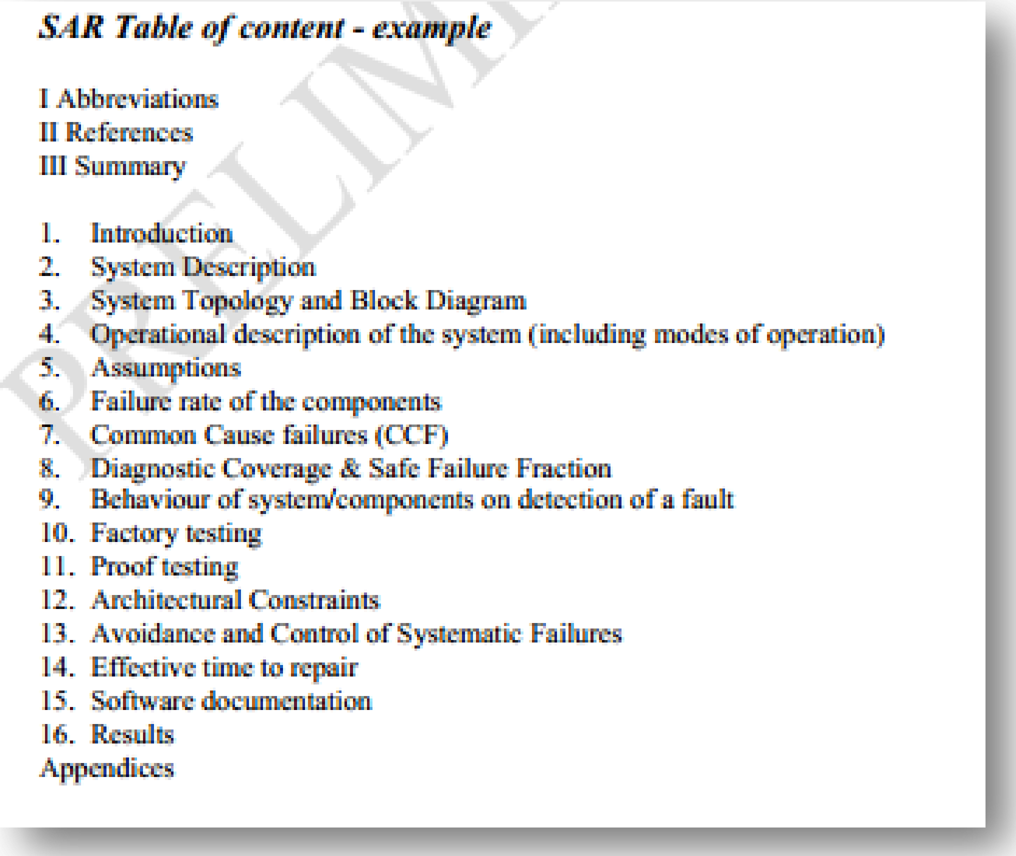
- Called “Safety analysis report” (SAR)
- Introduced as a concept in 2004
- SAR shall document the SIL capability of the various SIS equipment and components. These reports may include a number of assumptions that have relevance for operation:
  - Requirements and recommendations related to operation, maintenance and proof testing (e.g. tools, methods and test intervals)
  - Constraints related to response times, closure times, demand rates and other parameters relevant for the SIS performance

SAR

- Main purpose is to demonstrate compliance of a delivery (“specific application”)
- To be produced by each equipment supplier
- Can be more simple and generic for devices
- More extensive for subsystems (logic solvers) and systems (fire detection system, fire pump system) – and may comprise generic as well as application specific information

Same as SM per IEC 61511?

Extensive version:



SAR Table of content - example

I Abbreviations
II References
III Summary

1. Introduction
2. System Description
3. System Topology and Block Diagram
4. Operational description of the system (including modes of operation)
5. Assumptions
6. Failure rate of the components
7. Common Cause failures (CCF)
8. Diagnostic Coverage & Safe Failure Fraction
9. Behaviour of system/components on detection of a fault
10. Factory testing
11. Proof testing
12. Architectural Constraints
13. Avoidance and Control of Systematic Failures
14. Effective time to repair
15. Software documentation
16. Results

Appendices

Concluding remarks and basis for further discussions

- It is not very clear what the safety manual should contain
  - Modify/align existing **operation and maintenance manual**
- Collection of information/document that is not covered elsewhere or where the information would be difficult to subtract from a high number of document, e.g. proof/function test strategy and constraints/restrictions to consider in case of modifications.
- For whom should the manual be prepared?
  - Hardware designers
  - Assessors and reliability analysts
  - Application program developers
  - Engineers in end user organization ("equipment responsible")?
  - Operators and maintenance personnel in plant?

BUREAU VERITAS 1828

BUREAU
VERITAS

Move Forward with Confidence