





Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

**ACOS Workshop VII:
Frankfurt
9-10 March 2004**

Functional safety of electrical, electronic and programmable electronic safety-related systems

Ron Bell

Convenor/IEC/SC65A/MT13 (Maintenance of IEC 61508)

Convenor/IEC/SC65A/WG14 (Guidance for IEC 61508)



Objectives

- 1. To provide an overview of the key principles for the design of complex electrical, electronic or programmable safety-related systems with particular reference to IEC 61508***
- 2. To provide an update on the IEC guidance material being developed on functional safety***



Contents




- **Chapter 1: Examples of systems and subsystems under consideration**
- **Chapter 2: What's the problem?**
- **Chapter 3: Essentials of functional safety**
- **Chapter 4: Outline of IEC 61508**
- **Chapter 5: Guidance material available**
- **Chapter 6: Concluding comments**



Contents

- **Chapter 1: Examples of systems and subsystems under consideration**
- Chapter 2: What's the problem?
- Chapter 3: Essentials of functional safety
- Chapter 4: Outline of IEC 61508
- Chapter 5: Guidance material available
- Chapter 6: Concluding comments

Examples of systems, subsystems & devices under consideration

- electro-mechanical  **Low complexity**
 - solid state electronic  **Low complexity/Complex**
 - programmable electronic  **Complex**
-
- ✓ programmable Controllers {PCs};
 - ✓ programmable Logic Controllers {PLCs};
 - ✓ microprocessor based systems;
 - ✓ application specific integrated circuits (ASICs)
 - ✓ intelligent sensors/transmitters/actuators etc
 - ✓ digital communication systems (e.g. bus systems)
 - ✓ internet based technologies

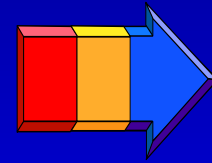
Examples of applications under consideration

The following are examples of safety-related systems:

- an emergency shut-down system in a hazardous chemical process plant;
- railway signalling and train protective systems;
- guard interlocking systems and emergency stopping systems for machinery;
- variable speed motor drives used to control the speed as a necessary means of safety;
- information based safety-related systems

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

Electrical, Electronic & Programmable Electronic



E/E/PE

Example: E/E/PE device; E/E/PE system



Contents

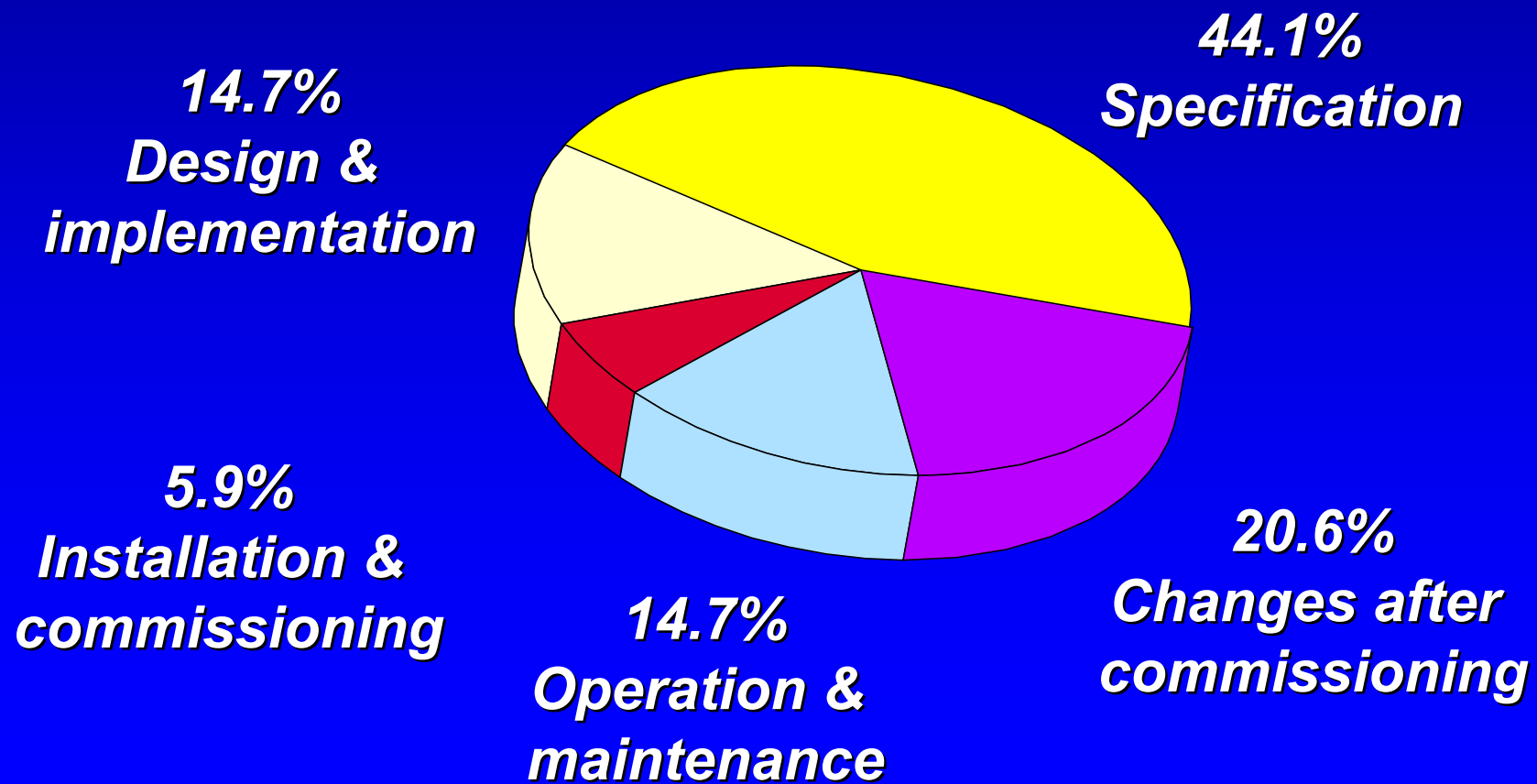
- *Chapter 1: Examples of systems and subsystems under consideration*
- ***Chapter 2: What's the problem?***
- *Chapter 3: Essentials of functional safety*
- *Chapter 4: Outline of IEC 61508*
- *Chapter 5: Guidance material available*
- *Chapter 6: Concluding comments*

