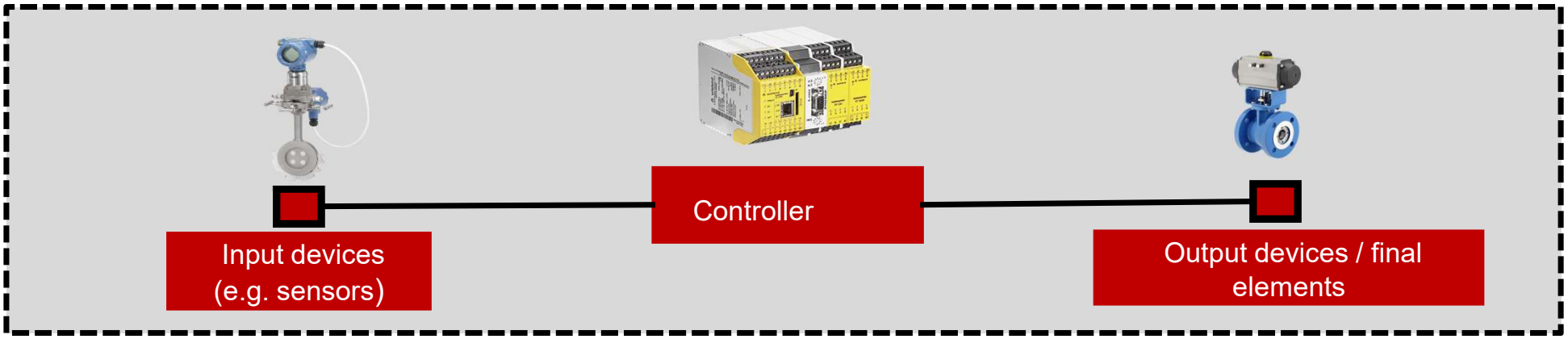
Overview of IEC 61508 & Functional Safety

Market Environment

- Increasing dependence on safety critical systems to achieve Target Risk levels
- Increasing need to justify that you have achieved adequate levels of safety
- Safety Regulators using international standards as basis of what is reasonable ("accepted good practice")
- Increasing formality of safety culture, management of functional safety, competence of the organisation and personal competence
- Increasing interest in management of legacy systems
- Business reputation in relation to safety a key business driver

Electrical, Electronic & Programmable Electronic safety–related system



The example shows a typical Electrical, Electronic & Programmable Electronic safety-rated system usually referred to as an E/E/PE safety -related system.

- "Electrical" relates to electrical elements/devices (e.g. electromechanical relays);
- "Electronic" relates to electronic elements/devices (e.g. semiconductors);
- "Programmable Electronic" relates to computer-based element/devices (e.g. Programmable Controllers).
- The example on the screen shows a safety system which would undertake a specified safety function (e.g. when the speed or acceleration of a mobile equipment (e.g. equipment carrying a patient exceeds X m/s then the valve closes to bring the mobile to a safe stop).
- The functionality of the safety function would be determined by the Hazard Analysis
- The performance of the safety function would be determined by the Risk Assessment

IEC 61508 Objectives

- Release the potential of E/E/PE technology;
- Enable technological developments to take place within an overall safety
- Provide a technically sound, system based approach, with sufficient flexibility for the future;
- Provide risk based approach for determining the required performance of safety-related systems to achieve specified risk which may be specified in quantitative or semi-quantitative terms;
- Provide a generically-based standard that can be used directly by industry but can also help with developing sector standards (e.g. machinery, process chemical plants) or product standards (e.g. power drive systems);
- Provide means for users and regulators to gain confidence when using computer-based technology;
- Provide requirements based on common underlying principles to facilitate:
  - improved efficiencies in the supply chain for suppliers or elements (e.g. sensors, controllers);
  - Improvements in communication and requirements (i.e. increase clarity of what is required to be specified);
  - the development of techniques and measures that could be used across all sectors;
  - The development of conformity assessment services if required.

Typical examples of E/E/PE/ safety-related systems

In principle, IEC 61508 is applicable to any system that uses Electrical, Electronic and Programmable Electronic (E/E/PE) safety related systems….low complexity to complex. Sector/product specific applications include:

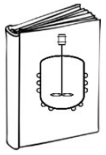
1. emergency shut-down systems
2. fire and gas systems
3. turbine control systems
4. gas burner management systems
5. crane automatic safe-load indicators
6. guard interlocking and emergency stopping systems for machinery
7. medical devices
8. railway signalling systems (including moving block train signalling)
9. automotive systems
10. variable speed motor drives used to restrict speed as a means of protection
11. safety critical information systems
12. remote monitoring, operation or programming of a network-enabled process plant
13. information-based decision support tools where erroneous results affect safety
14. dynamic positioning system (control of a ship's movement)
15. highly distributed critical monitoring systems

