Disclaimer: Examples of risk reduction factors, targets, etc. are simplified and for illustration only. These do not represent recommendations or actual procedures. Individual companies need to determine and adopt a complete system of factors and targets along with boundary conditions and assumptions for use.
Itinerary for SIS 0101

• Safe Process
• Terminology
• Safety System Overview
• Engineering Considerations
• Application
• Closing
Safe Process
Many aspects of safe process design.

Core design contains and limits potential hazards. Inner protection layers are scenario specific. Outer layers need to respond to more general risks.
A Means to Reduce Risk

Risk = Function (severity \textit{[without safeguards]}, frequency)
A Means to Reduce Risk

Safe Process

Protection Layer 1
Protection Layer 2
Protection Layer X

Lower FREQUENCY Lower RISK
Safe Process Test

1. T/F In a properly designed process a relief valve should usually activate before an automatic shutdown.

2. Risk is a function of (pick 2):
   A. Severity
   B. Frequency
   C. Likelihood of being fired
   D. Loss of production

3. T/F We can reduce the likelihood of a hazardous event by adding layers of protection.
Terminology
Basic Definitions – Instrumented Systems

- A Safety Instrumented System (SIS) is all the sensors, logic solver and final elements for all the safety Loops “SIF’s” combined together.

- A Safety Instrumented Function (SIF) is a single set of actions within a SIS, for a specific hazard, taken to bring the process or equipment to a safe state, following detectable abnormal operating conditions.

- SIF components have an estimated Probability of Failure on Demand (PFD). The PFD values are combined to determine if the SIF meets the required Safety Integrity Level.
Basic Definitions – Instrumented Systems

- **SIL** – Safety Integrity Level is defined as the performance criteria for a SIF defining the probability of the SIF failing to perform its function on demand.
  - Each SIF has its own SIL rating.
  - Higher SIL rating is less likely to fail when needed.

<table>
<thead>
<tr>
<th>Safety Integrity Level (SIL)</th>
<th>Average Probability of Failure on Demand (PFD)</th>
<th>Availability (%)</th>
<th>Corresponding Risk Reduction Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL-4</td>
<td>$10^{-4}$ to $10^{-5}$</td>
<td>99.99 - 99.999</td>
<td>4</td>
</tr>
<tr>
<td>SIL-3</td>
<td>$10^{-3}$ to $10^{-4}$</td>
<td>99.9 - 99.99</td>
<td>3</td>
</tr>
<tr>
<td>SIL-2</td>
<td>$10^{-2}$ to $10^{-3}$</td>
<td>99 - 99.9</td>
<td>2</td>
</tr>
<tr>
<td>SIL-1</td>
<td>$10^{-1}$ to $10^{-2}$</td>
<td>90 - 99</td>
<td>1</td>
</tr>
</tbody>
</table>

- **BPCS** – Basic Process Control System such as a DCS
Basic Definitions – Hazard and Risk Analysis

- HAZOP – Hazard and Operability study. A small team with knowledge of the process identifies potential credible hazards and safeguards.
- LOPA – Layer Of Protection Analysis. Often follows HAZOP; a small team applies rules of independence and applicability to safeguards. Used to define the SIS requirements.
- H&RA – Hazard and Risk Analysis is a general term for the combination of HAZOP and LOPA, or other similar analysis, used to define the required performance the SIS.
Basic Definitions – Hazard and Risk Analysis

- **Risk** – An organization’s assessment of potential consequence severity and frequency. Not directly comparable across organizations due to differences in assessment methods and detailed definitions.

- **PL** – Protection Layer is any process plant feature or operational procedure that is separate from a scenario’s initiating cause and may serve to prevent the initiating cause from causing a hazardous event.

- **IPL** – Independent Protection Layer is a protection layer that meets standards of independence and effectiveness sufficient to credit it with a frequency reduction in a quantitative analysis.

