IEC 61508 and IEC 61511: What, when, why?

Mary Ann Lundteigen

Department of Production and Quality Engineering
Norwegian University of Science and Technology
mary.a.lundteigen@ntnu.no
Overview
Content of presentation

This lecture includes:

- A brief introduction to SIS
- Background for the development of IEC 61508 and IEC 61511
- Main content of IEC 61508 and IEC 61511
- Key concepts and principles
- Discussion issues
Overview

SIS

Background
Concepts
Application
Example

Need for standards

IEC standards

Key concepts

Life cycle phases

Safety integrity

Discussion topics
Understanding why safety systems are required

- An hazardous event: hazardous situation that may lead to harm.
- Accident: An unintended event or sequence of events causing death, injury, environmental, or material damage (DEF-STD00-56)
- Risk may be used to characterize an accident; (1) what can go wrong, (2) how likely is it, and (3) what are the consequences.
- Risk: $R = s_i, p_i, c_i$, where $s_i$ characterize scenario $i$ (answer to question 1), $p_i$ is the probability for the scenario (answer to question 2), and $c_i$ is the consequence (answer to question 3). (Kaplan)
Understanding why safety systems are required

- Hazard
- Hazard
- Hazard
- Hazard
- Hazard
- Hazard
- Hazard
- Hazard

e.g., gas leakage

May lead to harm if propagating

Hazardous Initiating event

Results in harm

e.g., explosion

Accident

Hazard
Understanding why safety systems are required

Hazardous events may be caused by:

- Release or loss of control with hazardous materials (e.g., chemical reactions, leakage of toxic materials)
- Release of large energies (e.g., burst)
- Unexpected operation/movement (for equipment with moving parts)
- High pressures or high temperatures (e.g., melting, burst, rupture)
- Design deficiencies (e.g., too fragile components, wrong installation)
- Excessive exposure from harsh environment (e.g., burst, rupture, fail to function)
- Sparks/flame arc in areas with hydrocarbons (e.g., fire)

The purpose of a safety system is to detect the onsets of hazardous events and mitigate their effects on humans, environment, and material assets.
So what is a SIS?

- A *safety instrumented system* (SIS) is used perform safety functions, that is to:
  1. Detect the onset of hazardous event, and
  2. Mitigate their consequences to personnel, environment and assets

- The SIS comprises input elements, logic solvers, and final elements

- The safety functions implemented in the SIS are often referred to as *safety instrumented functions* (SIF)
The difference between a SIS and a SIF may be illustrated as in the figure below:

An emergency shutdown system

A fire and gas system
SIS may be used as barrier elements

Production? stopped

Detected & isolated (primary)?

Detected and isolated (secondary)?

Input elements

Logic solver

Final elements

e.g., PSD

No

Yes

No

Yes

Input elements

Logic solver

Final elements

e.g., ESD

Above text is not to be quoted
A SIS example

A high integrity pressure protection system (HIPPS) may be implemented as follows:\(^1\):

1. Usually, at least two shutdown valves are operated, but here only one valve is illustrated.
Need for standards
Need to manage new technology

- 1970s: SIS based on simple devices and logic:
  - Pneumatic, pneumatic/hydraulic systems
  - Direct wired systems
  - Electromechanical devices (relays, timers)
  - Solid state relays

- Late 1970s:
  - Programmable electronic systems (PES) were introduced, e.g., PLC, micro-computers.

