EMC –Related Functional Safety Seminar

22 March 2001

Functional Safety & IEC 61508

Ron Bell
Technology Division
Health & Safety Executive, UK

HSE

Functional Safety & IEC 61508

- Introduction to IEC 61508
- Key terms and concepts
- Safety Integrity Levels
- Strategy to achieve Functional Safety
- Conclusions and way ahead

Functional Safety & IEC 61508

Introduction to IEC 61508

IEC 61508 and Functional Safety

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

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

IEC 61508 and Functional Safety

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

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

IEC 61508 is a basic IEC safety publication

The Parts of IEC 61508

- **Part 1: General requirements**
- **Part 2: Requirements for electrical,electronic, programmable electronic systems**
- **Part 3: Software requirements**

The Parts of IEC 61508

- Part 1: General requirements
- Part 2: Requirements for electrical,electronic, programmable electronic systems
- Part 3: Software requirements

- Part 4: Definitions and abbreviations

The Parts of IEC 61508

- 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 & 6
- Part 7: Overview of techniques and measures

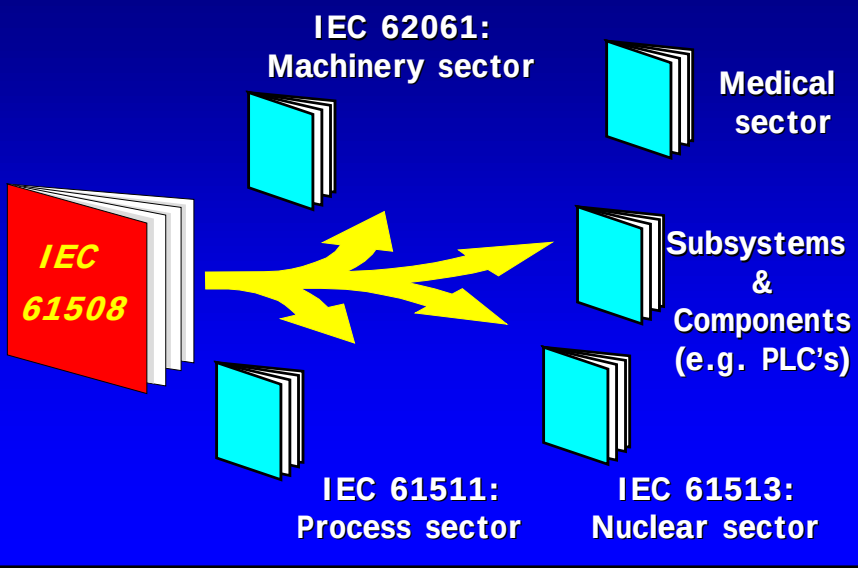
IEC 61508: Functional safety of electrical, electronic & programmable electronic systems

Electrical, Electronic & Programmable Electronic systems

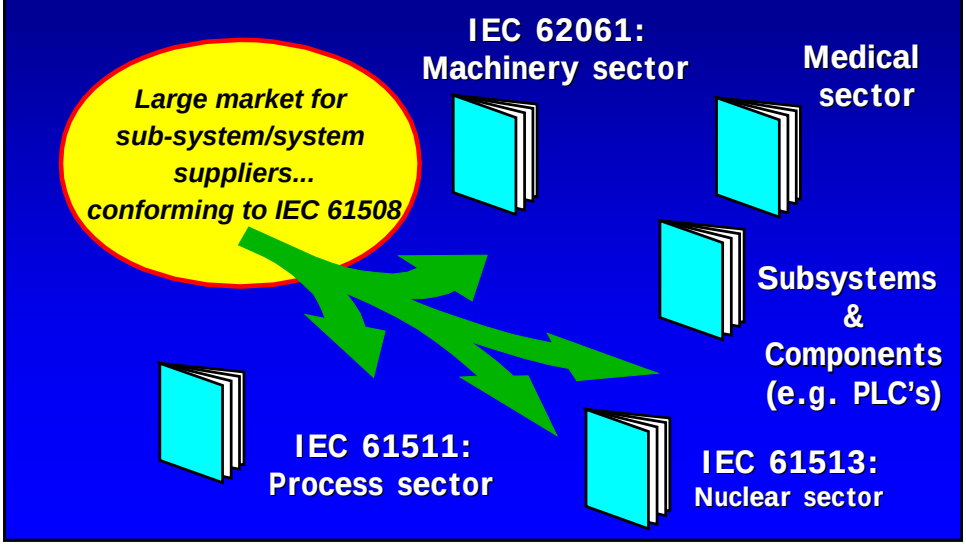
E/E/PE

E/E/PES

Generic and application sector standards



Generic and application sector standards



IEC 61508 and Functional Safety

Scope: *Mainly concerned with E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment.....could also be used to specify any E/E/PE system used for the protection of equipment or product*

em disturbances can cause dangerous em interference on E/E/PE safety-related systems.....hence em phenomena is an important issue when determining the safety performance of such systems