Standalone & sector / product standards

Standalone

Example: Sector & product implementations

IEC 62061: Machinery



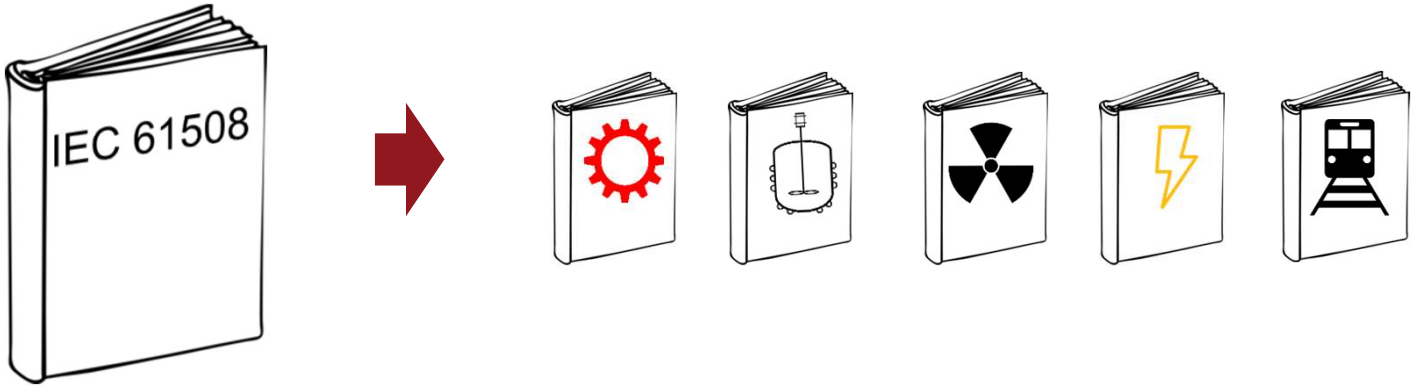
IEC 61511: Process

IEC 61513: Nuclear

IEC 61800-5-2: Power drives

Standalone & sector / product standards

Market benefits of generic elements



Elements to IEC 61508 used in sector & product standards

Large market for generic elements & conforming to IEC 61508

What is Functional Safety?

What is the relationship is between Safety and Functional Safety?

- Safety: freedom from unacceptable risk
- Functional safety: part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

From these two definitions, *functional safety* is part of *safety*

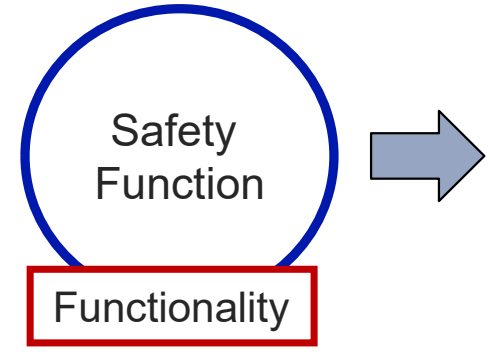
Safety Integrity

Safety Integrity:

Definition: Probability of the safety-related system performing the specified safety functions under all the stated conditions with the stated period of time

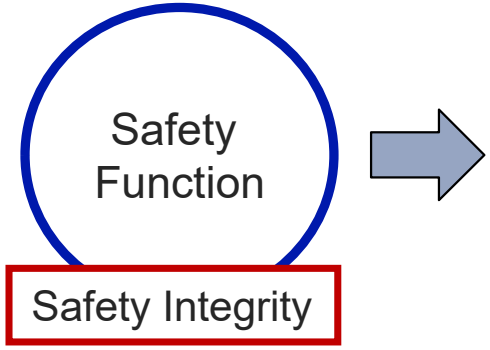
- The concept of safety integrity was developed to encompass dangerous failures from both random hardware failures and systematic failures such as software
- A high safety integrity means a low dangerous failure rate or a low probability of failure of the safety function when required to operate

