Functional Safety Processes and SIL Requirements

Jordi Campos
TÜv Süd Process Safety
Business Manager
Jordi.campos@tuev-sued.es
Terminology

- Safety Instrumented Systems (SIS)
- Safety Integrity Level (SIL)
- Critical Control Systems
- Safety Shutdown Systems (SSD)
- Protective Instrumented Systems
- Equipment Protection Systems
- Emergency Shutdown Systems (ESS)
- Safety Critical Systems
- Interlocks
A Safety Instrumented System (SIS) is a form of process control that performs specified functions to achieve or maintain a safe state of the process when unacceptable or dangerous process conditions are detected. Safety instrumented systems are separate and independent from regular control systems but are composed of similar elements, including sensors, logic solvers, actuators and support systems.

Safety Integrity Level (SIL) is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a Safety Instrumented System.
SIS is designed to:

- respond to conditions in the plant which may be hazardous in themselves or,

- if no action was taken, could eventually give rise to a hazard, and

- to respond to these conditions by taking defined actions that either prevent the hazard or mitigate the hazard consequences.

Input ---- Logic Solver ---- Output
What is functional.....**Safety**?

**Safety**...

Something is safe when the residual risk is accepted.

**Today, do not use the elevator if you can.**

(You can be locked)
What is functional.....Safety?

**Functional**

when safety depends on a system or equipment operating correctly in response to its inputs is called functional safety.

Temperature Sensor?

- ✓

Thermal isolator?

- ❌

Residual risk?
**Functional Safety** must be considered in relation to the whole system and measures defining the concept of overall security.

![Risk Level Diagram]

- **Initial Risk:** not acceptable
- **Final Risk:** acceptable
- **Residual Risk**

...no functional

...functional
Examples of Safety Instrumented Systems

• High fuel gas pressure furnace initiates shutdown of main fuel gas valves.
• High reactor temperature initiates fail open action of coolant valve.
• High column pressure initiates fail open action of pressure vent valve.
Regulations & Standards

OSHA & EPA
Process Safety Management

Emergency Shutdown Systems, Control, Relief Systems

Written Internal Guidelines
Mentor/Engineering Practices
Industry Codes & Standards

GOOD ENGINEERING PRACTICE
Standards and guidelines must be integrated with SIS standards!

- ISA, Instrumentation Systems and Automation Society
- IEC, International Electrotechnical Commission

NFPA

ISA 84.01-2003

IEC 61508

ASME

IEC 61511

Boiler Codes

ISO

AICHE Books

API

Books
Safety Instrumented System Standards

**IEC 61508** - “Functional Safety: Safety Related Systems”
Functional safety of electrical/electronic/programmable electronic safety-related systems


**ISA 84.01-2003** - “Functional Safety: Safety Instrumented Systems for the Process Industry Sector”
Identical to IEC 61511 with inclusion of grandfather clause
To be published October 2003
Safety Lifecycle

Planning

Front End Engineering

Management of Change

Operations & Maintenance

Commissioning

Engineering Design
1. Inherent process safety, e.g. non-hazardous substances, low energy content/supply (m, p, T, ...)

2. Preventive measures, e.g.
   - avoidance of ignition sources (mechanical/electrical sparks, hot surfaces, electrostatic discharges etc.)
   - inertization

3. Mitigation systems, e.g.
   - pressure/pressure-shock resistant construction, pressure relief valves, rupture disks, detection systems etc.

4. Plant Emergency Response, e.g. sprinklers, internal fire brigade etc.
Basic Rules to Define SIS-SIL

• Risk Analysis
• Classification
  – Basic Process Control Systems
  – Process Monitoring Systems
  – Safety Instrumented Systems
  – (Safety Instrumented) Mitigation Systems
• Defining Requirements
  – Risk Graph $\rightarrow$ SIL
Preparing a Risk Analysis

• Scope Definition
  – very important in view of the results expected
  – by or in discussion with the requester
  – time available and depth required
Preparing a Risk Analysis

- **Team Formation**
  - establish a team comprising as much knowledge and experience as possible
  - not more than 6-8 persons
  - no “incompatible” persons
  - persons that are available for the planned meetings
Preparing a Risk Analysis

Tasks

- Team Leader
  - The Team Leader is not the person knowing most about the subject but the one knowing most about the method

- organisation and administration
  (collect information, organize meeting rooms, writing the protocol)

- stimulate the team (foster imagination)

- keeping pace

- focus discussion

- moderate disputes

- ensure “equal rights” to all team members

- report to requester
Preparing a Risk Analysis

- Collecting Information
  - P & I Schemes
  - Operating Procedures
  - Maps
  - Material Data (e.g. MSDS)
  - Standards and Guidelines
  - Legislation

- Do it before the Meeting!
Preparing a Risk Analysis

- **Look at Reality**
  - Whenever possible visit the area, pant installation which is subject to your study
Hazard Identification

- **Hazard Identification**
- **The Most important step!**
- **Source:**
  - knowledge, experience and imagination of the team members
Hazard Identification

• How to ensure completeness?