Safety issues of complex systems

- Complexity (software/hardware/system integration)
...many factors involved
- Testing necessary but not sufficient
- Prediction of system performance (safety integrity) difficult;
- Only random hardware failures can be quantitatively predicted with confidence
- Demands systematic approach throughout the safety lifecycle
- Demands high level of competence throughout the safety lifecycle

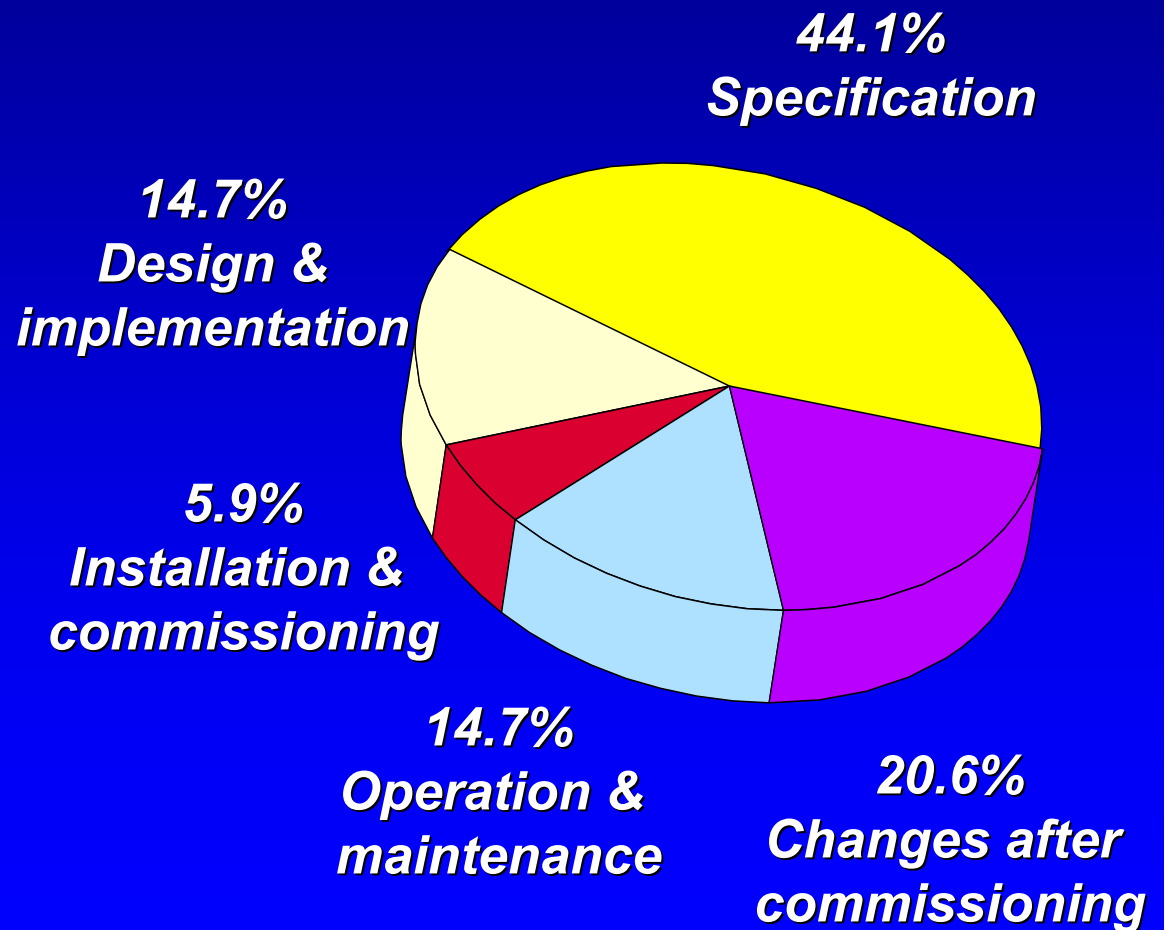
Primary cause (by lifecycle phase) of control system failure [based on 34 incidents]

Failures by lifecycle phase



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

All lifecycle phases need to be addressed if functional safety is to be achieved
.....IEC 61508 does this





Contents

- *Chapter 1: Examples of systems and subsystems under consideration*
- *Chapter 2: What's the problem?*
- ***Chapter 3: Essentials of functional safety***
- *Chapter 4: Outline of IEC 61508*
- *Chapter 5: Guidance material available*
- *Chapter 6: Concluding comments*

Safety and functional safety

Safety is the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly as a result of damage to property or to the environment