- 1990s:
  - PLCs are getting more advanced
  - Bus systems for communication
  - Smart field devices
  - Mixing of technologies
  - Security issues
Need to learn from accidents

- Several large accidents in the 1970s and 1980s:
  - Flixborough plant 1974: Explosion
  - Seveso plant 1976: Large chemical release
  - Piper Alpha 1988: Large fire, oil and gas leakage

- Lead to new legislations and directives:
  - Occupational Safety and Health Administration (OSHA) Process Safety management (PSM) legislation, USA
  - Seveso II directive on prevention of large chemical accidents, Europe
  - Health and Safety Executive (HSE), UK
Need to cope with globalization

End users and SIS manufacturers operate in a global market:

- End users like e.g., oil companies have plants in several countries
- SIS manufacturers make products that may be used in several industry sectors

The need to cope with new technology, to learn from accidents, and operate in a global market have stimulated the development of international standards.
IEC standards
IEC 61508 was based on existing standards

- DIN 19250 (1994) - German standard: *Fundamental safety aspects to be considered for measurement and control equipment*

- Hoscher and Rader (1984) - German standard: *Microcomputers in Safety Technology*

- DIN VDE 801 (1990) - German standard: *Principles for computers in safety-related systems*

- ANSI/ISA-84.01 (1996) - US standard: *Application of Safety Instrumented Systems for the Process Industries*


- HSE (1987) - UK standard: Programmable electronic systems in safety related applications
IEC 61508 scope

The objective of IEC 61508 is to:

- Serve as a guideline for development of sector specific standards.
- Serve as a standard where sector specific standards do not exist or has certain restrictions on application areas.
Relationship to authority regulations

- IEC standards are not mandatory as such.
- They become mandatory if National authorities make reference to the standards.
- The Norwegian Petroleum Safety Authority makes reference to IEC 61508 and OLF 070 in the facility regulations, § 7.
IEC 61508 content

IEC 61508 comprises seven parts:

Part 1:  General requirements
Part 2:  Requirements for E/E/PE safety-related 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 IEC 61508-2 and IEC 61508-3
Part 7:  Overview of techniques and measures

The first three parts are mandatory, whereas the other are informative.
IEC 61508 covers all SIS life cycle phases
Sector specific IEC standards

- **IEC 61511** *Functional safety – Safety instrumented systems for the process industry*

- **IEC 62061** *Safety of machinery – Functional safety of electrical, electronic and programmable electronic systems*

- **IEC 61513** *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

- **EN 50126** *Railway applications – The specification and demonstration of reliability, availability, maintainability, and safety (RAMS)*

- **EN 50128** *Railway applications – Software for railway control and protection systems*

- **EN 50129** *Railway applications – Safety related electronic systems for signalling*

- **IEC 60601** *Medical electrical equipment*

---

2 The Instrument Society of America (ISA) has developed a US version ISA 84.00.01 that addresses OSHA requirements (e.g., 'grandfathering')

3 EN 50126, EN 50129 and EN 50128 were based on earlier drafts of IEC 61508. IEC standards that are based on the EN standards: IEC 62278, IEC62425, IEC 62279
National adoption of IEC standards

- **Guide to the application of IEC 61511 to safety instrumented systems in the UK process industries (draft):** Developed by the Energy Industry Council (EIC), Engineering Equipment Manufacturers and Users Association (EEMUA), United Kingdom Offshore Operators Association (UKOOA), and HSE.

- **ANSI/ISA-84.00.01-2004, Functional safety: Safety instrumented systems for the process industry sector (IEC 61511 mod):** Developed by ISA for application in the US.

- **OLF 070 Guidelines for the application of IEC 61508 and IEC 61511 in the Norwegian petroleum industries:** The OLF 070 guideline has been developed by the Norwegian Oil Association.
Focus of this lecture

- In this lecture, we focus primarily on the oil and gas industry
- As a result, we discuss the main principles of IEC 61508, IEC 61511, and OLF 070.
IEC 61508, IEC 61511, and OLF 070 apply to the oil and gas industry:

<table>
<thead>
<tr>
<th></th>
<th>IEC 61508</th>
<th>IEC 61511</th>
<th>OLF 070</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td>Generic New technology</td>
<td>Process industry Proven technology</td>
<td>Oil and gas (Norway) Both</td>
</tr>
<tr>
<td><strong>Risk reduction</strong></td>
<td>Analysis</td>
<td>Analysis with suggested techniques</td>
<td>Minimum SIL requirements</td>
</tr>
<tr>
<td><strong>Reliability</strong></td>
<td>Standard beta factor/Reliability block diagram</td>
<td>Standard beta factor/Suggest several modeling techniques</td>
<td>PDS method (“extended” version of the standard beta factor model)</td>
</tr>
</tbody>
</table>
Standards that apply to the oil and gas industry