Safety Function: Functionality & Safety Integrity



Determined from the hazard analysis

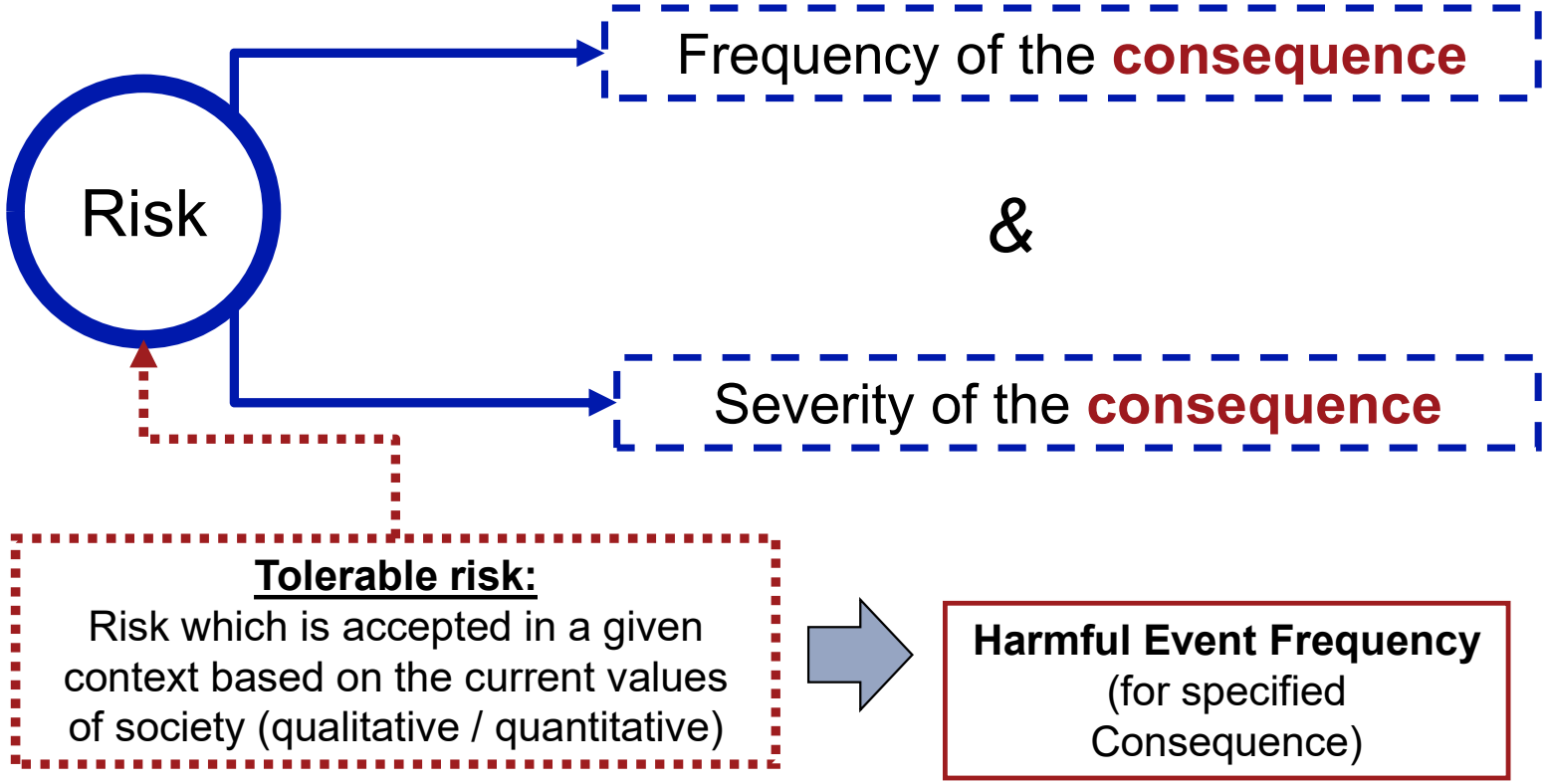
"what has to be done" to ensure that the specified hazardous event does not take place or to mitigate the consequences of the specified hazardous event.



Determined from the risk assessment

the "safety performance" of the safety function"; the likelihood of the safety function being achieved

Key terms and concepts: Risk



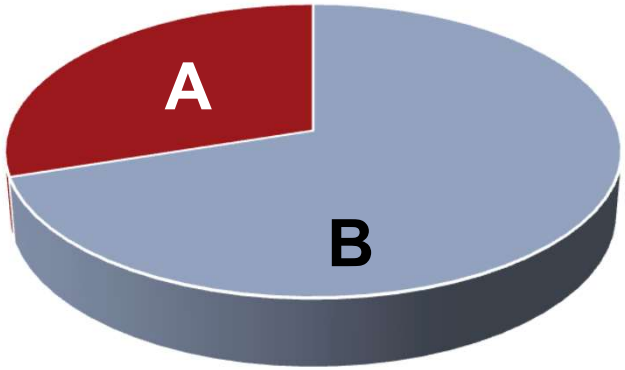
- IEC 61508 adopts a risk based approach for determining the required performance of the safety function
- Specify the risk…determine the safety integrity of the safety function…build the E/E/PE safety-related system to meet tolerable risk!

Failure Categories

Failures are categorised into:

A

Random Hardware Failures in a dangerous mode arising from degradation mechanisms



B

Systematic Failures in a dangerous mode arising from, for example:

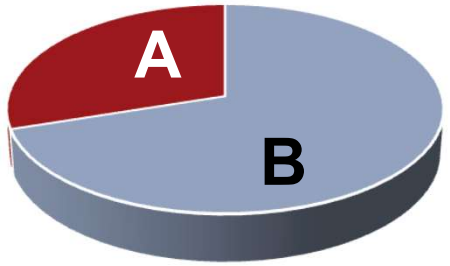
- Incorrect specification h/w or s/w
- Omissions in the safety requirements specification (e.g. omission of necessary safety functions)
- Systematic hardware failure mechanisms
- Software errors
- Human error
- Electromagnetic Interference (EMI)
- Maintenance and modification

Failure Categories

In the 1970's main design focus was on Random Hardware Failures

A

Random Hardware Failures in a dangerous mode arising from degradation mechanisms



With complex systems much more attention had to be taken of Systematic Failures

The driver for the concept of Safety Integrity Level (SIL) is because of the importance of Systematic Failures!