General definition for functional safety

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs

Safety and functional safety

General definition

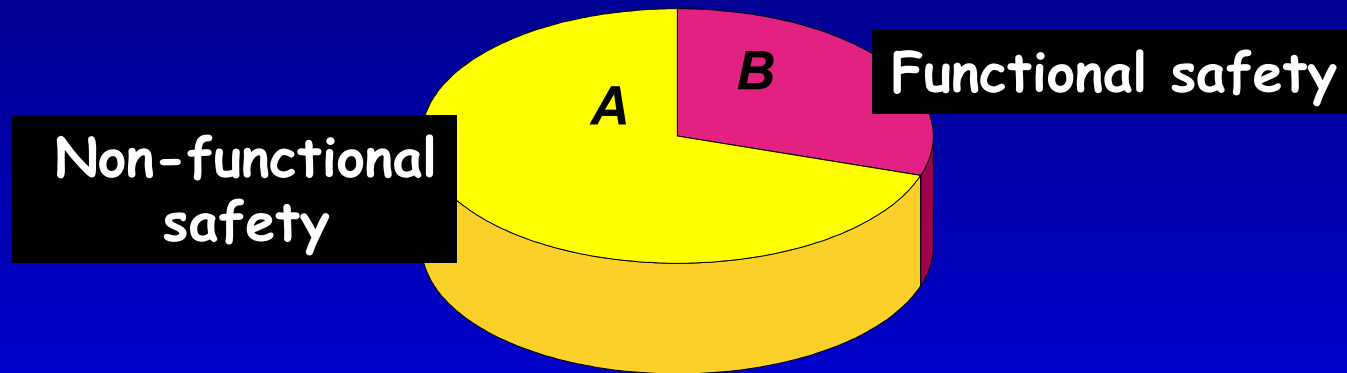
Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs

Definition applied to E/E/PE safety-related systems

Part of the overall safety relating to the equipment and its associated control system which depends on the correct functioning of electrical, electronic and programmable electronic safety-related systems.....”.

Functional Safety

Overall safety = A + B



A: safety achieved by measures reliant on passive systems e.g. insulation

B: safety achieved by active systems (e.g. temperature measurement and de-energisation of contactor)

Key terms and concepts

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**

Key terms and concepts

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 function & safety integrity of the safety function

Safety function



“what has to be done”

Determined from the hazard analysis

Safety integrity of safety function



the “safety performance” of the safety function”; the likelihood of the safety function being achieved

Determined from the risk assessment

Safety function & safety integrity of the safety function

Safety function



“what has to be done”

Safety integrity of safety function

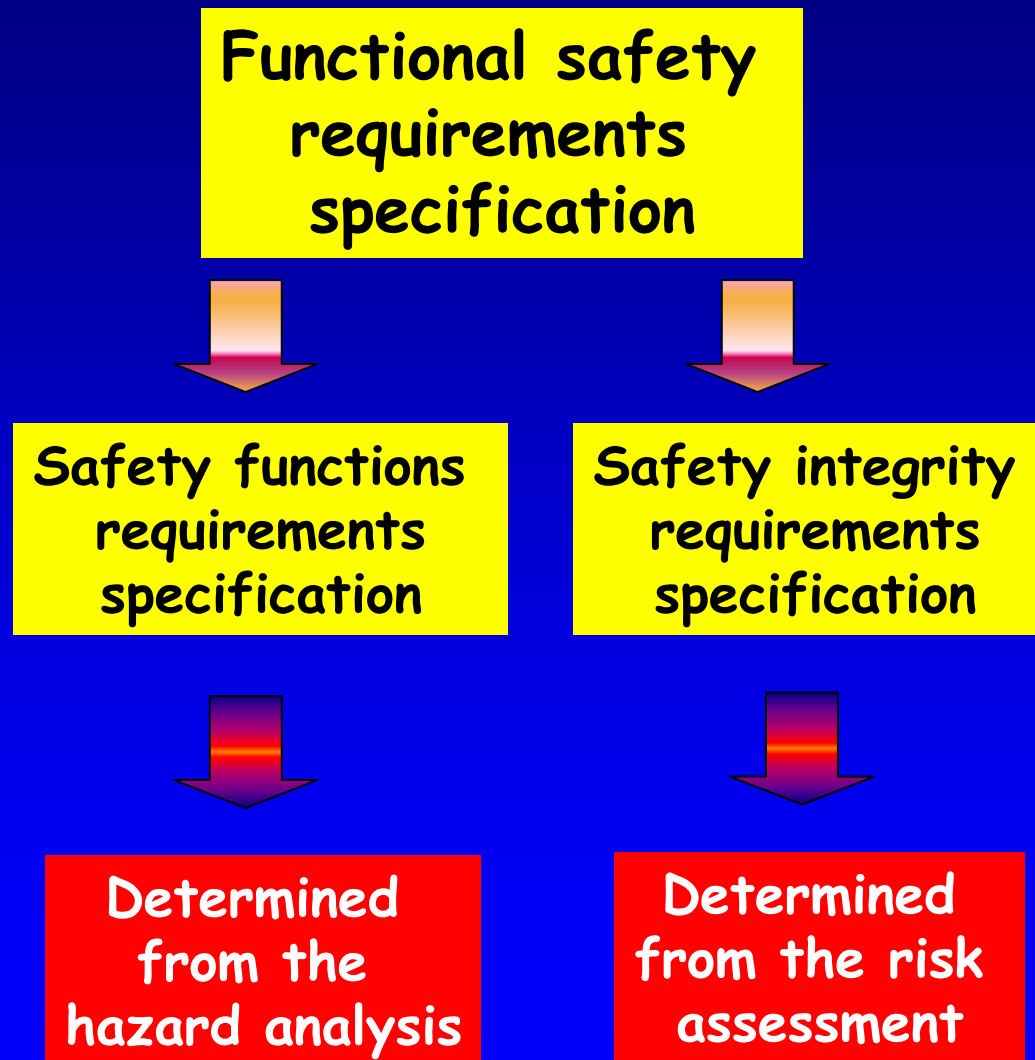


“the safety performance required of the safety function”

Example

- **Safety function**: In order to prevent the rupture of pressure vessel “X”, valve “Y” should open in 2 seconds when the pressure in the vessel reaches 2.6 bar.
- The safety integrity of the safety function shall be “Z”.

