Safety Instrumented System
A Critical Barrier

Presented by:
Sujith Panikkar, CFSE
Contents

→ The Safety Instrumented System
→ A review of Chemical Industry Accidents
→ Evolution of Regulations and Standards
→ Preventing Accidents: Risk Reduction
→ Concept of risk reduction
→ Accidents and Causes: The Human Factor
→ Safety Instrumented Systems as a safety barrier
→ Design & Engineering SIS: IEC 61508/ 61511 & FSM
→ Operation & Maintenance
→ Safety Lifecycle expectation & expectations on users
The Safety Instrumented System
What is a Safety Instrumented System ???

A Safety Instrumented System is a system that provides an independent and predetermined emergency shutdown path in case a process runs out of control.

Safety System – “IPS”, “ESD”, “SGS” etc... = SIS
SIS: The need for Protection

EUC = Equipment Under Control

If something runs out of control a dangerous situation can arise ==> a demand for a protective action

Consequences
(how serious, how much money, how many injuries, how many fatalities)

Demand Rate
(frequency, how many times per how many year)
What has to be Protected?

Society
- People outside plant
- Inside plant

Environment

Plant owner

Assets

Off-spec production

Corporate image

Process

RISK
Chemical Industry Accidents - History
Some of the major ones...

- 1974: Flixborough
- 1976: Seveso
- 1984: Bhopal
- 1988: Piper Alpha

And many more...

- 2010: BP Gulf of Mexico

the Consequences...
Piper Alpha platform, July 1988
• 61 survivors, but many badly burnt
• 167 fatalities
• Piper Alpha was producing about 125,000 bpd in 1988
• Insured losses of over US$ 3.4 Billion
Evolution of Regulations and Standards
History of Functional Safety Standards

Accidents

- 1974 Flixborough (U.K.) Vapor cloud explosion
- 1976 Seveso (Italy) TCDD cloud
- 1984 Bhopal (India) MIC cloud (US company)
- 1989 Piper Alpha (U.K.) Oil platform fire

Law / rules

- 1982 Seveso directive EC
- 1984 CIMAH HSE U.K.
- 1992 PSM / PSA OHSA U.S.
- 1999 Seveso directive II EC

Standards

- 1989 DIN Germany
- 1996 ISA S84 U.S.
- 1999 IEC 61508
- 2003 IEC 61511
Preventing Accidents: Risk Reduction
**Def. Risk**

“Combination of the frequency of occurrence of harm and the severity of that harm”

(IEC 61508 / IEC 61511)

**Risk** = Impact \( \times \) Frequency

**Impact** = $$, Life, Environment
How to reduce the Risk?

- **Impact**
  - Low
  - Medium
  - Major

- **Frequency**
  - Low
  - Medium
  - High

**Unacceptable risks!**

**Acceptable risks!**
Risk Reduction

Hazard Rate

Risk without any Protection

Tolerable Risk, ALARP

Reduction

Consequence

DCS
Process risk

Required overall risk reduction

- Mechanical
  - relief valves
  - rupture disks
  - break pins

- Analysed Process Risk
  - e.g. 0.0001

- Initial process risk level (not tolerable)
  - e.g. 0.1

- Tolerable risk level
  - e.g. 0.001

- Residual risk level
  - e.g. 0.00001

- External (mitigation)
  - drain systems
  - fire walls
  - dykes
  - Fire and Gas system

- Design
  - piping classes
  - control systems
  - operational envelopes

- SIS (functional safety)
  - sensor(s)
  - logic solver
  - final element(s)

- SIS
  - sensor(s)
  - logic solver
  - final element(s)
Onion...Layer of Protection Analysis (LOPA)

- Community Emergency Response
- Plant Emergency Response
- Physical Protection (Bund wall)
- Automatic SIF (ESD&FGS)
- Critical Alarms and Manual Intervention
- Basic Controls (DCS)
- Process Design
Case Study: Reliability of Instrumentation:
BP AMOCO Texas City Refinery: Isomerization Unit Explosion, March 2005
BP AMOCO EXPLOSION MARCH ‘05