B

Systematic Failures in a dangerous mode arising from, for example:

- Incorrect specification h/w or s/w
- Omissions in the safety requirements specification (e.g. omission of necessary safety functions)
- Systematic hardware failure mechanisms
- Software errors
- Human error
- Electromagnetic Interference (EMI)
- Maintenance and modification

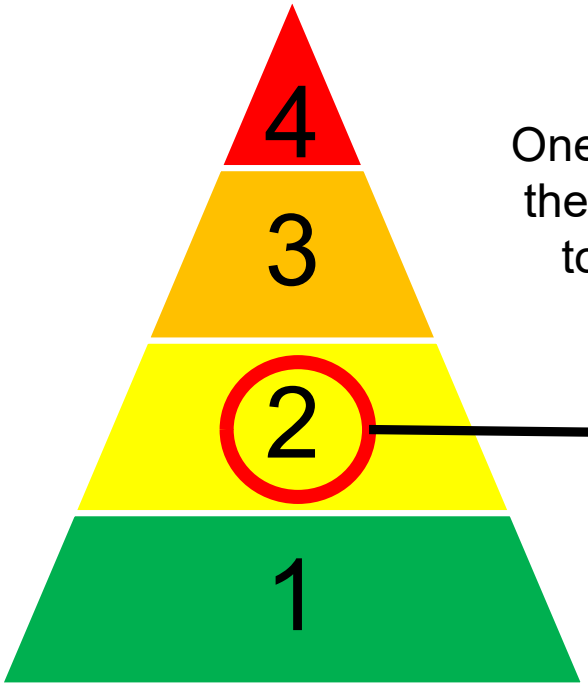
Safety Integrity Level

Safety Integrity Level (SIL):

Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the electrical, electronic and programmable safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

SIL is a property of a safety function

Safety Function: Safety Integrity Levels (SILs)



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

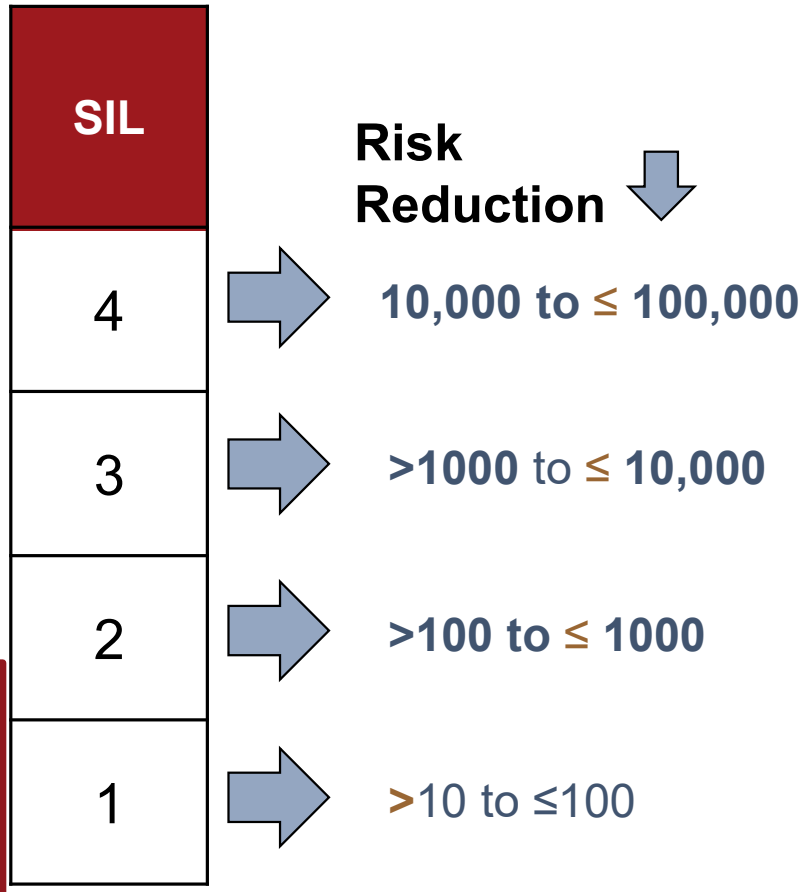
Safety Integrity Level 2 = SIL 2

- The higher the SIL of the Safety Function the greater its risk reduction properties.
- SIL 4 provides the highest risk reduction and SIL 1 the lowest risk reduction.
- The SIL determined by knowing the tolerable risk and taking into account other risk reduction measures.

SILs & Risk Reduction

For each SIL, SIL 1 to SIL 4, there is a quantified Target Failure Measure.

