

---

# COMMON ISSUES ON THE ADOPTION OF IEC 61508 AND IEC 61511

SANDRO BOLOGNA  
bologna@casaccia.enea.it  
**ENEA - CASACCIA**

SIPI61508 Workshop  
Stresa, 16-17 October, 2003

---

## **WHY SHOULD INDUSTRY COMPLY TO IEC 61508 AND IEC 61511 STANDARDS ? (1/2)**

- **INDUSTRY IS EXPECTED TO ADOPT GOOD ENGINEERING PRACTICES**
- **COMPLIANCE TO THE STANDARD WOULD SUPPORT JUSTIFICATION  
IN CASE OF UNDESIRED EVENT**
- **AVOIDING INDUSTRIAL ACCIDENTS IMPROVES COMPANY'S  
REPUTATION AND PROFITABILITY**
- **IN A HIGHLY COMPETITIVE GLOBAL MARKET IT MAKES GOOD  
BUSINESS SENSE TO COMPLY WITH NATIONAL AND  
INTERNATIONAL STANDARDS**

---

## **WHY SHOULD INDUSTRY COMPLY TO IEC 61508 AND IEC 61511 STANDARDS ? (2/2)**

- IEC 61508 WERE PUBLISHED BY CENELEC IN DECEMBER 2001 AS A EUROPEAN STANDARD WITH THE NAME OF EN61508. ALL CENELEC MEMBER COUNTRIES HAD TO IMPLEMENT EN61508 FROM AUGUST 2002. CONFLICTING NATIONAL STANDARDS HAVE TO BE WITHDRAWN BY AUGUST 2004.**
- THE SEVESO DIRECTIVE II, ALTHOUGH CONCERNS SAFETY MANAGEMENT DOES NOT MENTION IEC 61508/61511.**

---

## **YOU DON'T LIKE IEC 61508 AS IT IS TODAY?**

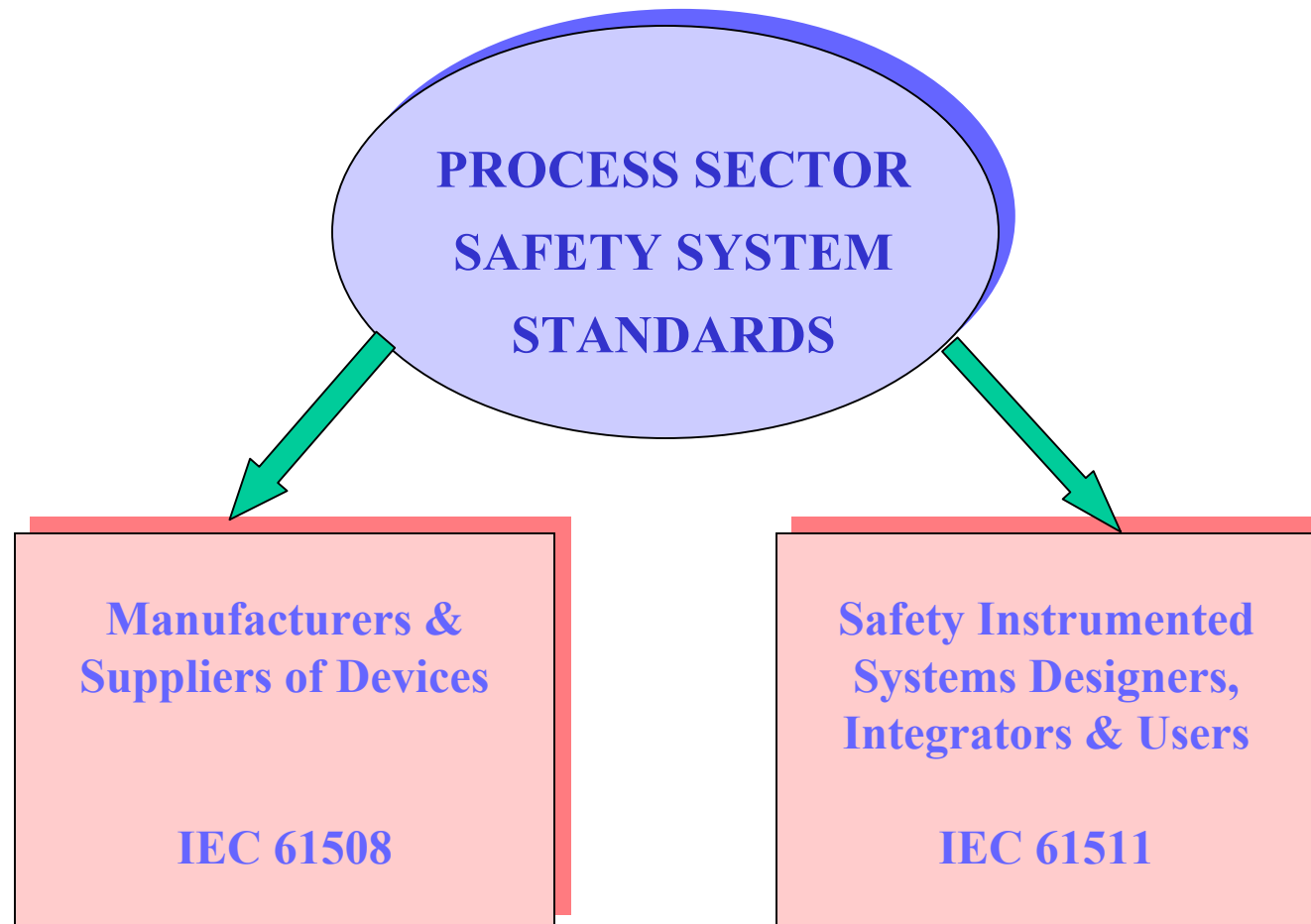
**THIS IS THE RIGHT TIME TO ASK FOR CHANGES. A REVISION OF  
IEC61508 IS IN PROGRESS THROUGH THE IEC 65A MT12 AND MT13**

## **WHAT TO DO?**

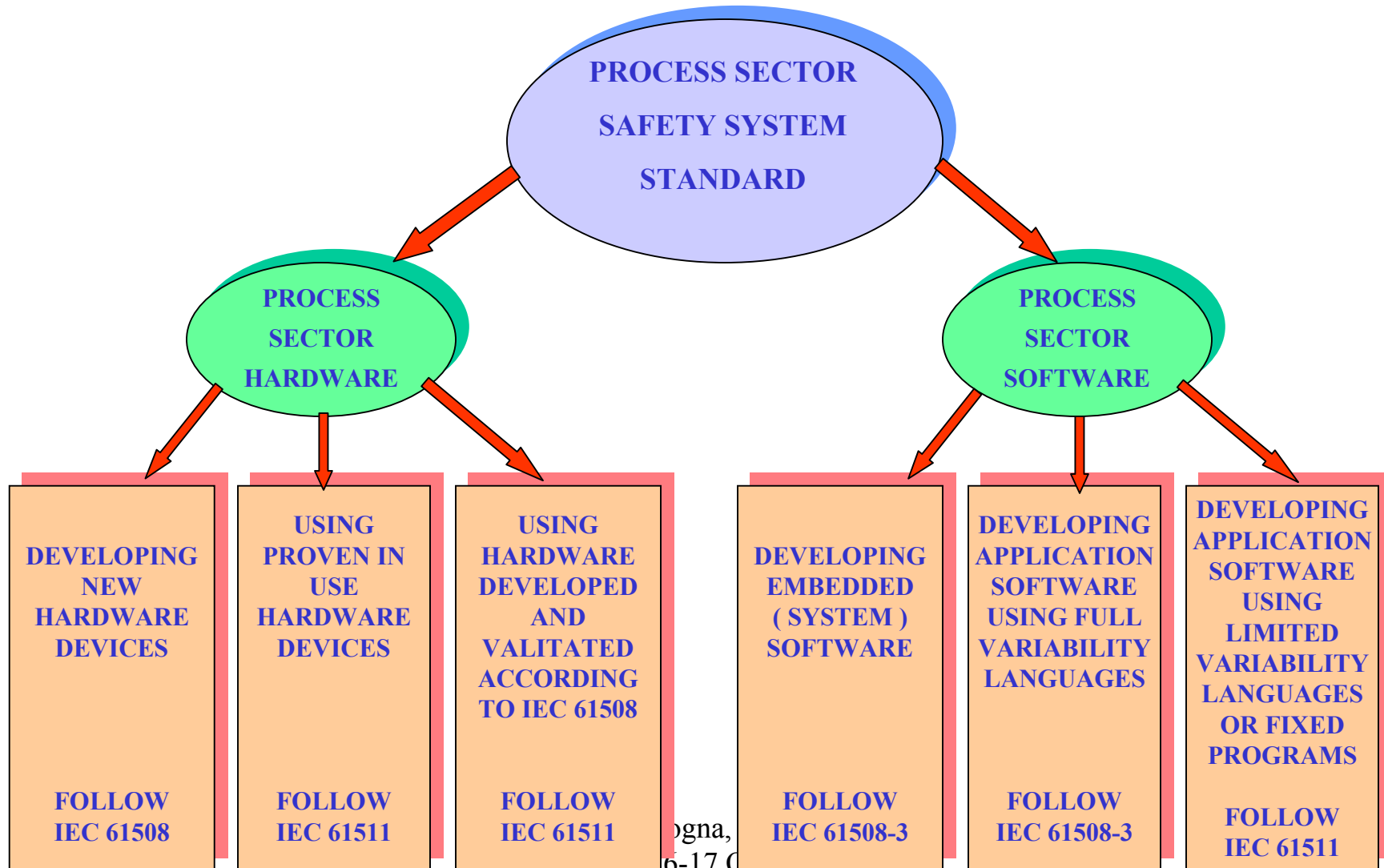
**FORWARD YOUR COMPLAINS TO YOUR IEC NATIONAL  
COMMITTEE OFFICE, IN ITALY CEI – SUBCOMMITTE 65A**