Functional Safety & IEC 61508

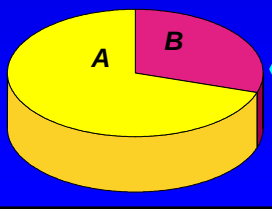
Key terms and concepts

Functional Safety

Definition

"Part of the overall safety relating to the equipment and its associated control system which depends on the correct functioning of electrical, electronic, programmable electronic (E/E/PE) safety-related systems…….".

Safety = A + B
Functional Safety = B



Required risk reduction achieved by means of E/E/PE safety-related systems

Functional Safety

Definition

"Part of the overall safety relating to the equipment and its associated control system which depends on the *correct functioning of electrical, electronic, programmable electronic (E/E/PE) safety-related systems……".*

The following are examples of E/E/PE safety-related systems:

- *an an emergency shut-down system in a hazardous chemical process plant;*
- *a railway signalling system;*
- *guard interlocking systems and emergency stopping systems for machinery;*
- *a variable speed motor drive used to control a restricted speed as a means of protection;*
- *other "non-dedicated" safety-related systems*

Safety function

- ***Function to be implemented by an E/E/PE safety-related system…….. which is intended to achieve or to maintain a safe state for the equipment under control, in respect of a specific hazardous event.***

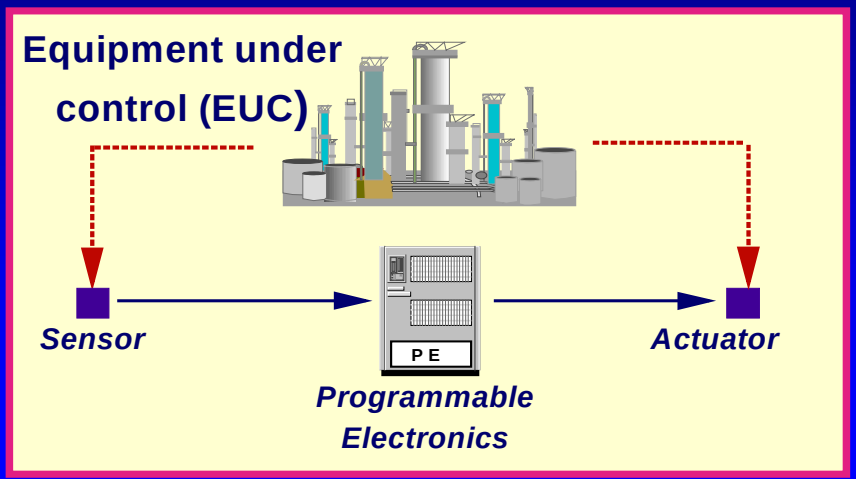
Safety-related system

Designated system that both:

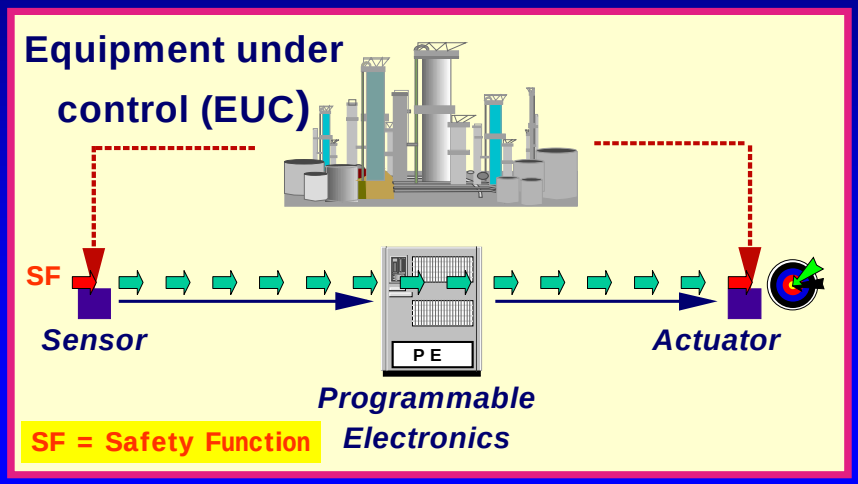
- **Implements the *safety functions* necessary to achieve or maintain a safe state for the equipment under control; *and,***

