ENGINEERING SAFETY CONSULTANTS

The Global Provider of Functional Safety Expertise and Technical Consultancy

The changes to IEC 61508/Edition 2
&
implications for users of the standard

Ron Bell
Engineering Safety Consultants Ltd
ron.bell@esc.uk.net
www.esc.uk.net

Revision of IEC 61508

1. Background
2. Some key changes of the revised standard
3. Using the new edition
4. Concluding comments

IEC 61508: Brief history

- I985: Task Group set up to assess viability of developing a generic standard on PES's
- Two working groups collaborated on development of IEC standard that was to become IEC 61508
- 1998 – 2000: The parts of IEC 61508 (1/2/3/4/5/6/7) Edition 1 were published
- 2005: PD IEC TR 61508-0 was published
- "ENs" adopted in same year as the IEC publication dates
- 2003: Revision of IEC 61508 / Edition started
- 2010: IEC 61508 / Edition 2 was published in April

IEC 61508 and Functional Safety

Title: Functional safety of electrical, electronic & programmable electronic safety-related systems….

A eight Part international standard covering all safety lifecycle activities...concept..... specification...design...implementation…operation maintenance & modification

IEC 61508 and Functional Safety

- Part 0: Functional safety and IEC 61508 (IEC TR 61508-0)
- Part 1: General requirements
- Part 2: Requirements for electrical, Electronic, programmable electronic 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 the application of Parts 2 & 3
- Part 7: Overview of techniques and measures

IEC 61508 and Functional Safety

- Part 0: Functional safety and IEC 61508 (IEC TR 61508-0)
- Part 1: General requirements
- Part 2: Requirements for electrical, Electronic, programmable electronic 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 the application of Parts 2 & 3
- Part 7: Overview of techniques and measures

- Parts 1, 2 & 3 contain normative & informative requirements
- Parts 0, 5, 6 & 7 contain only informative requirements
- A “shall” is a normative requirement
- A “should” is an informative requirement
- Notes are informative

The Parts of IEC 61508 revised

- ~~Part 0: Functional safety and IEC 61508~~ (Not revised)
- Part 1: General requirements
- Part 2: Requirements for electrical, Electronic, programmable electronic 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 the application of Parts 2 & 3
- Part 7: Overview of techniques and measures

Revision of IEC 61508

1. Background
2. Some key changes of the revised standard
3. Using the new edition
4. Concluding comments

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

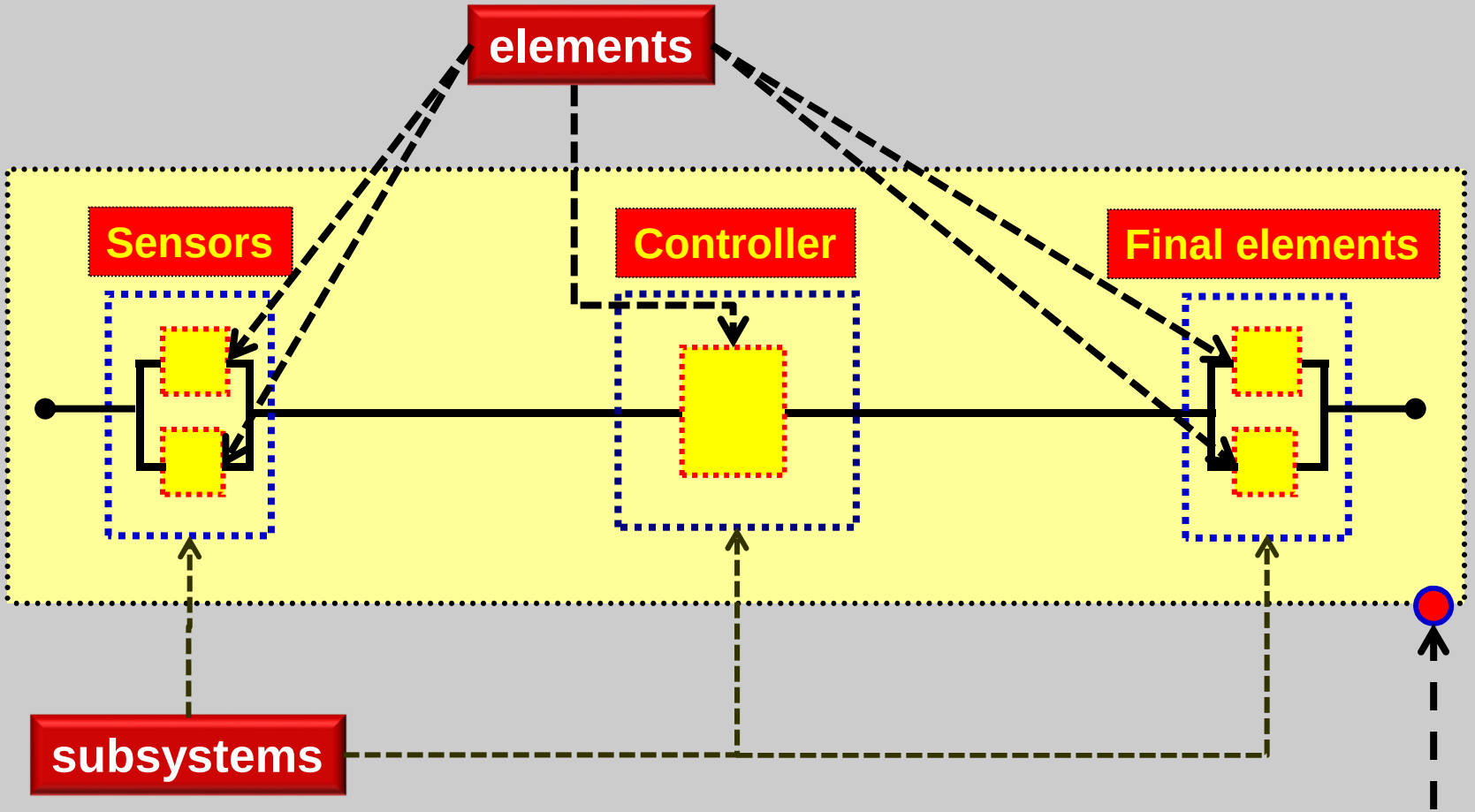
Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

Terminology

- Several important changes to the definitions
- Important they are examined …..the change may affect the interpretation as understood in IEC 61508/Edition 1
- Include **dangerous failure**, **safe failure**, **element** and **element safety function**.
- Example; **subsystem**:
  - Key feature…failure of the subsystem will result in the failure of the safety function
  - For correct usage of the term ….. necessary to have knowledge of the dangerous failures associated with the specified safety function…need to know the application

Terminology: System & Subsystem



Failure of the subsystem will result
in the failure of the safety function

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

Architectural Constraints

Route 1_H: based on hardware fault tolerance and safe failure fraction concepts; or,

Route 2_H: based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.

