



IEC 61508 - Functional Safety of E/E/PES safety related systems An Overview

Bill Black - Blacksafe Consulting Ltd
blackw@blacksafe.demon.co.uk

Safety consultant & member of the IEE
Functional Safety Professional Network
Executive Team



IEC 61508 - Functional Safety of E/E/PES safety related systems An Overview

- Emerging Standards and their relationship
- Determination of the safety requirement specification
- Realisation of the specification
- Operations and maintenance



IEC 61508 and process sector derivatives

- **ISA - S84.01 -1996 - Application of safety Instrumentation Systems for the Process Industries**
- **Draft IEC 61511 - Safety Instrumented Systems for the process industry sector**
- **IEC 61513 - Nuclear power plants - Instrumentation and control for systems important for safety - General requirements for systems**
- **ISO 10418 - Offshore production installations - Analysis, design, installation and testing of basic surface process systems**



Status of standards in the UK

- Not a legal requirement but recognised good practice
- Failure to comply could be seen as evidence of negligence
- Meeting all the requirements will not necessarily be sufficient to meet legal requirements e.g UK H & S at Work Act
- One way to demonstrate good practice in safety cases e.g. COMAH



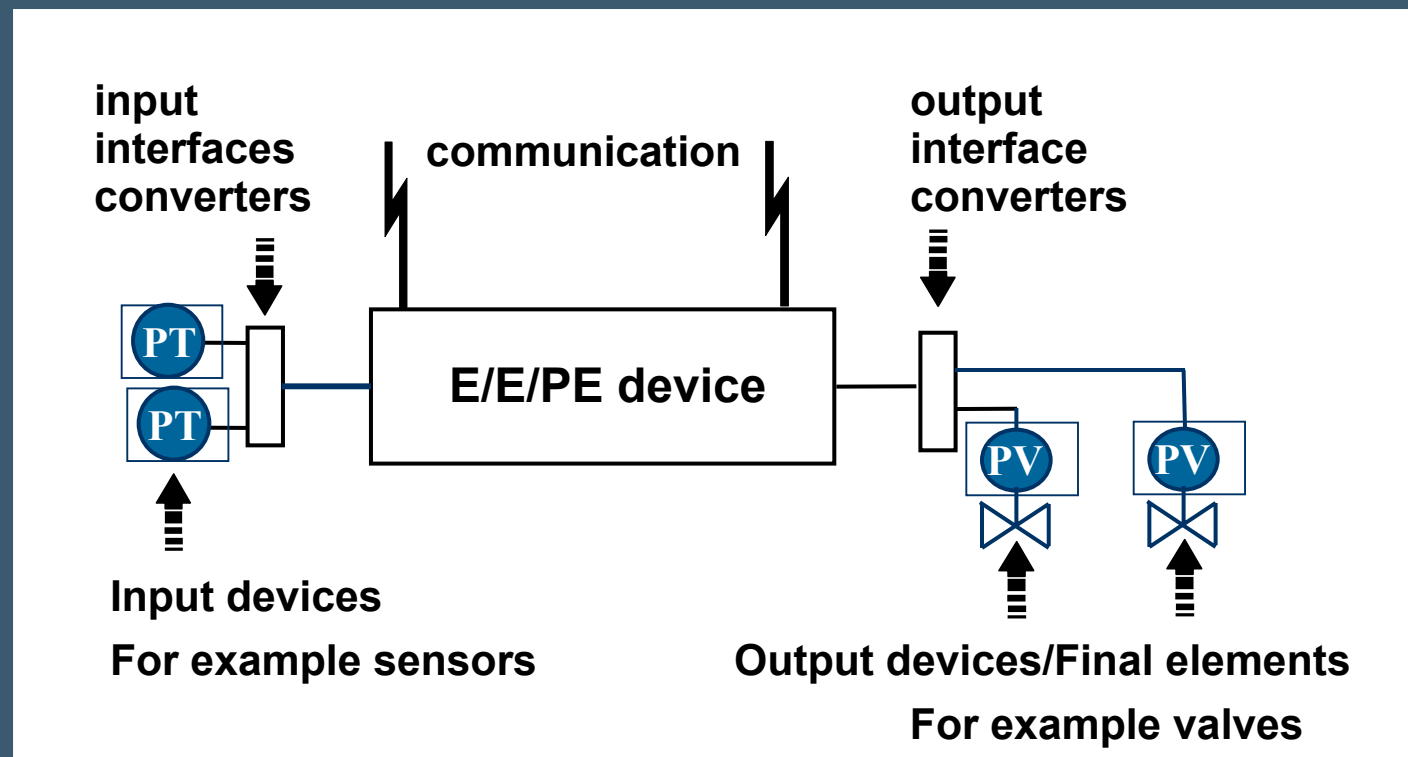
IEC 61508 Parts Structure

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

Safety related system

A designated system that implements the required safety functions necessary to achieve or maintain a safe state

extent of
E/E/PES

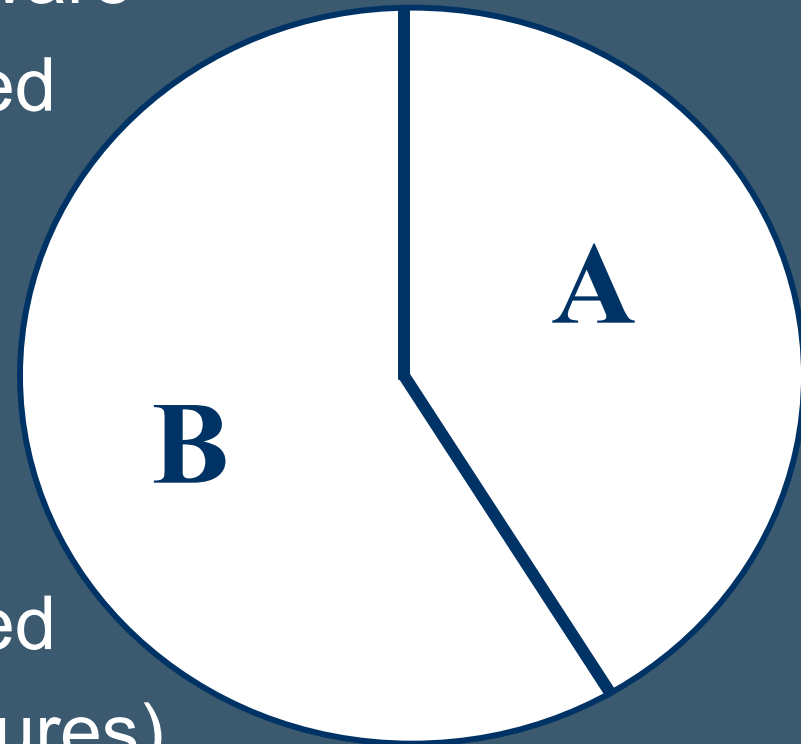




Concept of Failure Categories

A = Random hardware failures (caused by normal degradation)

B = Systematic failures (caused by human failures)