IEC 61508, IEC 61511, and OLF 070 are not the only standards that address SIS design, construction, and follow-up:

- Activity regulations §42, 46
- Management regulations §2, 18
- Facility regulations §7

Which refer to:

- NORSOK (S-001, I-001)
- IEC 61508
- IEC 61511
- OLF 070
- ISO 10418
- ISO 14224
- Z-016

Company specific requirements

Lifecycle requirements  Design requirements  Data collection & analysis

PSA: Petroleum Safety Authority Norway
IEC 61511 - Application areas

- IEC 61511 is the process sector version of IEC 61508
- Directed at the system level designers, integrators, and end users (‘end user standard’)
- There are three situations where IEC 61511 users are directed to IEC 61508:
  - A device is being modified and/or used in a manner not intended by the vendor. This is considered as development activities.
  - SIL 4 is specified.
  - A device is being programmed using a full variability language.
IEC 61511 versus IEC 61508

Overview
SIS
Need for standards
IEC standards
Previous standards
IEC 61508
Related standards
Process industry
IEC 61511
Key concepts
Life cycle phases
Safety integrity
Discussion topics

SIS design for the process sector

Hardware
- Developing NEW hardware devices
  - IEC 61508-1,2
- Using PROVEN-IN-USE hardware devices
  - IEC 61511
- Using hardware developed and assessed in accordance with IEC 61508
  - IEC 61511

Software
- Developing embedded software systems
  - IEC 61508-3
- Developing application software using FVL
  - IEC 61508-3
- Developing application software using LVL or FP
  - IEC 61511
IEC 61511 life cycle phases

Overview
SIS
Need for standards
IEC standards
Previous standards
IEC 61508
Related standards
Process industry
IEC 61511
Key concepts
Life cycle phases
Safety integrity
Discussion topics

Hazards and risk assessment (clause 8)
Allocation of safety function to protection layers (clause 9)

Development of the safety requirement specification for the SIS (clauses 10 and 12)
Design and engineering of SIS (clauses 11 and 12)

Installation, commissioning and validation (clauses 14 and 15)
Operation and maintenance (clause 16)
Modification (clause 17)
Decommissioning (clause 18)

Verification (clauses 7, 12.4, and 12.7)

No detailed requirements in IEC 61511
Requirements provided in IEC 61511

Management of functional safety and functional safety assessment and auditing (clause 5)
Safety life cycle structure and planning (clause 6.2)
IEC 61511 - main parts

IEC 61511 comprises three parts:

- **Part 1**: Framework, definitions, system, hardware and software requirements
- **Part 2**: Guidelines for the application of IEC 61511-1
- **Part 3**: Guidance for the determination of the required safety integrity levels

Part 1 is normative, whereas Part 2 and Part 3 are informative.
IEC 61511 - terms and concepts

The IEC 61508 and IEC 61511 do in some cases use different terms and concepts

<table>
<thead>
<tr>
<th>IEC 61508</th>
<th>IEC 61511</th>
</tr>
</thead>
<tbody>
<tr>
<td>Different definition of dangerous undetected (DU) failures</td>
<td>SIS</td>
</tr>
<tr>
<td>E/E/PE safety related system</td>
<td>SIS</td>
</tr>
<tr>
<td>PES</td>
<td>SIS</td>
</tr>
<tr>
<td>EUC control system</td>
<td>Basic process control system (BPCS)</td>
</tr>
<tr>
<td>EUC</td>
<td>Process</td>
</tr>
<tr>
<td>EUC risk</td>
<td>Process risk</td>
</tr>
<tr>
<td>Safety function</td>
<td>SIF</td>
</tr>
<tr>
<td>Proven-in-use</td>
<td>Prior use</td>
</tr>
<tr>
<td>Type A versus type B components</td>
<td>IE/FE/non-PE logic solvers versus PE logic solvers</td>
</tr>
<tr>
<td>Low demand versus high demand/continuous mode</td>
<td>demand versus continuous mode</td>
</tr>
</tbody>
</table>
Key concepts
EUC, EUC control system, and SIS

- **SIS** is (out of several means) to protect consequences of hazardous events within the EUC.