• Do your best to
  • Leave room for free discussion
  • BUT
  • follow an underlying structure

There is no guarantee for real completeness!
Risk Analysis Methodologies

- HAZOP
- FMEA
- FTA
- ZHA
- HAZID
- ...

When the only tool you have is a hammer, all the problems will look like nails.

- Abraham Maslow -
Basic Rules to Define SIS-SIL

• Risk Analysis
• Classification
  – Basic Process Control Systems
  – Process Monitoring Systems
  – Safety Instrumented Systems
  – (Safety Instrumented) Mitigation Systems
• Defining Requirements
  – Risk Graph $\rightarrow$ SIL
Consider the whole system

- Sensor
- Transmitter
- Logic Unit
- Switch
Design architecture of an SIS

- Sensor
  - (Transducer)
    - e.g. 4-20 mA

- Signal processing
  - Logic Solver

- Initiators
  - local
  - Final elements
    - Electrical switch room
    - Control room, field
Structure 1oo1 (1-out-of-1 system)

1 unit of 1 available is required for the operation

Structure 1oo2 (1-out-of-2 system)

1 unit of 2 available is required for the operation
**Designs**

**Single-channel design**
1 unit alone

**Redundant, two-channel design**
2 units – same type

**Completely redundant design**
2 units - different
(avoid systematic failure)

Two different technologies.
## Architecture and fault tolerance

<table>
<thead>
<tr>
<th>Integrity Levels</th>
<th>Minimum Fault tolerance</th>
<th>Typical Architecture</th>
<th>Minimum Fault tolerance</th>
<th>Typical Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 1</td>
<td>0</td>
<td>Single, 1oo1</td>
<td>0</td>
<td>Single, 1oo1</td>
</tr>
<tr>
<td>SIL 2</td>
<td>0</td>
<td>Single, 1oo1</td>
<td>1</td>
<td>1oo2 or 2oo3</td>
</tr>
<tr>
<td>SIL 3</td>
<td>1</td>
<td>1oo2 or 2oo3</td>
<td>2</td>
<td>1oo3</td>
</tr>
<tr>
<td>SIL 4</td>
<td>(2) not covered by SIS only</td>
<td>(1oo3) not covered by SIS only</td>
<td>Special requirements apply, see IEC 61508; not covered by SIS only</td>
<td></td>
</tr>
</tbody>
</table>
## SIS Requirements – Process Industry

<table>
<thead>
<tr>
<th>SIL</th>
<th>Requirements</th>
<th>Percentage</th>
</tr>
</thead>
</table>
| 7-8   | SIL4  
- Change of the process is required  
- Can not be covered by SIS only.  
- Primary protection measures (non-instrumentation based, “passive”) are necessary. | 0%         |
| 5-6   | SIL3  
**SIS:**  
- Redundancy 1oo2 for sensors and final elements, if necessary relying on different technologies  
- Logic solvers single + self-monitoring or 1oo2 redundancy  
- Regular proof single (<= 1 year, depending on conditions of use of the SIS)  
- Extensive information requirements (documentation) | <0.5%      |
| 4     | SIL2  
**SIS:**  
- Single-channel design  
(sensor/transducer/signal processing/actors)  
- Partial redundancy under conditions of increased severity  
- Automatic function monitoring if necessary  
- Regular proof tests (<= 1 year, depending on conditions of use of the SIS)  
- Extensive information requirements (documentation) | 1.5-2%     |
| 2-3   | SIL1  
- No special safety requirements  
- No safety system requirement (basic process control system) | 98%        |
### SIS Requirements – Demand Mode

#### Low demand: hazard event less than 1 per year

<table>
<thead>
<tr>
<th>SIL</th>
<th>PFD (probability of failure on demand)</th>
<th>Maximum failures acceptables</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 1</td>
<td>$\geq 10^{-2} a &lt; 10^{-1}$</td>
<td>1 hazardous failure in 10 years</td>
</tr>
<tr>
<td>SIL 2</td>
<td>$\geq 10^{-3} a &lt; 10^{-2}$</td>
<td>1 hazardous failure in 100 years</td>
</tr>
<tr>
<td>SIL 3</td>
<td>$\geq 10^{-4} a &lt; 10^{-3}$</td>
<td>1 hazardous failure in 1.000 years</td>
</tr>
<tr>
<td>SIL 4</td>
<td>$\geq 10^{-5} a &lt; 10^{-4}$</td>
<td>1 hazardous failure in 10.000 years</td>
</tr>
</tbody>
</table>