---

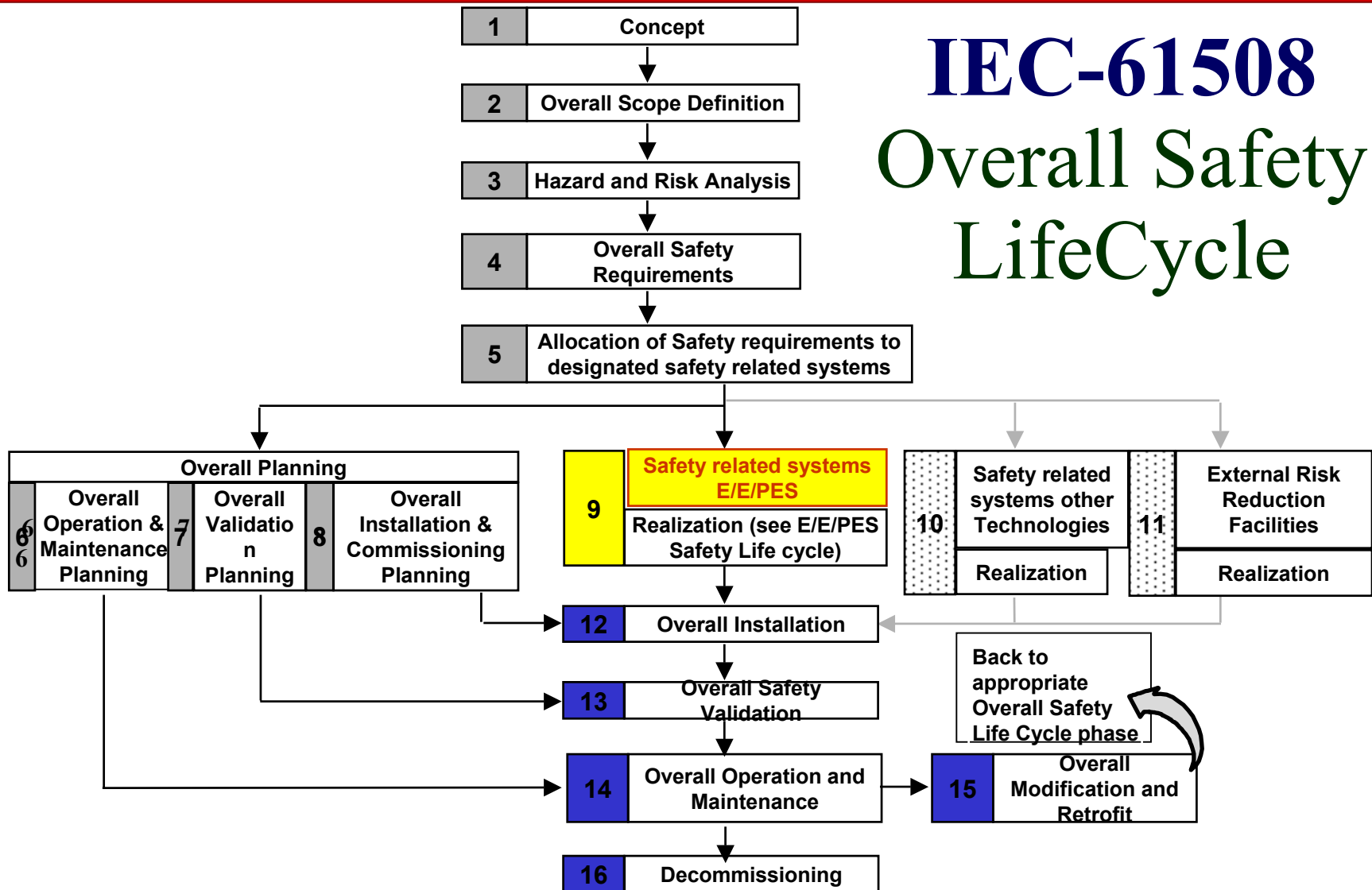
## RELATIONSHIP OF IEC 61508 & IEC 61511



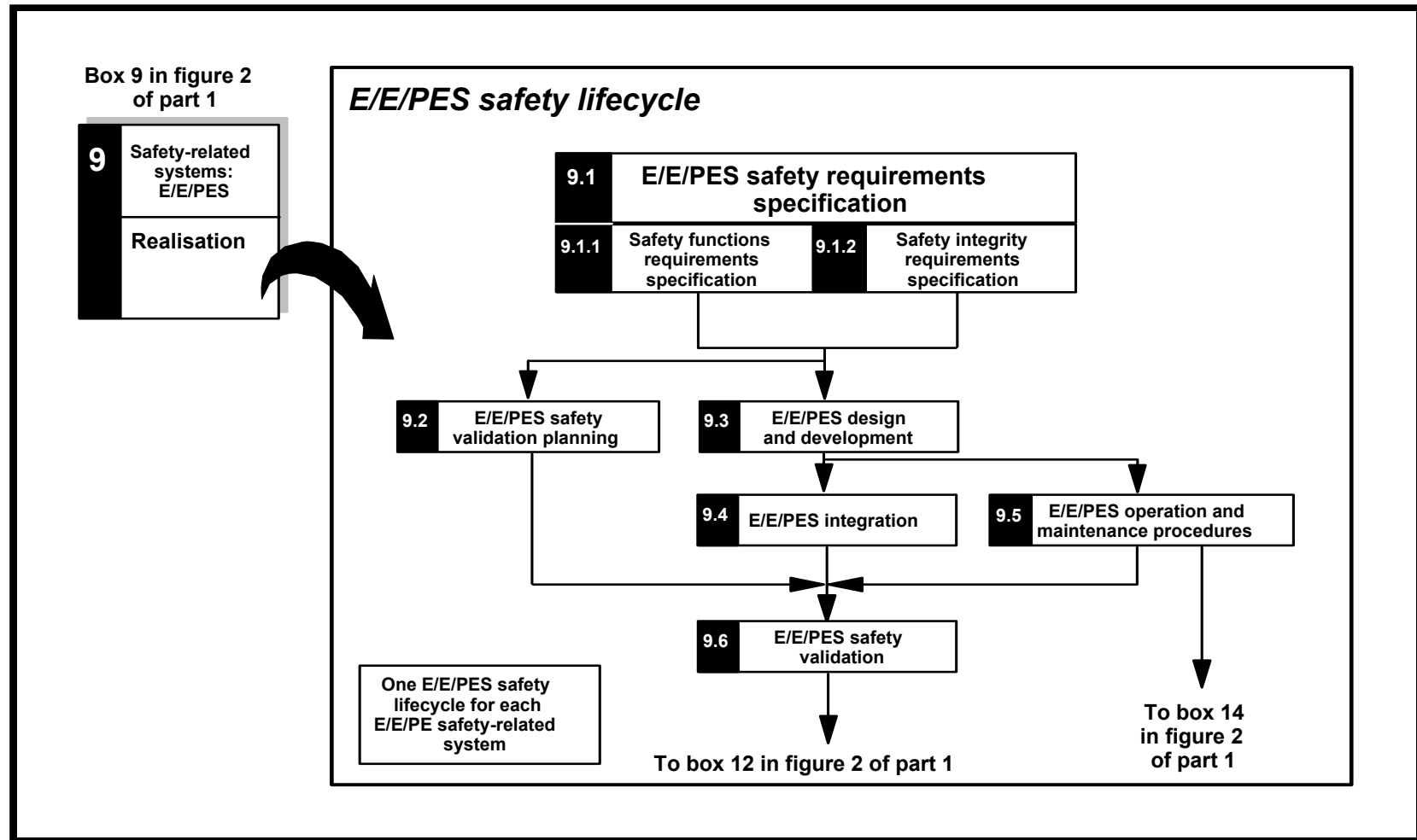
## RELATIONSHIP OF IEC 61508 & IEC 61511 (Clause 1,2 )