15 DEAD
100 INJURED
30 PUBLIC INJURED
8 IN CRITICAL CONDITION
The total cost of this incident for BP: over $US 2 Billion
Failure of Raffinate Splitter Level Instrumentation

- DCS Level High Alarm was ignored
- Independent Level switch connected to alarm system did not work

Source: Fatal Accident investigation Report:
Accidents and Causes: The Human Factor
Layers of protection

- Initiating event
- Deficiency in the protection
- Incident
Causes of Accidents

39.5% Human failures

34.5% Random reasons:
- wrong material, corrosion, etc.
- power loss
- negligent maintenance
- static electricity
- sabotage
- short circuit
- design

26% Equipment failures

Failure of SIS: 4%

source: TNO investigations of 216 accidents
Safety Instrumented Systems as a Safety Barrier
SIS Function in the Process

Human influence

- Unsafe Condition
- Safety Instrumented System (SIS) action
- Alarm Condition
- Operator takes action
- Normal Condition
- Process value

Time

- Mechanical safety level
- Trip level
- High alarm level
- High level
- Low level

Boom?
The position of SIS

Process

Sensor

Sensor

3 X

Valve

Valve

Logic Solver (ProSafe RS)

Control System

SCADA (Fast Tools)

Operator Interface

Annunciation

ESD panel

PAS (Centum CS 3000)

= Safety related
Design & Engineering SIS: IEC 61508/ 61511 & FSM
The IEC 61508 / 61511 Standard


IEC 61511: functional safety for the process industry = identical to ISA-84.00.01 (except for grandfather clause)
Overall planning

1. Concept
2. Overall scope definition
3. Hazard and risk analysis
4. Overall safety requirements
5. Safety requirements allocation
6. Overall operation & maintenance planning
7. Overall safety validation planning
8. Overall installation & commissioning planning
9. E/E/PE Safety system requirement specification
10. E/E/PE Safety system realization
11. Other risk reduction measures
12. Overall installation & commissioning
13. Overall safety validation
14. Overall operation, maintenance & repair
15. Overall modification & retrofit
16. Decommissioning or disposal

Source: IEC 61508-1 fig. 2
SIS: Analysis and Design phase
Hazard and Risk Analysis, SIL Allocation

1. Concept
2. Overall scope definition
3. Hazard and risk analysis
4. Overall safety requirements
5. Safety requirements allocation

9. E/E/PE
   Safety system requirement specification

10. E/E/PE
    Safety system realization

HAZOP Study
Identify Safety Functions
Allocate Safety Functions to IPLs

Safety Functions and SIL targets for SIS

source: IEC 61508-1 fig. 2

IEC 61508: part 5
- ALARP
- Risk Graph
- Risk Matrix

IEC 61511: part 3
- FTA: Fault Tree Analysis
- LOPA: Layers Of Protection Analysis
SIS: Realization Phase
Three basic requirements have to be fulfilled in order to claim any SIL:

1. Hardware fault tolerance for the claimed SIL to be justified.

2. $\text{PFD}_{\text{AVG}}$ (of all elements within a SIF) shall be within the claimed SIL bandwidth

3. Systematic Capability shall comply with the requirements for the claimed SIL
## Hardware Safety Integrity: SIL Classification & PFD

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Risk Reduction Factor (RRF)</th>
<th>Average Probability of failure on demand (PFD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>&gt; 10 000</td>
<td>≥ 10^{-5} to &lt; 10^{-4}</td>
</tr>
<tr>
<td>3</td>
<td>1 000 - 10 000</td>
<td>≥ 10^{-4} to &lt; 10^{-3}</td>
</tr>
<tr>
<td>2</td>
<td>100 - 1 000</td>
<td>≥ 10^{-3} to &lt; 10^{-2}</td>
</tr>
<tr>
<td>1</td>
<td>10 - 100</td>
<td>≥ 10^{-2} to &lt; 10^{-1}</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td>(No Safety Requirements)</td>
</tr>
</tbody>
</table>

For Low Demand rate (less than once per year)

IEC 61508-1, table 2
PFD : Probability of a Failure on Demand, derived from the safety parameters of the equipment.