Functional safety requirements specification



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 electrical, electronic and programmable electronic safety-related systemsthe required **safety integrity** for the safety functions.

Functional safety requirements specification

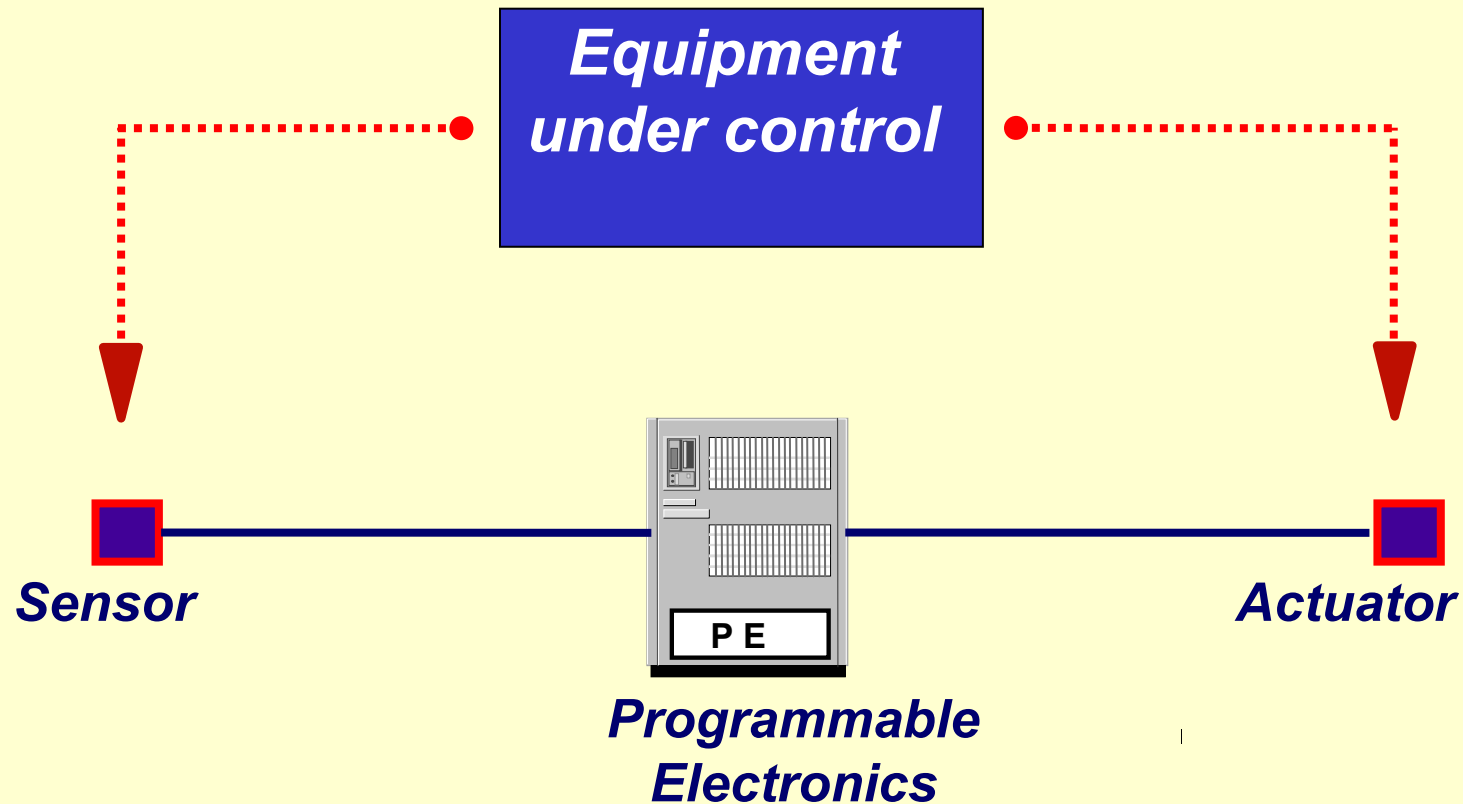
Safety-related system

```
graph TD; A[Safety-related system] --> B[Carries out safety functions to the required safety integrity specified for each safety function];
```

Carries out safety functions to the required safety integrity specified for each safety function

Implementation of the safety function by the safety-related system...