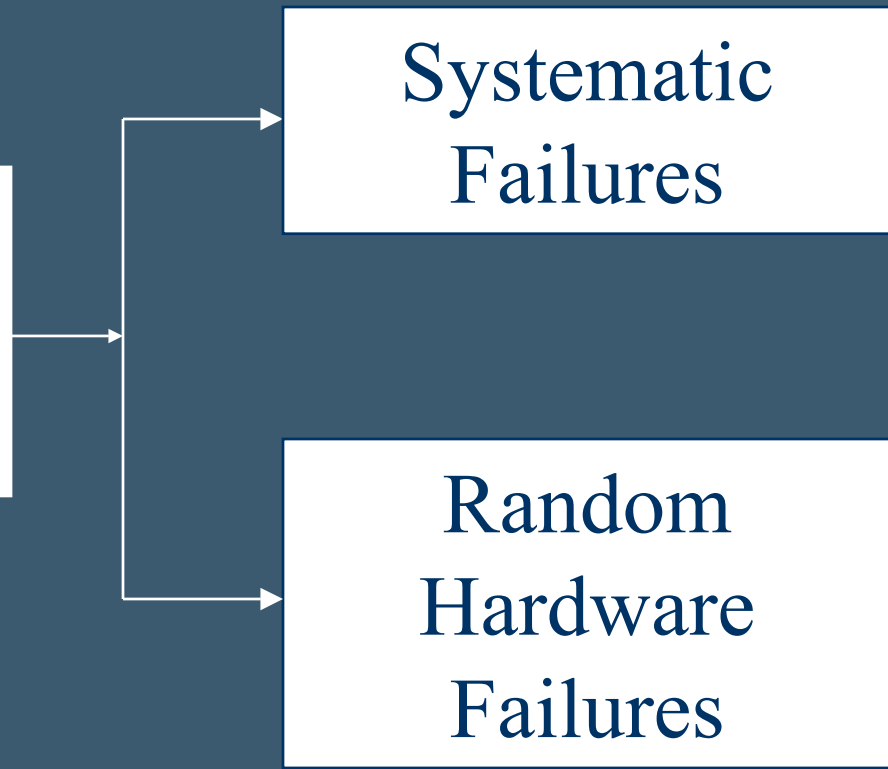


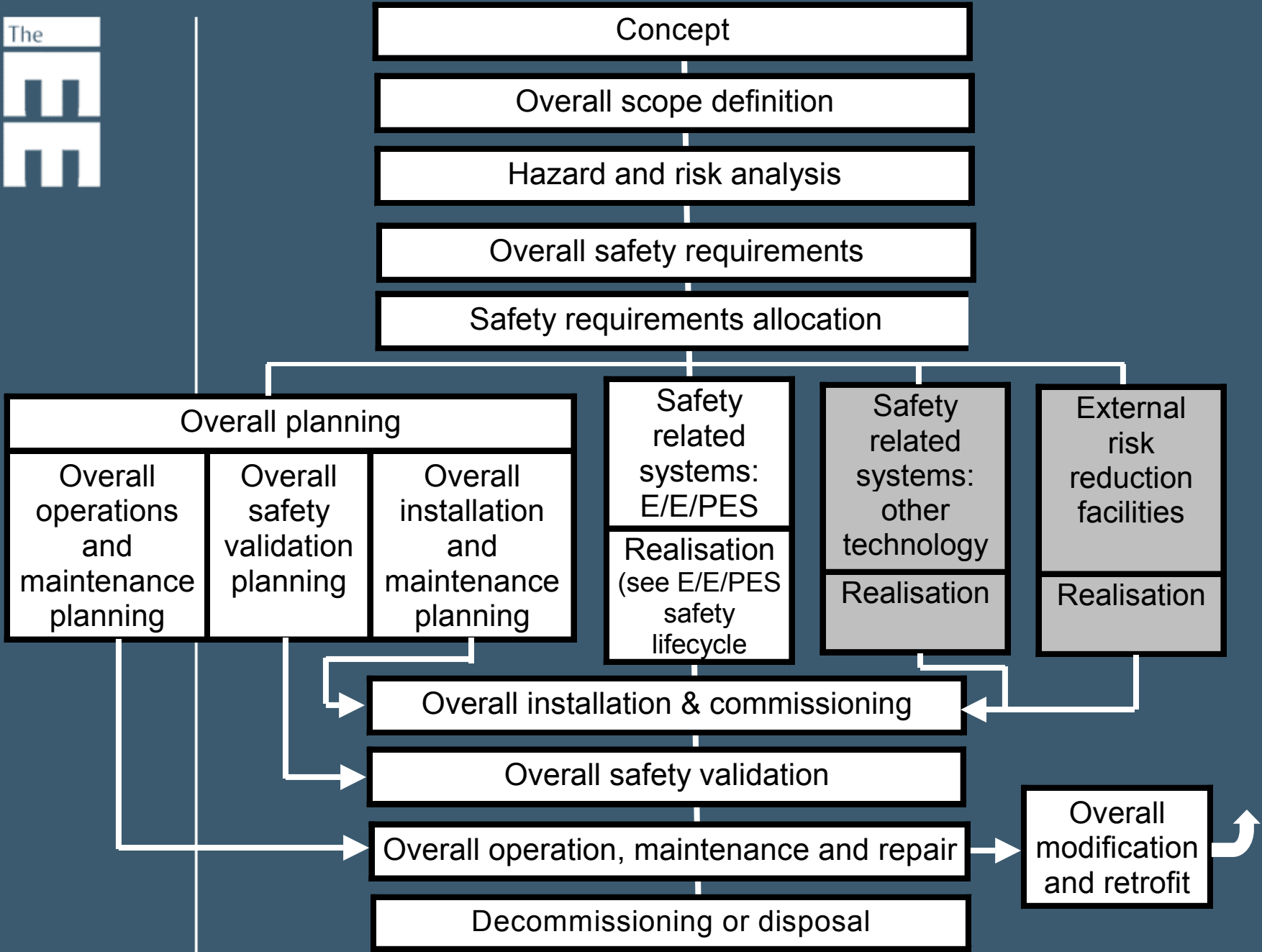
IEC61508 Strategy

Design and
Assessment
must tackle both

Systematic
Failures

Random
Hardware
Failures







Safety requirement specification

1. Concept

2. Overall scope definition

3. Hazard and risk analysis

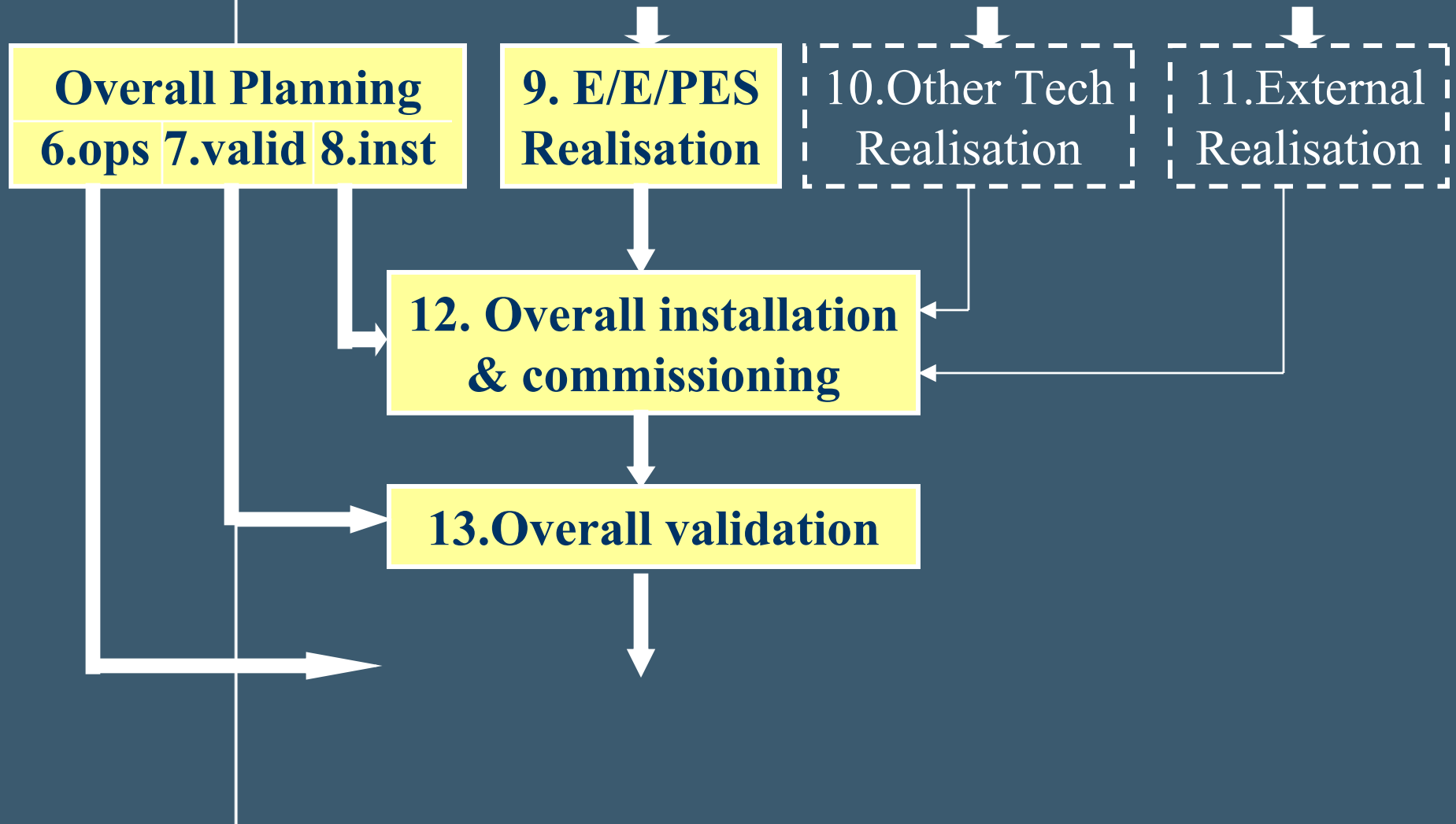
4. Overall safety requirements

5. Safety requirements allocation



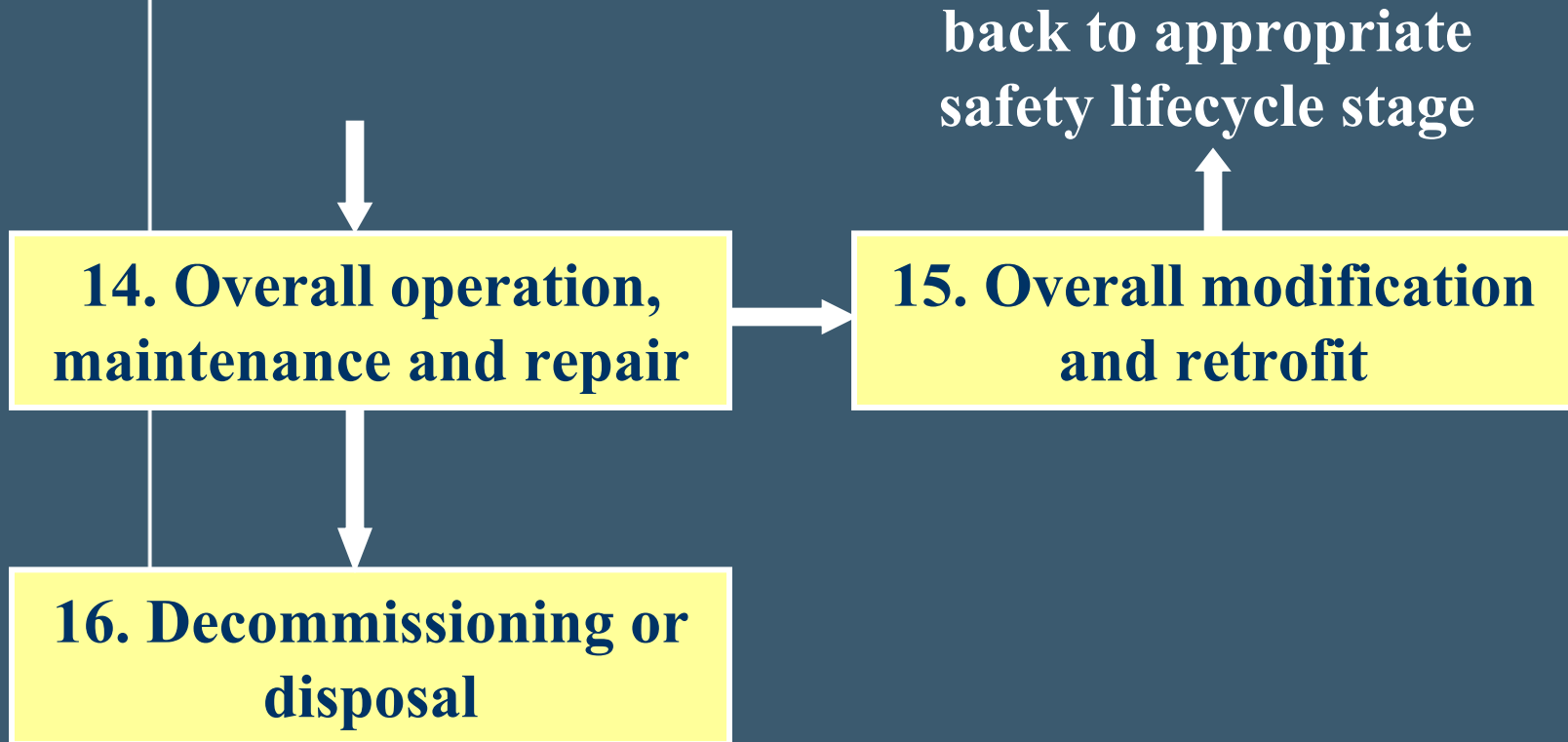


E/E/PES Realisation





Operations and maintenance





Requirements common to all lifecycle phase

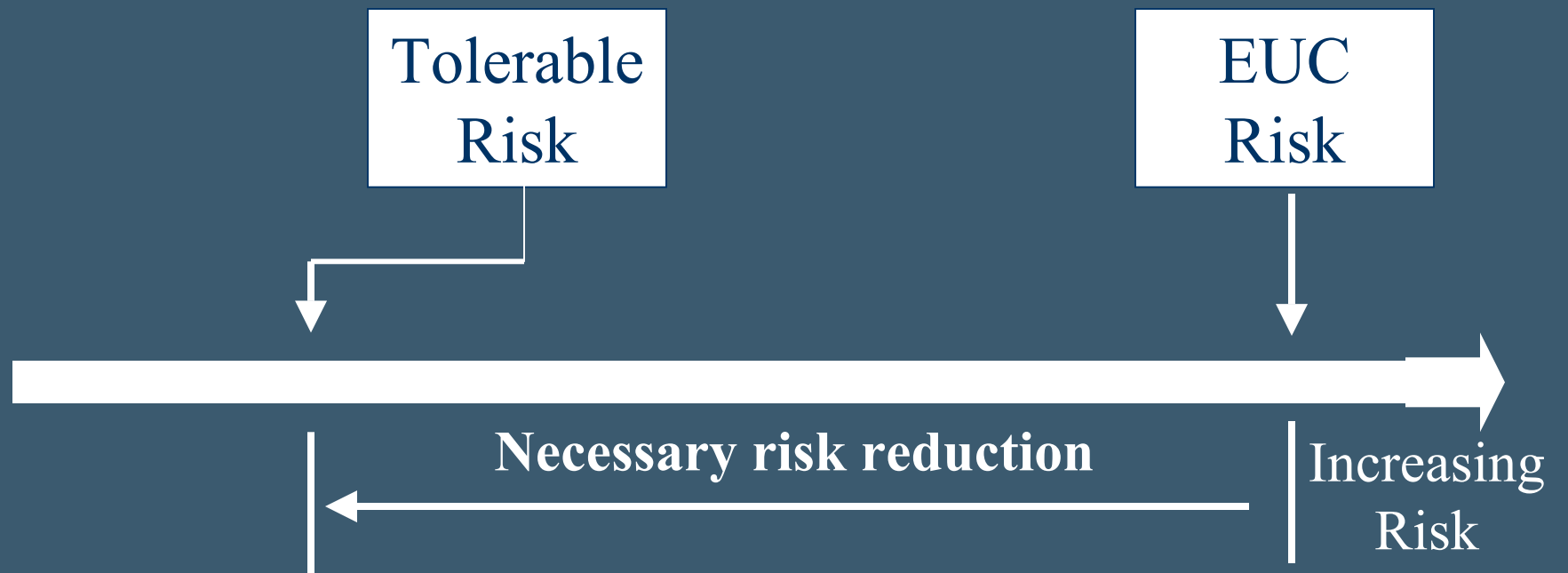
- Management of functional safety
- Competency
- Verification
- Documentation
- Functional safety assessment



Requirements for hazard and risk assessment

- **Undertake a hazard and risk analysis under all reasonably foreseeable circumstances**
- **Determine event sequences leading to the hazards**
- **Consider elimination of the hazards**
- **Determine likelihood and potential consequence**
- **Evaluate or estimate risk**
- **Qualitative or quantitative methods may be used**
- **Results documented and maintained throughout the overall safety lifecycle**

Risk reduction - general concepts





Requirements for specification

- Specify safety functions requirements
- Specify necessary risk reduction
- Sector standards referenced
- Requirements for control system if it is not to be considered as safety related
 - claimed failure rates supported by data
 - limit no lower than $1E-5$ failures per hour
 - reasonably foreseeable failures considered
 - control system separate and independent

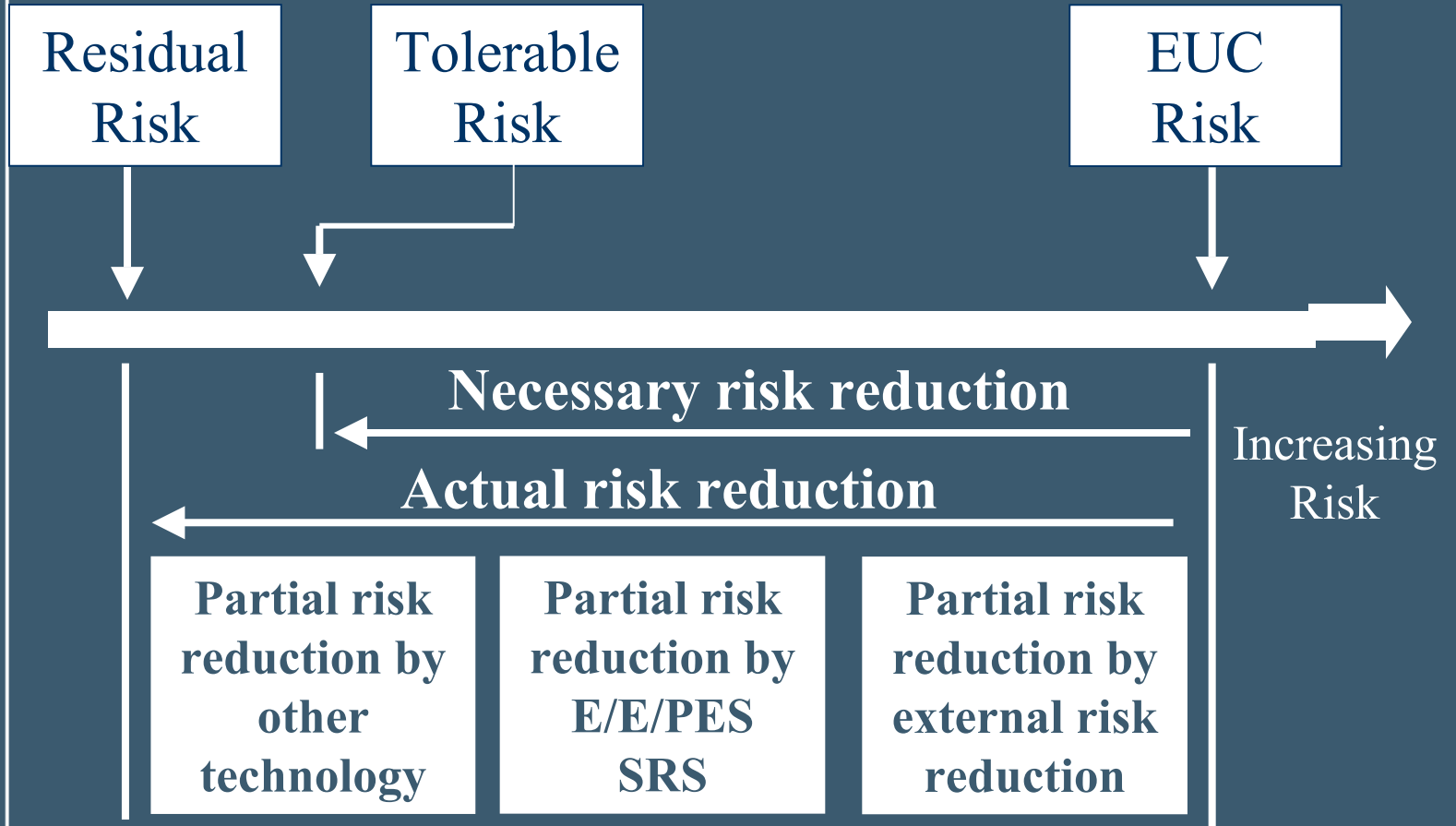


Requirements for allocation

- Allocate safety functions to E/E/PES, other technology and external risk reduction
- Allocate safety integrity levels to E/E/PES functions
- Skills and resources available shall be considered
- Safety integrity requirements qualified to indicate demand mode (low demand or high/continuous)