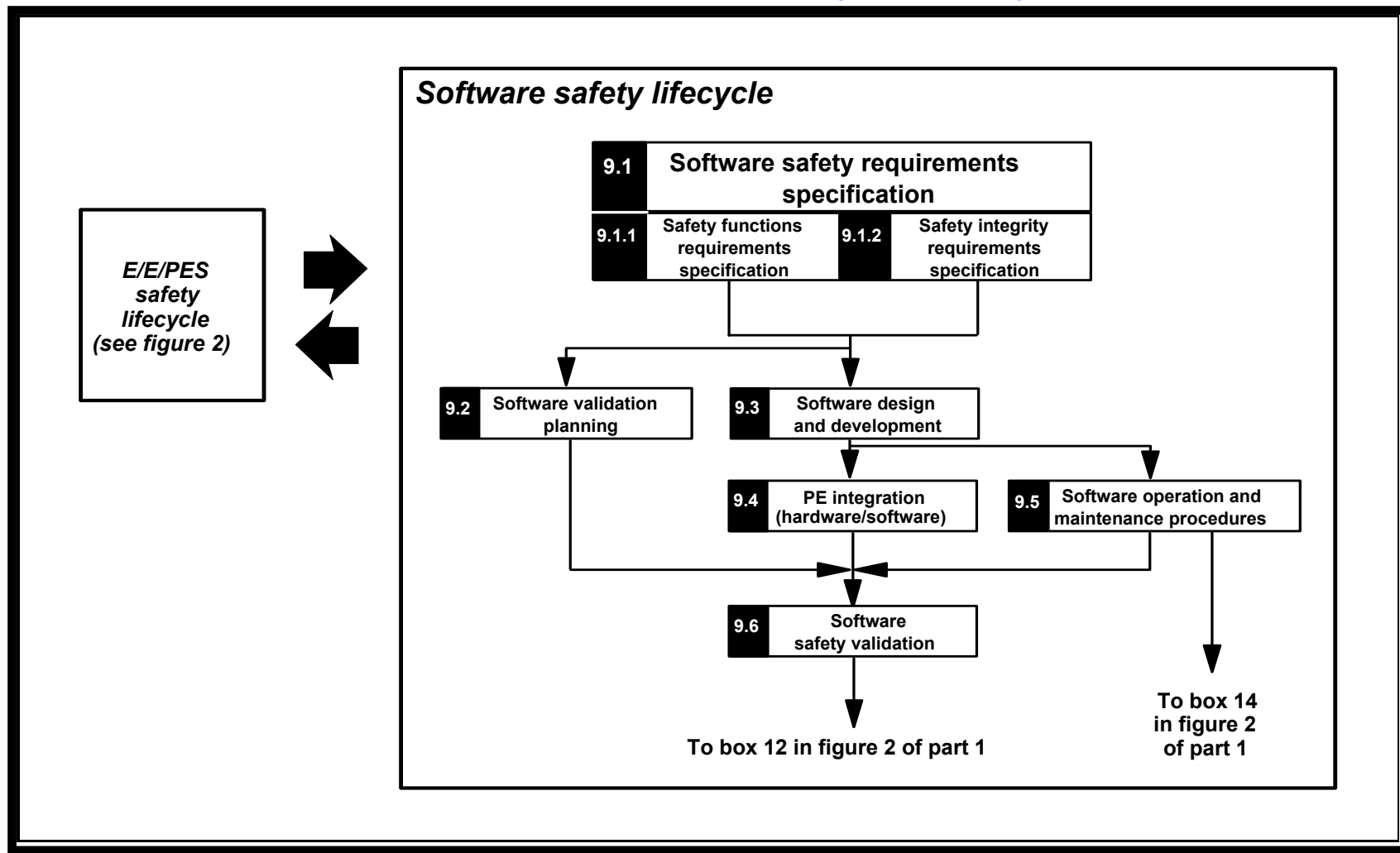
# IEC-61508 Overall Safety LifeCycle

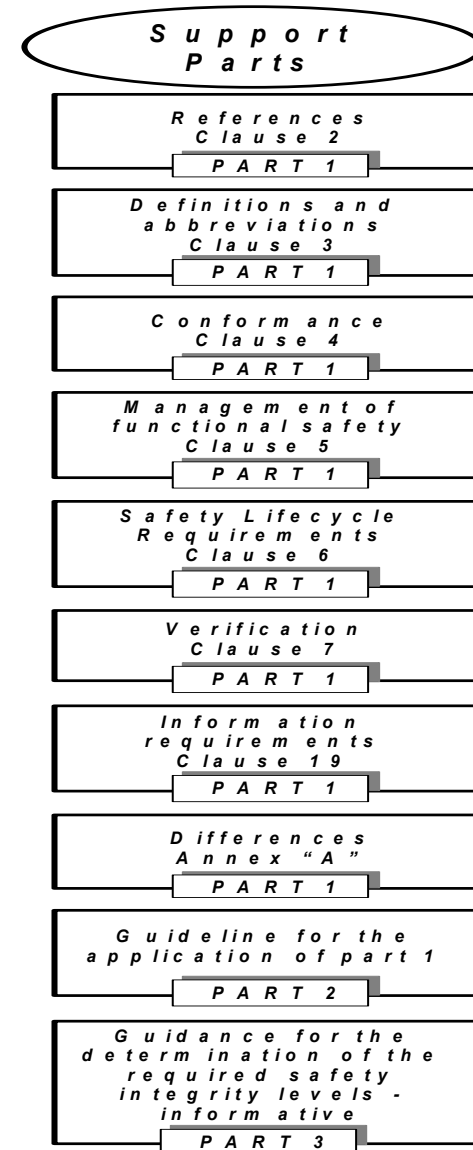
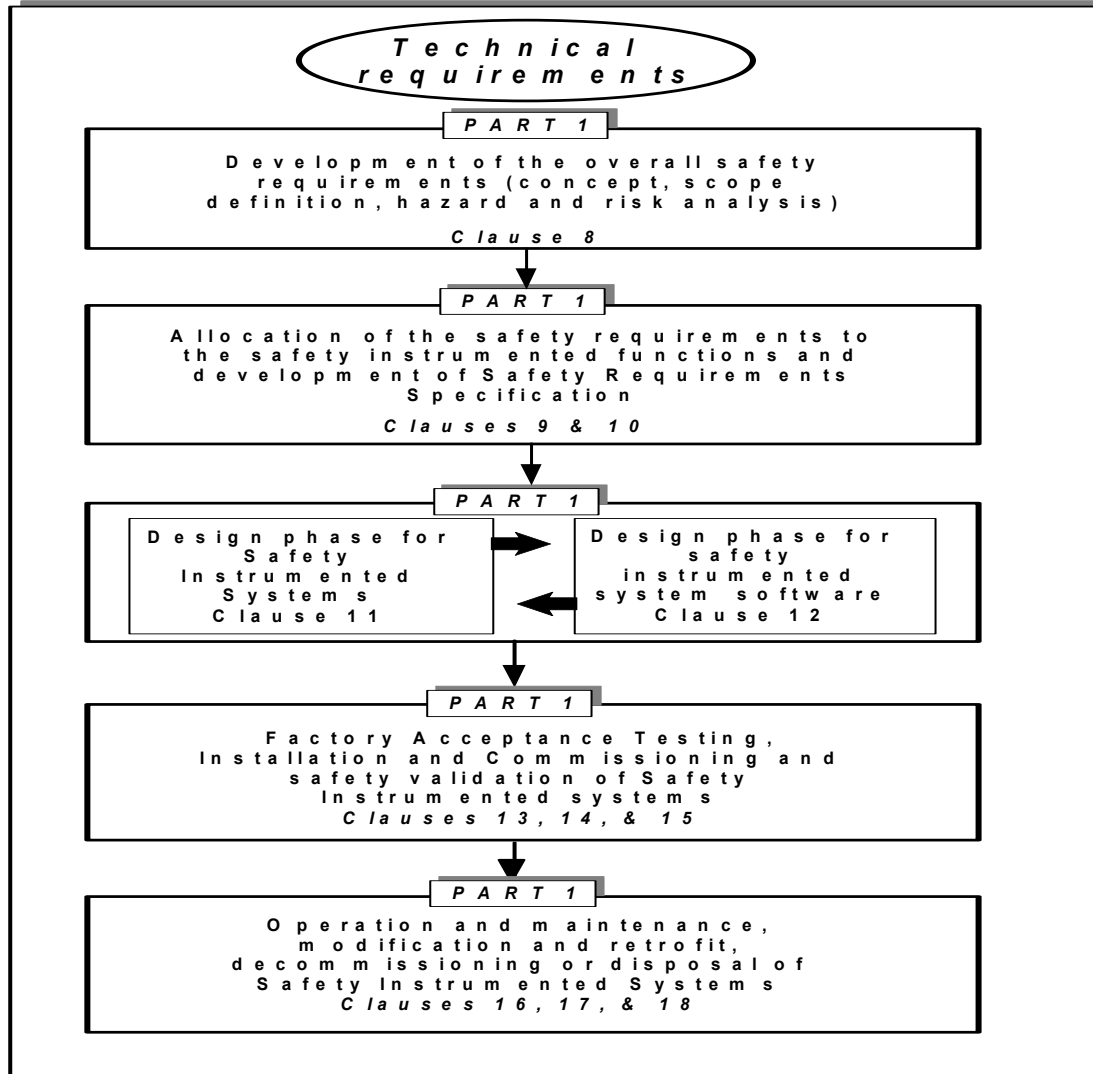


# E/E/PES safety lifecycle

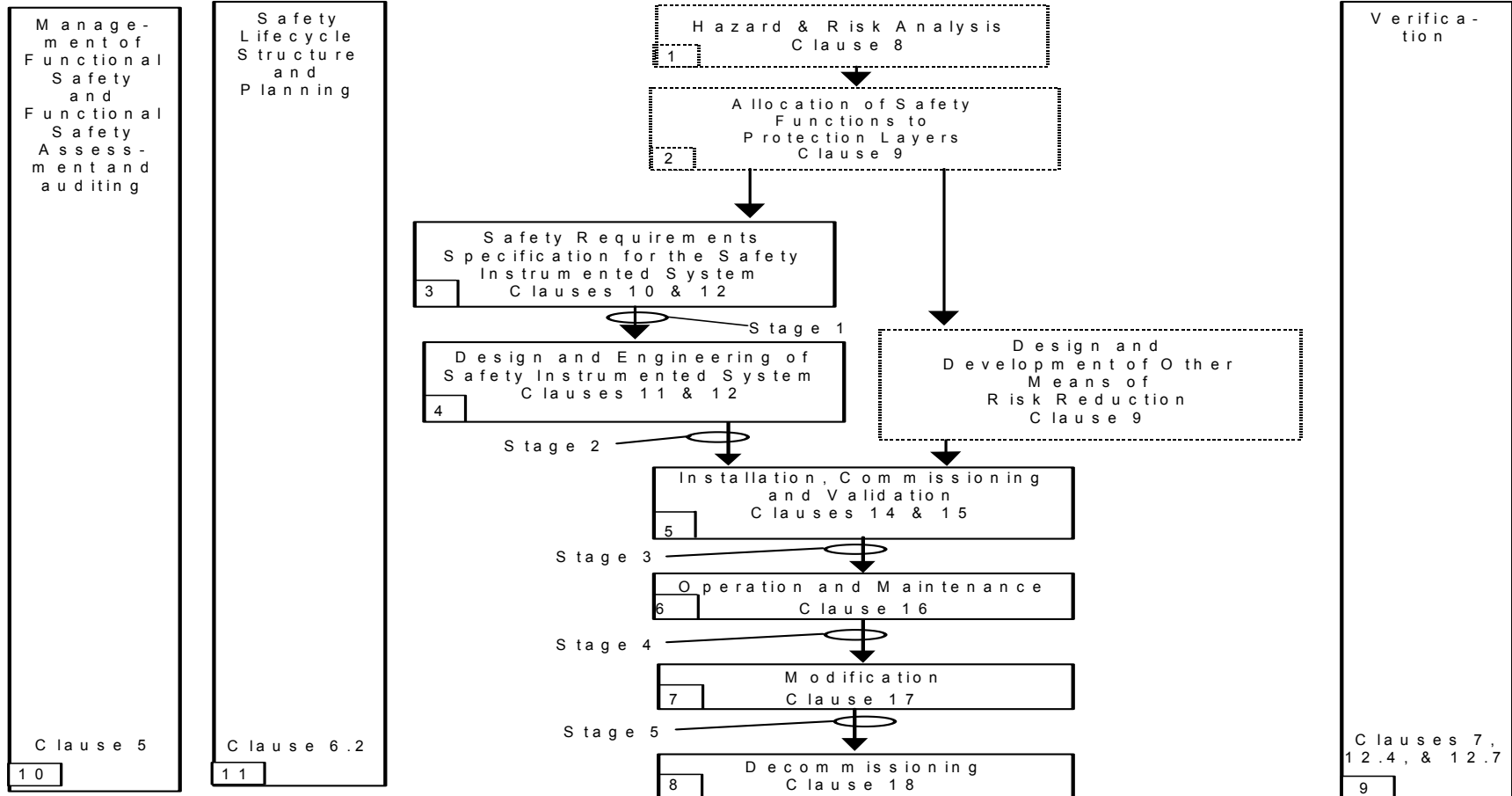


# Software safety lifecycle





**Overall framework of IEC61511 standard**



**Legend :**

- Typical direction of information flow .
- ⋯ No detailed requirements given in this standard .
- ▭ Requirements given in this standard .

**NOTES :**

1. Stages 1 through 5 inclusive are defined in clause 5.2.6.1.3 .
2. All references are for Part 1 unless otherwise noted .

---

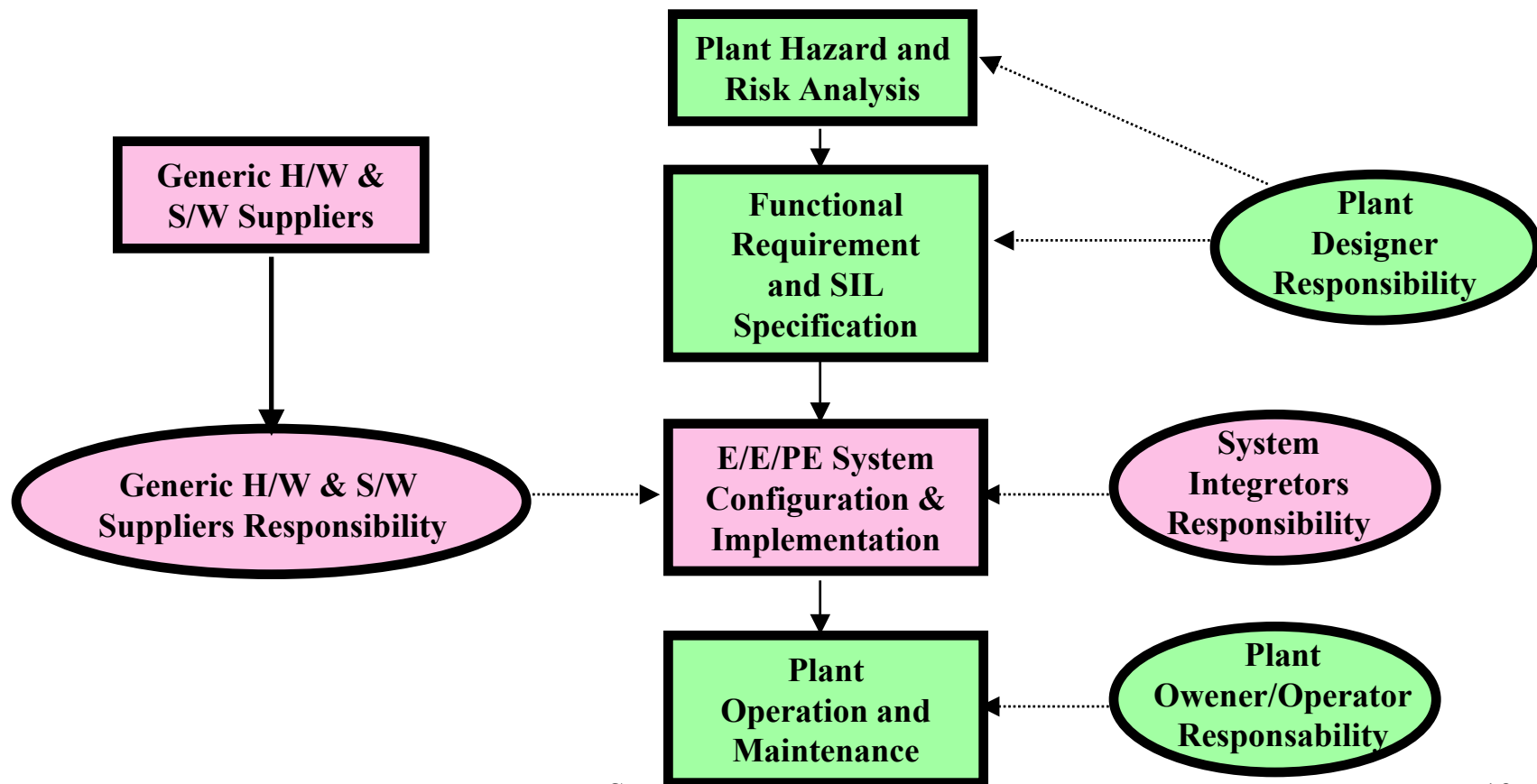
## **IEC 61508 Lifecycle vs. IEC 61511 Lifecycle**

**The IEC 61508 Lifecycle phases 1-8 and 12-16 apply to end-users and system integrators. The manufacturers of safety-related equipment need to take into account phase 9 of the overall lifecycle and the associated hardware and software lifecycles.**