Architectural Constraints

Route 1_H: based on hardware fault tolerance and safe failure fraction concepts; or,

Route 2_H: based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.

Architectural 1_H: Constraints Route 1_H

- Based on hardware fault tolerance and safe failure fraction concepts;
- Some changes made to the method of calculating the maximum SIL that can be claimed;
- new definitions of safe & dangerous failures will also have an impact on maximum SIL that can be claimed;
- Important the clauses are read before applying the Tables!

Architectural Constraints

Route 1_H: based on hardware fault tolerance and safe failure fraction concepts; or,

Route 2_H: based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.

Architectural Constraints: Route 2_H

IEC 61508-2: Clause 7.4.4.3.1

- A hardware fault tolerance of 2 for a specified safety function of SIL 4 unless the conditions in clause 7.4.4.3.2 apply.
- A hardware fault tolerance of 1 for a specified safety function of SIL 3 unless the conditions in clause 7.4.4.3.2 apply.
- A hardware fault tolerance of 1 for a specified safety function of SIL 2, operating in a high demand or continuous mode of operation, unless the conditions in clause 7.4.4.3.2 apply.
- A hardware fault tolerance of 0 for a specified safety function of SIL 2 operating in a low demand mode of operation.
- A hardware fault tolerance of 0 for a specified safety function of SIL 1.

Architectural Constraints: Route 2_H

IEC 61508-2: Clause 7.4.4.3.2

- **For Type A elements only:** HFT can be reduced to those specified in 7.4.4.3.1 providing there is evidence that:
  - by following the requirements in 7.4.4.3.1 would introduce additional failures and would lead to a decrease in overall safety of the EUC; and
  - if HFT is reduced to zero the failure modes, in the element carrying out the safety function, can be excluded because the associated dangerous failure rates are very low compared to the target failure measure for the safety function

A note to 7.4.4.3.2 indicates that fault tolerance is the preferred solution

Architectural Constraints: Route 2_H (cont'd)

- If Route 2_H is selected then reliability data used for quantifying the effect of random hardware failures shall be:
  - based on field feedback
  - collected in accordance with international standards
  - evaluated …to estimate uncertainty levels
- The data uncertainties shall be [taken into account] when calculating the target failure measure
- The system shall be improved until there is a confidence greater than 90% that the target failure measure has been achieved
- All type B elements used in Route 2H shall have, as a minimum, a diagnostic coverage of not less than 60 %.

Architectural Constraints: Route 2_H

IEC 61508-2 / 7.4.4.3

SIL	Low Demand Mode	High Demand or continuous	For Type A elements: HFT can be reduced if an HFT > 0 is specified by 7.4.4.3.1 but which would lead to a decrease in the overall safety
SIL 1	0	0	0
SIL 2	0	1	(Can be reduced to 0 if λ_D is very low)
SIL 3	1	1	(Can be reduced to 0 if λ_D is very low)
SIL 4	2	2	1 (Can be reduced to 0 if $\lambda_D$is very low

Note: λ_D is very low if the sum of the dangerous failure frequencies of all serial elements, on which fault exclusion is being claimed, does not exceed 1 % of the target failure measure for the safety function (see 7.4.4.3.2 (b))

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

Systematic safety integrity
Three Routes to compliance

- **Route 1_S:** Requirements for the avoidance (prevention) and requirements for the control of systematic faults

- **Route 2_S:** Evidence that the equipment is “proven in use” (PIU)

- **Route 3_S:** Pre-existing software elements only: compliance with the requirements of IEC 61508-3 (7.4.2.12)

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

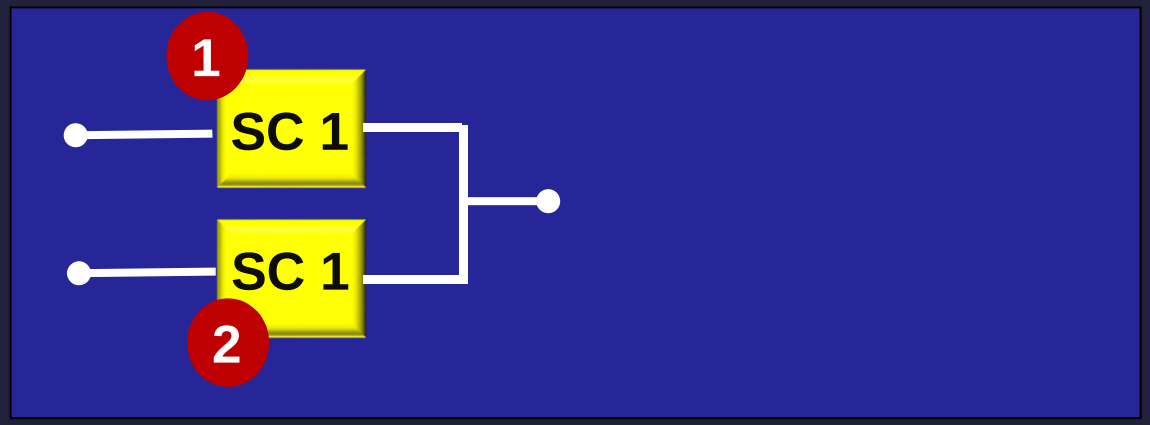
Revision of IEC 61508: Overview

Systematic Capability

Measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function…

The concept of Systematic Capability is new to IEC 61508/Edition 2

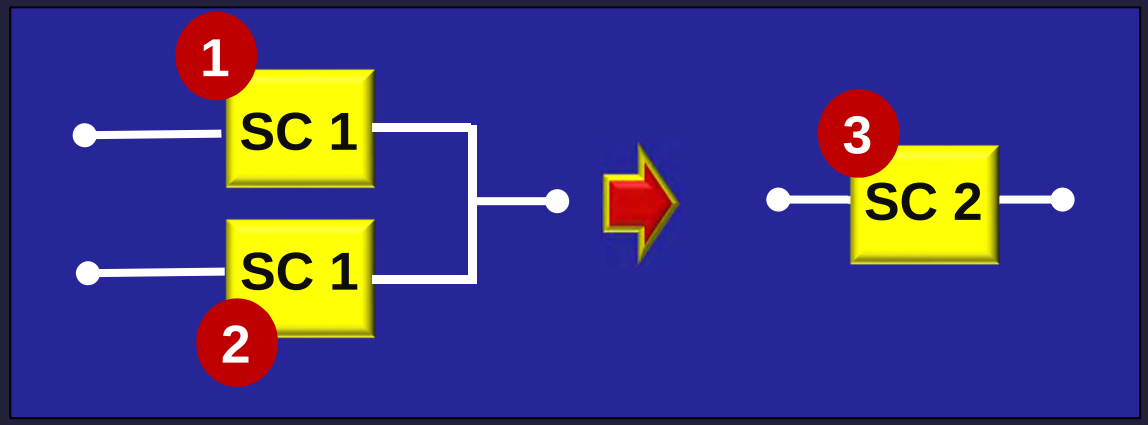
IEC 61508-2: 7.4.3: Synthesis of elements to achieve the required systematic capability