- Appropriate techniques for the combination of probabilities shall be used during allocation
- Allocation shall take account of common cause



Risk reduction - general concepts





Risk Reduction Requirements

Risk reduction requirements	Safety integrity level
10,000 – 100,000	4
1000 – 10,000	3
100 - 1000	2
10 - 100	1



Safety integrity levels - Table 2

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$



Safety integrity levels - Table 3

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
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 $< 10^{-5}$



Modes of Operation

Low demand mode

Demand frequency < 1 per year and
Test frequency $> 2 \times$ Demand Frequency

High / Continuous Demand mode

Demand frequency > 1 per year or
Test frequency $< 2 \times$ Demand frequency



Example safety requirement specification

- Safety function requirements
If pressure rises above 50 bar, then the flow in line X shall be reduced below F (a specified value) within 5 seconds
- Safety integrity requirements
The function shall be achieved with a performance requirement of SIL2
- Mode of operation is low demand



System Integrity Level Requirements Model

System Integrity Level



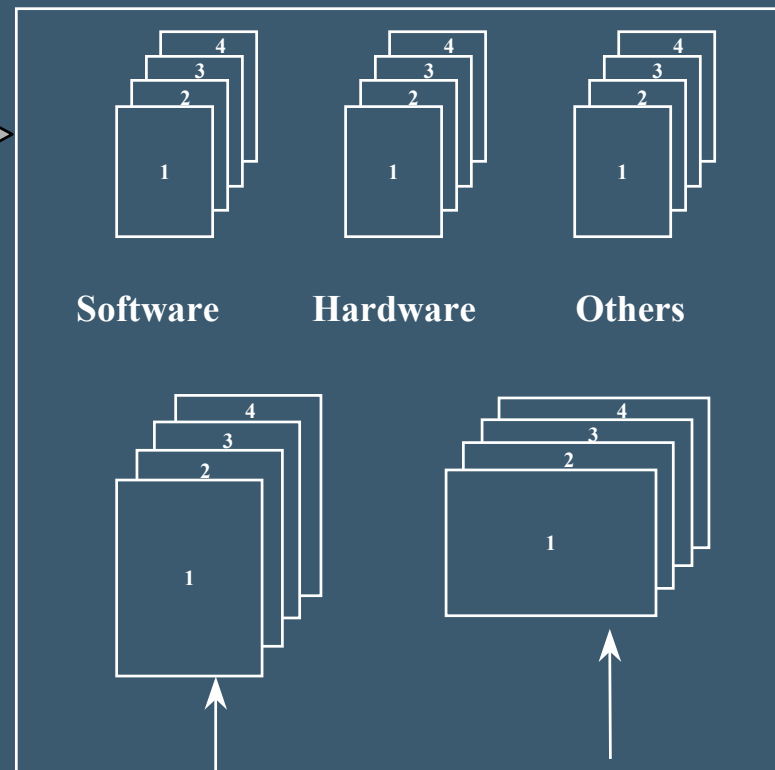
Systematic Integrity



Hardware Integrity



Requirements



Safety Related Continuous Control Systems

Safety Related Protection Systems



Safety requirements specification

- **Derived from the allocation of safety requirements**
- **Expressed and structured to be clear, precise, unambiguous, verifiable, testable, comprehensible**
- **Include safety functions and specify:**
 - **all modes of operation of EUC, system and behaviour**
 - **interfaces to other systems and operator**
 - **actions, constraints, throughput and response**
- **Include safety integrity requirements and specify SIL for each function, proof test facilities, environment**
- **Appropriate techniques and measures**