- **EUC** stands for equipment under control and denotes the system or equipment that need some protection.

- **EUC control system** is the system used to handle start-up, controlled shutdowns, and normal operation.
EUC, EUC control system, and SIS

Overview
SIS
Need for standards
IEC standards
Key concepts
EUC
Requirements
SIL
Failure classification
Life cycle phases
Safety integrity
Discussion topics

Safety instrumented system (SIS)
EUC control system
Equipment under control (EUC)
Safety-related systems based on other technology
Other risk reduction facilities
Functional safety and safety integrity

IEC 61508 and IEC 61511 distinguish between two safety requirements:

- The safety requirements comprise two elements:
  1. Functional safety requirements ("what to perform")
  2. Safety integrity requirements ("how well to perform")
What is meant by integrity/safety integrity

➤ Integrity:

- State of being unimpaired
- The state of quality of being entire and complete
- Related to data: The quality of correctness, completeness, wholeness, soundness and compliance with the intention of the creators of the data.

➤ Safety integrity (IEC 61508, IEC 61511):

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

or in other words, safety integrity is the same as reliability when the application is safety-related.
What is meant by safety integrity *level* or SIL?

- Safety integrity level (SIL) is used to classify safety integrity requirements.

- It is defined as a:
  - Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, [...].

- In other words; each SIF is associated with a SIL requirement.

- The SIL requirement determined based on e.g., layers of protection analysis (LOPA), risk graph, minimum SIL requirements in *OLF 070*. 
How may a SIF comply to a SIL requirement?

<table>
<thead>
<tr>
<th>Overview</th>
<th>SIS</th>
<th>Need for standards</th>
<th>IEC standards</th>
<th>Key concepts</th>
<th>EUC</th>
<th>Requirements</th>
</tr>
</thead>
</table>

**SIL**

- **Failure classification**
- **Life cycle phases**
- **Safety integrity**
- **Discussion topics**

To comply to a **SIL** requirement, the **SIF** must be selected and verified against the:

- Hardware safety integrity requirements (1) and (2)
- Software safety integrity requirements (3)
- Systematic safety integrity requirements (4)

In addition, the standards may have requirements that apply to all **SILs**.
➤ All safety integrity categories must be ‘at the SIL level’.

➤ Thus; to e.g., demonstrating compliance to the PFD target range is not enough...
Failure classification

- Failures may be classified according to their:
  - Causes:
    - Random hardware failures
    - Systematic failures (including software failures)
    - Common cause failures
  - Effects:
    - Safe failures
    - Dangerous failures
  - Detectability:
    - Detected
    - Undetected
Failure classification

*) Some systematic failures may be included in historical databases. Some systematic failures may also be catered for in the CCF rate.
Life cycle phases
The objective is to:

- Develop an understanding of the EUC and its environment
Overall scope definition

The objective is to:

- Determine the boundary of the EUC and the EUC control system
Hazard and risk analysis

The objectives are to:

- Determine the hazards and the hazardous events of the EUC and the EUC control system in all modes of operation.
  - Must consider all reasonable foreseeable circumstances, including fault conditions and misuse
- Determine the associated EUC risk
- Identify the tolerable EUC risk

One approach is to perform a hazard and operability study (HAZOP) complemented by e.g., layers of protection analysis (LOPA) or event tree analysis.
Overall safety requirements

The objectives are to:

➤ Develop the specification for the overall safety requirements, the safety requirement specification (SRS) with:

