Introduction to IEC61508 and Functional Safety
Why have Functional Safety Systems?

To prevent risk to people, environment and business

HOW?

- By good management safety and quality systems
- Design to standards / best practices
- Using competent resources to deliver

WHAT HAPPENS IF THESE GO WRONG?
Have You Been Asked This?

‘Regulator’

“How can you demonstrate that you are safe?”
Safety Issues for End User / Operators

- How do you demonstrate that your operations are ‘safe’?
- How do you demonstrate that your equipment is ‘safe’?
- How do you demonstrate that your safety and protective systems protect against your hazards?

You can answer these questions by demonstrating compliance with Industry Safety Standards

IEC61508 - Functional safety of electrical / electronic / programmable electronic safety-related systems
What is IEC61508?

- An international standard relating to the Functional Safety of electrical / electronic / programmable electronic safety related systems
  - 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
- It is an industry best practice standard to enable you to reduce the risk of a hazardous event to a tolerable level
Features of IEC61508

- Generic Standard which may be applied by all Sector variants (machinery, process plant, medical, rail)
- International standard - end users and suppliers operate internationally
- Guidance on use of Electrical, Electronic and Programmable Electronic Systems which perform safety functions
- Comprehensive approach involving concepts of Safety Lifecycle and all elements of protective system
- Risk-based approach leading to determination of Safety Integrity Levels (S.I.Ls) - measures proportionate to the risk reduction required
- Considers the entire Safety Critical Loop
- Aims to facilitate improvements in both safety and economic performance through effective use of the (PES) technology
Overall Safety Lifecycle in IEC 61508

1. Concept
2. Overall Scope Definition
3. Hazard Risk Analysis
4. Overall Safety Requirements
5. Safety Requirements Allocation
6. Overall Operational and Maintenance Planning
7. Overall Validation Planning
8. Overall Installation and Commissioning Planning
10. Safety Related Systems: Other Technology Realisation
11. External Risk Reduction Facilities Realisation
12. Overall Installation and Commissioning
13. Overall Safety Validation
14. Overall Operation and Maintenance
15. Overall Modification and Retrofit
16. Decommissioning

Back to appropriate overall safety lifecycle phase
Why this lifecycle?

- Maps directly to the normal work pattern of the project in a ‘cradle-to-grave’ process.
- Maps directly to asset life cycle
- Seen by the Regulatory Authorities as industry best practice
- Can be used in any business, any sector.
- Applies to all aspects of the end user supply chain relationship
- Will be used to demonstrate regulatory compliance
- Generates efficiencies in ‘cost of safety’
  - Common terminology
  - Defined document / responsibility interfaces throughout the supply chain
  - Common practices
Summary of the Key Messages in IEC 61508

Safety Management System
- Life cycle
- Planning
- Assessing compliance
- Supply chain

Technical Requirements
- Choice of technologies
- Assessment of risk
- Specifications of function & integrity level

Competencies
- Roles & responsibilities
- Skills & training
Benefits of a Safety Management System

- A defensible method of managing risks
- Coherent approach to the whole subject
- Facilitates specification, design and purchase
- Allows self regulation
What is Risk?

- The probable rate of occurrence of a hazard causing harm

AND

- the degree of severity of the harm
  - Qualitatively - Words
  - Quantitatively - Figures
Risk and Determination of Safety Integrity Levels

Increasing Severity

Increasing Likelihood

SIL 4
SIL 3
SIL 2
SIL 1
No Protection

Basic Design Unacceptable
Levels of Risk and ALARP

Unacceptable Risk

Risk cannot be justified except in extraordinary circumstances

Broadly acceptable risk

(No need for detailed working to demonstrate ALARP)

The ALARP or Tolerability Region

(Risk is undertaken only if a benefit is desired)

Negligible risk

Tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained

As risk is reduced, there is a proportional decrease in the cost of further reduction, this concept of diminishing proportion is represented by the triangle.

Necessary to maintain assurance that risk remains at this level
Risk reduction: General concepts

- Actual risk remaining
- Risk to meet level of safety
- Plant under Control risk

Necessary minimum risk reduction

Actual risk reduction

Partial risk covered by other technology safety-related systems
Partial risk covered by E/E/PES protective systems
Partial risk covered by External Risk Reduction Facilities

Risk reduction achieved by all protective systems and external risk reduction facilities
Technologies Under Consideration

- Electrical
  - Electro-mechanical / relays / interlocks
- Electronic
  - Solid state electronics
- Programmable Electronic Systems
  - Programmable Logic Controllers (PLC’s);
  - Microprocessor based systems
  - Distributed Control Systems
  - Other computer based devices
    - ("smart" sensors / transmitters / actuators)
Extent of a E/E/PE safety-related system