- A systematic fault of element 1 does not cause a failure of the specified safety function but does so only in combination with a second systematic fault of element 2

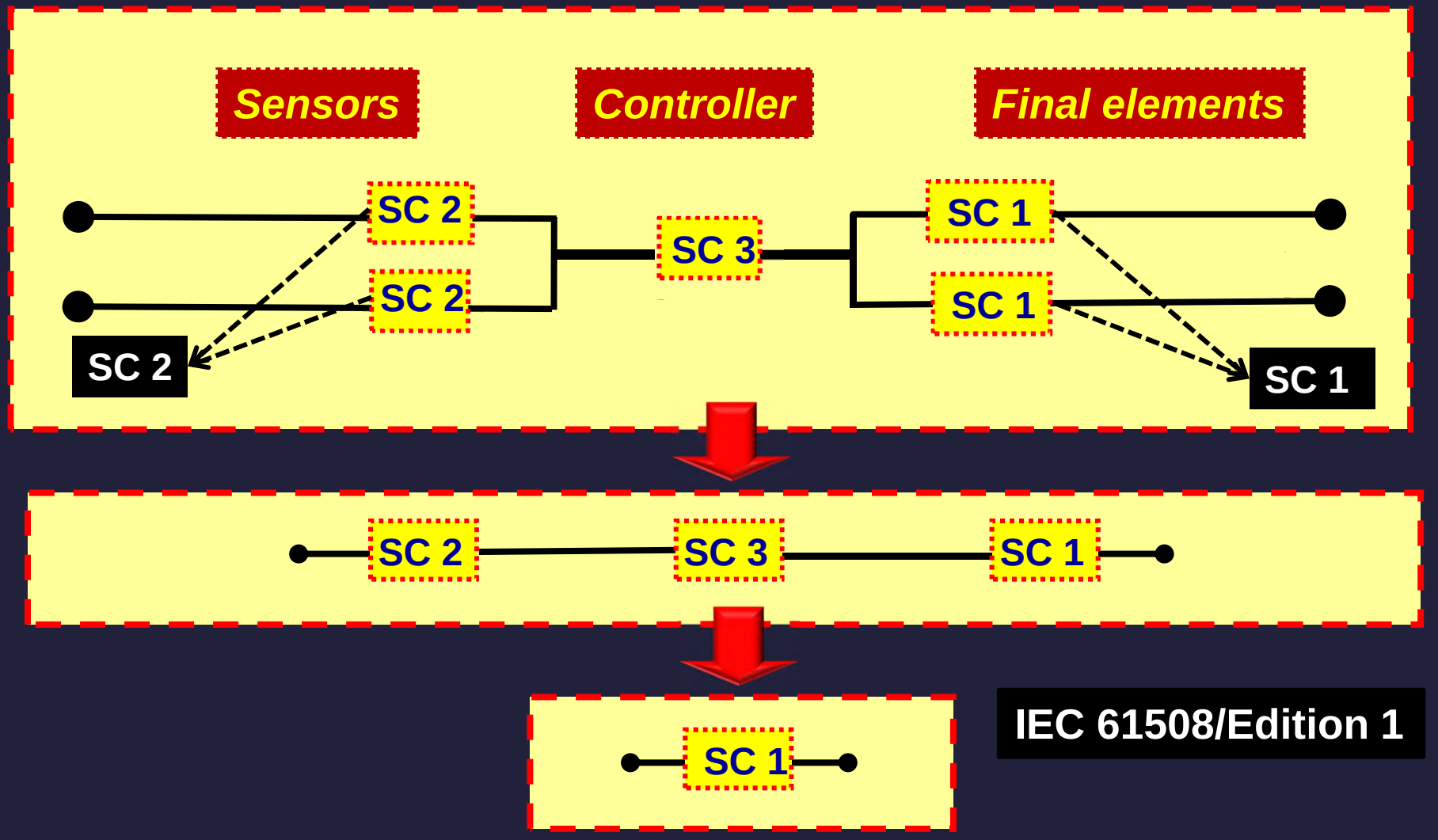
- Elements 1 & 2 sufficiently independent of each other

IEC 61508-2: 7.4.3: Synthesis of elements to achieve the required systematic capability



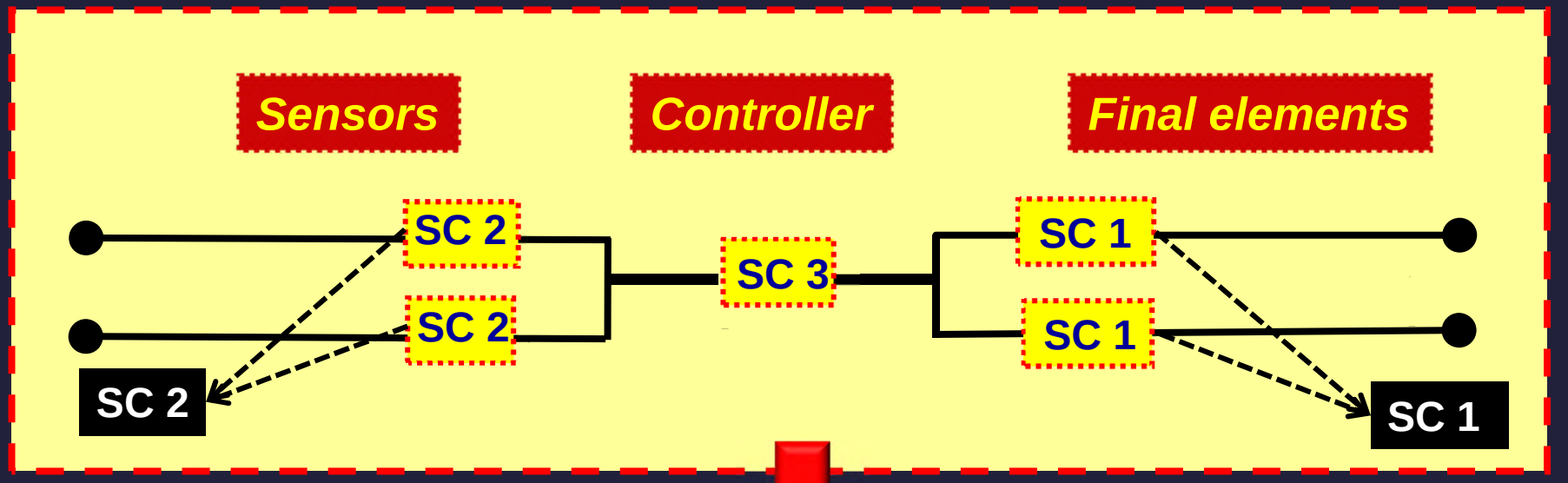
- A <u>systematic fault</u> of element 1 does not cause a failure of the specified safety function but does so only in combination with a second <u>systematic fault</u> of element 2
- Elements 1 & 2 sufficiently independent of each other
- The combination of elements 1 & 2 leads to systematic capability of SC 2