➤ Functional safety requirements
➤ Safety integrity requirements (SIL)
Safety requirement allocation

The objectives are to:

- Allocate the functional safety and safety integrity requirements to technology and functions:
  - Safety instrumented system: One or more
  - Other technology (e.g., pure mechanical devices)
  - External risk reduction facilities (e.g., fire walls)
The objectives are to:

- Develop plans for overall operation and maintenance: Procedures, competence needs, scheduling, follow-up

- Develop plans for overall safety validation: Plan for factory acceptance testing, site acceptance testing, pre-start-up testing, functional safety assessments and audits.

- Develop plans for installation and commissioning: Procedures for installation, inspections, testing, labeling, temporary installations.
The objectives are to:

- Develop more specific requirements for the SIS, taking into account the SRS
- Design and construct the SIS hardware and software according to the requirements
- Verify hardware, software, and integration of hardware and software against the requirements for hardware safety integrity, software safety integrity, and systematic safety integrity by testing, design reviews, audits, and reliability analysis.
Overall installation and commissioning

The objectives are to:

- Perform overall installation and commissioning according to the plans.
- Focus on revealing failures and avoid introducing failures.

“Overall” means that all safety systems that are specified in the allocation process are considered.
Overall safety validation

The objectives are to:

- Perform overall validation according to the plans.
- Focus on revealing failures and avoid introducing failures.
Overall operation, maintenance, and repair

The objectives are to:

- Perform overall operation and maintenance according to the plans.
- Focus on revealing failures and avoid introducing failures.
- Establishment of procedures, work practises, and responsibilities for follow-up.
- Collect data and use these data to verify the SIS against the requirements.
- Ensure that all SIS related modifications are handled as a separate phase.
- Ensure that personnel have adequate competence and training.
Overall modification and retrofit

The objectives are to:

- Ensure adequate handling and documentation of all SIS related modifications, including:
  - Impact of the modification
  - Decision on which phase to return to
  - Plan and schedule implementation
  - Approvals

- Modifications may be due to a number of causes, for example SIS design deficiencies, changing operating or environmental conditions, process design changes.
Decommissioning and disposal

The objectives are to:

- Ensure adequate handling decommissioning activities:
  - Decommissioning may concern a complete SIS, or be restricted to some safety functions.

- Adequate means that functional safety is maintained during these activities, to avoid that the tolerable risk level is exceeded.
Management of functional safety

The objectives are to:

▸ Specify the management and technical activities that are necessary within each phase of the SIS life cycle.

   ➤ This is where a SIS manufacturer, system integrator, end user specify what type of activities they will perform to meet the objectives for each of the safety life cycle phases.

   ➤ May be developed for each project or implemented as a general process description.

▸ Specify the persons, departments, and organizations that have an overall responsibility and those that have a more specific responsibility in each of the safety life cycle phases/life cycle activities.

   ➤ This may be specified in an organization chart, and complemented by a work process description.
Management of functional safety

Activities include:

- Follow-up of recommendations and findings
- Assuring competence and training
- Recording of events/Analysing O&M performance
- Policy and strategy for functional safety
- Procedures for handling modifications
- Procedures for configuration management
- Procedures for documentation
- Periodic functional safety assessments
- Work process and organization charts

Overview
- SIS
- Need for standards
- IEC standards

Key concepts

Life cycle phases
- Concept
- Scope
- Analysis
- Requirements
- Allocation
- Planning
- Realization
- Installation
- Validation
- Operation
- Modifications
- Decommissioning

Management
- Safety integrity
- Discussion topics

Policy and strategy for functional safety
Safety integrity
Hardware safety integrity requirements

- Hardware safety integrity requirements give guidance and restrictions to the selection of hardware.