Equipment Under Control

SENSOR — PE — ACTUATOR

PE = Programmable Element
Example method of calculating a Target Safety Integrity Level

- Hazard studies and HAZOPs
- Evaluate possible consequences
- Establish tolerable frequencies vs ALARP
- Build event chain
- Estimate demand rates
- Define protection required
- Specify required Safety Integrity Level
## Risk Reduction Requirements

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Risk Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10 - 100</td>
</tr>
<tr>
<td>2</td>
<td>100 - 1,000</td>
</tr>
<tr>
<td>3</td>
<td>1,000 - 10,000</td>
</tr>
<tr>
<td>4</td>
<td>10,000 - 100,000</td>
</tr>
<tr>
<td>SIL Level</td>
<td>Reliability</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>SIL 1</td>
<td>90% - 99%</td>
</tr>
<tr>
<td>SIL 2</td>
<td>99% - 99.9%</td>
</tr>
<tr>
<td>SIL 3</td>
<td>99.9% - 99.99%</td>
</tr>
<tr>
<td>SIL 4</td>
<td>99.99% - 99.999%</td>
</tr>
</tbody>
</table>
Protective System Technology

SIL 1: Standard components, single channel or twin non-diverse channels

SIL 2: Standard components, 1 out of 2 or 2 out of 3, possible need for some diversity. Allowance for common-cause failures needed

SIL 3: Multiple channel with diversity on sensing and actuation. Common-cause failures a major consideration. Should rarely be required in process industry

SIL 4: Specialist design. Should never be required in the Process Industry
Protective System Design, Test and Maintenance Requirements

- **SIL 1**: Relatively inexpensive to design, build and maintain. Test interval unlikely to be less than 3 months.

- **SIL 2**: Moderately expensive to design, build and maintain. Test interval unlikely to be more than 3 months.

- **SIL 3**: Expensive to design, build and maintain. Test interval likely to be 1 month.

- **SIL 4**: Extremely expensive to design, build and maintain. Test interval as for SIL 3 (diminishing returns below 1 month).
IEC 61508 - ownership of phases

**PRE-DESIGN**
(Phases 1 to 5)

End user / operator

**DESIGN AND INSTALLATION**
(Phases 6 to 13)

Engineering Contractors / Equipment Supplier

**OPERATION**
(Phases 14 to 16)

End user / operator
## Pre-Design: Phases 1 - 5

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Concept</td>
</tr>
<tr>
<td>2</td>
<td>Overall Scope Definition</td>
</tr>
<tr>
<td>3</td>
<td>Hazard Risk Analysis</td>
</tr>
<tr>
<td>4</td>
<td>Overall Safety Requirements</td>
</tr>
<tr>
<td>5</td>
<td>Safety Requirements Allocation</td>
</tr>
</tbody>
</table>

- Can you demonstrate that you have identified all your hazards?
- Can you demonstrate that you are using adequate and correct methods of hazard protection?
### Design & Implementation: Phases 6 - 13

How do you ensure competencies for all these activities?

<table>
<thead>
<tr>
<th>Overall Planning</th>
<th>Overall Operational and Maintenance Planning</th>
<th>Overall Validation Planning</th>
<th>Overall Installation and Commissioning Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>7</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

Can you demonstrate that you pass the necessary information into these activities?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Realisation</td>
<td>Realisation</td>
<td>Realisation</td>
</tr>
</tbody>
</table>

Can you demonstrate that all necessary information has been passed to you from these activities?

<table>
<thead>
<tr>
<th>12 Overall Installation and Commissioning</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>13 Overall Safety Validation</th>
</tr>
</thead>
</table>
Can you demonstrate that you maintain / test / analyse your protective systems correctly?

Can you demonstrate that you are in control of your modification process?
IEC 61508 - Three Phases for Protective Functions

- **PRE-DESIGN** (Phases 1 to 5)
  - End user / operator

- **DESIGN AND INSTALLATION** (Phases 6 to 13)
  - Engineering Contractors / Equipment Supplier

- **OPERATION** (Phases 14 to 16)
  - End user / operator

Set the Target SIL

Designed SIL

Demonstrate
Achieved = Design = Target
IEC 61508 Responsibilities: End Users / Operators

- Functional Safety Specification Requirements
  - Contribution from all Safety Function Technologies and Risk Reduction Methods
    - Target SIL for the E/E/PES contribution
- Overall Responsibility for the Management of Functional Safety
- Functional Safety Plan at the outset of the work - Identification of Functional Safety Assessments for the project duration
- Overall Validation and Verification
- Commissioning and acceptance
- Operations and Maintenance
- Modification and Retrofit
Power and productivity for a better world™