  - Required Attributes:
    - Independence
    - Functionality
    - Integrity
    - Reliability
    - Auditability
    - Access Security
    - Management of Change
A safety system is not just a PLC even if TUV rated for the application.
- SIL rating of the PLC does not apply to the entire system, but to each individual safety function.
- A common mistake is for people to say they have a SIL 2 PLC or a SIL 2 transmitter and figure they have a SIL 2 SIF.
Every SIF has its own SIL rating

Diagram of Process Plant type installation
Terminology Test

1. T/F: Having a SIL3 rated PLC means you have a SIL 3 Safety Instrumented System.

2. SIL stand for:
   a. Safety Integrated Level
   b. Safety Integrity Level
   c. Safety Integrated Layer
   d. Safety Instrumented Layer

3. T/F: A Safety Instrumented Function must be separate from the Initiating Event.
Safety System Overview
Regulations and Standards

- OSHA Federal Regulation 29 CFR 1910.119
- ANSI/ISA-84.00.01-2004 (IEC 61511-1 Mod)
  - Known as **ISA 84**
- Guidelines for Safe Automation of Chemical Processes, CCPS, AIChE.
- NFPA
- API
- Plus many others applicable codes and standards
Engineering Considerations
Key Engineering Considerations

- **Safety**
  - personnel safety
  - environmental impact

- **Reliability**
  - financial impact
    - loss of production
    - equipment damage
    - minimization of nuisance trips

- **Cost**
  - Design
  - Maintenance
  - Upgrades and scalability
Hazard and Risk Assessment

ISA 84 requires a “process hazard and risk assessment” (H&RA) be carried out to determine the safety functions / risk reduction requirements related to SIS.

Determines the required SIL rating for a SIF.

The H&RA documentation provides a linkage between SIF and specific scenarios they are designed to protect.
Hazard and Risk Assessment

- A Risk matrix shows a relationship between Severity and Frequency that may be acceptable to an organization.

- Severity is a prediction and Frequency is an estimate. These systems quantify decision making with respect to applying resources to improve safety.

- Part of an overall detailed H&RA procedure.

---

**Example Risk Table**

<table>
<thead>
<tr>
<th>Risk Tolerance Frequency (event per yr)</th>
<th>1x10^-2</th>
<th>1x10^-3</th>
<th>1x10^-4</th>
<th>1x10^-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence Category</td>
<td>I</td>
<td>II</td>
<td>III</td>
<td>IV</td>
</tr>
<tr>
<td>Personnel Safety</td>
<td>Minor Injuries, No serious injuries</td>
<td>Single serious injury or multiple minor injuries</td>
<td>Multiple serious injuries</td>
<td>One or more fatalities</td>
</tr>
<tr>
<td>Public Safety</td>
<td>No off-site health or safety consequences</td>
<td>No off-site health or safety consequence</td>
<td>Off-site injuries</td>
<td>Off-site fatality</td>
</tr>
<tr>
<td>Environmental</td>
<td>Reportable quantity released</td>
<td>Reversible, self correcting affect</td>
<td>Reversible impact to non sensitive area</td>
<td>Impact to sensitive area or extended cleanup required</td>
</tr>
<tr>
<td>Public Relations</td>
<td>None</td>
<td>Letters or calls of complaint from local public</td>
<td>Local news coverage, damage to public image</td>
<td>National new coverage or threat to right to continue operations</td>
</tr>
<tr>
<td>Business Impact</td>
<td>&lt;$100,000</td>
<td>$100,000 - $1,000,000</td>
<td>$1,000,000 - $10,000,000</td>
<td>&gt;$10,000,000</td>
</tr>
</tbody>
</table>
Hazard and Risk Assessment

Design H&RA Methods

- Risk Reduction Credits
- Event Tree
- LOPA Equations
- Others as defined and adopted by user companies

- LOPA Equations represent a process of comparing event tree results with user company risk tolerance requirements.

- LOPA is widely used in the process industries in the United States and is used in examples below.
Hazard and Risk Assessment

### LOPA Equation

LOPA Equation is satisfied when:

\[
\frac{\text{Tolerable Risk Frequency}}{\text{Consequence Frequency}} \leq 1.0
\]

\[
1.0 \leq \frac{f_i}{f_1 \times f_2 \times f_n}
\]

**Initiating Event**

<table>
<thead>
<tr>
<th>Initiating Event</th>
<th>IPL1</th>
<th>IPL2</th>
<th>IPL3</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated Frequecy</td>
<td>$f_i = x$</td>
<td>$f_1 = x \times y_1$</td>
<td>$f_1 = x \times y_1$</td>
<td>$PFD_1 = y_1$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Safe Outcome</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Safe Outcome</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Safe, but Undesired Outcome</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Consequence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f_3 = x \times y_1 \times y_2 \times y_3$</td>
</tr>
</tbody>
</table>
SIS Design Concepts

Basically, the SIL defines the level of availability required to bridge the gap between the allowable level of risk and the layers of protection designed in the process.