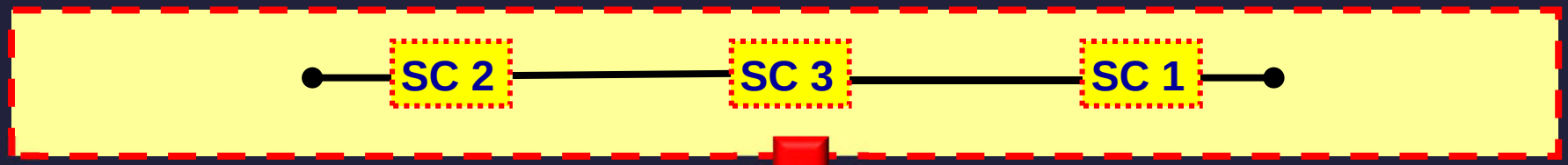
Simplified Example:
Systematic Safety Integrity / Systematic Capability



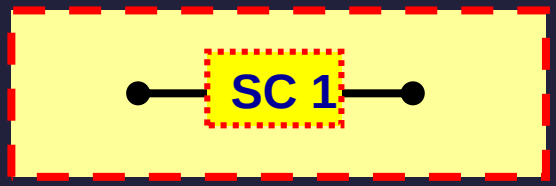
System limited to SIL 1 for specified safety function

Simplified Example:
Systematic Safety Integrity / Systematic Capability





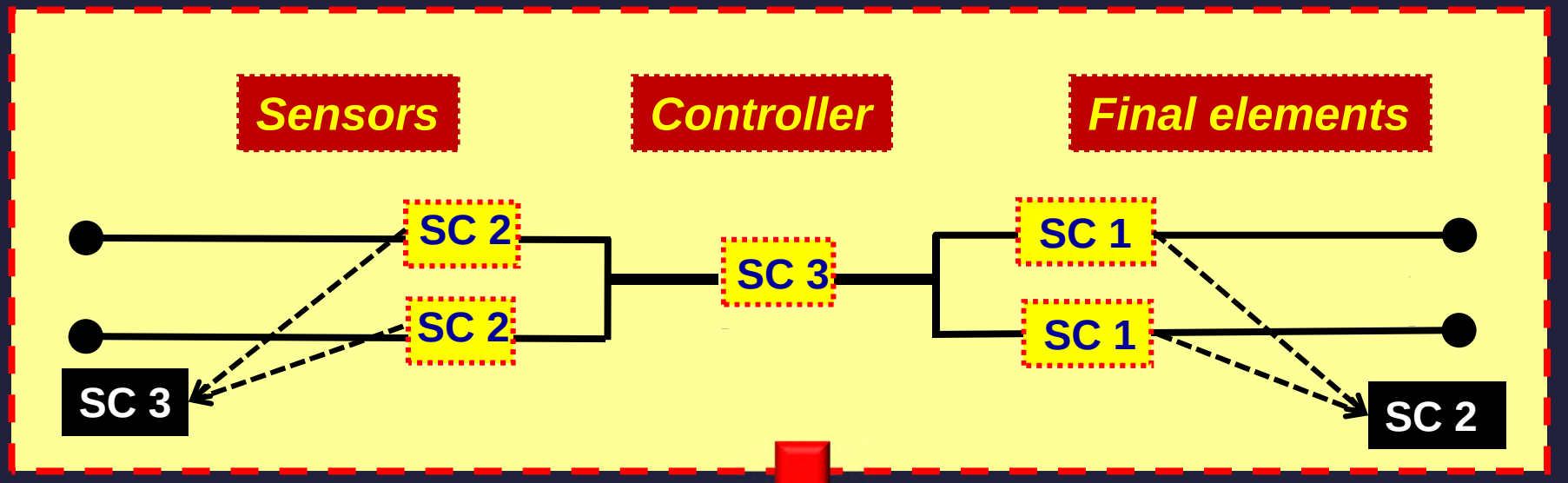
Sensors & Final elements not sufficiently independent!

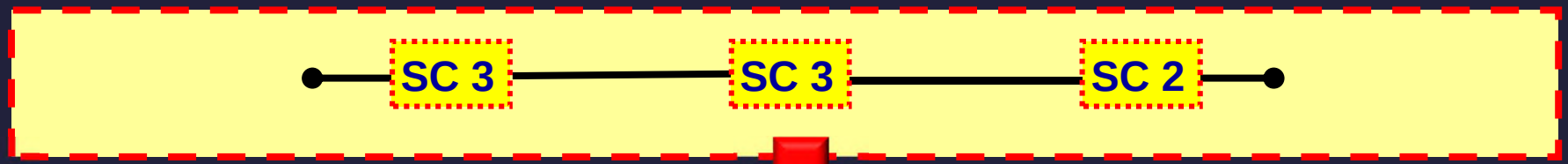


IEC 61508/Edition 2

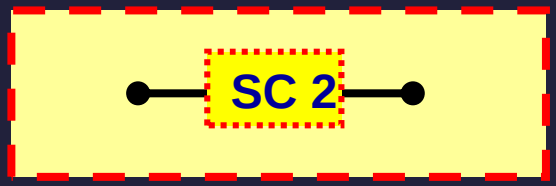
System limited to SIL 1 for specified safety function

Simplified Example:
Systematic Safety Integrity / Systematic Capability





Sensors & Final elements sufficiently independent!



IEC 61508/Edition 2

System limited to SIL 2 for specified safety function

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

Security aspects

- Requires malevolent and unauthorised actions to be addressed during hazard and risk analysis. If security threat is seen as being reasonably foreseeable, then:
  - a security threats analysis should be carried out
  - if security threats have been identified then a vulnerability analysis should be undertaken in order to specify security requirements.