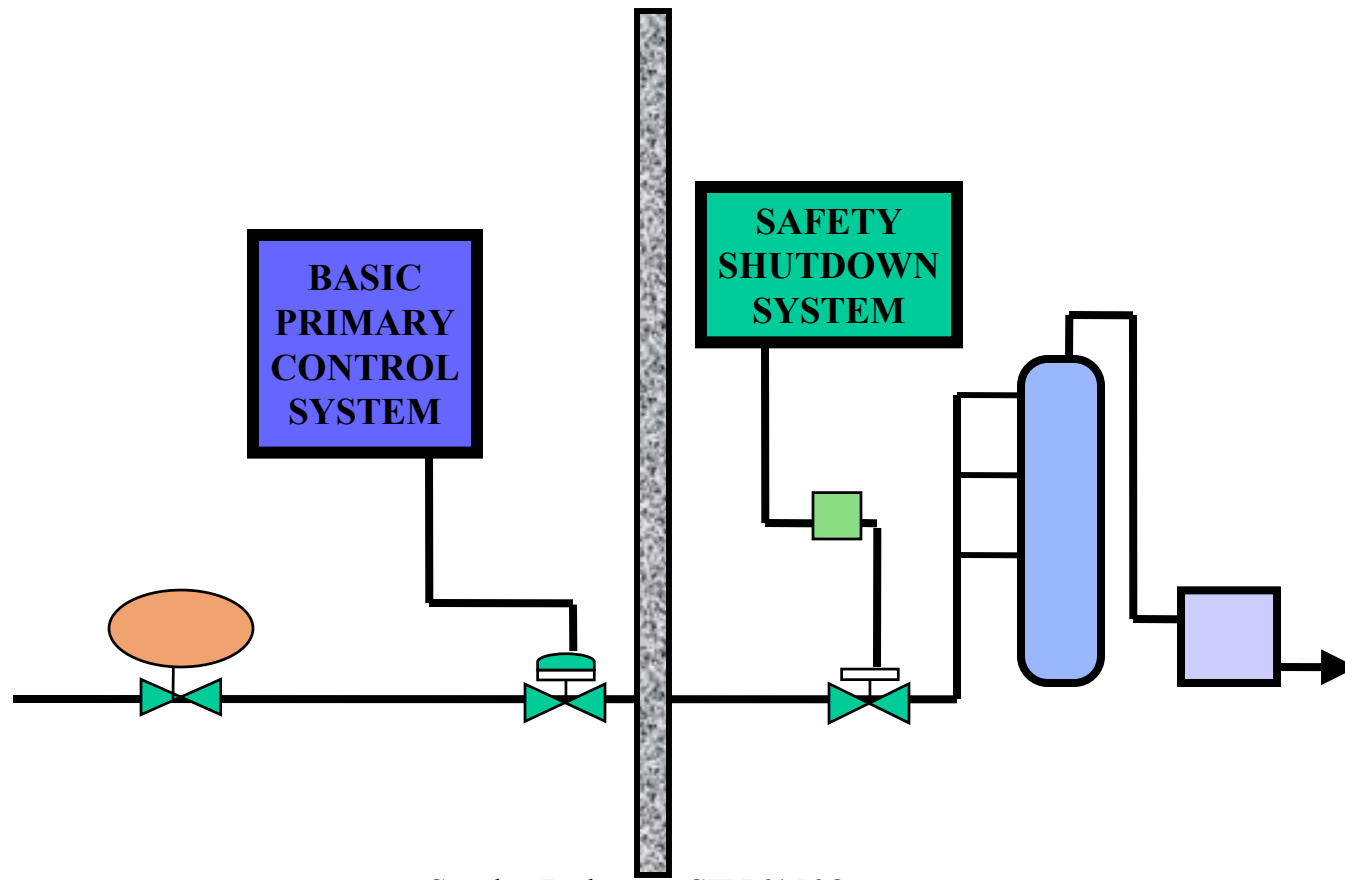
**The IEC 61511 is for end-users and integrators and thus all phases of the lifecycle of 61511 need to be taken into account.**

# Responsibilities Distribution

IEC 61508 and IEC 61511 apply to the the whole life cycle



# Separate Control and Safety Interlock



Sandro Bologna, SIPI61508  
Workshop, 16-17 October 2003

---

## SIS vs. BPCS vs. DCS

**IEC 61508 Part 2 Clause 7.4.2.3 states: “Where an E/E/PE safety-related system is to implement both safety and non-safety functions, then all the hardware and software shall be treated as safety-related unless it can be shown that the implementation of the safety and non-safety functions is sufficiently independent (i.e. that the failure on any non-safety related functions does not cause a dangerous failure of the safety-related functions). Wherever practicable, the safety-related functions should be separated from the non-safety-related functions”.**

**IEC 61511 Part 1 Clause 11.2.2 states: “Where the SIS is to implement both safety and non-safety.....”**

**IEC 61511 Part 1 Clause 11.2.3 states: “Where the SIS is to implement safety instrumented functions of different safety integrity level.....”**

---

## **SIF vs. SIL vs. SIS**

**The attribute SIL can only be used for the SIF and the underlying instrumentation loop implementing the SIF, normally referred as SIS. It cannot be used for the single components making the SIS**

## **Diagnostic Coverage vs. Proof Testing vs. Multiple Architecture**

**Multiple Architecture is not an option but it is mandatory for the different SIL**

**Diagnostic Coverage and Proof Testing can be balanced depending from cost/benefits analysis**

## IEC 61511 Cl 9 demand mode of operation vs. continuous mode of operation

<b>DEMAND MODE OF OPERATION</b>		
<b>Safety Integrity Level (SIL)</b>	<b>Average Probability of Failure on Demand</b>	<b>Risk Reduction</b>
4	$\geq 10^{-5}$ to $<10^{-4}$	$>10,000$ to $\leq 100,000$
3	$\geq 10^{-4}$ to $<10^{-3}$	$>1000$ to $\leq 10,000$
2	$\geq 10^{-3}$ to $<10^{-2}$	$>100$ to $\leq 1000$
1	$\geq 10^{-2}$ to $<10^{-1}$	$>10$ to $\leq 100$

<b>CONTINUOUS MODE OF OPERATION</b>	
<b>Safety Integrity Level (SIL)</b>	<b>Frequency of Dangerous Failures Per Hour</b>
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

**Tabella 2. Tolleranza ai guasti dell'Hardware: IEC 61508-2 Cl 7.4.3.1 vincoli progettuali per i sottosistemi di sicurezza del tipo A (nota 1)**

Safe failure fraction	Hardware fault tolerance (nota 2)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60% - 90 %	SIL2	SIL3	SIL4
90% - 99%	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

NOTA 1 un componente o sottosistema è del tipo A quando sono ben definite tutte le modalità di guasto del componente o dei componenti. Normali trasmettitori analogici, sensori del tipo interruttori di livello e di pressione, logiche a relays o a stato solido sono considerati di tipo A

NOTA 2 la tolleranza ai guasti dell'hardware rappresenta il numero massimo di guasti in un sottosistema, attribuibili a guasti casuali dell'hardware, che si possono verificare senza dar luogo ad un malfunzionamento. Una tolleranza di guasto dell'hardware pari a zero significa che un singolo guasto può essere causa di malfunzionamento.

**Tabella 3. Tolleranza ai guasti dell'Hardware: IEC 61508-2 Cl 7.4.3.1 vincoli progettuali per i sottosistemi di sicurezza del tipo B (nota 1)**

Safe failure fraction	Hardware fault tolerance (nota 2)		
	0	1	2
< 60%	not allowed	SIL1	SIL2
60% - 90%	SIL1	SIL2	SIL3
90% - 99%	SIL2	SIL3	SIL4
>99%	SIL3	SIL4	SIL4

NOTA 1 Un componente o sottosistema è del tipo B quando non è ben definita la modalità di guasto del componente o di almeno uno dei componenti. PLC, logiche programmabili, bus da campo, smart sensors, smart valves sono considerati di tipo B.

NOTA 2 La tolleranza ai guasti dell'hardware rappresenta il numero massimo di guasti in un sottosistema, attribuibili a guasti casuali dell'hardware, che si possono verificare senza dar luogo ad un malfunzionamento. Una tolleranza di guasto dell'hardware pari a zero significa che un singolo guasto può essere causa di malfunzionamento.

**Tabella 6. Tolleranza ai guasti dell'Hardware: IEC 61511-1 CI 11.4 vincoli progettuali per i sottosistemi di sicurezza del tipo A (nota 1)**

<b>Integrity Levels</b>	<b>Minimum Fault Tolerance (nota 2)</b>
SIL 1	0
SIL 2	1
SIL 3	2
SIL 4	Special requirements apply – see IEC 61508

NOTA 1 un componente o sottosistema è del tipo A quando sono ben definite tutte le modalità di guasto del componente o dei componenti. Normali trasmettitori analogici, sensori del tipo interruttori di livello e di pressione, logiche a relays o a stato solido sono considerati di tipo A

NOTA 2 la tolleranza ai guasti dell'hardware rappresenta il numero massimo di guasti in un sottosistema, che si presenta a seguito di guasti casuali dell'hardware, che si possono verificare senza dar luogo ad un malfunzionamento. Una tolleranza di guasto dell'hardware pari a zero significa che un singolo guasto può essere causa di malfunzionamento.

**Tabella 5. Tolleranza ai guasti dell'Hardware: IEC 61511-1 Cl. 11.4 vincoli progettuali per i sottosistemi di sicurezza del tipo B (Nota 1)**

Integrity Levels	Minimum Fault Tolerance (nota 2)		
	SFF < 60%	SFF 60% to 90%	SFF > 90%
SIL 1	1	0	0
SIL 2	2	1	0
SIL 3	3	2	1
SIL 4	Special requirements apply, see IEC 61508		

NOTA 1 Un componente o sottosistema è del tipo B quando non è ben definita la modalità di guasto del componente o di almeno uno dei componenti. PLC, logiche programmabili, bus da campo, smart sensors, smart valves sono considerati di tipo B.

NOTA 2 La tolleranza ai guasti dell'hardware rappresenta il numero massimo di guasti in un sottosistema, che si presenta a seguito di guasti casuali dell'hardware, che si possono verificare senza dar luogo ad un malfunzionamento. Una tolleranza di guasto dell'hardware pari a zero significa che un singolo guasto può essere causa di malfunzionamento.

<b>Table 3 from IEC 61508 – Architectural constraints on Type B</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

<b>IEC 61511 – Minimum hardware fault tolerance</b>						
<b>Table 5 – PE logic solvers</b>				<b>Table 6 – other devices</b>		
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	

**COMPARISON ELABORATED FROM BILL BLACK FOR EPIGRAM SUMMER 2003**

Diagnostic Coverage (DC) di un componente o sottosistema è definito come il rapporto tra il rateo medio dei guasti random hardware dannosi ma rivelabili dalla autodiagnostica e il rateo medio dei guasti random hardware dannosi totali. Diagnostic Coverage non include i guasti rivelati durante i test periodici (proof tests).

$$DC = \sum \lambda_{DD} / \sum \lambda_D = \sum \lambda_{DD} / (\sum \lambda_{DU} + \sum \lambda_{DD})$$

Dove:

$\lambda_D$  è il rateo medio di guasti dannosi;

$\lambda_{DD}$  è il rateo medio di guasti dannosi rivelabili dalla autodiagnostica;

$\lambda_{DU}$  è il rateo medio di guasti dannosi non rivelabili dalla autodiagnostica.

$$\lambda_D = \lambda_{DD} + \lambda_{DU}$$

Safe Failure Fraction (SFF) di un componente o sottosistema è definito come il rapporto tra la somma del rateo medio dei guasti random hardware sicuri e dei guasti random hardware dannosi ma rivelabili e il rateo medio dei guasti random hardware totali (sicuri e dannosi)

$$SFF = \frac{(\sum \lambda_S + \lambda_{DD})}{(\sum \lambda_S + \lambda_D)}$$

Dove:

$\lambda_S$  è il rateo medio dei guasti sicuri.