- **Is intended to achieve, on its own or with other E/E/PE safety-related systems ……the required *safety integrity* for the safety functions.**

Extent of the safety-related system

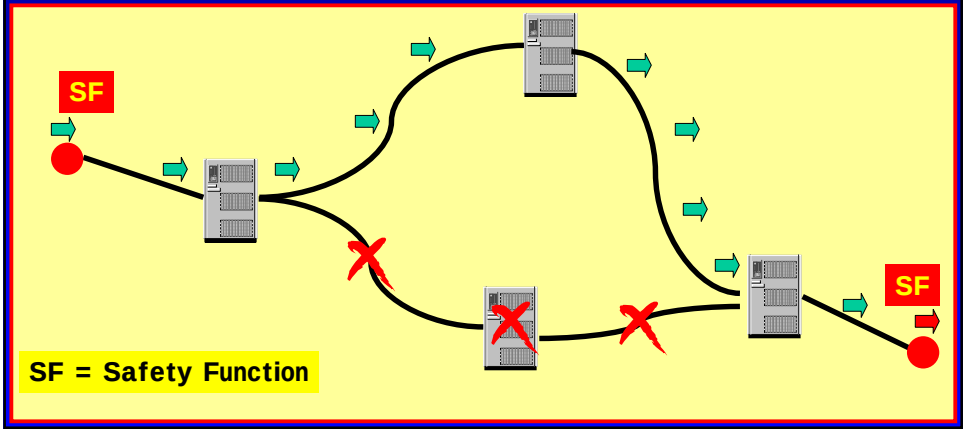


Implementation of the safety function by the safety-related system



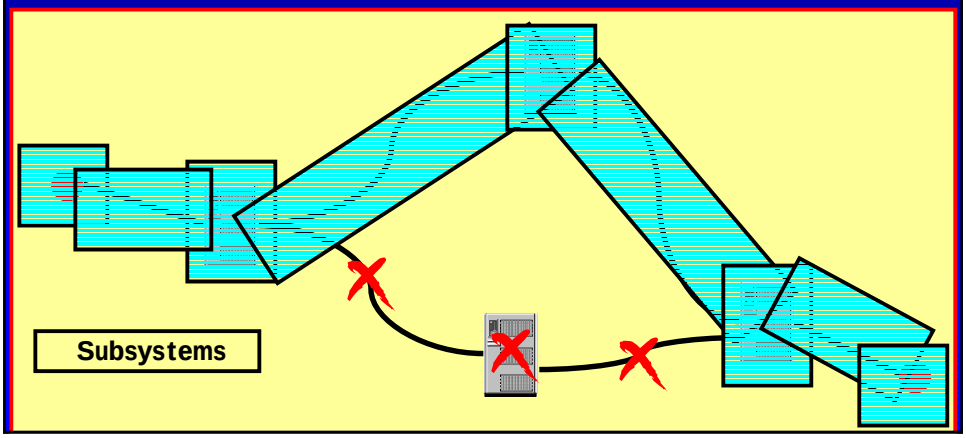
Safety function & safety-related system

The safety-related system includes the all those subsystems that are involved in the carrying out the safety function



Subsystems of a safety-relate system

Each subsystem has to be characterised in accordance with IEC 61508 ……..in order that the subsystems can be integrated together to form a safety-related system which itself meets the requirements of IEC 61508 (or a sector implementation of IEC 61508)



Safety Integrity

- *Probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time*

Safety Integrity Level

Safety Integrity Levels

4
3
2
1

One of four possible discrete levels for specifying the safety requirements of the safety functions to be allocated to the safety-related systems

- 4 Highest
- 1 Lowest
- Target Failure Measure

Safety Integrity Level

Safety Integrity Levels

4
3
2
1

One of four possible discrete levels for specifying the safety requirements of the safety functions to be allocated to the safety-related systems…….

Therefore the concept of a SIL applies to the complete safety-related system and not to a subsystem (e.g. a sensor)