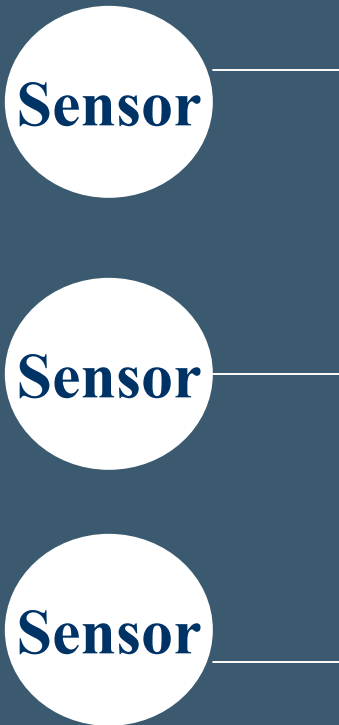
Design Requirements

- Hardware safety integrity requirements :
 - architectural constraints for fault tolerance
 - reliability to meet target failure rates
- Systematic safety integrity requirements :
 - measures for avoidance of failures and control of faults OR
 - evidence of proven in use
- System behaviour on fault detection



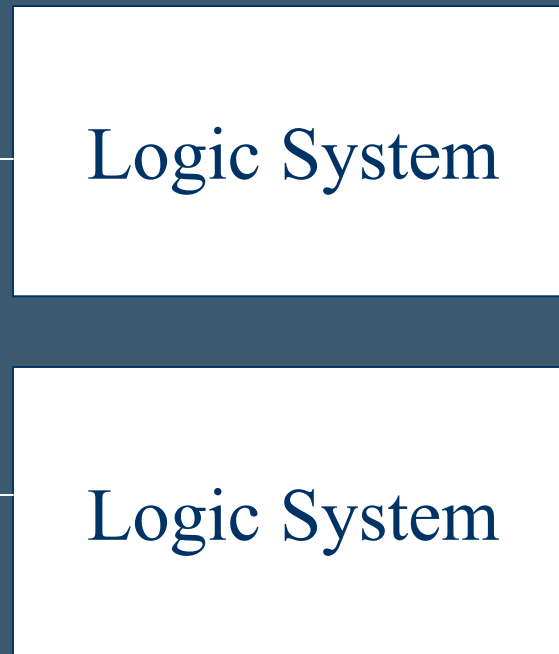
Architectures and sub-systems

Sensor sub-system



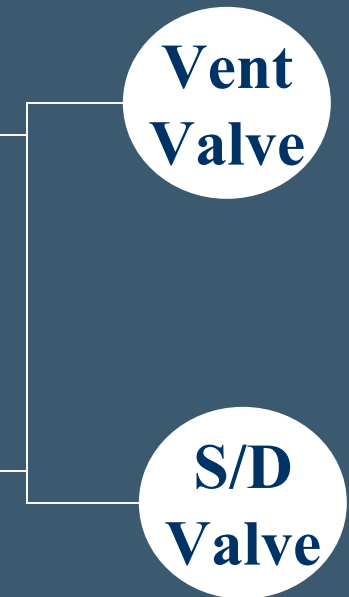
**Architecture
2 out of 3**

Logic sub-system



**Architecture
1 out of 2**

Final actuator sub-system



**Architecture
1 out of 1**



Diagnostic coverage and Safe Failure Fraction

Determined by a failure mode and effect analysis

Diagnostic coverage for dangerous failures

$$= \frac{\sum \lambda_{dd}}{(\sum \lambda_{dd} + \sum \lambda_{du})}$$

Safe failure fraction

$$= (\lambda_s + \sum \lambda_{dd}) / \lambda$$

where

λ = overall failure rate

λ_s = safe failure rate

λ_{dd} = dangerous detected failure rate

λ_{du} = dangerous undetected failure rate

λ_{du}	λ_{dd}
λ_s	



Type A sub-system

A subsystem can be regarded as type A if, for the components required to achieve the safety function:

- **the failure modes of all constituent components are well defined; and**
- **the behaviour of the subsystem under fault conditions can be completely determined; and**
- **there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met (see 7.4.7.3 and 7.4.7.4).**



Fault tolerance - Type A

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60%	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
\geq 99 %	SIL3	SIL4	SIL4



Type B sub-systems

A subsystem shall be regarded as type B if for the components required to achieve the safety function

- **the failure mode of at least one constituent component is not well defined; or**
- **the behaviour of the subsystem under fault conditions cannot be completely determined; or**
- **there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures (see 7.4.7.3 and 7.4.7.4).**



Fault tolerance - Type B

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60%	N/A	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
\geq 99 %	SIL3	SIL4	SIL4



Reliability requirements

Part 2 requires:

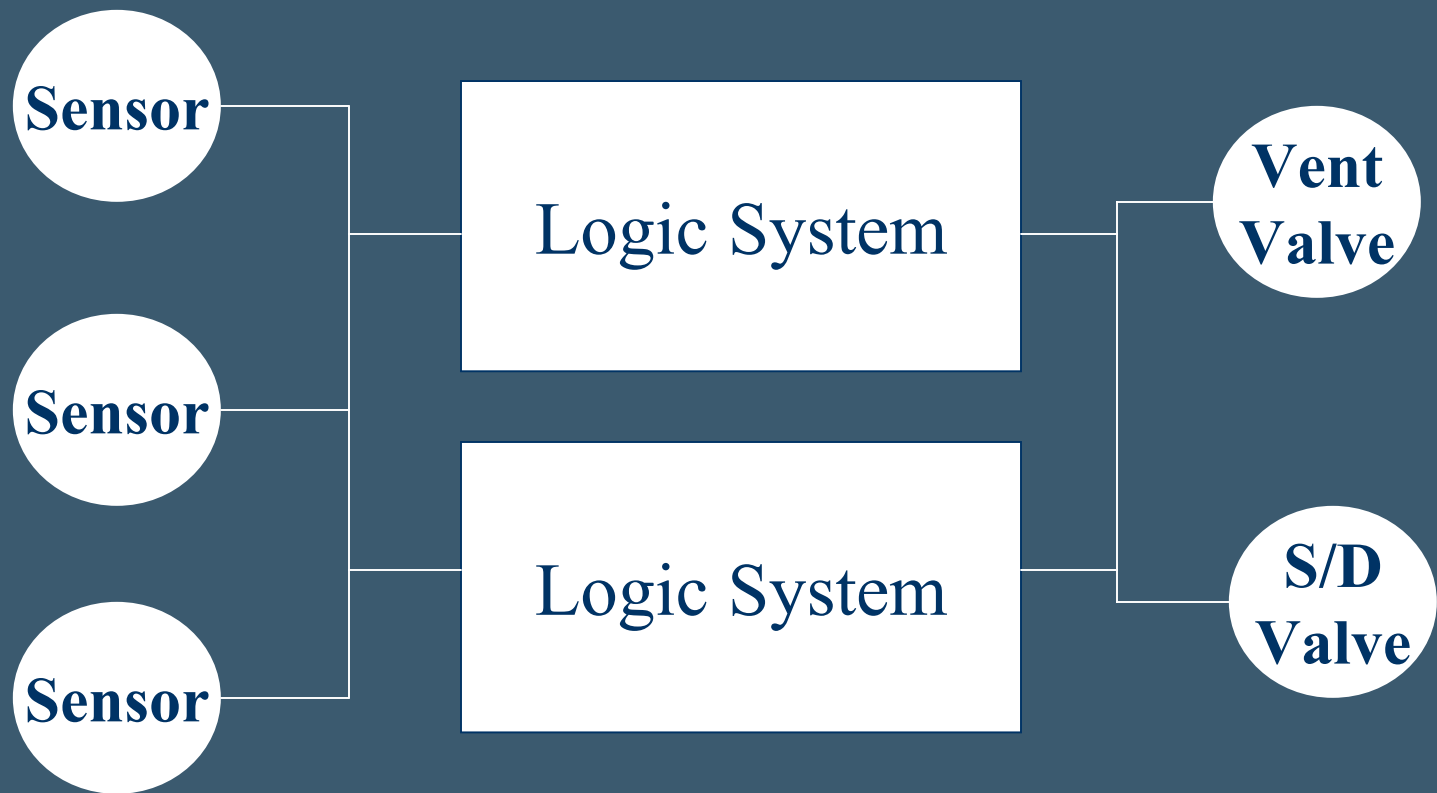
Confirmation by reliability analysis that the proposed systems has a probability of failure that meets the safety integrity requirements

Part 6 provides:

- examples of calculation methods
- tables for simple configurations
- worked example of diagnostic coverage
- a methodology for hardware common cause



Reliability requirements



PFD function = PFD sensor + PFD logic + PFD valves

PFD function must be less than target for SIL



Systematic failures

Measures and techniques defined in:

- 19 tables in Part 2 - Annex A. Techniques and measures for control of failures
- 6 tables in Part 2 - Annex B. Avoidance of systematic failures during the different phases of the lifecycle
- 19 tables in Part 3 - Annex A & B. Software techniques and measures