$\lambda = \lambda_S + \lambda_D$  è il rateo medio totale dei guasti

Per i componenti e sottosistemi complessi (tipicamente PLC) si assume come realistica una ripartizione tra il 50% di guasti sicuri ( $\lambda_S$ ) e il 50% di guasti dannosi ( $\lambda_D$ ).

---

L'introduzione del concetto di SFF permette di fatto di rendere meno onerosi i vincoli sulle architetture imposti dalle Tabelle 2, 3, 4, 5. Infatti, assumendo realistica la ripartizione 50% tra guasti sicuri e guasti dannosi e assumendo per esempio che il 30% dei guasti dannosi sia rivelabile dall'autodiagnostica, abbiamo:

$$DC = 30\%$$

$$SFF = (50\% + [50\% \times 30\%]) = 65\%$$

Con un evidente guadagno sui vincoli imposti sulle architetture.

Elevando opportunamente DC al 90% abbiamo:

$$SFF = (50\% + [50\% \times 90\%]) = 95\%$$

I valori di DC e di SFF per i componenti o sottosistemi che verranno usati in una catena di strumentazione digitale per applicazioni di sicurezza dovranno essere forniti dai fornitori di componenti e certificati da competenti Agenzie di certificazione (TUV, DNV, ...).

---

## DC vs. SFF vs. SIS

Suppose you have an Intelligent Pressure Transmitter TR. Assume  
DC = 30%

The SFF will be 65% if we assume 50/50 ratio between Safe and  
Danger failures.

According to table 3 (B type component) the limits will be:

1 TR = SIL 1

2 TR's (1oo2) = SIL 2

3 TR's (2oo3) = SIL 2

3 TR's (1oo3) = SIL 3

---

## DC vs. SFF vs. SIS

Applying a Safety Certified TR with the DC around 95 - 98 %

SFF will be between 90 and 99 %.(50/50 ratio)

According to table 3 (B type component) the limits will be:

1 TR = SIL 2

2 TR's (1002) = SIL 3

3 TR's (2003) = SIL 3

3 TR's (1003) = SIL 4

---

## DC vs. SFF vs. SIS

No any DC gives a SFF of 50 %.(50/50 ratio)

In this case according to Table 3.

- 1 TR = not allowed
- 2 TR's (1002) = SIL 1
- 3 TR's (2003) = SIL 1
- 3 TR's (1003) = SIL 2

---

## THE SOFTWARE NIGHTMARE

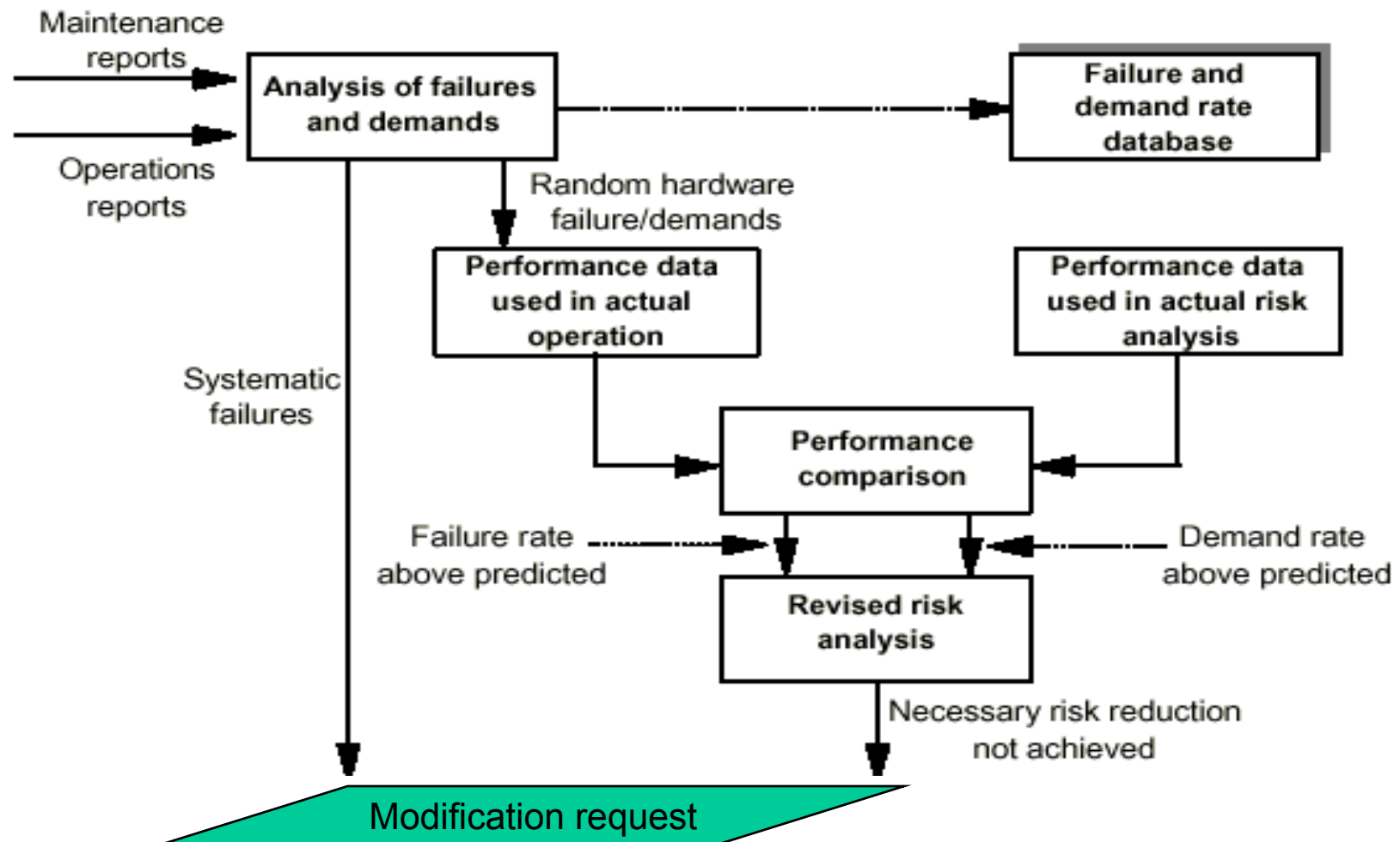
**THE TABLES FOR FAILURE RATES FOR SILs IN PART 1 HAVE NOTHING TO DO WITH SOFTWARE.**

**THERE ARE NO SOFTWARE-RELATED FAILURE RATES WHICH ARE NECESSARY REQUIREMENTS FOR SILs.**

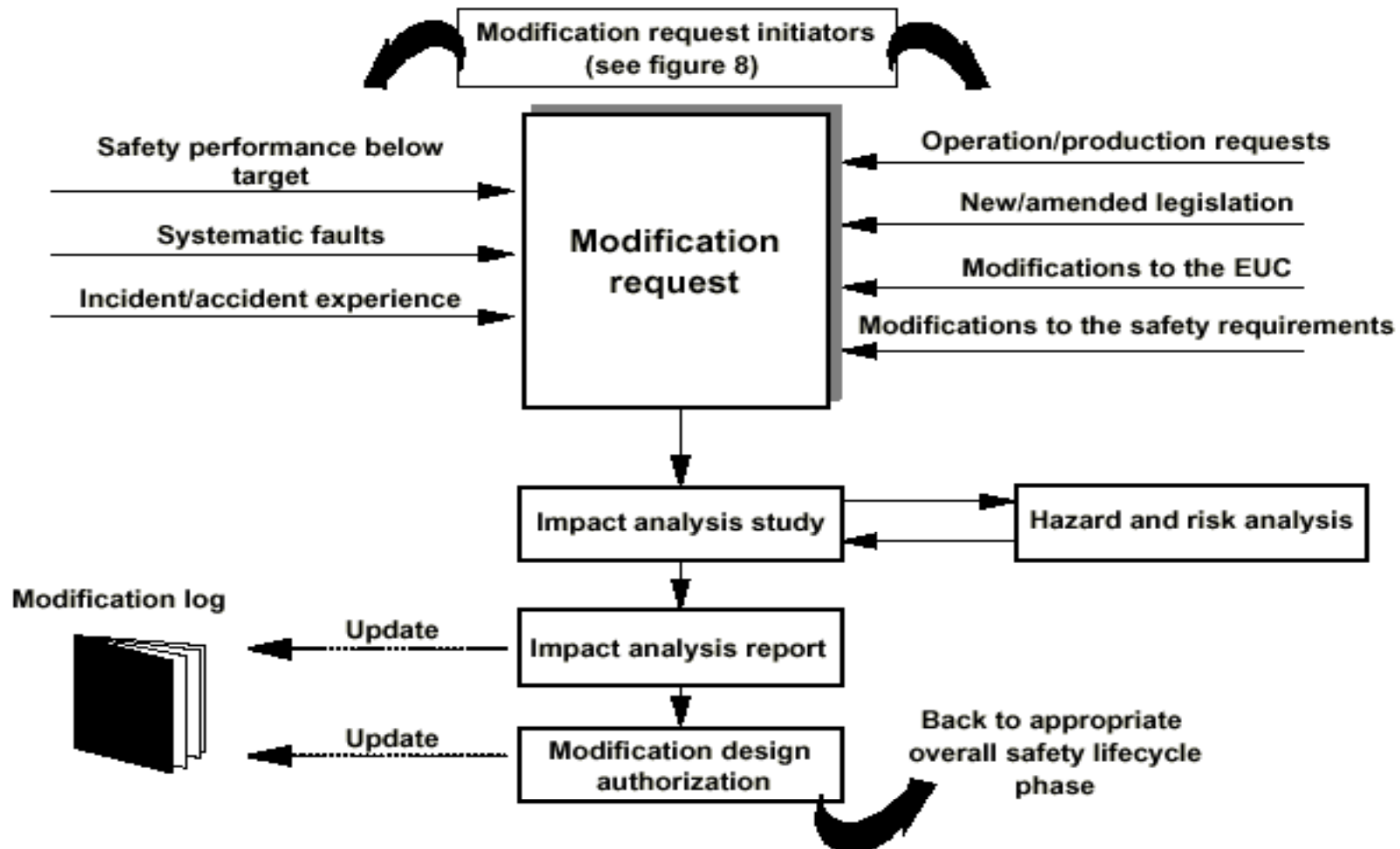
**THERE ARE NO REFERENCE IN PART 3 TO SOFTWARE RELIABILITY, FAILURE RATE OR MTBF. THERE ARE NO TECHNIQUES REFERENCED WHICH HAVE PREDICTED FAILURE RATES ASSOCIATED WITH THEM.**