The Risk Reduction of 80 is often stated as a Risk Reduction Factor [RRF] of 80 in the SIL 2 band

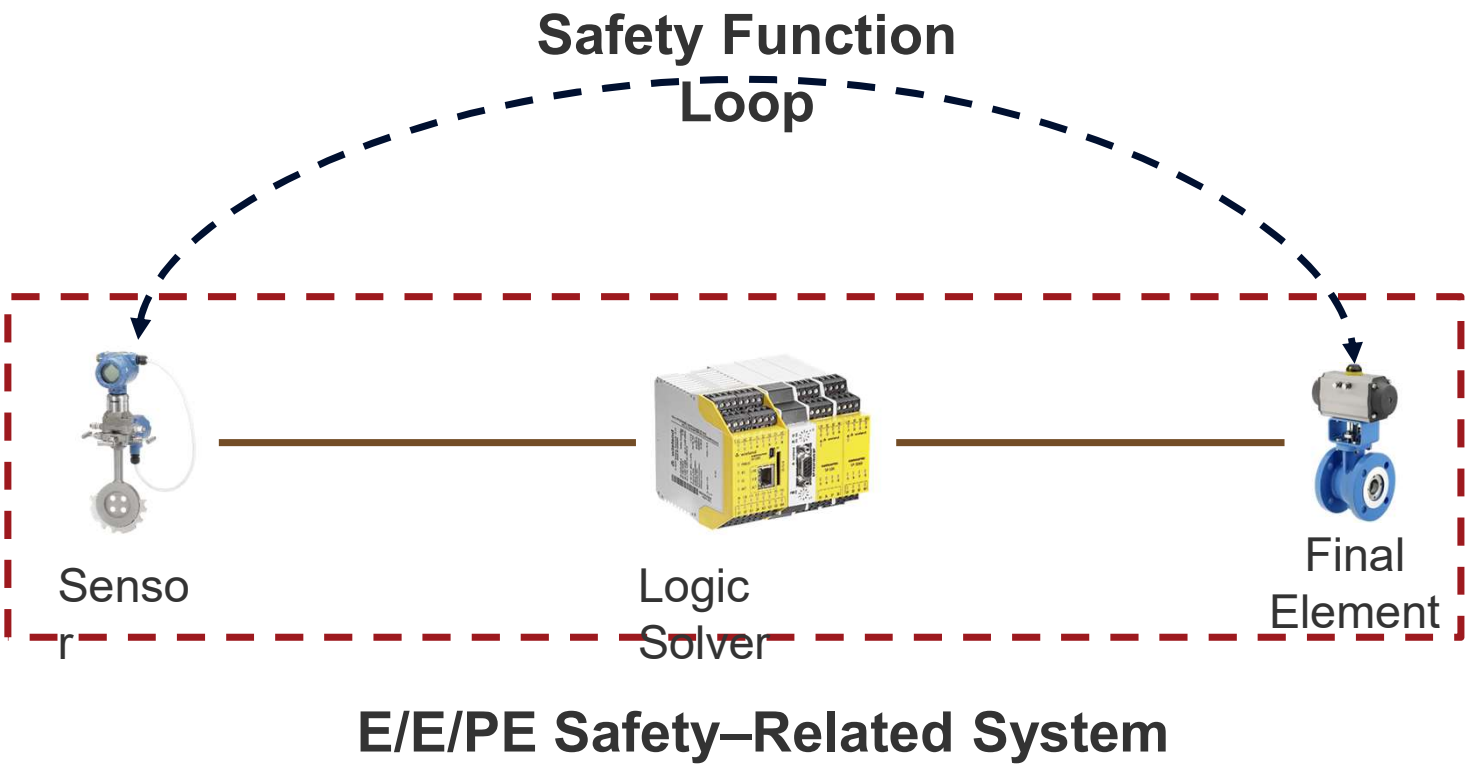


Example

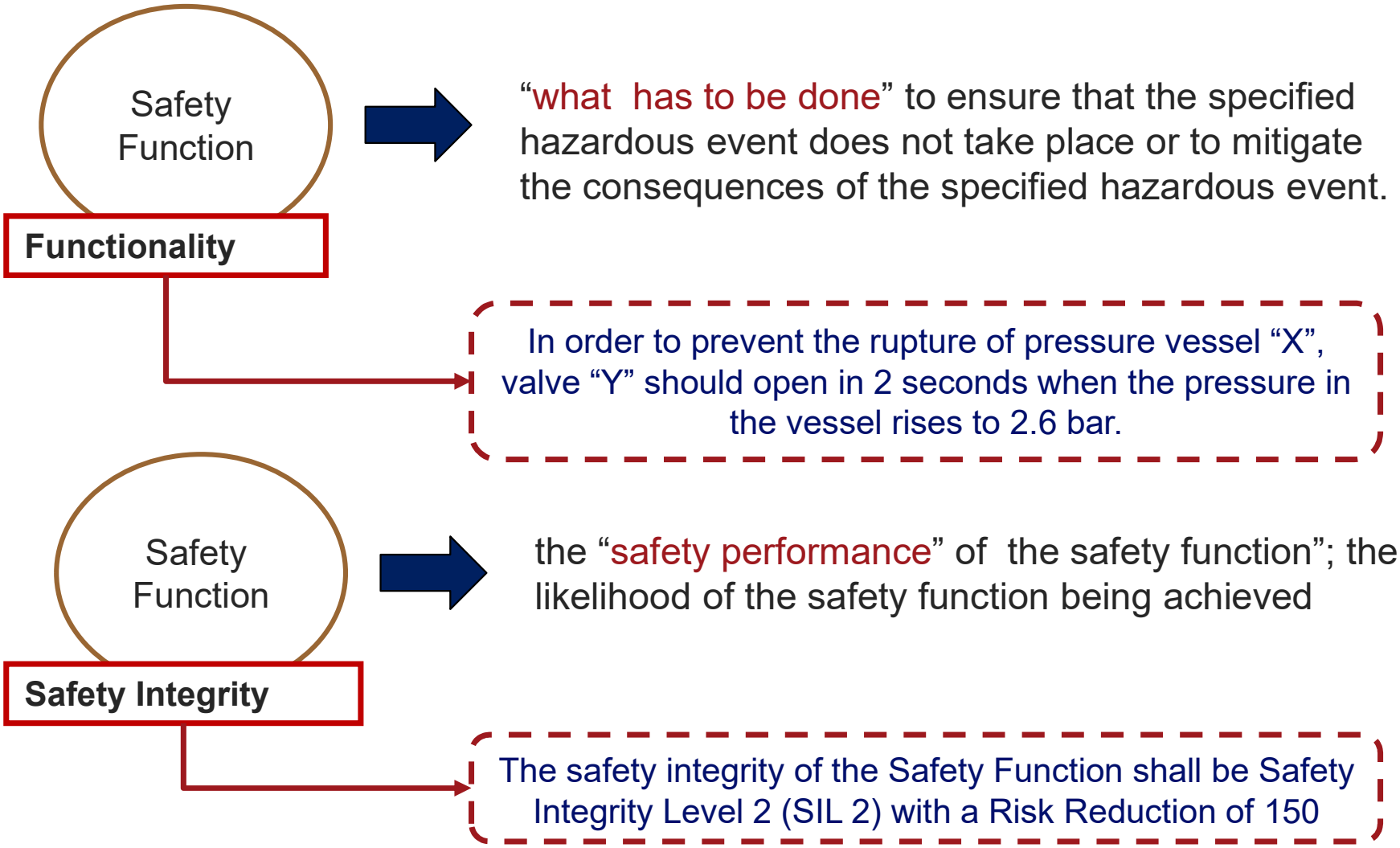
- Risk with NO Safety Function: Frequency is approximately 1 in 10 years for a Consequence of a single fatality.
- Risk with a Safety Function of SIL 1 with a Risk Reduction of 80: would reduce the Frequency of the Consequence to approximately 1 in 800 years (80 × 10).