Example table - Software module testing

Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
Probabilistic testing	Pt 7	-----	R	R	R
Dynamic analysis and testing	Pt 7	R	HR	HR	HR
Data recording and analysis	Pt 7	HR	HR	HR	HR
Functional and black box tests	Pt 7	HR	HR	HR	HR
Performance testing	Pt 7	R	R	HR	HR
Interface testing	Pt 7	R	R	HR	HR



Proven in use

- Clearly restricted functionality
- Adequate documentary evidence of performance in a similar environment
- Evidence to support claimed failure rates
- Failures have been detected and reported
- Sufficient operational time to establish the claimed failure rate to a single sided 70% confidence



System behaviour on fault detection

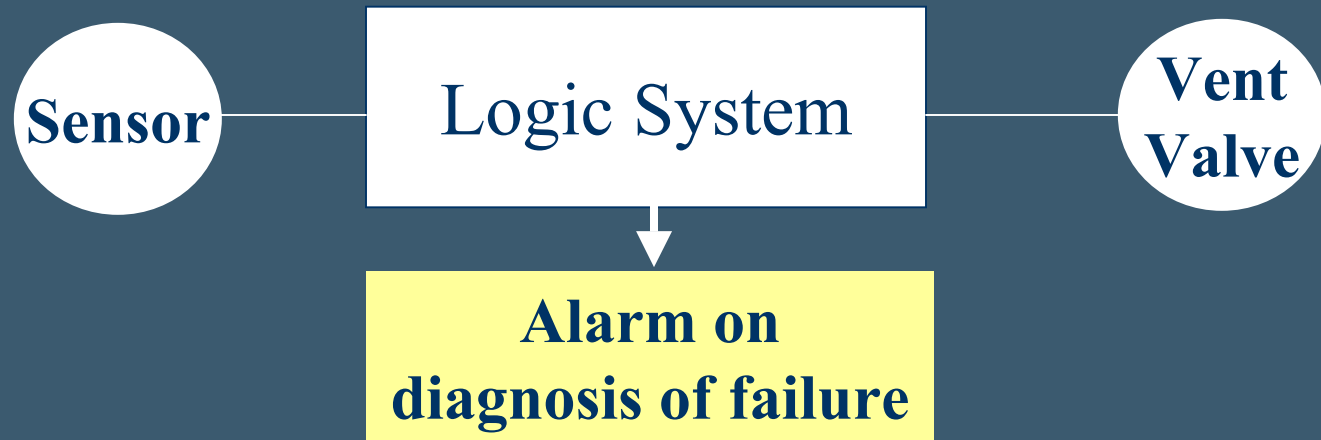
Actions required on detection of a dangerous fault by diagnostic tests, proof tests or by any other means depend on:

- Fault tolerance
- Mode of operation

(Note - This may determine architecture if continued operation is required after detection of a fault)



Systems with fault tolerance of 0

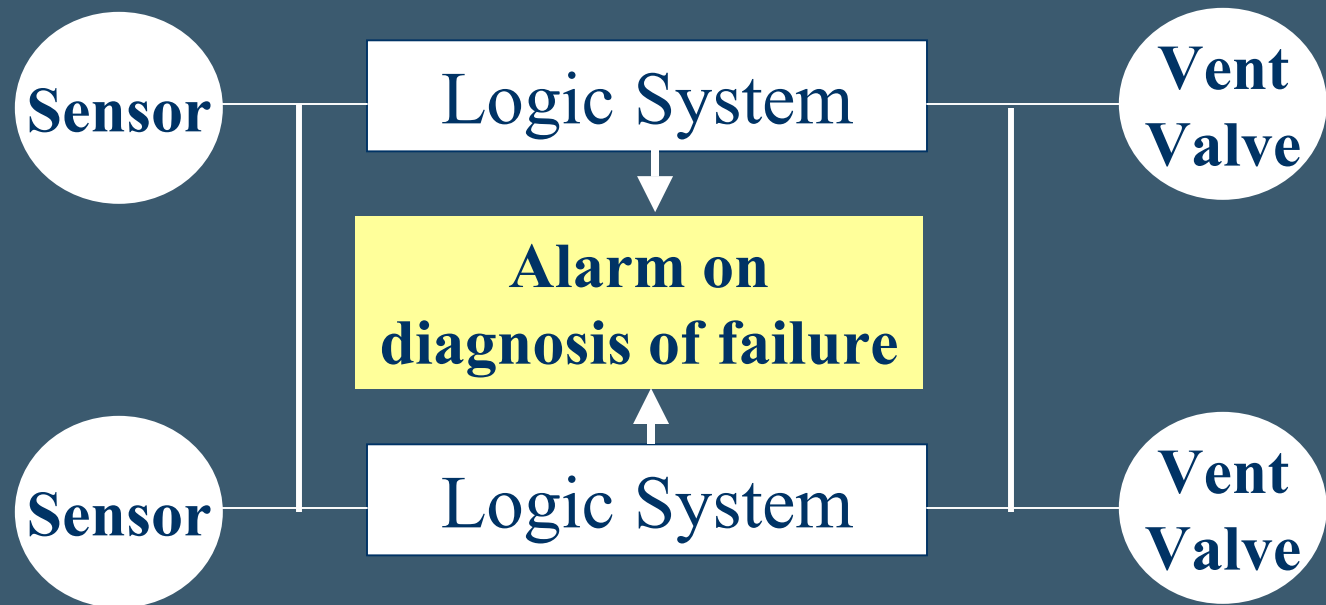


High demand/Continuous mode of operation
- a specified action to maintain a safe state

Low demand mode of operation
- a specified action to maintain a safe state or
- a repair in MTTR and additional measures
and constraints with equivalent risk reduction



Systems with fault tolerance > 0



All modes of operation

- a specified action to maintain a safe state or
- isolation of faulty part during MTTR

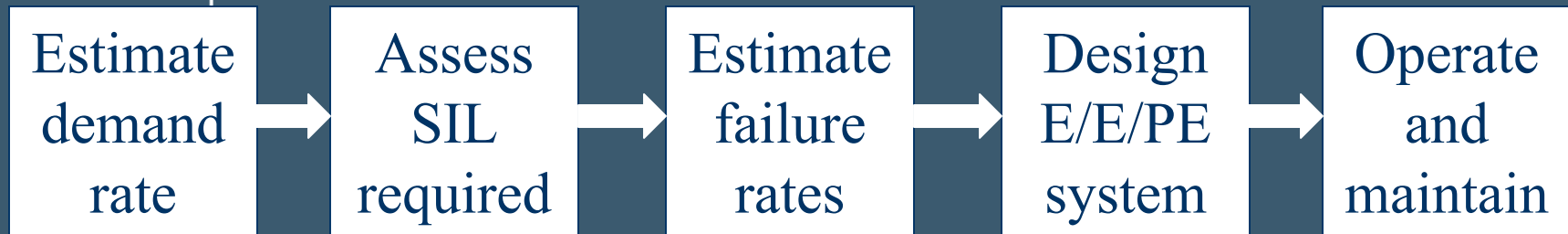


Operation and maintenance requirements

- Safety management procedures
- Maintenance schedules
- Maintenance of documentation
- Functional safety audits and assessments
- Modification procedures
- Performance monitoring
- Validation of design assumptions

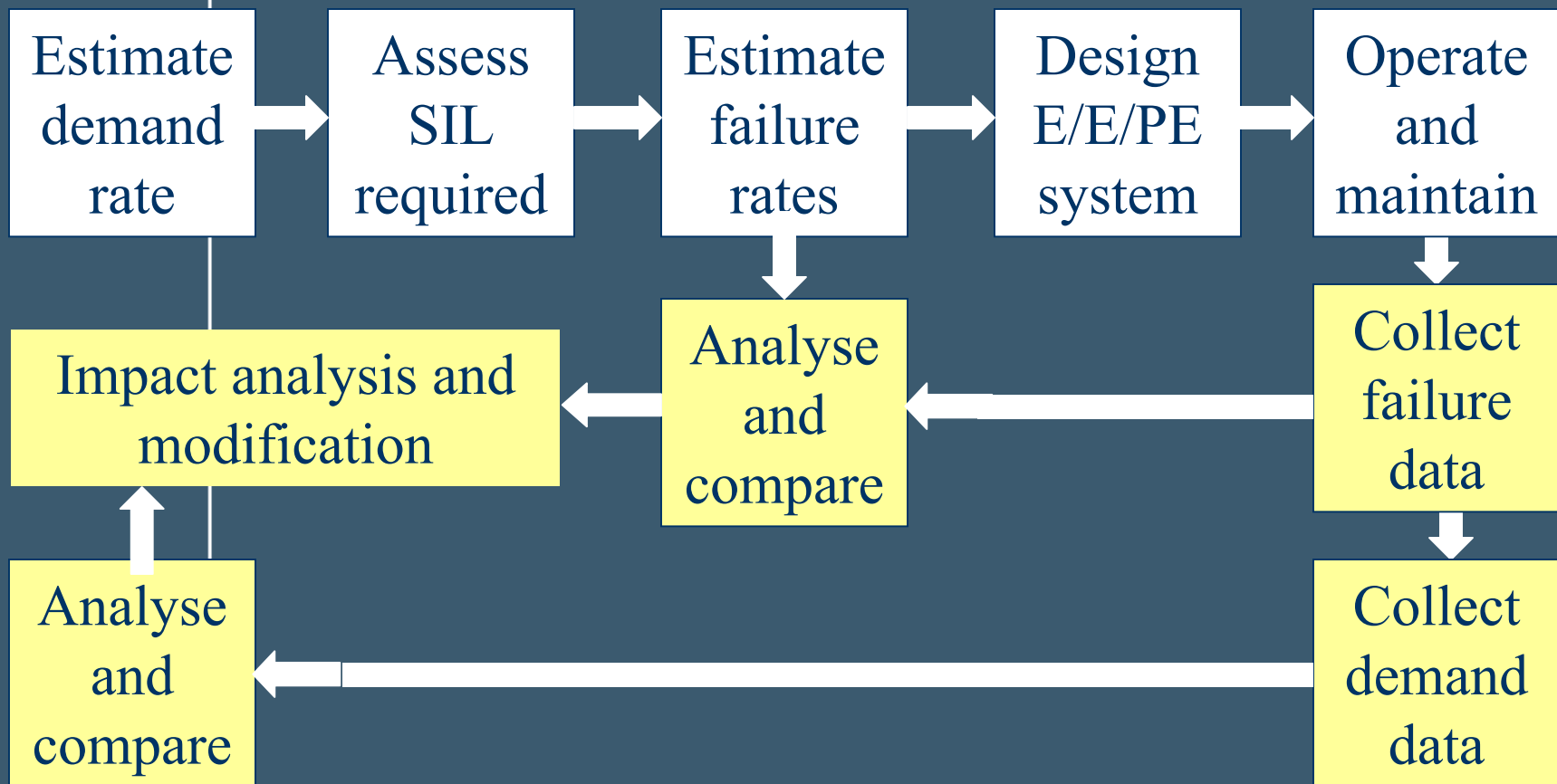


Design process





Validation of design assumptions





IEC 61508 - Functional Safety of E/E/PES safety related systems

Problem resolution

- The standards revision process
- Joint task team topics
- Task team 12 on software
- Task team 13 on systems
- Problems that cannot be resolved by revisions to standards