\[ PFD = 1 - e^{-\lambda_D u \cdot t} \]

\[ \text{PFD}_{\text{AVG}} = \frac{1}{T_L} \int_0^{T_L} \text{PFD}(t) \, dt \]

\( T_L \) = life time

\[ \text{PFD} = \lambda_D u \times t \]

\[ \text{PFD}_{\text{AVG}} = \frac{1}{2} \times \lambda_D u \times T_L \]
Hardware Safety Integrity: Average PFD for SIF

Pipe to pipe

SIL → $PFD_{\text{avg (target)}}$ for the SIF

$PFD_{\text{avg (SIF)}} = PFD_{\text{avg (sensors)}} + PFD_{\text{avg (logic solver)}} + PFD_{\text{avg (final elements)}}$
Hardware fault tolerance

- The target SIL indicates the maximum PFDAVG but also depending on type and quality of the used device double / triple voting devices (1oo2, 1oo3) might be required

Guidance: tables in both standards
Fault tolerance acc. IEC 61508-2

Table 2 — Hardware safety integrity: architectural constraints on type A safety-related subsystems

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance (see note 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 60 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>60 % - &lt; 90 %</td>
<td>SIL2</td>
</tr>
<tr>
<td>90 % - &lt; 99 %</td>
<td>SIL3</td>
</tr>
<tr>
<td>&gt; 99 %</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.
NOTE 2 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.
NOTE 3 See annex C for details of how to calculate safe failure fraction.

Type A: simple devices where the failure modes can easily be understood (mechanical devices, simple electronic devices like zener barrier, isolator etc.)

Table 3 — Hardware safety integrity: architectural constraints on type B safety-related subsystems

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance (see note 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 60 %</td>
<td>not allowed</td>
</tr>
<tr>
<td>60 % - &lt; 90 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>90 % - &lt; 99 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>&gt; 99 %</td>
<td>SIL1</td>
</tr>
</tbody>
</table>

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.
NOTE 2 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.
NOTE 3 See annex C for details of how to calculate safe failure fraction.

Type B: everything that is not simple, not type A.
Logic Solver: Fault Tolerant Architecture

1oo1D architecture

Other popular Architectures include:

- 1oo2D
- 2oo3
- VMR 1oo1D
Single SIL3 with high SFF

Redundant configuration for High Availability
Systematic Safety Integrity

Measures to avoid systematic failures

- Employment of safety competent personnel
- Controlled realization
- Verification processes
- Configuration management
- Document control (including software)
- Functional Safety Assessment
- Validation processes
- Controlled operation, proof testing and maintenance
- Controlled site modifications

Functional Safety Management System as per IEC 61508/ 61511

Responsibility of: End-user, Contractor, SIS equipment suppliers/ integrators
Topic

SIS: Operation and Maintenance phase
- Proof Testing
- Management of Change
A proof test means a complete test of the SIF, “pipe to pipe”.

The purpose of the test is to reveal all “dangerous undetected” failures that are present in the SIF

After the proof test the elements in the SIF should be in their initial state

Proof Test Coverage: The proof test of the system does not completely restore the initial state due to:
- Imperfect testing
- Imperfect repair
- Ageing
Impact of Proof testing on $PFD_{AVG}$

Without proof test $\Rightarrow$ $PFD = 1 - e^{-\lambda_{Du} t}$  
Or approximated as, $PFD = \lambda_{Du} t$  
and  
$PFD_{AVG} = \frac{1}{2} \lambda_{Du} T_L$

With proof test $\Rightarrow$ $PFD_{AVG} = \frac{1}{2} PC \times \lambda_{Du} T + \frac{1}{2} (1 - PC) \times \lambda_{Du} T_L$

Part of $\lambda_{Du}$ that is not detected by proof test

---

**SIL 1**

**SIL 2**

**SIL 3**
Prior to modifying the SIS functions on a running installation, a hazard and risk analysis needs to be carried out >> Management of Change procedure
Who should have a documented and auditable functional safety management system?

- Users/Plant owners
- Engineering Company
- SIL and integrated solutions
- System Integrators & Device Manufacturers
Functional Safety Management System in accordance with IEC 61508/61511
Thanks For Your Kind Attention!