- The Risk has been reduced by reducing the Frequency.
- That is, in this example the severity of the Consequence remains unchanged

The Target Failure Measure of the Safety Function

The Target Failure Measure relates to the ability of the safety function to meet a specified performance



Safety Function: Functionality & Safety Integrity



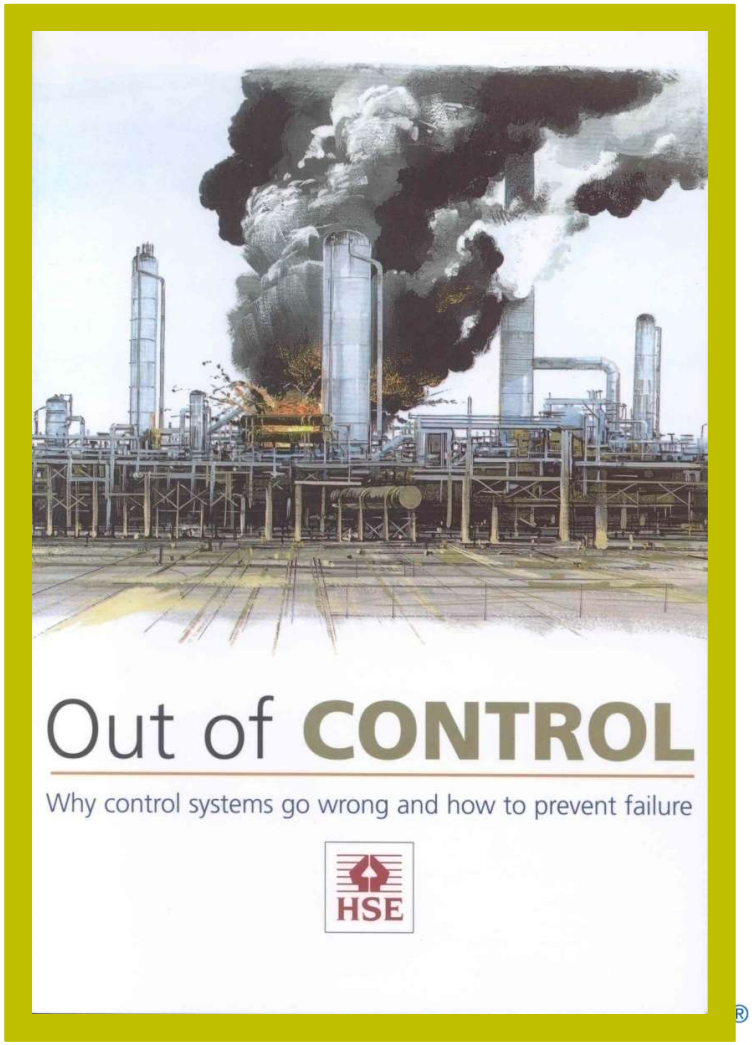
HSE “Out of control publication”