**THERE IS GUIDANCE IN PART 7 ABOUT ESTABLISHING SOME DEGREE OF CONFIDENCE IN THE CORRECTNESS OF THE SOFTWARE**

# IEC 61508 Part 1 Cl 7.16 Safety Life Cycle “Modification” Phase



# IEC 61508 Part 1 Cl 7.16 Safety Life Cycle “Modification” Phase



---

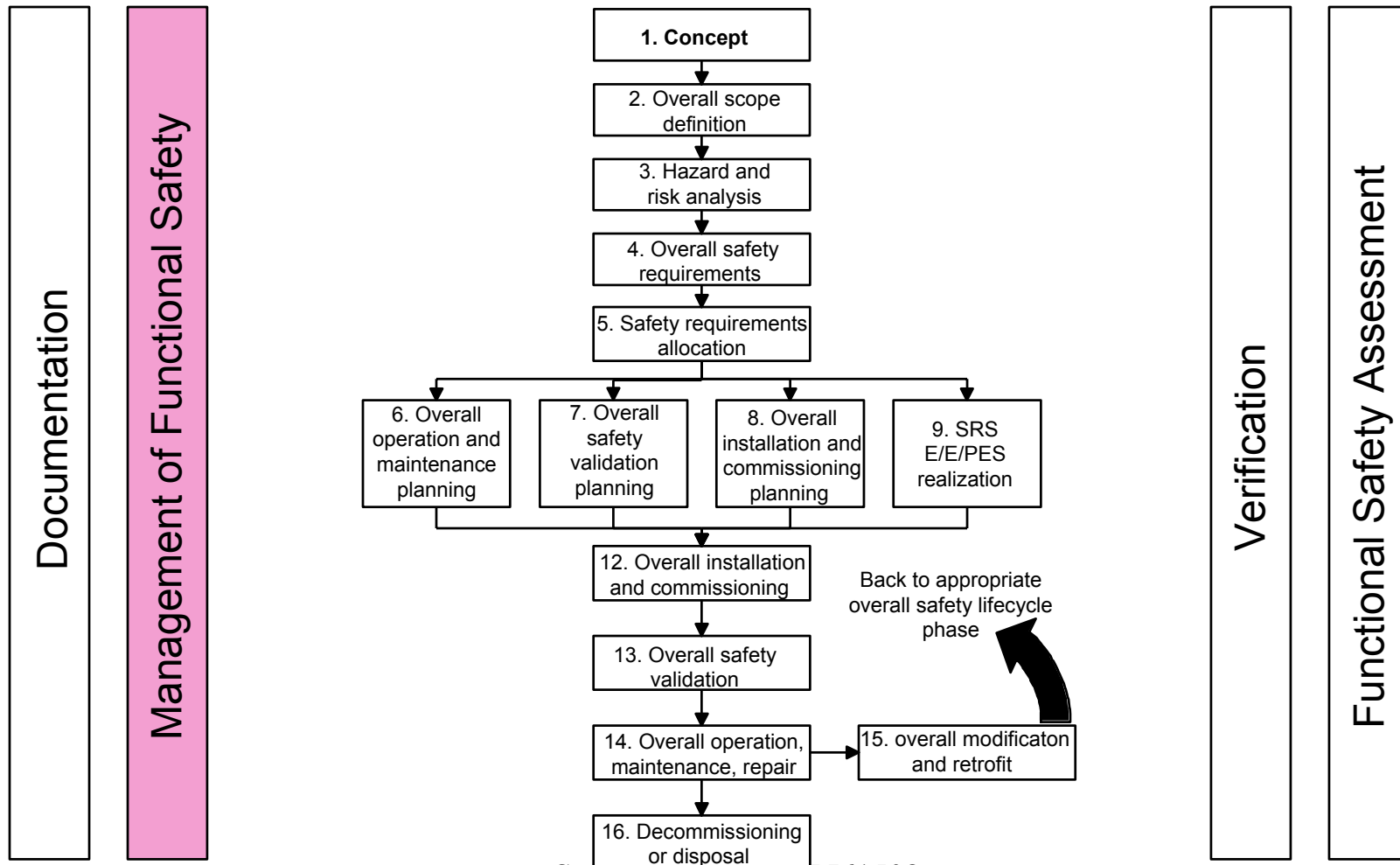
## CERTIFICATION – WHAT IS IT?

The word certification is never used in IEC 61508 Part 1-7

The word certification is used only two times in IEC 61511 Part 2 Annex E referring to the software tools used for developing application software.

The right expression to use is “.....to be compliant to.....”

# Management of Functional Safety (IEC 61508 Cl 6 and IEC 61511 Cl 5)



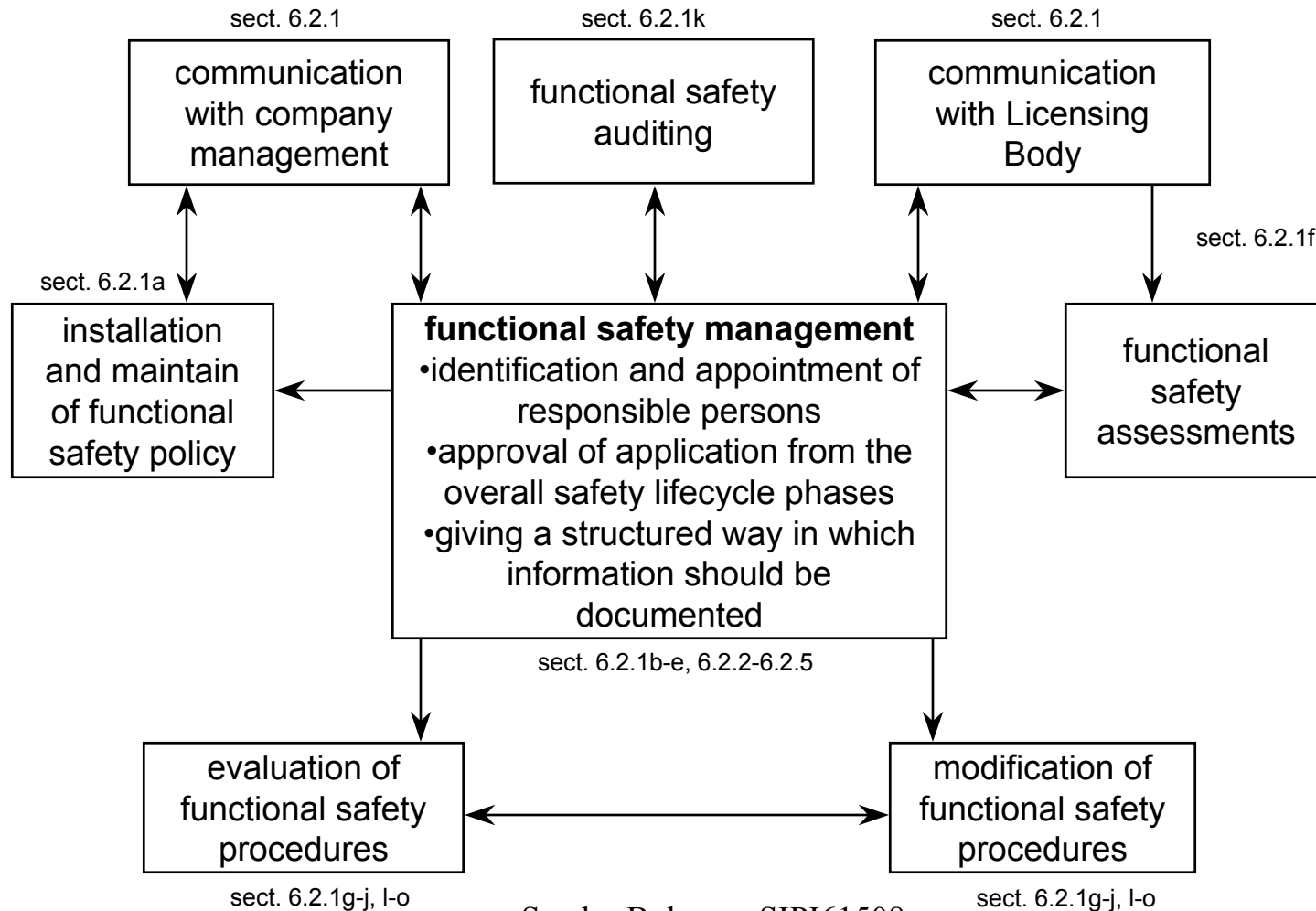
## FUNCTIONAL SAFETY MANAGEMENT

The objectives of Functional Safety Management is two-fold:

First, FSM defines all the management and technical activities required during the safety lifecycle phases of a product or process which are necessary for the achievement of the required level of functional safety.

Second, FSM specifies the responsibilities of persons, departments and organizations responsible for each safety lifecycle phase or for activities within each phase.

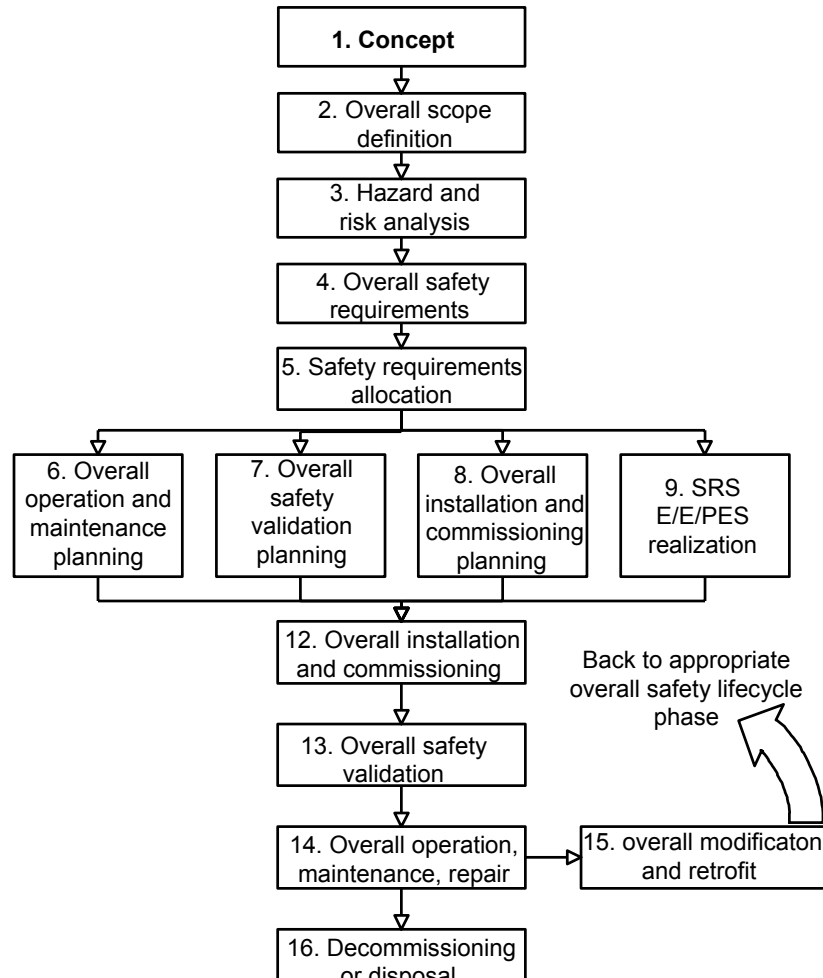
# Duties of functional safety management



# Functional Safety Assessment (IEC 61508 C1 8 and IEC 61511 C1 5)

Documentation

Management of Functional Safety



Verification

Functional Safety Assessment

**IEC 61508 applies to the the whole life cycle of a E/E/PES,**

<b>E/E/PES CONFIGURATION &amp; IMPLEMENTATION</b>					
<b>HARDWARE</b>		<b>SOFTWARE</b>		<b>INTEGRATION</b>	
I M P L E M E N T A T I O N	V E R I F I C A T I O N	I M P L E M E N T A T I O N	V E R I F I C A T I O N	I M P L E M E N T A T I O N	V E R I F I C A T I O N
<b>SIL EVALUATION</b>					
<b>E/E/PES FUNCTIONAL SAFETY ASSESSMENT</b>					