The standards revision process

All 7 Parts to be maintained in a synchronised manner in order to ensure that the revised version of IEC 61508 is coherent in all respects

The basis of the amendments will be based primarily on the comments from National Committees (NCs) and sufficient time will be allowed for NCs to collect and submit their comments

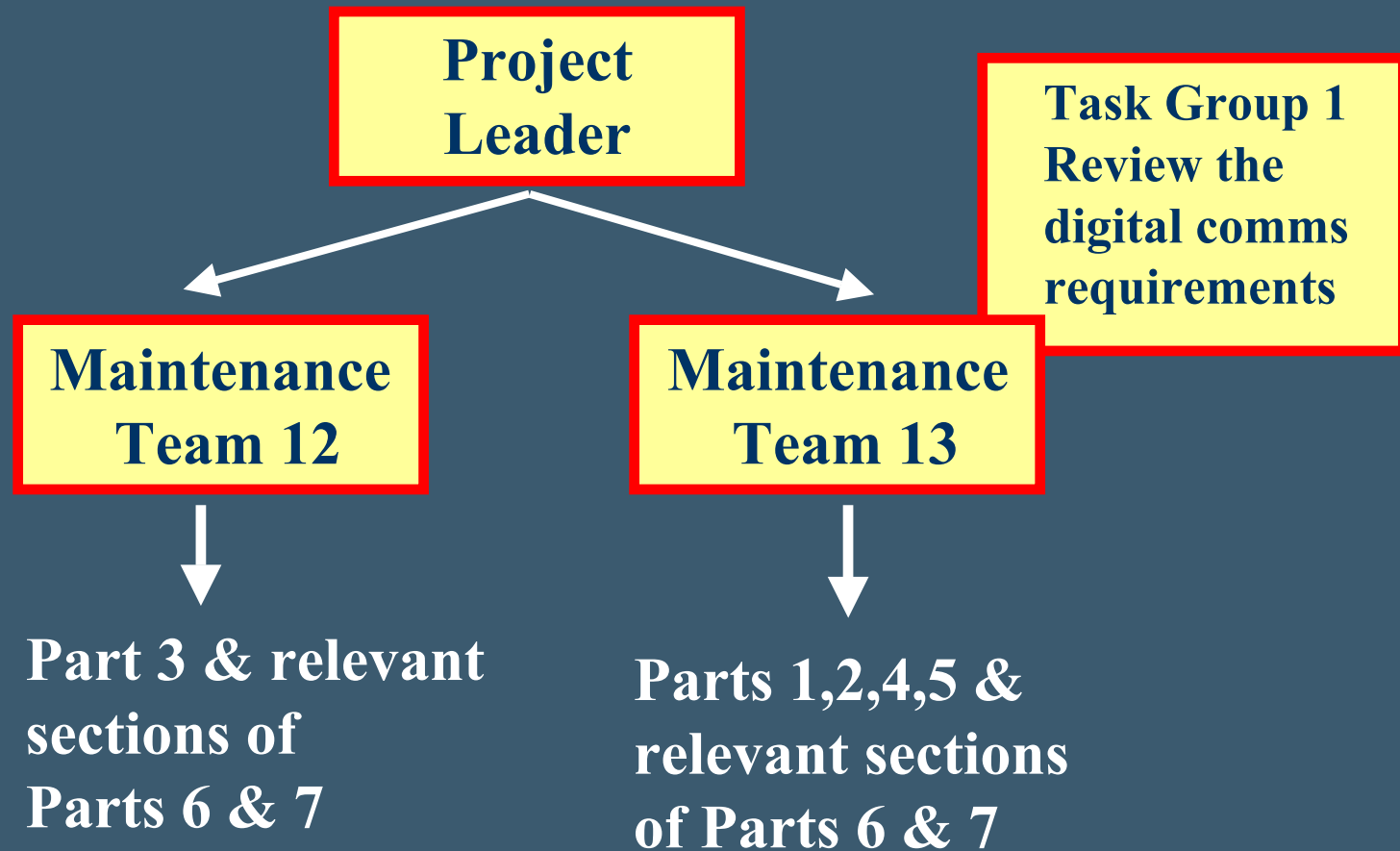


Revision schedule

Milestone	Target date
Maintenance Cycle Report finalised	February 2001
1st request to NC's for comments	February 2001
2nd request to NC's for comments on	October 2001
Consideration of NC comments by MT12 & MT13	February 2002
Maintenance Cycle Report to be sent to IEC/SC65A	March 2002
CD issued to NC's for comment	June 2004
CDV issued to NC's for comment and voting	February 2005
FDIS issued to NC's for voting	November 2005
Complete revision of IEC 61508; Parts 1-7	March 2006

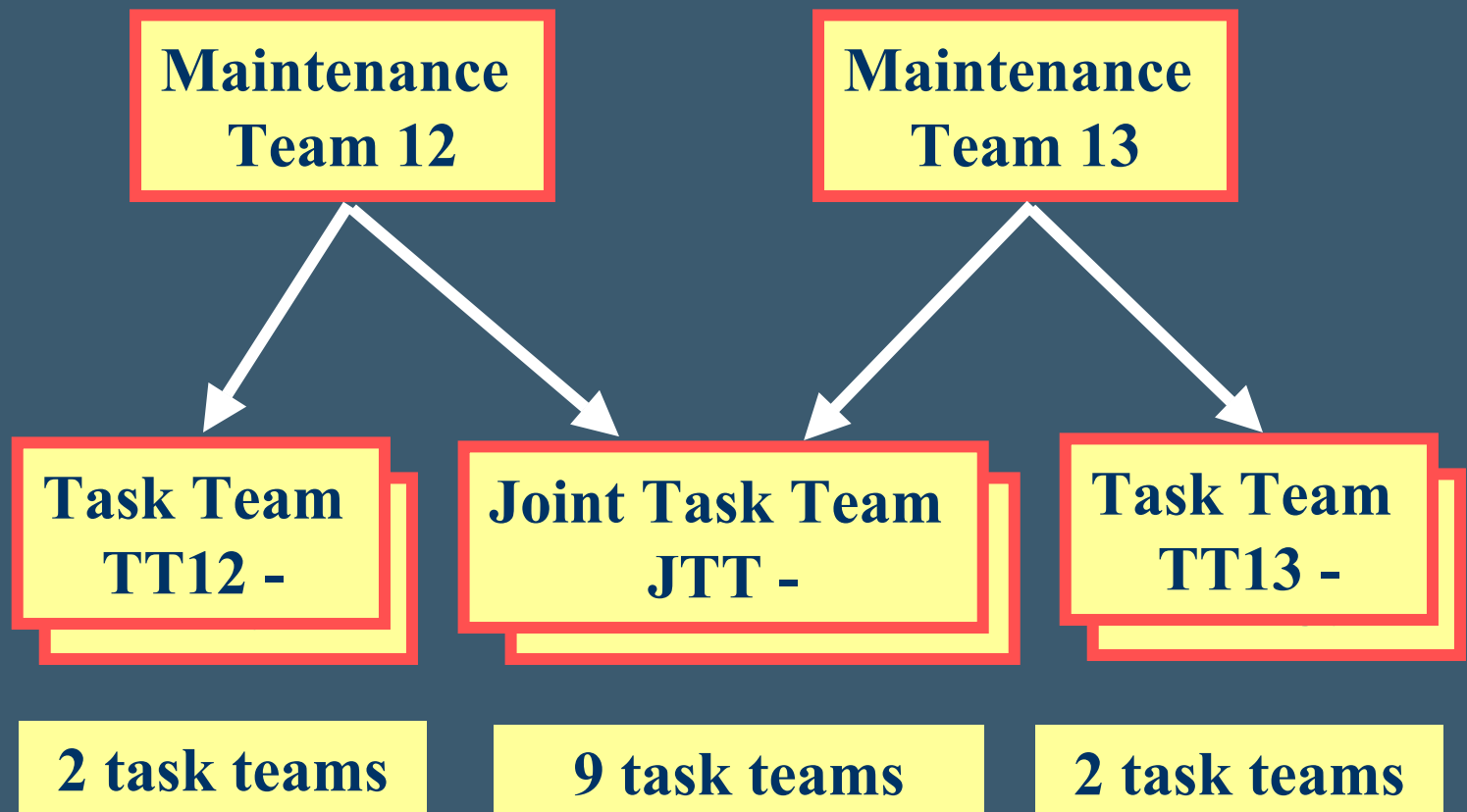


Revision basis





Task team working





Joint task team topics (1)

- Modes of operation
- Tools and techniques tables
- Architecture, sub-system requirements
- Complex integrated systems (ASICs)
- Component requirements
- Remote access and security



Modes of operation

National committee comments on:

- Need to clarify need for two tables
- Need to review current definitions of when the modes apply
- Need to provide examples of determining SILs for continuous mode functions



Modes of operation

Need two tables to model hazards:

- Low demand table based on Table 2
Hazard rate = demand rate x PFD(E/E/PES)

- Continuous based on Table 3:
Hazard rate = dangerous failure rate

- High demand rate based on Table 3:
Hazard rate (max) = dangerous failure rate

(examples of each will be included in Pt 5)
(all above assumes no other protection layers)



Modes of operation

- **low demand mode:** a safety function which is only performed on demand, at a rate no greater than 1 demand per year, in order to transfer the EUC into a specified safe state.
- **high demand mode:** a safety function which is only performed on demand, at a rate greater than 1 demand per year, in order to transfer the EUC into a specified safe state.
- **continuous mode:** a safety function that is intended to be performed continuously in order to retain the EUC in a safe state