- Study comprised 34 incidents involving control systems
- Chemical/petroleum plant and machinery within scope of the study
- Incidents characterized by originating **lifecycle phase**

Out of control: Why control systems go wrong and how to prevent failure
HSE Books ISBN 0-7176-2192-8

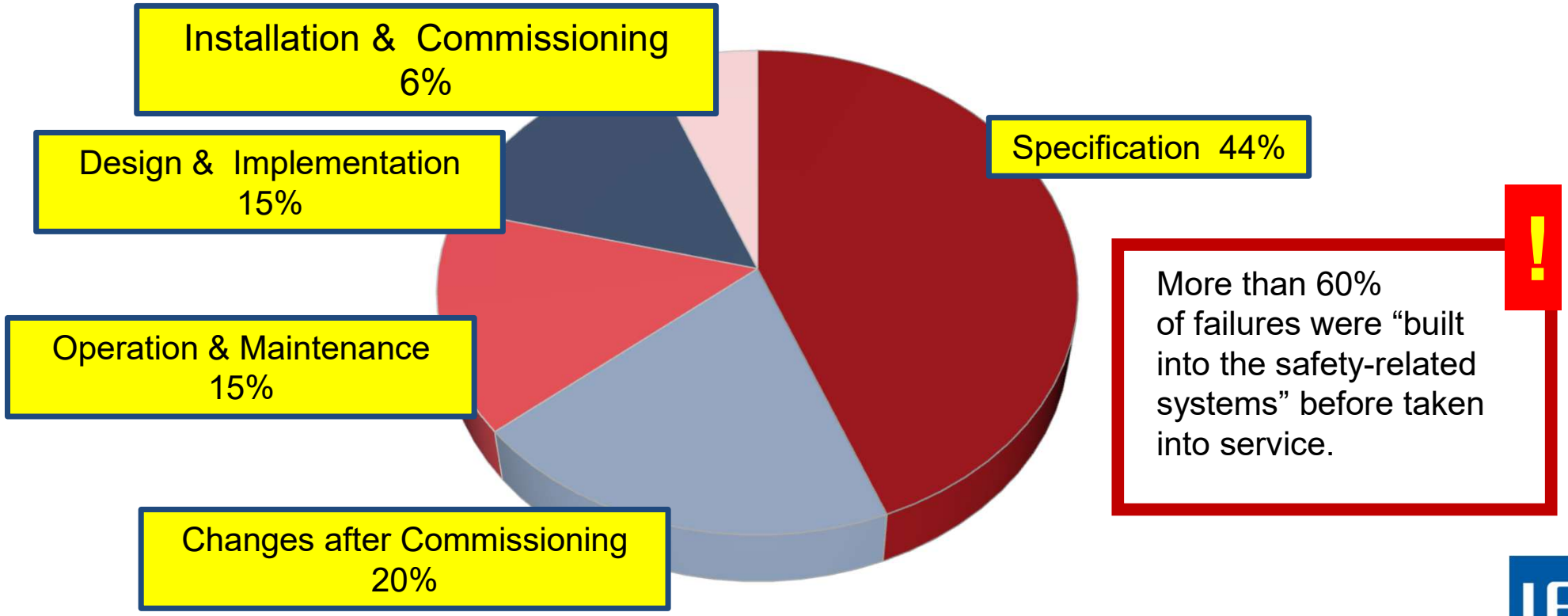
Free copy available for download at

https://www.hse.gov.uk/pubns/books/hsg238.htm[[Correct at 3rd November 2021]