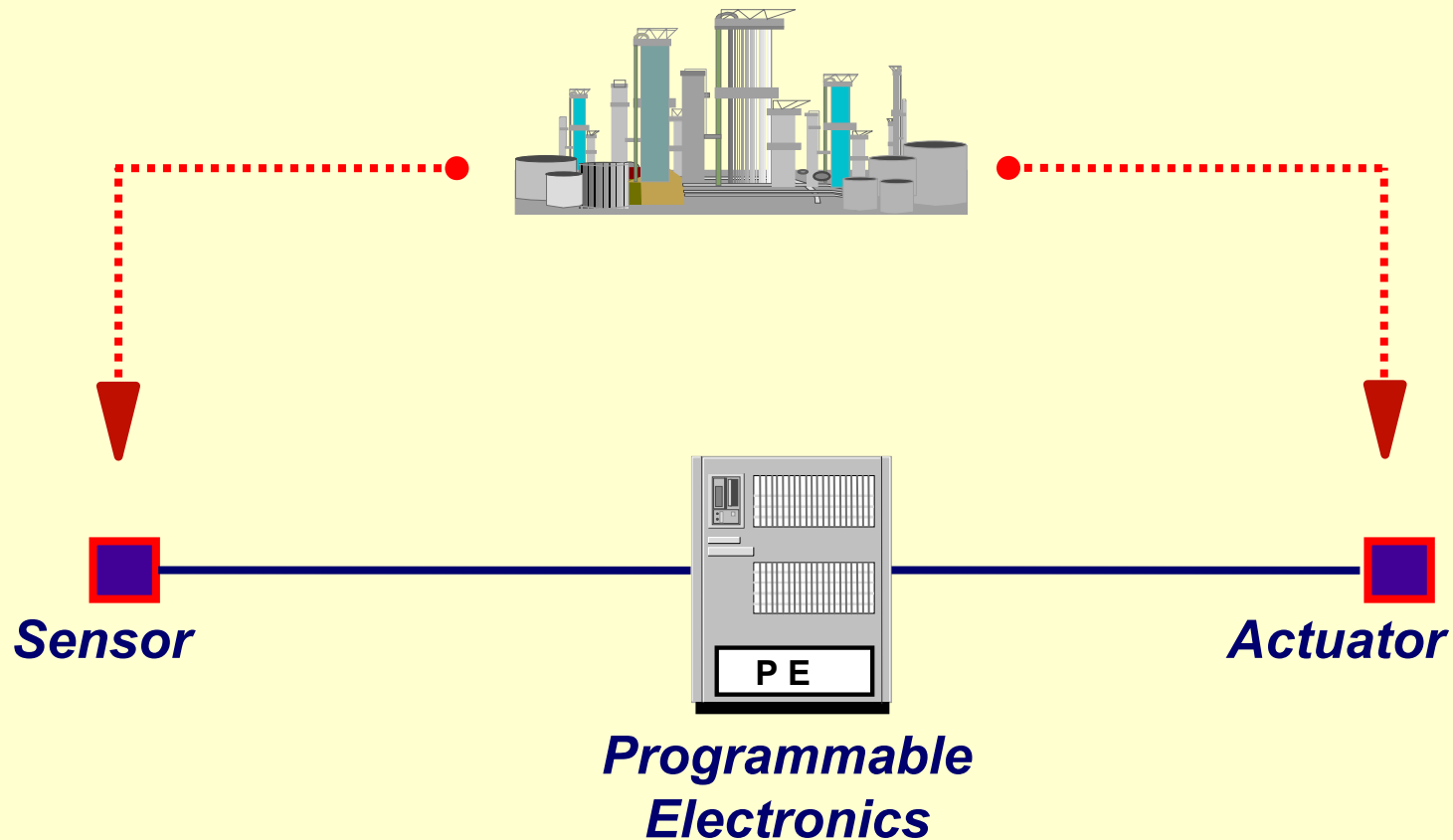
and determination of the extent of safety-related system



Implementation of the safety function by the safety-related system...