## IEC 61508 E/E/PES Functional Assessment Independency IEC 61508 CI 8

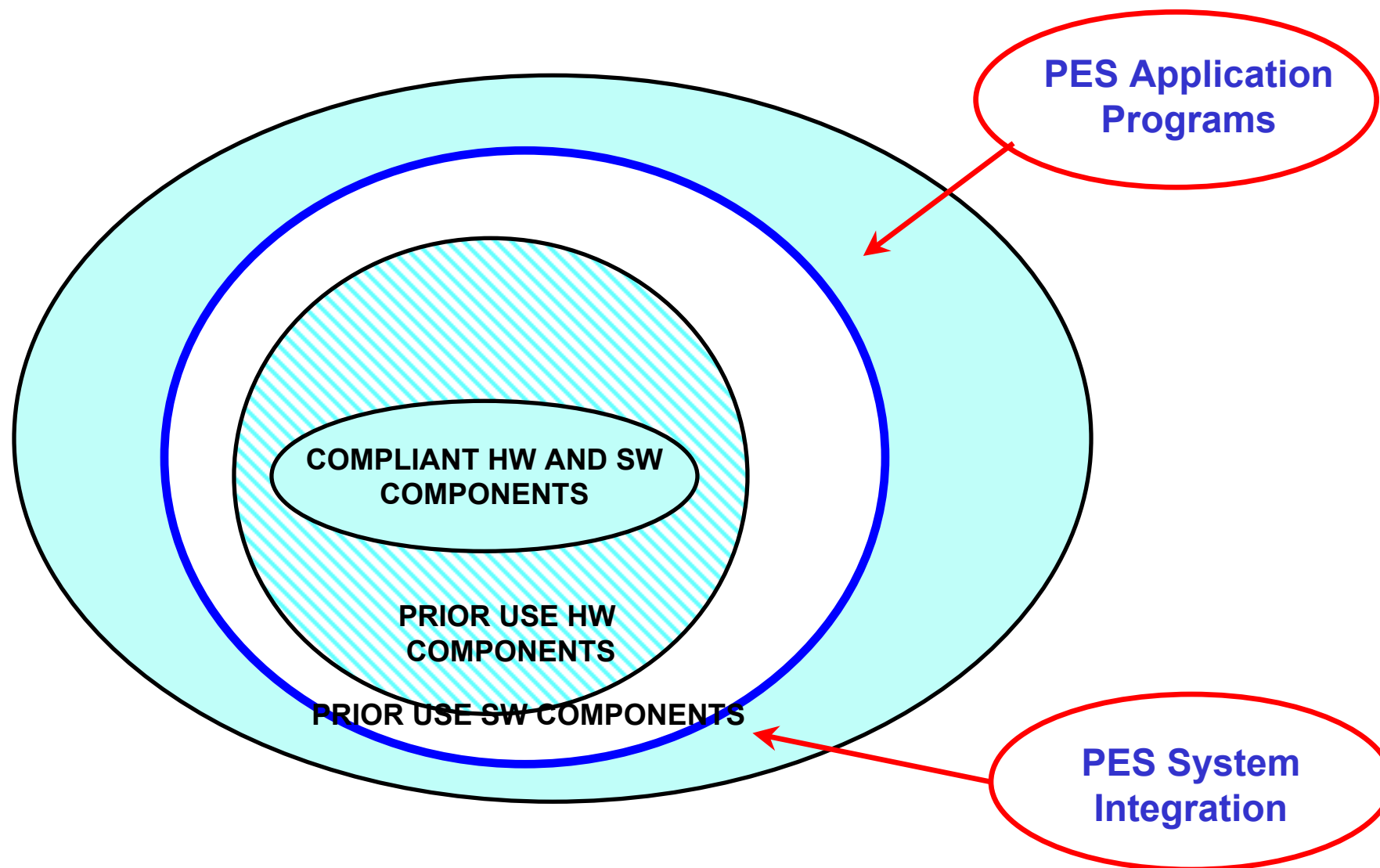
<b>Minimum level of independence</b>	<b>Safety Integrity level</b>			
	1	2	3	4
Independent Person	HR	HR	NR	NR
Independent department	—	HR	HR	NR
Independent organization	—	—	HR	HR

---

## IEC 61511 Cl 5.2.6 SIS Functional Assessment Independency

**Depending upon the company organisation and expertise within the company, the requirement for an independent assessor may have to be met by using an external organisation.**

# CLASSIFICAZIONE DEI COMPONENTI



---

## **PROVEN-IN-USE ( IEC 61511 11.5.3 GENERAL REQUIREMENTS)**

- **A PREVIOUSLY DEVELOPED SUBSYSTEM SHALL ONLY BE REGARDED AS PROVEN-IN USE WHEN THERE IS ADEQUATE DOCUMENTARY EVIDENCE WHICH IS BASED ON THE PREVIOUS USE OF A SPECIFIC CONFIGURATION OF THE SUBSYSTEM, DURING WHICH TIME ALL FAILURES HAVE BEEN FORMALLY RECORDED.**
- **THE DOCUMENTARY EVIDENCE SHALL DEMONSTRATE THAT THE LIKELIHOOD OF ANY FAILURE OF THE SUBSYSTEM (DUE TO RANDOM HARDWARE AND SYSTEMATIC FAULTS) IN THE **E/E/PE** SAFETY-RELATED SYSTEM IS LOW ENOUGH SO THAT THE REQUIRED SAFETY INTEGRITY LEVEL OF THE SAFETY FUNCTION WHICH USE THE SUBSYSTEM IS ACHIEVED.**
- **THE DOCUMENTARY EVIDENCE SHALL DEMONSTRATE THAT THE PREVIOUS CONDITIONS OF USE OF THE SPECIFIC SUBSYSTEM ARE THE SAME AS, OR SUFFICIENTLY CLOSED TO, THOSE WHICH WILL BE EXPERIENCED BY THE SUBSYSTEM IN THE **E/E/PE** SAFETY-RELATED SYSTEM.**

---

## **PRIOR USE ( IEC 61511 11.5.3 GENERAL REQUIREMENTS)**

### **REQUIREMENTS FOR SELECTION OF PROGRAMMABLE COMPONENTS AND SUBSYSTEMS BASED ON PRIOR USE:**

- 11.5.4 FIXED PROGRAM LANGUAGE (FPL) - TYPICALLY FIELD DEVICES - FOR SIL 3 APPLICATIONS A FORMAL ASSESSMENT SHALL BE CARRIED OUT**
- 11.5.5 LIMITED VARIABILITY LANGUAGES (LVL) - TYPICALLY LOGIC SOLVERS - FOR SIL2 APPLICATIONS A FORMAL ASSESSMENT SHALL BE CARRIED OUT**
- 11.5.6 FULL VARIABILITY LANGUAGES (FVL) – TYPICALLY LOGIC SOLVERS - FOR ANY SIL THE PROCEDURE SHALL BE IN ACCORDANCE WITH IEC 61508-2 AND IEC 61508-3**

---

# PROBLEM

- ① CAN A DEVICE BE QUALIFIED TO COMPLY WITH **IEC 61508** IRRESPECTIVE OF A SPECIFIC APPLICATION?

YES

“ TO COMPLY WITH **IEC 61508** MEANS THAT THE LIFECYCLE WITH ALL ASSOCIATED REQUIREMENTS USED FOR THAT DEVICE SHALL CONFORM WITH THE LIFECYCLES AND THEIR REQUIREMENTS AS DEFINED IN **IEC 61508 PART 2 AND PART 3**”

---

# Qualification of Generic Products for Safety Systems

## What Does Qualification Mean?

- **IEC 61508** applies to the whole system - a manufacturer cannot claim that a product intended to be part of a system has a defined **SIL** per se
- He can only claim that his product complies with **IEC 61508** and is suitable for use in an overall system which is required to comply with **IEC 61508**:
  - At a defined **SIL**
  - Under specified conditions of use (e.g. Application, Architecture, Installation, Operation, Proof test interval)