Rationale for the policy: Other IEC/ISO standards will be referenced that address this subject in depth

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

Target Failure Measures: Edition 1

Safety Integrity Level (SIL)	Target Failure Measures for a safety function allocated to an E/E/PE safety-related system	
	Low demand mode of operation Average probability of failure/demand See IEC 61508-4; 3.5.12	**High demand/continuous mode of operation** Dangerous failure rate [per hour] See IEC 61508-4; 3.5.12
4	**Low demand mode:** Where the frequency of demands for operation made on an SRS is no greater than: • one per year; and, • no greater than twice the proof-test frequency	**High demand/continuous mode:** Where the frequency of demands for operation made on an SRS is greater than: • one per year; or, • greater than twice the proof-test frequency
3		
2		
1		

Target Failure Measures: Edition 2

Safety Integrity Level (SIL)	Target Failure Measures for a safety function allocated to an E/E/PE safety-related system	
	Low demand mode of operation Average probability of failure/demand **See IEC 61508-4; 3.5.12**	**High demand/continuous mode of operation** Dangerous failure rate [per hour] **See IEC 61508-4; 3.5.12**
4	**Low demand mode:** Where the frequency of demands for operation made on an SRS is no greater than: • one per year; ~~and,~~ ~~• no greater than twice the proof-test frequency~~	**High demand/continuous mode:** Where the frequency of demands for operation made on an SRS is greater than: • one per year~~; or,~~ ~~• greater than twice the proof-test frequency~~
3		
2		
1		

Overview of key changes

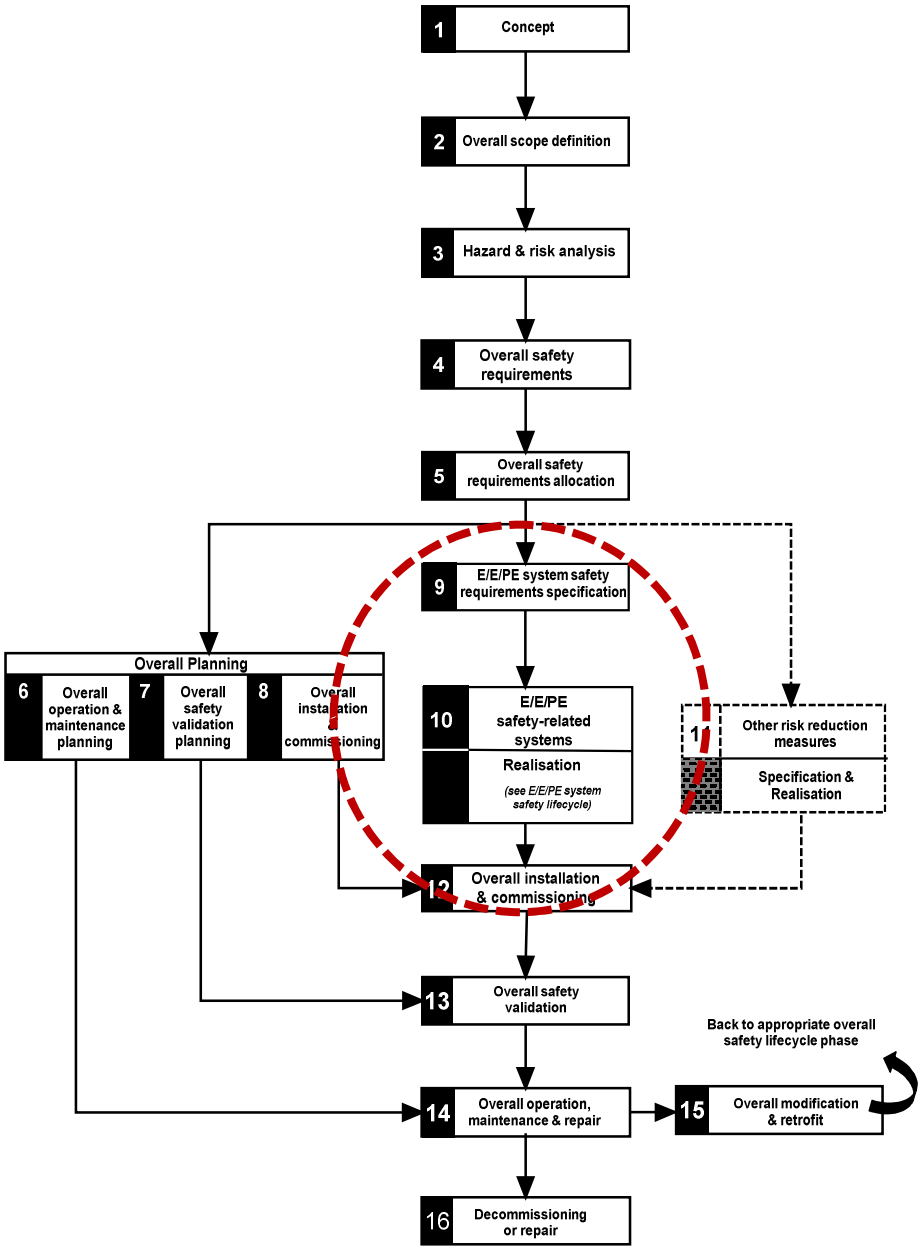
1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

E/E/PE safety requirements specification(s)

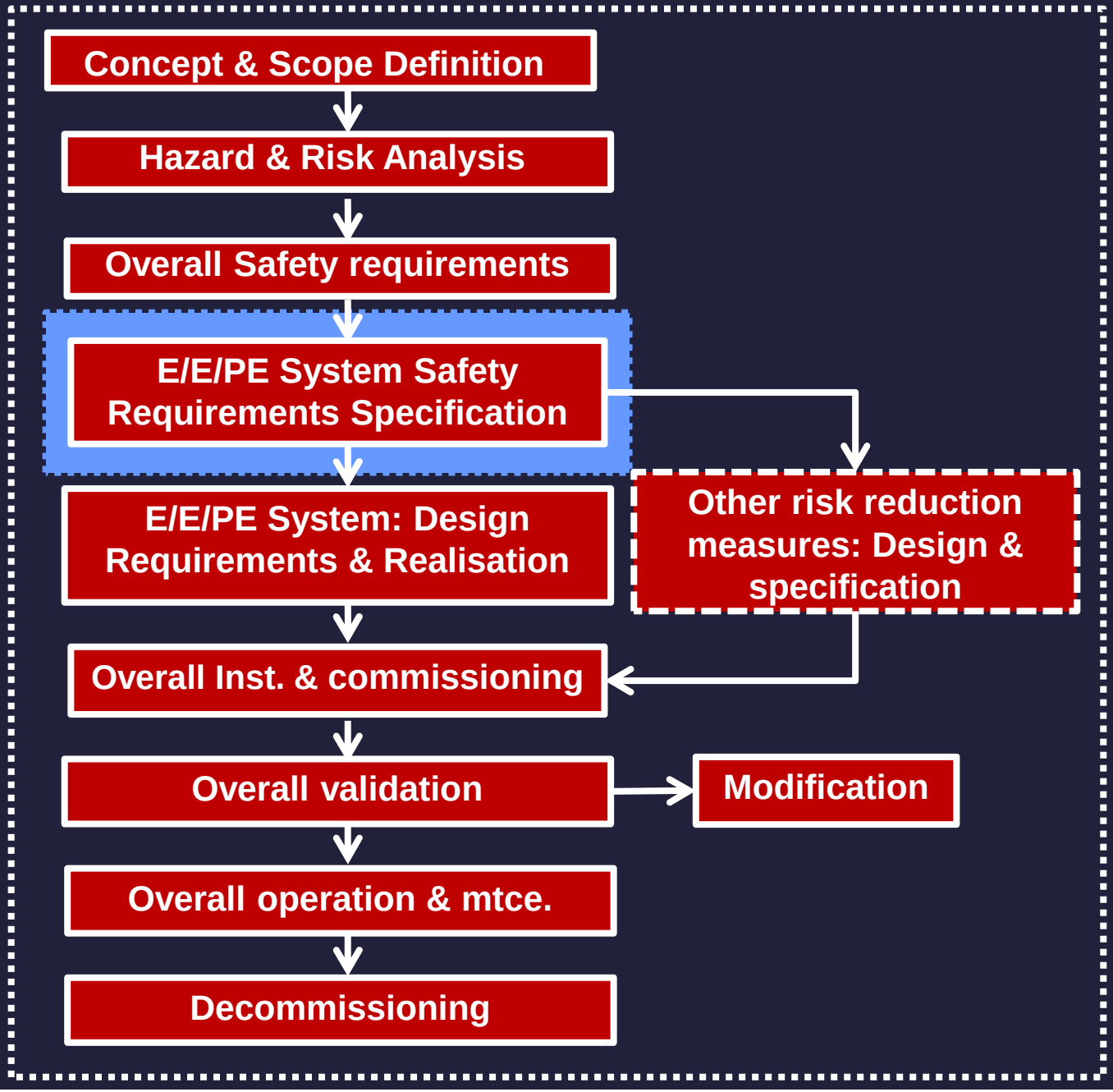
- Was a single specification …single step process:
  1. E/E/PES safety requirements specification