#### High demand: hazard event more than 1 per year

<table>
<thead>
<tr>
<th>SIL</th>
<th>PFH (Probability of failure per hour)</th>
<th>Maximum failures acceptables</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 1</td>
<td>$\geq 10^{-6} a &lt; 10^{-5}$</td>
<td>1 hazardous failure in 100.000 years</td>
</tr>
<tr>
<td>SIL 2</td>
<td>$\geq 10^{-7} a &lt; 10^{-6}$</td>
<td>1 hazardous failure in 1.000.000 years</td>
</tr>
<tr>
<td>SIL 3</td>
<td>$\geq 10^{-8} a &lt; 10^{-7}$</td>
<td>1 hazardous failure in 10.000.000 years</td>
</tr>
<tr>
<td>SIL 4</td>
<td>$\geq 10^{-9} a &lt; 10^{-8}$</td>
<td>1 hazardous failure in 100.000.000 years</td>
</tr>
</tbody>
</table>
Basic Rules to Define SIS-SIL

- Risk Analysis
- Classification
  - Basic Process Control Systems
  - Process Monitoring Systems
  - Safety Instrumented Systems
  - (Safety Instrumented) Mitigation Systems
- Defining Requirements
  - Risk Graph → SIL
Basic Rules to Define SIS-SIL

- Risk Analysis
- Classification
  - Basic Process Control Systems
  - Process Monitoring Systems
  - Safety Instrumented Systems
  - (Safety Instrumented) Mitigation Systems

- Defining Requirements

Risk Graph → SIL

TÜV SÜD Process Safety Slide 32
Determining the requirements to impose on this SIS

What reliability/integrity does this SIS need?

This question has to be answered by a risk assessment:
“What may happen if the SIS fails?”

The result of this risk assessment determines the respective integrity level.

Minimum technical and organizational measures are required in order to achieve the required integrity level.
1. Risk assessment
Risk classification according to IEC 61511 (Draft)

<table>
<thead>
<tr>
<th>W3</th>
<th>W2</th>
<th>W1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>6</td>
</tr>
</tbody>
</table>

- **DIN V 19250**: No safety system requirements
- **IEC61511**: No special safety requirements
- **VDI/VDE 2180**: Risk area I (low risk)
- **SIL 1**
- **SIL 2** (low risk)
- **SIL 3** (high risk)
- **SIL 4**: An SIS is not sufficient
- **SIL 4**: Cannot be covered by SIS only

**Risk Area I**
- C1
- C2
- C3
- C4

**Risk Area II**
- C1
- C2
- C3
- C4

**Risk Area III**
- C1
- C2
- C3
- C4

**Risk Area IV**
- C1
- C2
- C3
- C4
Risk graph method for risk analysis on safety instrumented systems

• Parameters for risk classification

The risk is proportional to the consequence and the probability of the hazardous event. The probability of the hazardous event is, in turn, a function of three parameters. Consequently, the risk graph method uses the following four parameters to describe the nature of the hazardous situation when safety instrumented systems fail or are not available:

– consequence of the hazardous event (C)
– frequency of, and exposure time in, the hazardous zone (F);
– possibility of failure to avoid the hazardous event (P);
– probability of the unwanted occurrence (W)
Classification of parameters

Consequence of the hazardous event (C):

- **C1**: Slight injury to persons or minor effects on the environment.
- **C2**: Serious permanent injury to one or more persons; death of one person or reversible major effects on the environment.
- **C3**: Death of several persons or long-term major effects on the environment.
- **C4**: Catastrophic effect, very many people killed.
Classification of parameters

**Frequency of, and exposure time in, the hazardous zone (F):**

- **F1:** Rare to fairly frequent exposure of the subject in the hazardous zone.
- **F2:** Frequent to permanent exposure of the subject in the hazardous zone.
Classification of parameters

Possibility of avoiding the hazardous event (P):

- P1: Possible under certain conditions.
- P2: Almost impossible.
Classification of parameters

Probability of the unwanted occurrence without the inclusion of an SIS (W):

- **W1**: A very slight probability that the unwanted occurrences will actually happen; very few unwanted occurrences are likely.
- **W2**: A slight probability that the unwanted occurrences will actually happen; few unwanted occurrences are likely.
- **W3**: A relatively high probability that the unwanted occurrences will actually happen; frequent unwanted occurrences are likely.
Risk classification according to IEC 61511

Risk area I (low risk)

- DIN V 19250: W3 = 1, W2 = - , W1 = -
- IEC61511: SIL 1
- VDI/VDE 2180: No safety system requirements

Risk area II (high risk)

- DIN V 19250: W3 = 5, W2 = 6, W1 = 7
- IEC61511: SIL 3
- VDI/VDE 2180: Cannot be covered by SIS only

SIL 1
- Risk area I (low risk)

SIL 2
- Risk area II (high risk)

SIL 3
- Risk area II (high risk)

SIL 4
- An SIS is not sufficient
Basic Rules to Define SIS-SIL

Key Take Away

• Risk Analysis
• Classification
  – Basic Process Control Systems
  – Process Monitoring Systems
  – Safety Instrumented Systems
  – (Safety Instrumented) Mitigation Systems
• Defining Requirements
  – Risk Graph → SIL
Functional Safety Processes and SIL Requirements

Jordi Campos
TÜv Süd Process Safety
Business Manager
Jordi.campos@tuev-sued.es