Safety Systems 101
Understanding Safety Instrumented Systems

Bob Stahl
Today’s Topics

• Functional Safety
• Safety Instrumented Systems
• Safety Instrumented Functions
• Layers of Protection Analysis
• Safety Integrity Level
• Risk Reduction Factor
What is Safety?

• Freedom from **unacceptable risk** of physical injury or of damage to the health of people either directly or indirectly as a result of damage to property or the environment
Functional Safety

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

• Functional Safety relies on active systems
Functional Safety Standards

- IEC 61508 is a standard written with an intent to help design and develop products which are SIL rated for any industry.

- IEC 61511 and ISA84.01 are almost identical standards which have been written to help analyze, design, realize, install, commission and maintain SIL loops for the process industry.
Which Standard to Use?

Safety Instrumented Systems
Users of Standards

IEC 61508

SIS Devices

Design and manufacture of:
- Safety PLCs hardware
- Embedded software
- Sensors and actuators

SIS Applications

- Process plant design teams
- Instrument engineers
- Process control systems designers
- System Integrators
- Operating companies
- Regulatory inspectors
- Process safety managers

IEC 61511
What is a Safety Instrumented System?

• An SIS is composed of any combination of
  - Sensors
  - Logic Solvers
  - Final Elements
What an SIS Does

Automatic Shutdown Action by the SIS

Mechanical Shutdown Action

Trip Level

Operator Action

High Alarm Level

High Level

Low Level

process value

Time

Boom!
Types of SIS

- Safety Related Systems
- Safety Interlocks
- Emergency Shutdown Systems (ESD)
- Fire & Gas Systems (F&G)
- Instrumented Protective Systems (IPS)
- Burner Management Systems (BMS)
- High Integrity Pressure Protection System (HIPPS)
Layers of Protection

- **MITIGATION**
  - Mechanical Mitigation Systems
  - Safety Instrumented Control Systems
  - Safety Instrumented Mitigation Systems

- **PREVENTION**
  - Mechanical Protection System
  - Process Alarms
  - Operator Supervision
  - Safety Instrumented Control Systems
  - Safety Instrumented Prevention Systems
  - Basic Process Control Systems
  - Monitoring Systems (process alarms)
  - Operator Supervision

- **COMMUNITY EMERGENCY RESPONSE**

- **PLANT EMERGENCY RESPONSE**

IEC 61511 LOPA Model

- **Safety Layer(s)**
  - **Mitigation:**
    - Fire and Gas Safety system
  - **Prevention:**
    - ESD Safety system
What is a SIF?

- Stands for Safety Instrumented Function
  - Sensor
  - Logic Solver
  - Final Element
SIS Consists of Multiple SIFs

Safety Instrumented System
What is SIL?

• Stands for Safety Integrity Level
• Quantifiable measurement of risk
• SIL applies only to a SIF
• IEC 61508 standard specifies 4 levels
Objectives of SIL Analysis

- Protection of Equipment
- Personnel Safety
- Profit
- Environmental Safety
- Protection from Litigation
BPCS and ESD (SIS) Separated Solution

Honeywell Field Products
Risk is defined as the combination of the frequency of occurrence of harm and the severity of that harm.

![Risk Diagram]

- **FREQUENCY**
- **SEVERITY**

**ACCEPTABLE RISK**

**UNACCEPTABLE RISK**
### Risk Based on Frequency & Severity of Consequences

<table>
<thead>
<tr>
<th>Severity</th>
<th>Frequency</th>
<th>Safety Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plane crash – 200 deaths</td>
<td>Once in 20 million flights globally per year, i.e. $5 \times 10^{-8}$</td>
<td>1 x $10^{-5}$ LOWER</td>
</tr>
<tr>
<td>Car crash – 2 deaths</td>
<td>1 times in 1000 road incidents per year in a large city, i.e. $1 \times 10^{-3}$</td>
<td>2 x $10^{-3}$ HIGHER</td>
</tr>
</tbody>
</table>
Hazard and Operability Study (HAZOP)

• Assesses the risk associated with a hazard
• Identifies and evaluates problems with a process
  - Risks to personnel or equipment
  - Potential operability problems
  - Potential deviations from design intent
  - Examines possible causes of deviations and assessment of consequences
• Qualitative technique
• IEC 61882 Hazard and Operability Studies (HAZOP) – Application Guide
Layers of Protection Analysis (LOPA)

- Widely used risk assessment technique
- Can be viewed as an extension of HAZOP
- Semi-quantitative risk analysis tool
- Determines required Risk Reduction Factor
From the HAZOP risk matrix for this application:

1. Risk = Frequency x Severity
2. Per the indicated Risk matrix:

Present Risk “H1” = 1 (1 Serious injury in 1 year)

Acceptable Risk “L” = .001 (1 Serious injury in 1,000 years)

Risk Reduction Factor (RRF) = 1/.001 = 1000
Risk and Risk Reduction

**Target Risk:**
1 serious injury per 1,000y

**Present Risk:**
1 serious injury per year

- Residual risk
- Acceptable risk
- EUC risk

**TOTAL Required RRF=1,000**

- Necessary risk reduction
  - Actual risk reduction
    - Partial risk covered by other technology safety-related systems
    - Partial risk covered by E/E/PE safety-related systems
    - Partial risk covered by external risk reduction facilities

- Risk reduction achieved by all safety-related systems and external risk reduction facilities
## Safety Integrity Levels

<table>
<thead>
<tr>
<th>PFD&lt;sub&gt;avg&lt;/sub&gt;</th>
<th>R in %</th>
<th>RRF</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0001</td>
<td>99.99</td>
<td>10,000</td>
<td>4</td>
</tr>
<tr>
<td>0.001</td>
<td>99.9</td>
<td>1,000</td>
<td>3</td>
</tr>
<tr>
<td>0.01</td>
<td>99</td>
<td>100</td>
<td>2</td>
</tr>
<tr>
<td>0.1</td>
<td>90</td>
<td>10</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Probability of Failure on Demand**
- **Reliability of Safety Functions**
- **Risk Reduction Factor**

**Standards**
- ISA S84.01
- IEC 61508
Standards Compliance

- Target SIL must be specified for each SIF based on hazard and risk analysis

- Processes for SIS throughout lifecycle must comply

- Each SIF must meet target SIL requirements for:
  - Random failure rate (PFD_{avg})
  - Architectural constraints
  - Development process for each component
SIL Verification Calculation Example

\[
PFD_{\text{avg}} (\text{SIF}) = PFD_{\text{avg}}(\text{sensor}) + PFD_{\text{avg}} (\text{logic solver}) + PFD_{\text{avg}} (\text{final element})
\]

Example \(PFD_{\text{avg}} (\text{SIF}) = 0.0555 \text{ (SIL 1)}\)

\[0.005 \text{ (SIL 2)} + 0.0005 \text{ (SIL 3)} + 0.05 \text{ (SIL 1)}\]
\[ PFD_{avg} (SIF) = PFD_{avg} \text{(sensor)} + PFD_{avg} \text{(logic solver)} + PFD_{avg} \text{(final elements)} \]

Example \( PFD_{avg} \text{(SIF)} = 0.008 \text{ (SIL 2)} \)

\[
0.005 \text{ (SIL 2)} + 0.0005 \text{ (SIL 3)} + 0.0025 \text{ (SIL 2)}
\]
Questions?