Safety integrity levels - Table 2

Safety integrity level	Low demand mode of operation (Average probability of a dangerous failure of the safety function on demand PFD _{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$



Safety integrity levels - Table 3

Safety integrity level	High demand mode of operation (Average probability of a dangerous failure of the safety function on demand in an hour)
	Continuous mode of operation (Average probability of a dangerous failure of the safety function in an hour)
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 $< 10^{-5}$



Tools and techniques tables

National Committees consider tables:

- prescriptive
- restrictive
- out of date
- not objective based



Tools and techniques

Based on properties required to reduce likelihood of systematic failure

e.g. for system requirements specification require:

- **completeness of the safety needs (1)**
- **correctness of the safety needs (2)**
- **focus on safety (3)**
- **internal completeness (4)**
- **internal consistency (5)**
- **clarity (6)**
- **unambiguousness (7)**



System requirements specification

Recommended methods	1	2	3	4	5	6	7	S1	S2	S3	S4
Inventory of the input docs	o	o						x	x	x	x
Inventory of paragraphs of input	o	o								x	
Inventory of statements of inputs	o	o									x
Forward traceability to the srs	o	o								x	x
Backward traceability from the srs		o	o		o						x
Forward traceability to Validation		o				o	o			x	x
Simulation / prototyping		o		o	o					x	x
Rigorous reasoning srs covers functions and integrity requirements		o		o	o		o			x	x
Avoidance of unnecessary reqd			o			o				x	x
Checklists and guidelines	o			o				x	x	x	x



System requirements specification

Recommended methods	1	2	3	4	5	6	7	S1	S2	S3	S4
Use of appropriate combination of specification languages	0	0		0	0	0	0	X	X	X	X
Tools and techniques to aid understanding of the srs		0		0	0	0	0	X	X	X	X
Coverage of the allowed tolerances	0	0		0		0	0			X	X
Evidence of acceptability of the requirements to stakeholders	0	0	0	0	0	0	0			X	X
Critical review of the srs	0	0	0	0	0	0	0	X	X	X	X
Critical review of the selection of specification languages		0		0	0	0	0			X	X



Architecture and sub-systems

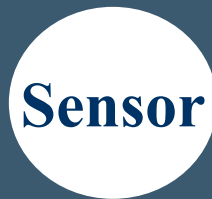
National committee comments:

- Define a methodology to enable SIL capability of overall function to exceed lowest SIL capability of sub-systems



Architectures and sub-systems

Sensor sub-system



SIL1 capable sensor

Logic sub-system



SIL3 capable logic system

Final actuator sub-system

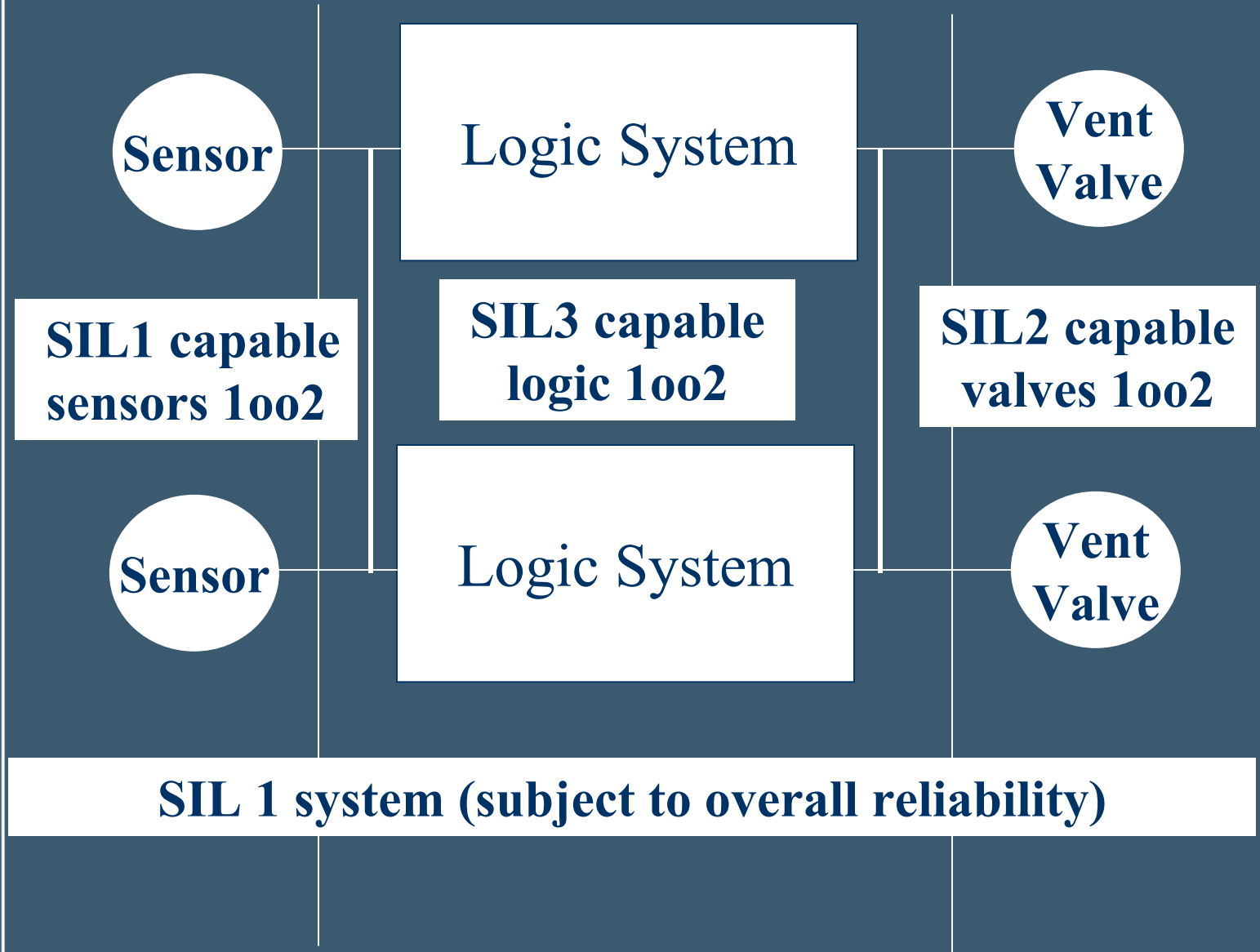


SIL2 capable valve

SIL 1 system (subject to overall reliability)



Architectures and sub-systems





Architecture and sub-systems

- Likelihood of systematic failure depends on complexity
- Capability of sub-system could depend on:
 - complexity of application?
 - diagnostic capability?
 - proven in use status?
 - software variability



Complex integrated systems

Requirements for ASICs

- Fault tolerance of a single ASIC can be greater than zero subject to requirements
- common cause failure based on basic β -factor called β_{B-ASIC} of 33 % (+ & -)
- Techniques and measures defined

Measures and techniques defined for user programmable ASICs, FPGAs and PLDs

Special requirements for FPGAs and PLDs



Component requirements

- Need to define requirements for compliance assessed products
- Function block based
- Will need to define application factors
- Define information and documentation requirements
- Requirements defined in Annex with references specific to products



Remote access and security

- Protection against intrusion from outside or malicious insiders
- Threat analysis for all lifecycle stages resulting in threat SIL (TSIL)
- Based in EALs in ISO/IEC 15408
- Management procedures based on ISO/IEC 15408 and ISO/IEC 17799
- Security analysis integrated into Hazard Analysis and documented



Remote access and security

- Safety related and security related software should/shall be kept separate
- Several echelons of defence shall always exist
- No part of safety related software shall be directly accessible from any public net
- Data transmission sender should/shall be identified
- Requirements for authenticity and Integrity of Software



Joint task team topics (2)

- Integrity and qualification of tools
- Human factors
- Safety manual for pre-existing components
- Configuration management
- Probabilistic modelling of systematic factors



Task team 12 topics (software)

- Application software characterisation
- Operational changes



Application software characterisation

Objective:

To define requirements for applications and sectors where the application logic is expressed as the critical configuration data of some otherwise standard system components.



Application software characterisation - proven in use

- “Proven -in use” in part 2 is a systems issue (hardware and software)
- Current basis of qualification is based on operational profile and statistical evidence
- Current basis is not adequate for complex applications, equipment or software
- Current basis requires “clearly restricted functionality”
- Nearly all software has pre -existing elements



Application software characterisation - proven in use

“Proven in use” for software needs:

- to allow a justification based on analysis for systematic failure
- recognise statistical basis is not sufficient
- clearly restricted functionality should not exclude the case where a convincing argument can be made that the extra functionality will not be triggered in SRS
- to take account of complexity, observability, evidence and SIL



Application software characterisation - Data driven

Additional requirements:

- ensure that appropriate methods are implemented to load data into the run-time system.
- where safety requirements are specified as application data
- where data defines the interface between software and external systems
- protection of operational parameters



Application software characterisation - Data driven

Additional requirements for

- design of the application software if pre-existing software is configured by data
- appropriate techniques and measures used to prevent introduction of faults
- specification of data structures
- verification of data



Operational changes

- **identify the different types of software change that may occur**
- **Provide recommendation on whom may perform the changes and the competency requirements**
- **define when change control is to be applied.**
- **provide guidance on the interface requirements between the operations personnel and the personnel performing the change.**
- **guidance on the hand-over**



Task team 13 topics

- Determination of safety requirements specification
- EMC and functional safety
- Markof modelling
- Safe failures
- Digital communications



Safety requirements specification

- Incident analysis suggests that poor specification is a major cause of accidents.
- Guidance is needed for deriving complete and unambiguous specifications from the results of hazard analysis.
- Work is needed to address mitigation and control systems particularly in the context of sectors other than process control.