and determination of the extent of safety-related system

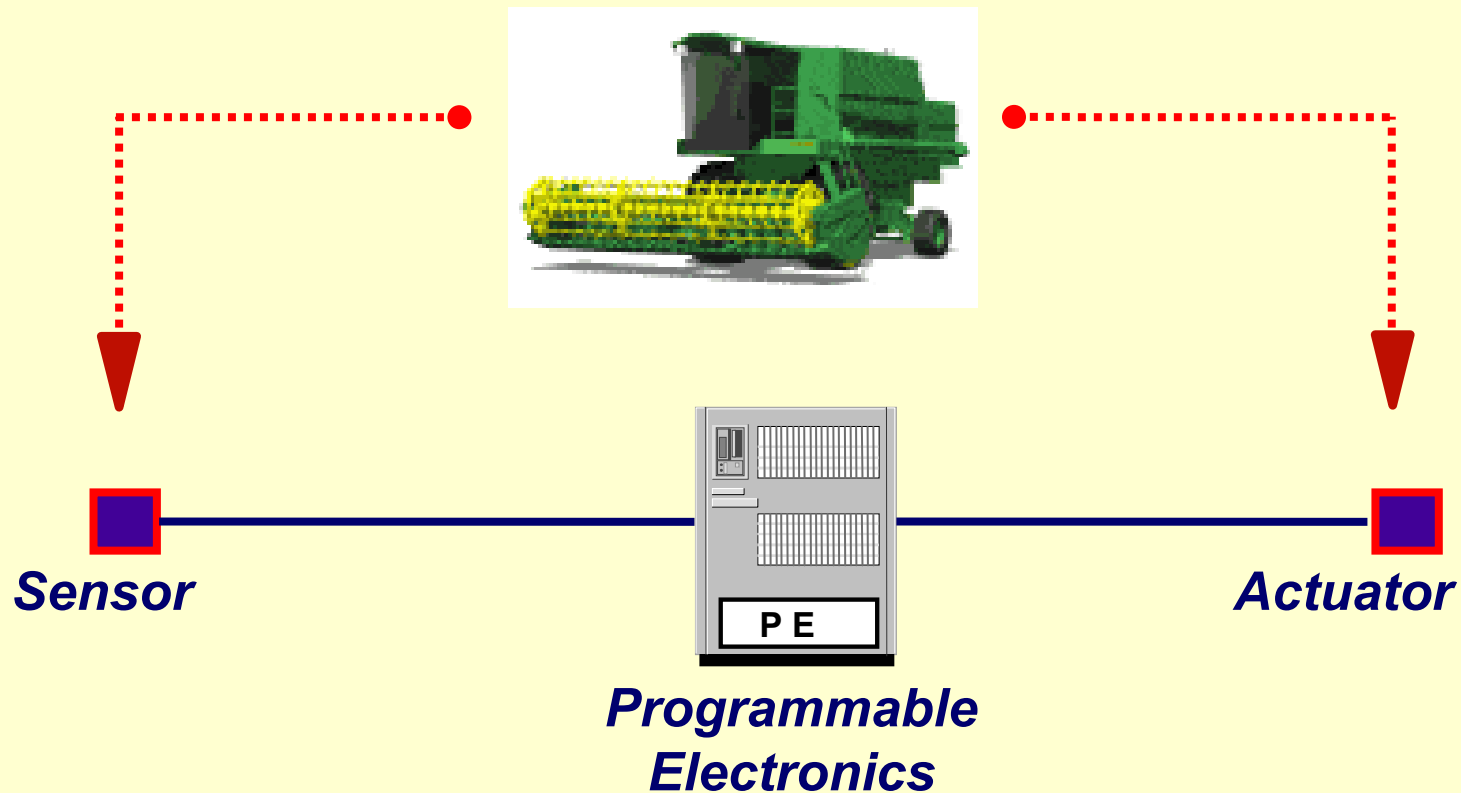
Equipment under control



Implementation of the safety function by the safety-related system...

and determination of the extent of safety-related system

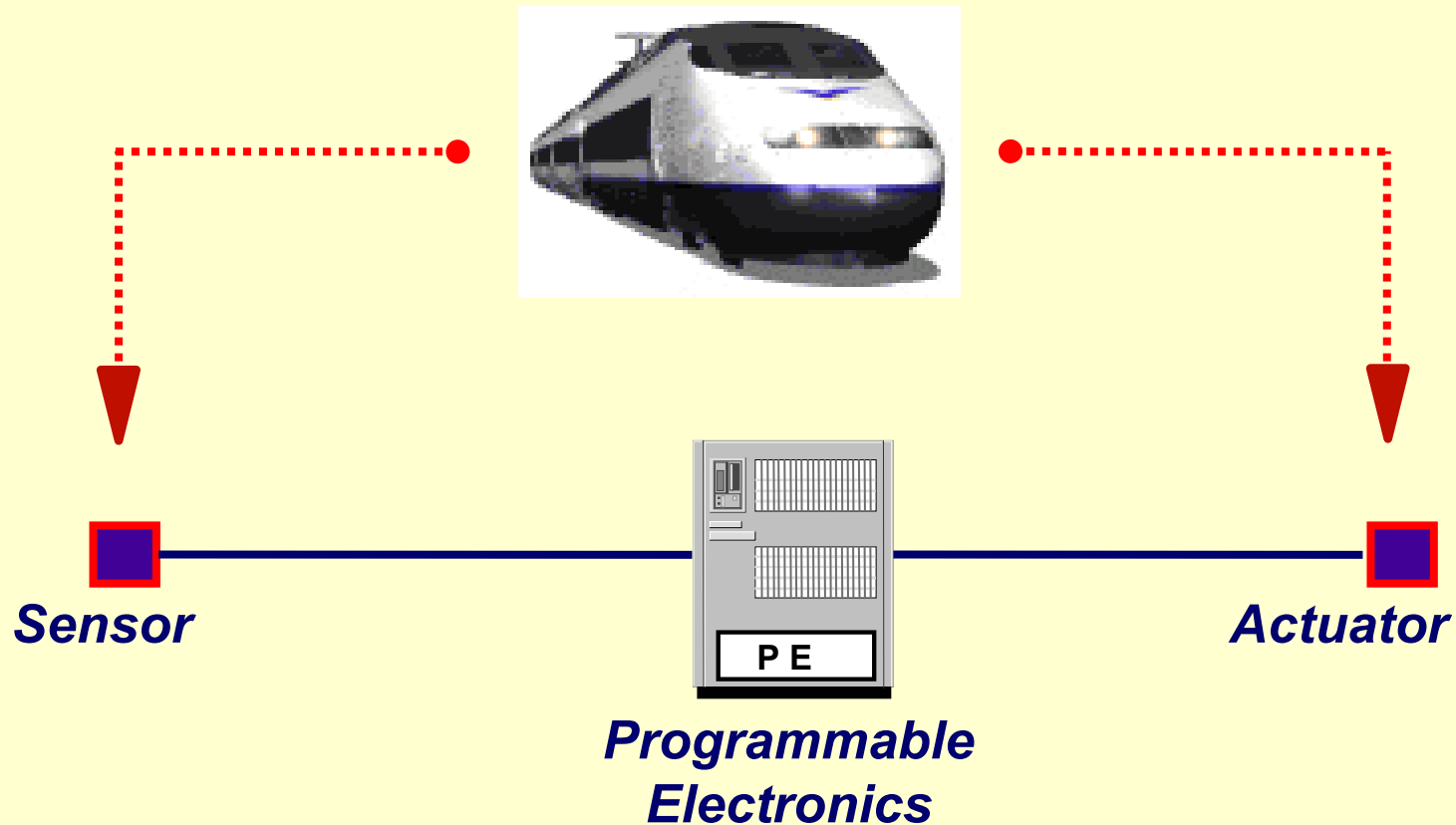
Equipment under control



Implementation of the safety function by the safety-related system...