- Now two specifications …two step process:
  1. E/E/PE system safety requirements specification (IEC 61508-1);
  2. E/E/PE system design requirements specification (IEC 61508-2).

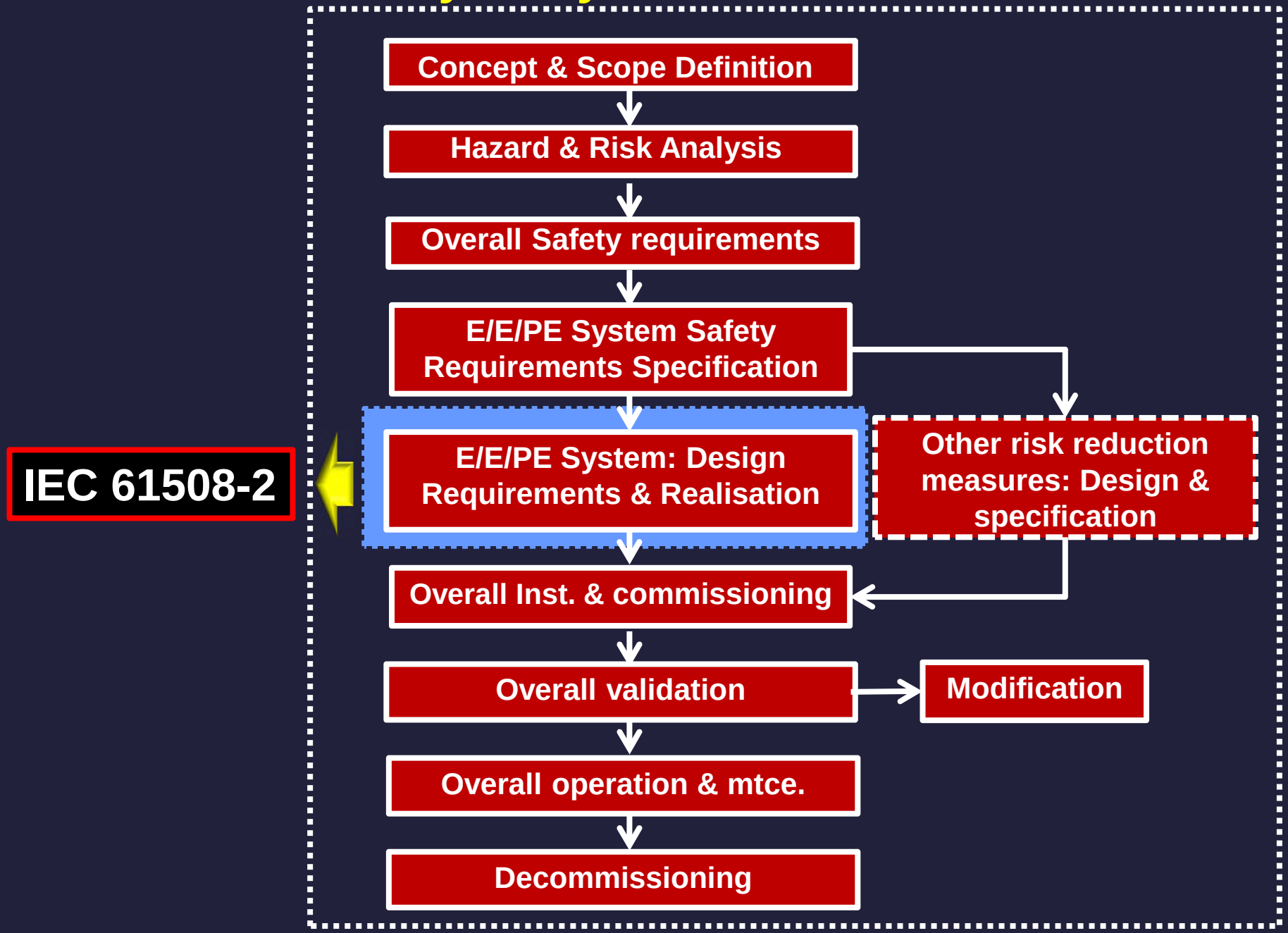
Overall Safety Lifecycle of IEC 61508



Overall safety lifecycle: IEC 61508 – Part 1



Overall safety lifecycle: IEC 61508 – Part 1



Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

Data Communications

- Digital Communications……the requirements have been elaborated
- White Channel and Black Channel architectures for data communications

Data Communications

Entire communication channel (including protocol, services & network components) comply with IEC 61508 & (IEC 61784-3 or IEC 62280)

WHITE CHANNEL

Interfaces comply with IEC 61784-3 or IEC 62280 (including services & protocols)

BLACK CHANNEL

Parts of the communication channel between the interfaces are <u>not</u> designed or validated to IEC 61508