- To verify adequate hardware safety integrity, it is necessary to analyze the SIF against the:
  
  ➤ Architectural constraints (AC)
  
  ➤ Requirements for the probability of a SIF failure due to a dangerous failure

- The probability of a SIF failure is calculated based on the random hardware failures.
Reliability measures are different for “demand mode” and “continuous mode”:

**Demand mode:** *(Average) probability of failure on demand*\(^4\).
- SIS passive during normal operation, e.g., emergency shutdown system.
- A dangerous failure may not lead to a hazardous situation.

**Continuous mode:** *Probability of a dangerous failure per hour.*
- SIS active during normal operation, e.g., railway signaling system.
- A dangerous SIS failure creates immediately a hazardous situation.

\(^4\)\(PFD \approx \frac{\lambda_{DU}}{2\tau}\) for a single component, where \(\lambda_{DU}\) is the rate of dangerous undetected failures and \(\tau\) is the functional test interval.
Reliability target ranges

For SIS operating in demand mode:

<table>
<thead>
<tr>
<th>Safety integrity level (SIL)</th>
<th>Target average probability of failure on demand (PFD)</th>
<th>Target risk reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$10^{-5}$ to $10^{-4}$</td>
<td>$10000$ to $100000$</td>
</tr>
<tr>
<td>3</td>
<td>$10^{-4}$ to $10^{-3}$</td>
<td>$1000$ to $10000$</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-3}$ to $10^{-2}$</td>
<td>$100$ to $1000$</td>
</tr>
<tr>
<td>1</td>
<td>$10^{-2}$ to $10^{-1}$</td>
<td>$10$ to $100$</td>
</tr>
</tbody>
</table>
Calculation approaches

- Familiarization:
  - Find out how the SIF is realized
  - What components and related failure modes are dangerous (DU or DD)?
  - Develop a functional block diagram

- Build a reliability model
- Develop a data dossier
- Calculate the reliability
- Compare the result with the specified reliability range
- (Perform sensitivity analysis)
What do the AC imply?

- The architectural constraints (AC) define the required *hardware fault tolerance* (HFT) of hardware configurations at the subsystem level.

- The HFT is defined as *the number of faults tolerated before a SIF fails*.

- The required HFT of a subsystem is based on the following three "parameters":
  1. The specified SIL of the SIF
  2. The component classification /complexity
  3. The safe failure fraction (SFF)
The AC are given in tables

The AC are given in tables in IEC 61508 and IEC 61511:

- For a given SFF and SIL requirement, the corresponding HFT is given.

IEC 61511 and IEC 61508 use a slightly different approach to component classification and for the SIL–SFF–HFT relationship.

<table>
<thead>
<tr>
<th>SFF/HFT</th>
<th>Type A</th>
<th></th>
<th></th>
<th></th>
<th>Type B</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>2</td>
<td></td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>&lt;60%</td>
<td>SIL1</td>
<td>SIL2</td>
<td>SIL3</td>
<td>-</td>
<td>SIL1</td>
<td>SIL2</td>
<td></td>
</tr>
<tr>
<td>60-90%</td>
<td>SIL2</td>
<td>SIL3</td>
<td>SIL4</td>
<td>SIL1</td>
<td>SIL2</td>
<td>SIL3</td>
<td></td>
</tr>
<tr>
<td>90-99%</td>
<td>SIL3</td>
<td>SIL4</td>
<td>SIL4</td>
<td>SIL2</td>
<td>SIL3</td>
<td>SIL4</td>
<td></td>
</tr>
<tr>
<td>&gt;99%</td>
<td>SIL3</td>
<td>SIL4</td>
<td>SIL4</td>
<td>SIL3</td>
<td>SIL4</td>
<td>SIL4</td>
<td></td>
</tr>
</tbody>
</table>
Step 1: Component classification and SFF

The initial step is to calculate the SFF and determine the component classification:

- The SFF is defined as:

\[
SFF = \frac{\sum \lambda_S + \sum \lambda_{DD} \lambda_{DU}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}}
\]

where \( \lambda \) is the failure rate, and the subscripts indicate the type of failures:

- **S**: Safe
- **DU**: Dangerous undetected
- **DD**: Dangerous detected

- Component classification (kind of complexity measure):
  - IEC 61508: Type A or type B
  - IEC 61511: PE logic solvers or non-PE logic solvers/IE/FE
Step 2: Find the required HFT in tables

The next step is then to determine the required HFT of each subsystem:

(i) Specified SIL?
(ii) Type A or B?
(iii) SFF?