Hazard and risk analysis

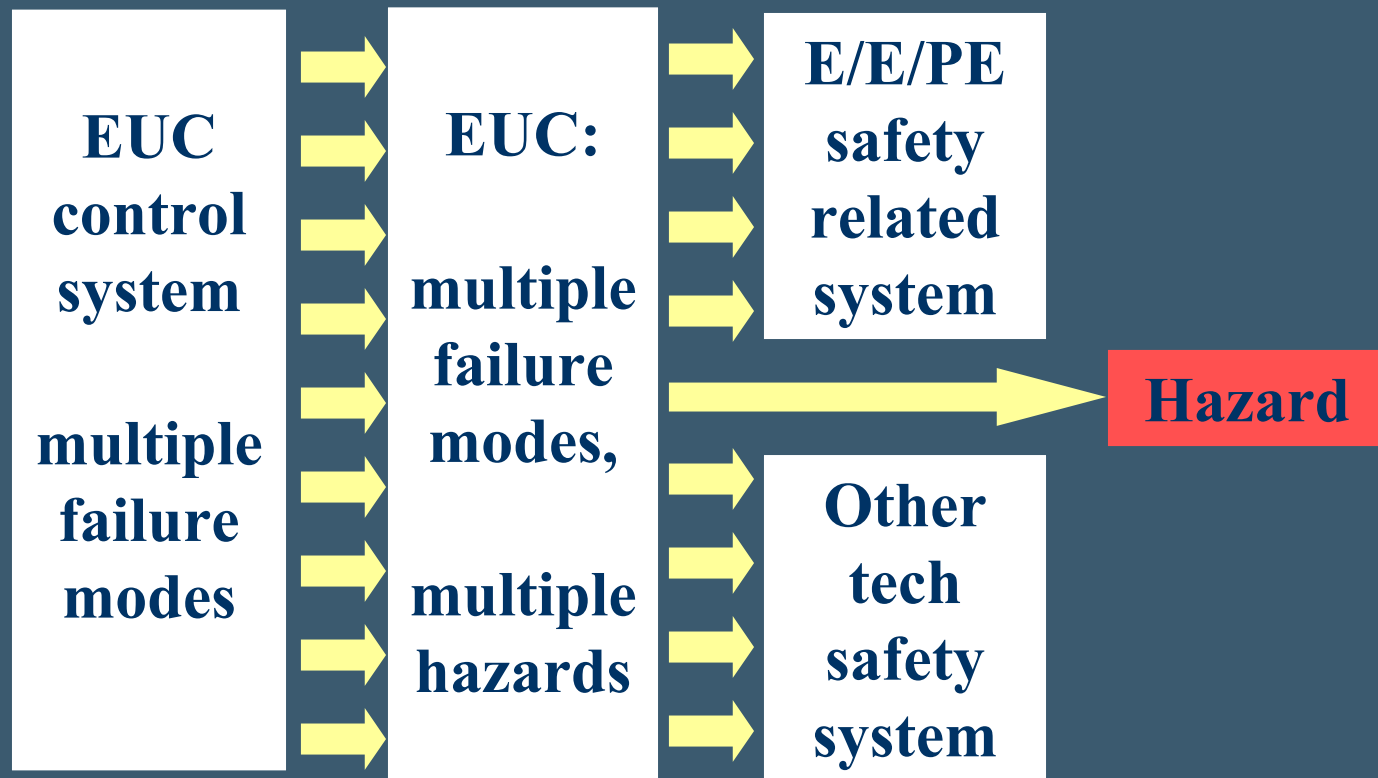
Current requirement

- All reasonably foreseeable dangerous failure modes of the EUC control system shall be determined and taken into account in developing the specification for the overall safety requirements

Question - How to do this for complex control systems with multiple inputs and outputs



Reasonably foreseeable?





Hazard and risk analysis

References

- BS IEC 61882:2001 Hazard and Operability studies (HAZOP) – Application Guidance
- System Safety: HAZOP and Software HAZOP by Felix Redmill

Problems

- Insufficient skills, time and information to undertake this for COTS used for EUC control



Hazard and risk analysis

Proposal to add list of what needs to be considered:

- all relevant human factor issues
- hardware failures of processors, communications and input and output modules
- software failures of embedded and application software
- failures that cause loss of alarm and operator display.



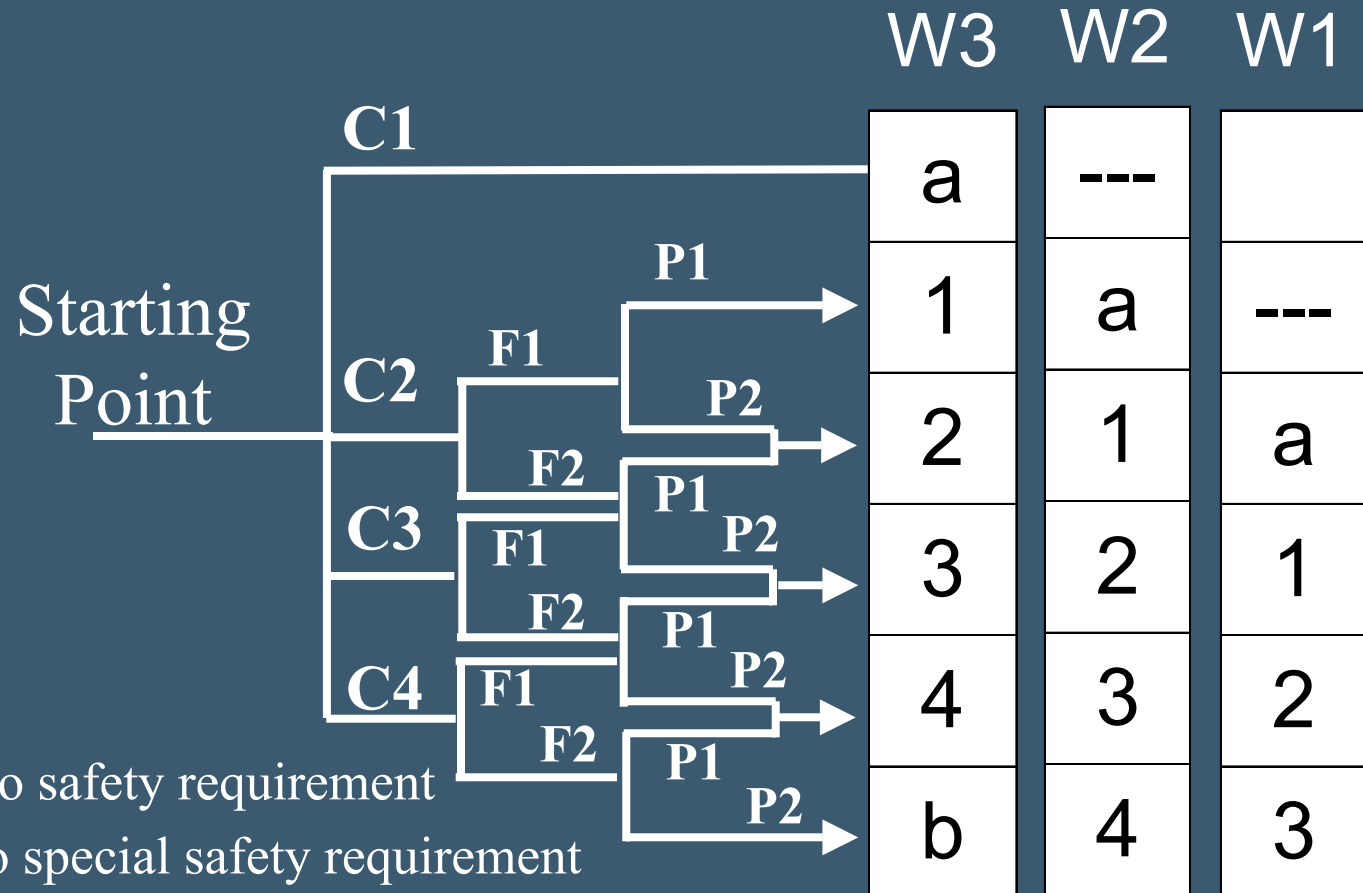
Risk reduction and allocation

Evidence that SIL determination is not being carried out correctly because

- Methods used are not auditable, repeatable and give no assurance that risks are reduced to corporate requirements
- Targets used do not take into account risks from other sources and other E/E/PES systems
- Environmental and commercial risks are not being considered



Risk graph determination of SIL



- no safety requirement
- a - no special safety requirement
- 1,2,3,4 - safety integrity level
- b - a single E/E/PES is not sufficient



Data on risk graph

Risk parameter		Classification
Consequence (C)	<i>C</i> ₁	Minor injury
	<i>C</i> ₂	Permanent injury or death to one person
	<i>C</i> ₃	Death to several people
	<i>C</i> ₄	Very many people killed
Frequency of, and exposure time in, the hazardous zone	<i>F</i> ₁	Rare to more often exposure in the hazardous zone
	<i>F</i> ₂	Frequent to permanent exposure in the hazardous zone
Possibility of avoiding the hazardous event	<i>P</i> ₁	Possible under certain conditions
	<i>P</i> ₂	Almost impossible
Probability of the unwanted occurrence	<i>W</i> ₁	A very slight probability that the unwanted occurrences will come to pass
	<i>W</i> ₂	A slight probability that the unwanted occurrences will come to pass
	<i>W</i> ₃	A relatively high probability that the unwanted occurrences will come to pass



Risk reduction and allocation

Proposed additional requirement:

In determining the necessary risk reduction account shall be taken of other risk that persons are exposed to such as:

- other non functional safety risks
- functional safety risks associated with other technology and external risk reduction facilities
- the number of E/E/PES systems required for functional safety



Risk reduction and allocation

Proposed additional guidance:

- Derivation of targets for individual risk for individual E/E/PES
- Targets for continuous improvement based on reducing the risk to as low as reasonably practicable
- Targets for societal risk



Safety requirements specification

Proposal to split specification into two stages

- a logical specification containing functional and integrity descriptions.
- a physical specification containing equipment hardware and software descriptions and drawings



Logical specification

- The specification should not contain descriptions of equipment hardware or software
- It shall be expressed in natural or formal language and/or logic, sequence or cause and effect diagrams.
- The logic specification shall be defined prior to E/E/PES design and development
- Verified against the results of the hazard identification



The physical specification

- The physical specification shall document the outcome of the design process including:
 - physical equipment used
 - hardware and software architecture
 - fault tolerance and reliability
 - diagnostics, interfaces, communications
- The physical specification is verified against the logical specification



Conclusions

In 2006 we will have an improved standard and improved guidance but:

- IEC 61508 will not be a textbook
- Will not define risk targets
- Will need competency and judgement to apply
- Will always be out of date - standards always lag experience