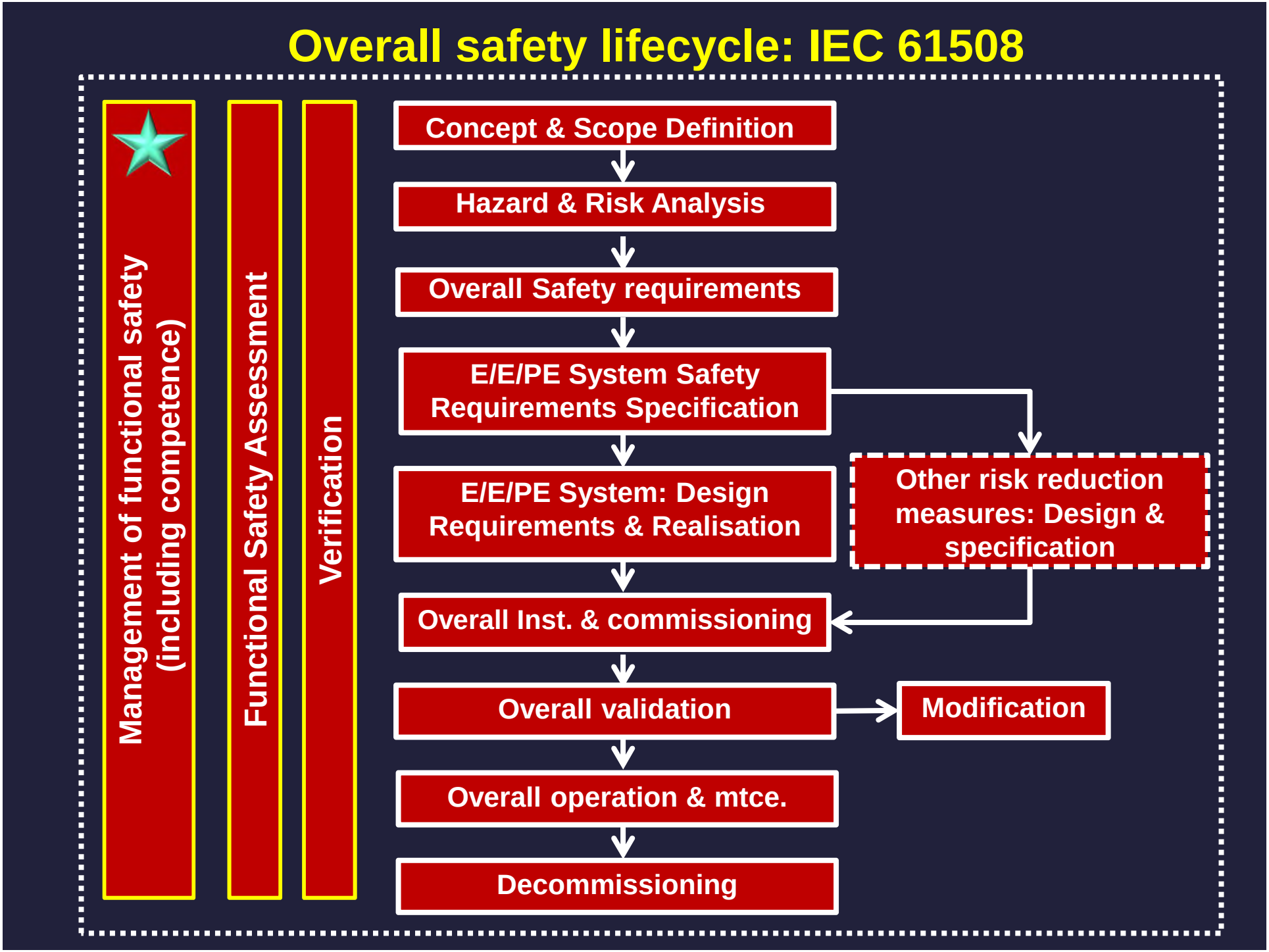
Data Communications

- IEC 61784-3: Industrial communication networks - Profiles – Part 3: Functional safety fieldbuses - General rules and profile definition
- IEC 62280: Railway applications - Communication, signalling and processing systems - Part 2: Safety-related communication in open transmission systems

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

Overall safety lifecycle: IEC 61508



IEC 61508 Clause Structure

For each clause:
The Objectives to be achieved are specified

For each clause:
The Requirements to achieve the Objectives are specified

Management of functional safety

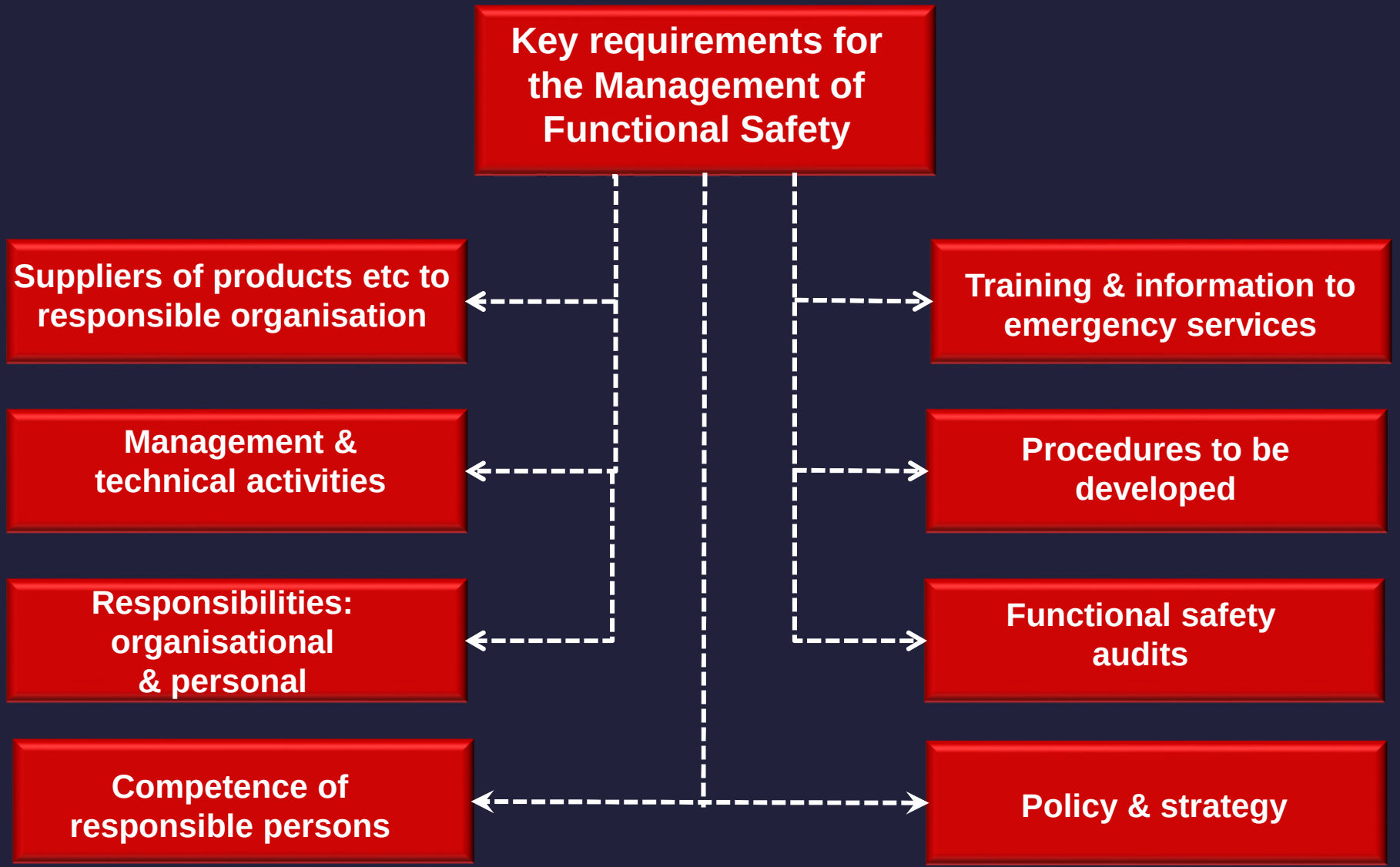
Objectives:

- To specify the responsibilities in the management of functional safety for an E/E/PE safety-related system, or for one or more phases of the overall, E/E/PE system and software safety lifecycles.