Primary cause of control system failure

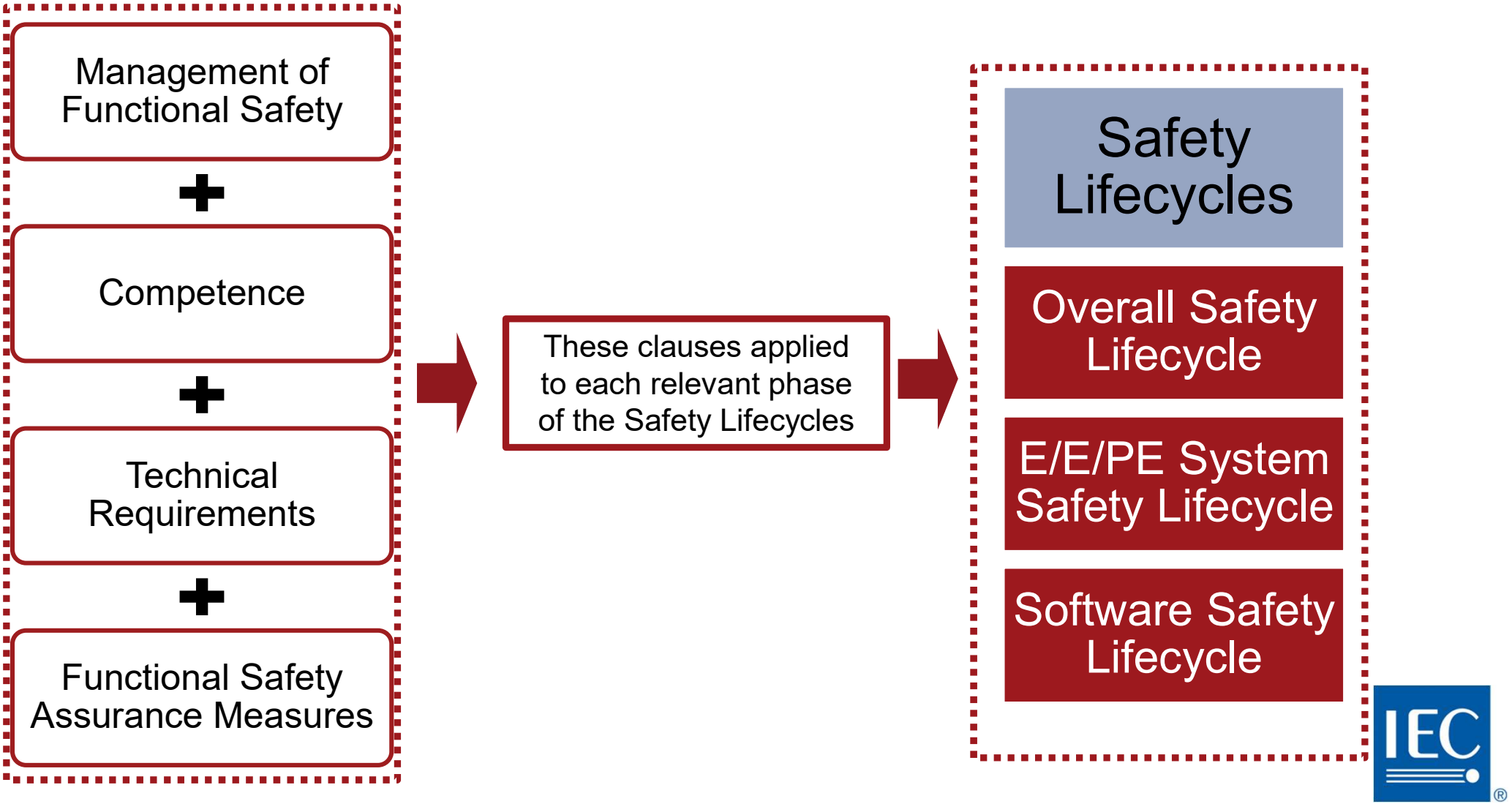
The primary causes of dangerous failures of the control system (by Safety Lifecycle phase) are indicated as follows:



The concept of a Safety Lifecycle in IEC 61508

- The figure represents a very simplified version of the Overall Safety Lifecycle.
- There are three Safety Lifecycles:
  - ✓ Overall Safety Lifecycle
  - ✓ E/E/PE system safety lifecycle
  - ✓ Software safety lifecycle
- Each phase of each lifecycle specifies the requirements for that phase.
- The requirements specified in each phase relate to the technical requirements.

Compliance to IEC 61508



Summary: Revisiting the objectives of IEC 61508

- Release the potential of E/E/PE technology;
- Enable technological developments to take place within an overall safety
- Provide a technically sound, system based approach, with sufficient flexibility for the future;
- Provide a risk based approach for determining the required performance of safety-related systems to achieve a specified risk which may be specified in quantitative or semi-quantitative terms;
- Provide a generically-based standard that can be used directly by industry but can also help with developing sector standards (e.g. machinery, process chemical plants) or product standards (e.g. power drive systems);
- Provide a means for users and regulators to gain confidence when using computer-based technology;
- Provide requirements based on common underlying principles to facilitate:
  - improved efficiencies in the supply chain for suppliers or elements (e.g. sensors, controllers);
  - Improvements in communication and requirements (i.e.to increase clarity of what is required to be specified);
  - the development of techniques and measures that could be used across all sectors;
  - The development of conformity assessment services if required.

Overview of IEC 61508 & Functional Safety