- 4 Highest
- 1 Lowest
- Target Failure Measure

Impact of Functional Safety on products & systems

Determination of Safety Integrity Levels

Determination of SILs

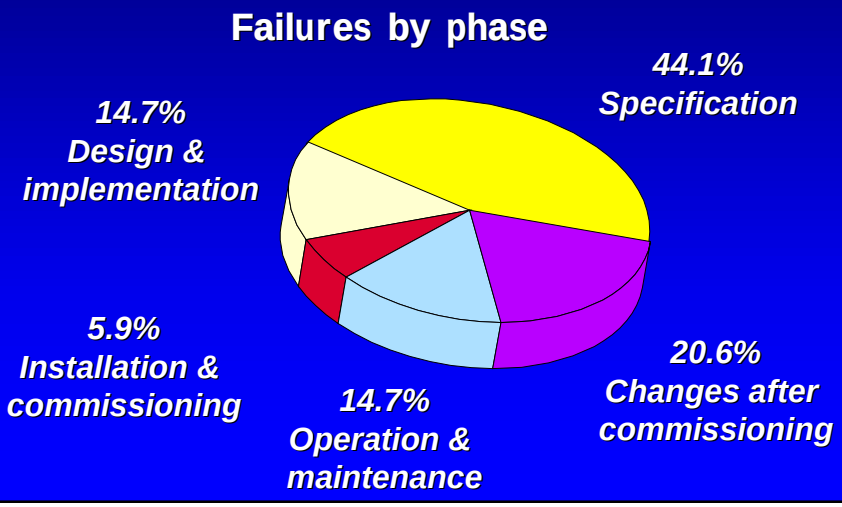
A key issue in the application of IEC 61508, or any sector implication of IEC 61508 will be the determination of the Safety Integrity Levels for the safety functions for specific applications.

Part 5 of IEC 61508 provides, and Part 3 of IEC 61511 will provide, examples and guidance on different approaches

Impact of Functional Safety on products & systems

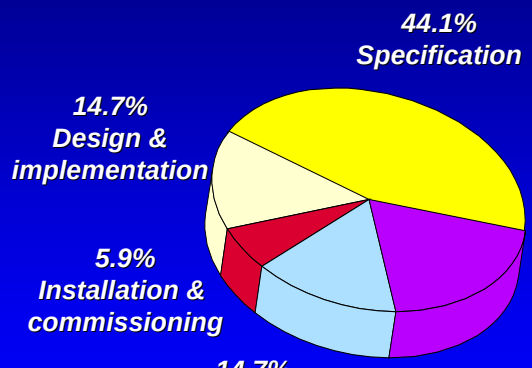
Strategy to achieve Functional Safety

Primary cause (by phase) of control system failure [based on 34 incidents]

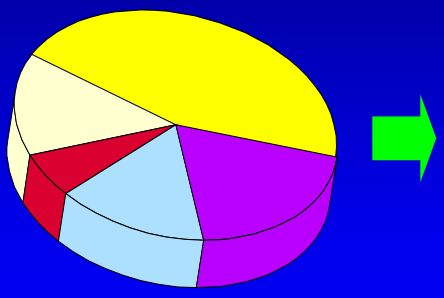


Primary cause (by phase) of control system failure [based on 34 incidents]

More than 60% of failures "built into the safety-related systems" before taken into service