and determination of the extent of safety-related system

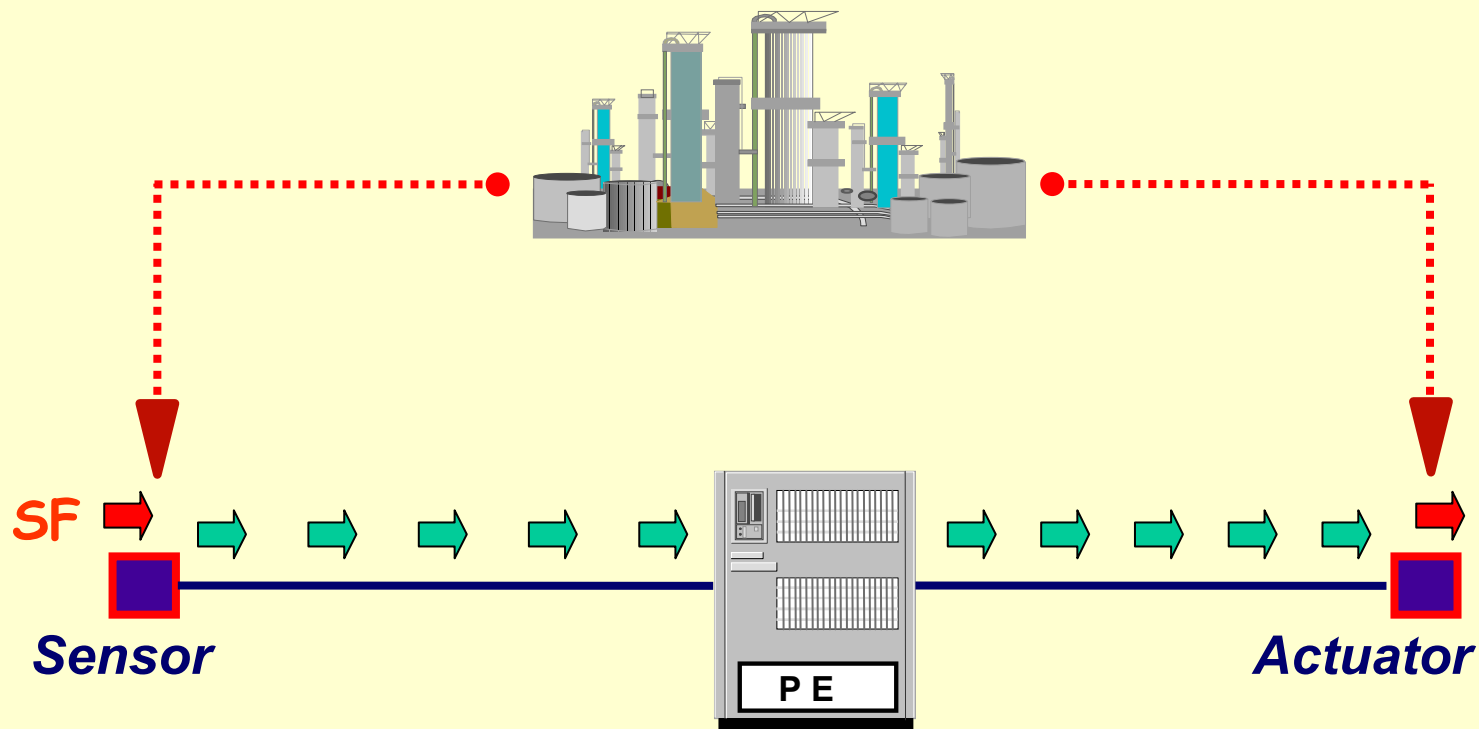
Equipment under control



Implementation of the safety function by the safety-related system...

and determination of the extent of safety-related system

Equipment under control



SF = Safety Function

Programmable
Electronics

Functional safety requirements specification

Functional safety requirements specification

Safety functions requirements specification

Safety integrity requirements specification

For each **safety function** the safety integrity is determined. This is categorised into one of four **Safety Integrity Levels (SILs)**

Safety Integrity Levels (SILs)

4

3

2

1

Strategy to achieve functional safety

Safety Integrity Levels (SILs)

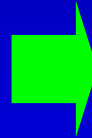
4

3

2

1

SIL determination of key importance when determining the design measures



Overall Safety Lifecycle [Simplified]

Specification

Design & implementation

Installation & commissioning

Operation & maintenance

Changes after commissioning



Contents

- *Chapter 1: Examples of systems and subsystems under consideration*
- *Chapter 2: What's the problem?*
- *Chapter 3: Essentials of functional safety*
- **Chapter 4: Outline of IEC 61508**
- *Chapter 5: Guidance material available*
- *Chapter 6: Concluding comments*

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



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

Parts structure of IEC 61508

Part 1: Normative
Part 5: Guidelines

Part 1
Overall safety
lifecycle

Part 4: Definitions
Part 7: Overview
of techniques &
measures

Part 2: Normative
Part 6: Guidelines

Part 2
E/E/PE safety
lifecycle

Part 3
Software safety
lifecycle

Part 3: Normative
Part 6: Guidelines



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

IEC 61508 and Functional Safety

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

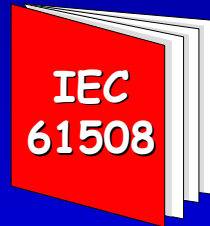
A seven Part international standard covering
all safety lifecycle activities...concept.....
specification...design...implementation...operation
maintenance & modification

IEC 61508 is a basic IEC safety publication.