Look up in HFT tables

<table>
<thead>
<tr>
<th>IEC 61508</th>
<th>Type A</th>
<th>Type B</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFF/HFT</td>
<td>0 1 2</td>
<td>0 1 2</td>
</tr>
<tr>
<td>&lt;60%</td>
<td>SIL1</td>
<td>SIL2</td>
</tr>
<tr>
<td>60-90%</td>
<td>SIL2</td>
<td>SIL3</td>
</tr>
<tr>
<td>90-99%</td>
<td>SIL3</td>
<td>SIL4</td>
</tr>
<tr>
<td>&gt;99%</td>
<td>SIL3</td>
<td>SIL4</td>
</tr>
</tbody>
</table>
Why do we need the AC?

Because we do not always believe that our prediction of reliability is good enough...

- AC have been introduced to achieve a sufficiently robust architecture, taking into account the level of subsystem complexity. See IEC 61508-2 (2000), NOTE 1 to 7.4.3.1.1

- In design, select a SIS design so that the predicted reliability complies with the desired reliability (i.e. SIL requirement)

- In the operation phase, plant specific data may be collected and used to estimate the actual reliability

- We would like to see the actual reliability according to the expectations from design.

- However, there are several reasons to why the predicted reliability may differ from the actual...
Predicted reliability versus actual

Overview
SIS
Need for standards
IEC standards
Key concepts
Life cycle phases
Safety integrity
Hardware
Systematic
Software
Discussion topics
Predicted reliability versus actual

*) See paper by Hauge, S. and Lundteigen, M.A. titled “A new approach for follow-up of safety instrumented systems in the oil and gas industry”, presented at the ESREL 2008 conference

**) Field data that is used to update generic data in e.g., OREDA data handbook
Our preliminary conclusions may be that...

- There are situations where we may expect the predicted reliability to be different from the actual reliability (for example, due to systematic failures).

- Under such circumstances, we may claim that some extra fault tolerance is needed.

- So having a sort of architectural constraints may be necessary...
The AC are being questioned!

- Many vendors and system integrators question the necessity of the architectural constraints, and, in particular, the suitability of the SFF.

- They find it sometimes hard to accept that even if the SIF meets the SIL target, there are additional requirements that enforce more hardware and higher costs.

- The HFT-SIL-SFF relationship is not theoretically founded, so we are not obligated to use the SFF.
Systematic safety requirements

- Some systematic requirements are “SIL independent” and some are “SIL dependent”

- Key issues are avoidance and control, see e.g.,

  ➤ IEC 61508-2 - appendix A.3:
    - Control failures caused by hardware and software design errors
    - Control failures caused by environmental stress and influences
    - Control failures during operation

  ➤ IEC 61508-2 - appendix B:
    - Avoid mistakes during SIS design
Software safety requirements

As with systematic safety integrity:

➤ Some systematic requirements are “SIL independent” and some are “SIL dependent”

➤ Key issues are avoidance and control

➤ Requirements address application software as well as the development platform

➤ The IEC 61511 may be used for certain software developments (conditions given in the standard)
Discussion topics
Discussion topics

- Redundancy may often lead to more spurious trips. On the other hand, more redundancy may improve the PFD. How should we treat this issue? What aspects are of importance?

- Systematic failures are not quantified. At the same time, we include CCFs. Their failure causes are often similar. What is the difference between systematic failures and CCFs?

- A SIL requirement is specified for each SIF. Under what circumstances may the SIL requirement become invalid?

- What are the (main) concerns for not quantifying the contribution from systematic failures and software failures when we calculate the PFD?

- Other topics?