- To specify the activities to be carried out by those with responsibilities in the management of functional safety.

The clause applies to those who have responsibility for an E/E/PE safety-related system or for one or more phases of the overall E/E/PE system and software safety lifecycles.

Management of Functional Safety
IEC 61508-1; Clause 6



Management of functional safety

Completely restructured….more comprehensive normative requirements including:

- **Appointment of one or more persons by an organisation with responsibility for one or more phases…….**
- **Identification of all persons undertaking defined activities**
- **All those persons undertaking defined activities shall be competent for the duties they have to perform.**
- **The competence of those with defined responsibilities shall be documented**
  - ✓ **Important change …in IEC 61508/Edition 1, the normative requirement was restricted to the Functional Safety Assessment activity.**

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

IEC 61508-2/Annex D: Safety manual for compliant items

Purpose: 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.

IEC 61508-2/ 7.4.9: Requirements for E/E/PE system implementation

- 7.4.9.6 Suppliers shall provide a safety manual for compliant items, in accordance with Annex D, for each compliant item that they supply and for which they claim compliance with IEC 61508 series.

- 7.4.9.7 The supplier shall document a justification for all the information that is provided in each safety manual for compliant items.

IEC 61508-2/Annex D: Safety manual for compliant items

- For every function, the safety manual shall contain (example):
  - Failure modes / failure rates for the specified modes;
  - Failure modes that are detected by diagnostics / failure rates of the failure modes;
  - Failure modes of the diagnostics….that result in failure to detect failures of the function
  - For every failure mode detected by diagnostics internal to the compliant item, the diagnostic test interval
  - Classification as Type A or Type B
  - The Systematic Safety Integrity
  - The Hardware Fault Tolerance
  - The Safe Failure Fraction
  - …….etc

IEC 61508-2/Annex D: Safety manual for compliant items

Note!

- **Failure modes can only be classified as being safe or dangerous when the application of the compliant item is known**

- **No claims shall be made in the safety manual, in respect of the hardware fault tolerance or the safe failure fraction or any other functional safety characteristic that is dependent on knowledge of safe and dangerous failure modes, unless the underlying assumptions, as to what constitute safe and dangerous failure modes, are clearly specified.**

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

ASICS & ICs

- An appropriate group of techniques and measures shall be used that are essential to prevent the introduction of faults during the design and development of ASICs

  Note: The definition of ASIC covers a range of devices FPGAs, PLDs…...

- Techniques and measures that support the achievement of relevant properties are given in informative Annex F.

- Special architecture requirements for integrated circuits (ICs) with on-chip redundancy are given in normative Annex E.

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

Software

- Properties have been introduced(such as completeness, correctness and predictability) for the output of each lifecycle phase to assist in the selection of the techniques & measures

- Given the large number of factors that affect software systematic capability it is not possible to give an algorithm for combining the techniques and measures that will be correct for any given application.

- The purpose of Annex C is:
  - ✓ to give guidance on selecting specific techniques from Annexes A and B to achieve software systematic capability;
  - ✓ to outline a rationale for justifying the use of techniques that are not explicitly listed in Annexes A and B.

Software

- Extended requirements for the selection and justification of software development tools.
- Allowing software elements not originally developed with safety in mind to be re-used in safety related applications by the provision of suitable evidence including evidence of successful use in other applications.
- Revision to the set of technique and measures in Annexes A and B, to remove obsolete or little-used techniques and introduce current methods.

Overview of key changes

1. Terminology
2. Architectural Constraints
3. Systematic safety integrity
4. Synthesis of elements/Systematic Capability
5. Security
6. Modes of operation
7. E/E/PE requirements specification(s)
8. Data Communications
9. Management of Functional Safety
10. Safety Manual
11. ASICS
12. Part 3
13. Parts 5/6/7

Revision of IEC 61508

1. Background
2. Some key changes of the revised standard
3. Using the new edition
4. Concluding comments

Using the new edition:

- **The current IEC 61508/Edition 2 has replaced IEC 61508 Edition 1. The Foreword states:**

> **This second edition cancels and replaces the first edition published in 1998. This edition constitutes a technical revision.**
>
> **This edition has been subject to a thorough review and incorporates many comments received at the various revision stages.**

Using the new edition

New projects:

- Taking into account the to paragraph in the Foreword it would be sensible to use IEC 61508/Edition 2 for new projects

Existing systems:

- There are no specified rules for conformance requirements for systems comprising elements conforming to IEC 61508/Edition 1 and elements conforming to IEC 61508/Edition 2. Is this an issue?

Migration to the new edition:

- With respect to health and safety legislation the concept of “reasonable practicability” applies and that would need to be taken into account in the decision-making process.

Revision of IEC 61508

1. Background
2. Some key changes of the revised standard
3. Using the new edition
4. Concluding comments

Concluding comments

- The revision of IEC 61508 has tackled a number of important issues and provided more options in seeking compliance.
- Both IEC 61508 Edition 2 & EN 61508 available.
- IEC 61508 Standards+:
  - Identifies the revisions referenced to Edition 1
  - provides hyperlinked notes of explanation….this will be invaluable to those already using the standard.
- IEC FAQs are available on the IEC website (see next slide)

Further information

- IEC: http://www.iec.ch/ Accessed 14 October 2014
- IEC Functional Safety Technology Sector. (Formerly called “Functional Safety Zone”): http://www.iec.ch/functionalsafety/ Accessed 14 October 2014
- Standards+ version of IEC 61508/Edition 2: http://www.iec.ch/functionalsafety/standards/ Accessed 14 October 2014
- Managing safety competences/ Competence criteria (IET/HSE/BCS guidance): http://www.theiet.org/factfiles/msc/index.cfm 14 October 2014

ENGINEERING SAFETY CONSULTANTS

The Global Provider of Functional Safety Expertise and Technical Consultancy

The changes to IEC 61508/Edition 2

&

implications for users of the standard

Thank you

Version 14 10 2014