This means that any IEC product/sector standard covering
functional safety of E/E/PE...have to meet IEC 61508
requirements...but not for low complexity safety-related systems

Standalone & and sector/product standards

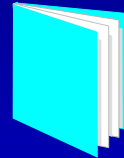
Standalone



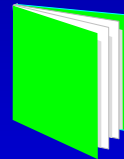
Systems, components
& subsystems
to IEC 61508

Compliance
to IEC 61508

Sector & product implementations



IEC 62061: Machinery



IEC 61511: Process



IEC 61513: Nuclear



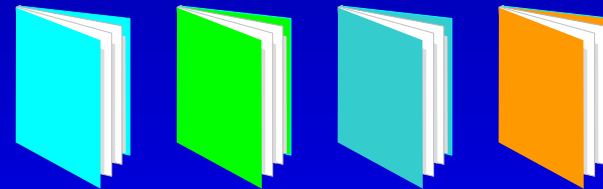
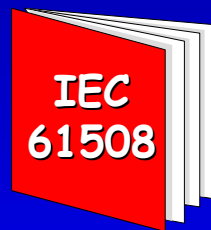
Product (e.g. PLCs;
smart sensors)

Compliance
to IEC xxxxx

Standalone & and sector/product standards

Market benefits of generic subsystems & components

Sector & product standards



Systems, components & subsystems to IEC 61508 used in sector & product standards



Large market for generic subsystems & components conforming to IEC 61508

How can I use IEC 61508 ?

IEC 61508

- Can be used as a stand-alone standard where no application sector standard exists...or until one is published
- Aimed at subsystem/product designers ...**even when a sector standard does exist**

How do I use a sector implementation of IEC 61508 ?

- Aimed at system designers, system integrators & users
- Will contain sector terminology
- May have constraints thought to be appropriate for the specific sector
- Clauses in Sector standard will reference IEC 61508 or repeat them in the standard



Contents

- *Chapter 1: Examples of systems and subsystems under consideration*
- *Chapter 2: What's the problem?*
- *Chapter 3: Essentials of functional safety*
- *Chapter 4: Outline of IEC 61508*
- **Chapter 5: Guidance material available**
- *Chapter 6: Concluding comments*

Approach adopted by WG14

- A **guidance package** was considered the best solution in order to assist the very diverse target audience
- A Web based approach was adopted in order to have global accessibility and provide guidance in the time scale to meet the needs of user's of the standard.
- WG14 would develop the **guidance package** and put it directly onto the web
- Discussions took place with IEC Central Office and this lead to the setting up of the **IEC Functional Safety Zone** (www.iec.ch/functionalsafety)

Current guidance package

The **guidance package**, now on the Functional Safety Zone on the IEC web site, currently comprises:

- **IEC Brochure on IEC 61508**: A leaflet sized 12 page document (which is also available as a text publication)
- **"Functional Safety and IEC 61508"**: An 11 page downloadable document which gives a general introduction to functional safety and approach of the standard. This is now being processed as a Technical Report
- **Frequently Asked Questions**:

The **Functional Safety Zone**: Frequently Asked Questions

- Answers to over 50 FAQs on IEC 61508 (scope, its relationship to other standards, (including a page for each sector standard), revision timetable, etc
- A link to allow the purchase of IEC 61508
- Feedback form to allow users to submit comments and suggest new questions

The Functional Safety Zone: Frequently Asked Questions

- The opening page of the Zone currently receives 500-600 hits a week and this ranks as one of the most popular pages on the whole of the IEC web site
- A search using the phrase "IEC 61508" in Google results in over 8000 entries with the IEC Functional Safety Zone rated number 1

www.iec.ch/functionalsafety

Way ahead

- **FAQs:** Continue adding further FAQs
- **Further guidance material:** It is proposed to add presentation style material together with explanatory notes (e.g. use of Power Point with associated notes)
- **Extension of the scope of WG14:** To cover FAQs relating to sector/product implementations of IEC 61508



Contents

- *Chapter 1: Examples of systems and subsystems under consideration*
- *Chapter 2: What's the problem?*
- *Chapter 3: Essentials of functional safety*
- *Chapter 4: Outline of IEC 61508*
- *Chapter 5: Guidance material available*
- **Chapter 6: Concluding comments**

Concluding comments

- E/E/PE technology is increasingly being used as a key part of the safety strategy for industrial solutions across the whole spectrum of industrial sectors
- IEC 61508 and its application sector implementations provide a sound basis for utilizing this technology in a safe and effective manner
- The maintenance of IEC 61508 is moving forward to plan and MT12 and MT13 are working closely together to ensure the standard is maintained in a coherent manner. However, the programme schedule is ambitious given the size and complexity of the standard.

Concluding comments

- Amended versions of IEC 61508 (all 7 Parts) scheduled for March 2006 and this should lead to an improved standard
- Much work has to be done ...dissemination of the concepts of functional safety is of key importance
- IEC 61508 will never be a prescriptive standard and will require competent judgements to be made....this will be key to the effective application of IEC 61508 and its sector/product implementations

Concluding comments

- Dissemination of the concepts of IEC 61508 to facilitate better understanding is of key importance...the **Functional Safety Zone** has an important part to play in this context

www.iec.ch/functionalsafety



Contents

- Chapter 1: Examples of systems and subsystems under consideration
- Chapter 2: Why the problem?
- Chapter 3: Essentials of functional safety
- Chapter 4: Outline of IEC 61508
- Chapter 5: Guidance material available
- Chapter 6: Concluding comments

Thank-you for your attention!