Strategy to achieve functional safety



Failures by phase

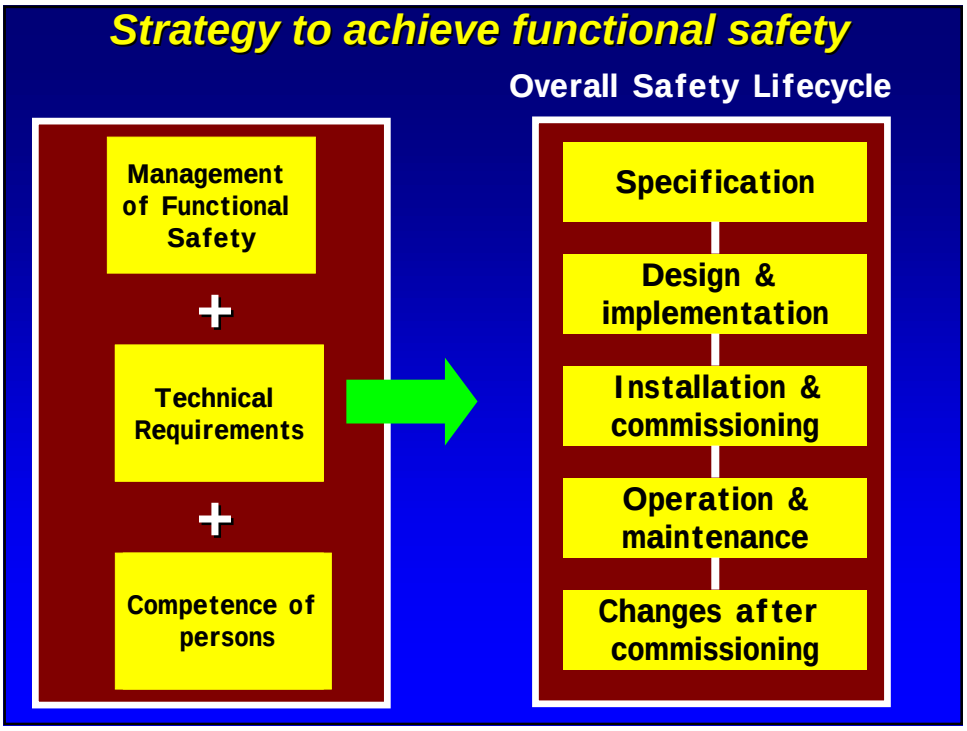
Management of Functional Safety

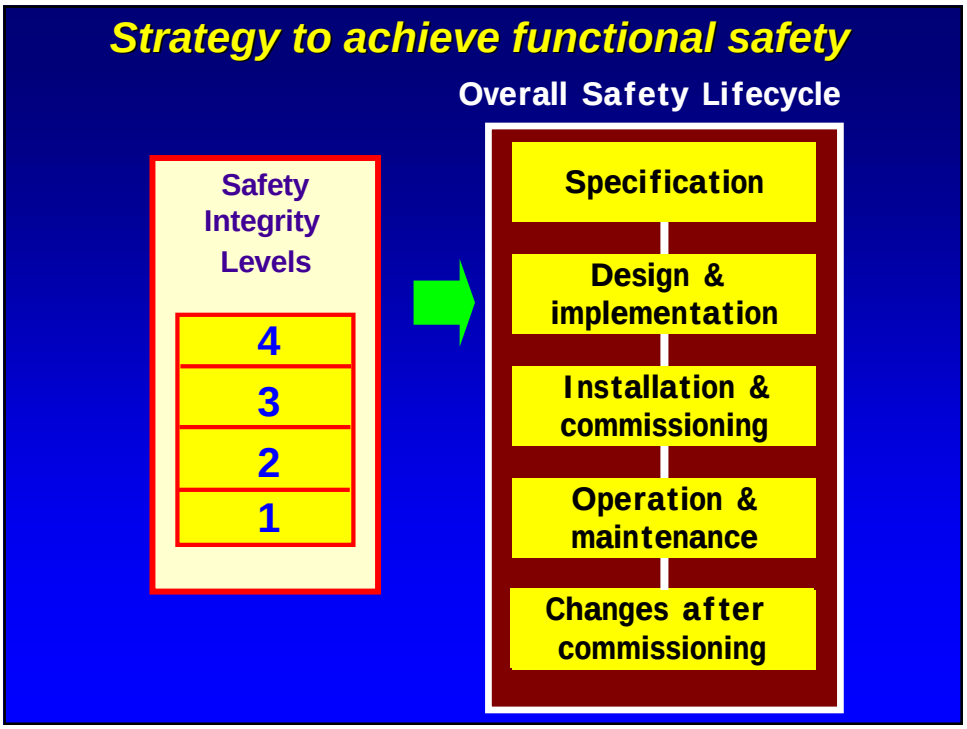
+

Technical Requirements

+

Competence of persons


Strategy to achieve functional safety
Overall Safety Lifecycle
Management of Functional Safety
+
Technical Requirements
+
Competence of persons
Specification
Design & implementation
Installation & commissioning
Operation & maintenance
Changes after commissioning


Strategy to achieve functional safety
Overall Safety Lifecycle
Safety Integrity Levels
4
3
2
1
Specification
Design & implementation
Installation & commissioning
Operation & maintenance
Changes after commissioning

Design strategy to achieve a specified Safety Integrity Level (SIL)

Design & implementation

Design measures to combat Random Hardware failures

Design measures to combat Systematic failures

Systematic Failures causes

Examples of systematic failure causes that the Safety Lifecycle measures must address

- Errors in the Safety Requirements Specification
- Software induced failures
- Systematic hardware failures
- Maintenance & modification induced failures
- Failures arising from environmental factors…e.g. insufficient immunity against em disturbances leading to dangerous em interference. Need to address specification… design… ..implementation..maintenance… modification ……..

Required measures linked to the Safety Integrity Level of the E/E/PE safety-related system

Impact of Functional Safety on products & systems

Conclusions and the way ahead

Conclusions and the way ahead

- The concept of a safety function and a safety-related system are of fundamental importance
- Complex systems are with us and will not go away..we need an approach that delivers the functionality with functional safety
- The achievement of adequate immunity against dangerous em interference is an important issue that needs further resolution
- A good start has been made in developing an approach to matching the required immunity against dangerous em interference to the functional safety requirements ….but there is a long way to go.
- Experts in functional safety & emc need to work together to provide the required guidance in this important area


Thank-
you
HSE