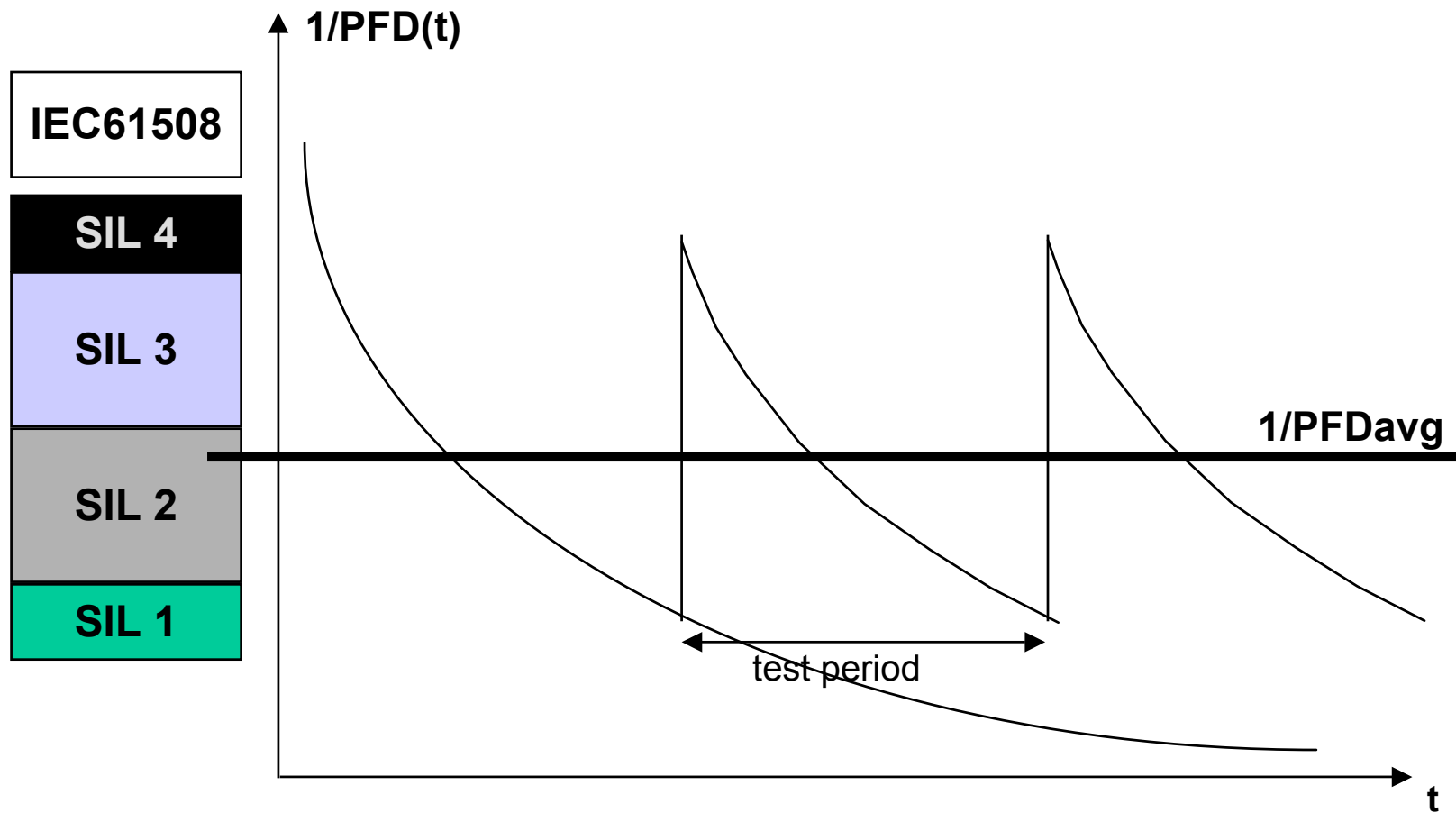
---

# Qualification of Generic Products for Safety Systems

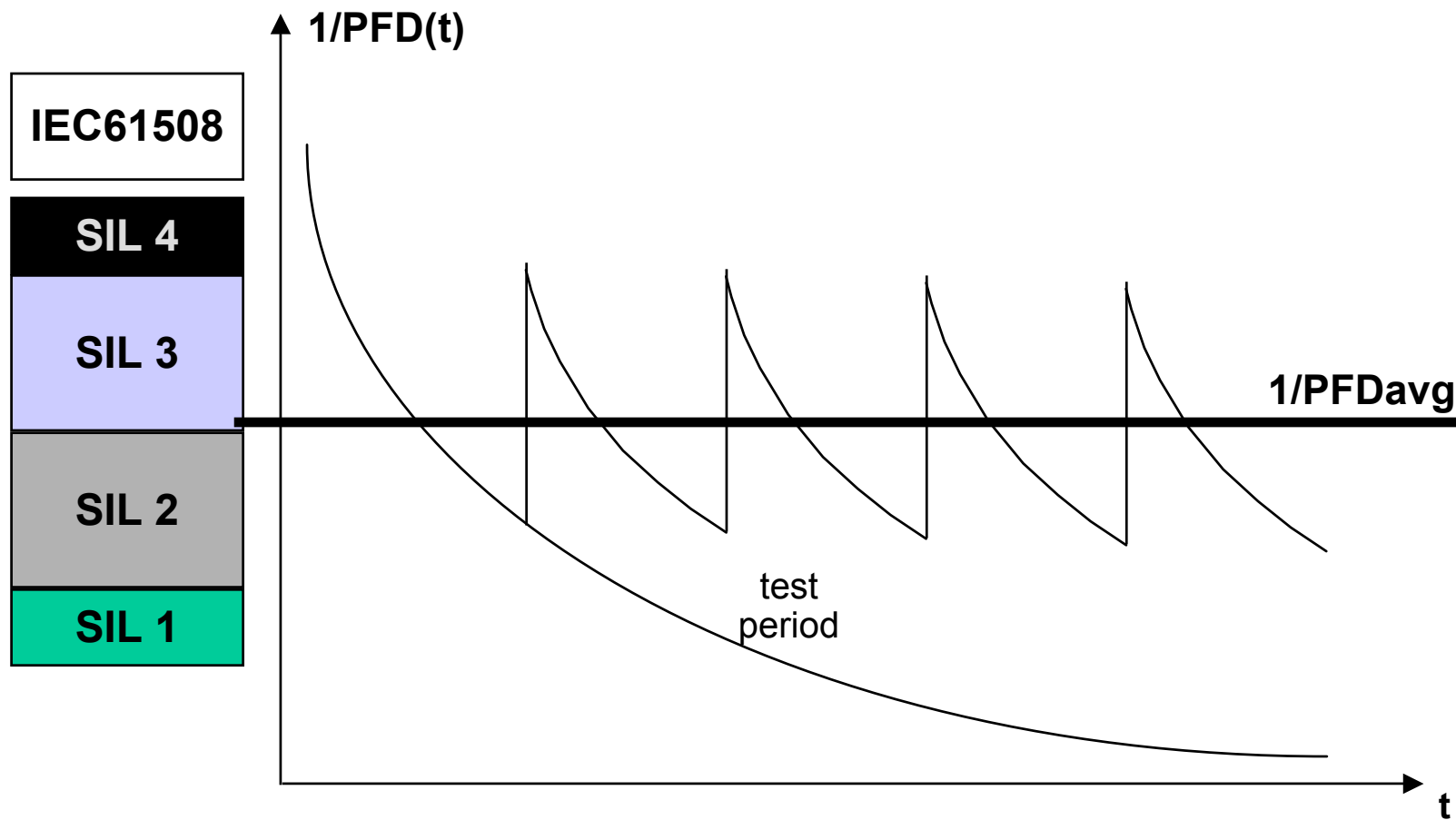
## Achieving the Required SIL for the Overall System

- **SIL is achieved and maintained by a combination of factors:**
  - Performance/reliability of components parts
  - System architecture (e.g. 1001, 1002, 2002, 2003)
  - Design techniques and features
  - Management, operating and maintenance procedures
  - Proof testing on system in use
- **Inferior performance of one factor or one part of a system can be compensated by enhanced capability in another. For example, lack of on-line fault diagnostics can be compensated by more frequent off-line proof testing and/or redundancy.**
- **Defining the conditions of use is thus an essential aspect of product qualification**

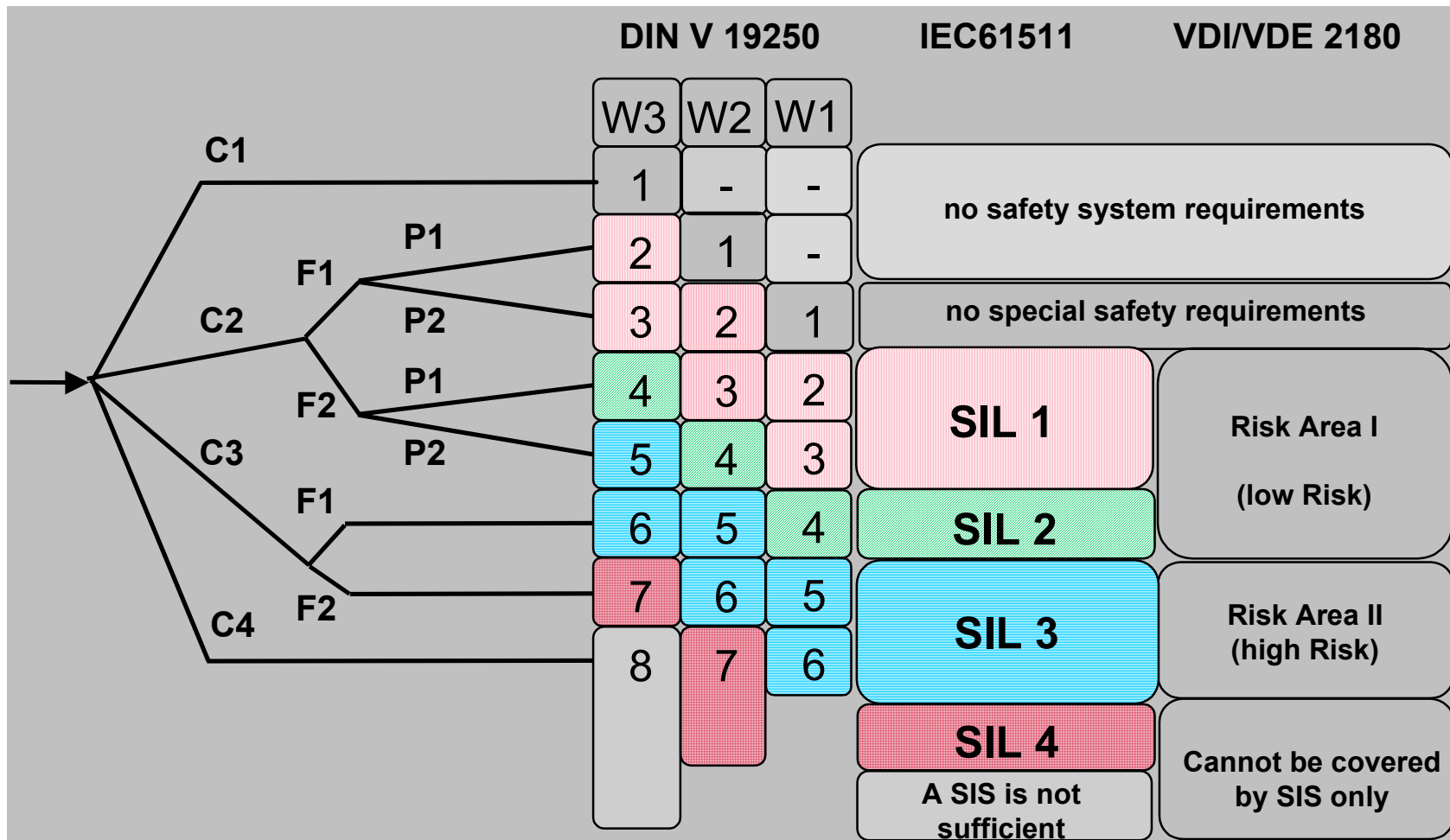
# INFLUENCE OF THE TEST PERIOD ON SAFETY



# INFLUENCE OF THE TEST PERIOD ON SAFETY



## IEC 61511-3 Annex E DIN V 19250 vs. IEC 61511 vs. VDI/VDE 2180



---

## SOME COMMON QUESTIONS

**HOW TO CLASSIFY A VALVE CLOSED BY MULTIPLE INDEPENDENT SAFETY FUNCTIONS (SIFs) INVOLVED WITH DIFFERENT HAZARDS? – THE VALVE MUST MEET THE MOST STRINGENT SIL IMPOSED ON IT BY THE INDIVIDUAL SIFs**

**THE OVERALL SIL OF A SYSTEM MADE OF MULTIPLE INDEPENDENT SAFETY FUNCTIONS (SIFs) IS REQUIRED TO BE SIL2. EACH OF THE SIF CONSISTS OF THE SAME TYPE OF TRANSMITTERS AND ACTUATORS, WITH A COMMON LOGIC SOLVER AMONG ALL OF THEM. WHAT IS THE RELATION BETWEEN THE SIL OF THE INDIVIDUAL SIFs AND THE OVERALL SIL? – SINCE THE CHANCES OF TWO OR MORE SIFs FAILING SIMULTANEOUSLY IS SMALLER THAN A SINGLE FAILURE WE TAKE THE OVERALL SIL TO BE EQUAL TO THE LEAST STRINGENT SIL OF THE MULTIPLE SIFs**

---

## SOME COMMON OVERSIGHTS

- **CONSIDER ONLY THE PROBABILISTIC REQUIREMENTS ON SIL TARGET FAILURE MEASURE AND NOT CONSIDER THE DETERMINISTIC REQUIREMENTS ON HARDWARE ARCHITECTURAL CONSTRAINTS**
- **MIX UP FAILURE MEASURES FOR SINGLE COMPONENTS WITH SIL TARGET FAILURE MEASURE FOR E/E/PES**
- **MIX UP E/E/PES SIL TARGET FAILURE MEASURE NUMERICAL EVALUATION WITH E/E/PES FUNCTIONAL SAFETY ASSESSMENT [CLAUSE 8, IEC 61508-1]**

---

## FINAL CONSIDERATIONS (1/2)

- **FROM TECHNICAL/PRODUCT ORIENTED APPROACH TO PROCESS/ORGANIZATIONAL ORIENTED APPROACH**
- **MANY OF THE ACTIVITIES REQUIRED BY THE IEC 61508 & IEC 61511 SAFETY LIFE CYCLE ARE ALREADY COVERED BY GOOD ENGINEERING PRACTICE BUT UNDER DIFFERENT NAMES**
- **MOST OF THE DOCUMENTATION REQUIRED BY THE IEC 61508 & IEC 61511 IS NEW FOR THE PROCESS INDUSTRY WITH ADDITIONAL COSTS**
- **IEC 61508-3 IS NEARLY UNAPPLICABLE TO THE SAFETY APPLICATION SOFTWARE, NORMALLY IMPLEMENTED USING RELAY LADDER PROGRAMMING LANGUAGE FOR PROGRAMMABLE CONTROLLER**
- **IN ALL CASES SOFTWARE ERRORS ARE DEALT ONLY QUALITATIVELY AND NEVER QUANTITATIVELY DURING SIL EVALUATION**

---

## FINAL CONSIDERATIONS (2/2)

- A MANUFACTURER CANNOT CLAIM THAT A PRODUCT INTENDED TO BE PART OF A SYSTEM HAS A DEFINED **SIL** PER SE
- THE PRINCIPLE OF “DE-ENERGISED TO TRIP” IS STRONGLY RECOMMENDED INSTEAD OF “ENERGISED TO TRIP”
- **SIL** IS ACHIEVED AND MAINTAINED BY A COMBINATION OF FACTORS, SPECIAL ATTENTION SHOULD BE DEVOTED TO THE PROOF TESTING INTERVAL
- **E/E/PES SIL** TARGET FAILURE MEASURE NUMERICAL EVALUATION AND **E/E/PES** FUNCTIONAL SAFETY ASSESSMENT ARE TWO DISTINCT ACTIVITIES
- APPLICATION SPECIFIC GUIDELINES, CONFORMANCE ASSESSEMENT SCHEME AND SUPPORTING TOOLS ARE NECESSARY FOR DAILY PRACTICAL USE