How do we know our system meets the SIL rating?

1. A detailed study of each device in the SIF loop must be analyzed to determine the average PFD for the entire loop.
2. Industry and vendor data is available for these devices but it’s up to the engineer to interpret the data and fashion these as a system in order to determine the overall average PFD.
   a. OREDA publications
   b. IEEE 500
   c. Vendor data (common source)
   d. Privately published compilations of data (common source)
   e. First hand (user) data in the process application (best source)
SIS Design Concepts

How do we know our system meets the SIL rating? Contd.

- The PFD number is required for the necessary SIL rating as shown in the table below.
- Remember, these include all transmitters, the logic solver (each individual piece) and the final safety elements like shutdown valves and solenoids. Some sample PFD data is shown below taken from some of the above reference sources.

\[ P_{avg} = P \left( \bigcup_{i=1}^{N} P_i \right) = \sum_{i=1}^{N} P \]

<table>
<thead>
<tr>
<th>Device (Generic)</th>
<th>Average PFD Data (Test interval once per year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Stop</td>
<td>8.90 \times 10^{-3}</td>
</tr>
<tr>
<td>Flow Switch</td>
<td>1.02 \times 10^{-2}</td>
</tr>
<tr>
<td>Pressure Transmitter</td>
<td>3.39 \times 10^{-1}</td>
</tr>
<tr>
<td>Safety PLC</td>
<td>Specific to Vendor</td>
</tr>
<tr>
<td>Solenoid</td>
<td>8.47 \times 10^{-1}</td>
</tr>
<tr>
<td>Butterfly Valve</td>
<td>1.69 \times 10^{-2}</td>
</tr>
</tbody>
</table>
The safety instrumented system lifecycle is illustrated in Figure 4.1. The relevant clauses from the industry-standard ANSI/ISA 84.00.01-2004/IEC 61511 are shown. The lifecycle begins with the process design and continues through decommissioning of the SIS.

Our focus today
Safety System Design Test

1. Things one might consider when designing a Safety Instrumented System are: (list all that apply)
   a. Cost
   b. Reliability
   c. Safety
   d. Are the fish biting

2. T/F: ISA 84 requires a “process hazard and risk assessment” (H&RA) be carried out to determine the safety functions / risk reduction requirements related to SIS.

3. T/F: To get reliability data to document my PFD numbers I must do years of extensive testing.
Application
Hazard Identification:
Safety & Health
Environmental
Process Safety
Consider scenario:
1. Consequence (Severity)
2. Causes
3. Safeguards

Determines:
1. Are designed safeguards sufficient to mitigate risk?
2. Are the layer independent?
3. Are additional layers required?
4. IPL Frequencies (PFD)

1. Select Instrumentation
2. Select Logic Solver
3. Select the detail installation requirements
4. Develop the SRS
5. Define the Test Interval

1. Develop Spec Sheets for Instrumentation
2. Develop Detail Drawing Package
3. Design interface to operator console

1. Install
2. Test
3. Train
4. Turnover to operations
5. Follow-up support
6. Upgrade or decommission at end of life.

Send Data to:
1. Mechanical Integrity and Maintenance Coordinator
2. Place data in the system used for tracking Action Items

SAFETY SYSTEM DESIGN LIFECYCLE
Event Tree (LOPA) Example

Risk = Function (severity \[without safeguards\], frequency)

PHA Team Determines:
1. Overpressure scenario could fail the tower Severity 4
2. Potential Cause of the overpressure is failed control loop
3. Safeguards are DCS Alarm and Relief Valve
Event Tree (LOPA) Example

Risk = Function (severity [without safeguards], frequency)

PHA Team Determines:
1. Overpressure scenario could cause leaks Severity 4
2. Potential Cause of the overpressure is failed control loop
3. Safeguards are DCS Alarm and Relief Valve

LOPA Team Determines:
1. Accepts overpressure could cause leaks (S4) 1E-4/yr target
Risk = Function (severity [without safeguards], frequency)

**PHA Team Determines:**
1. Overpressure scenario could cause leaks Severity 4
2. Potential Cause of the overpressure is failed control loop
3. Safeguards are DCS Alarm and Relief Valve

**LOPA Team Determines:**
1. Accepts overpressure could cause leaks (S4) 1E-4/yr target
2. Accepts the potential cause of the overpressure is failed control loop (BPCS Failure)
**Event Tree (LOPA) Example**

**Risk = Function (severity [without safeguards], frequency)**

**PHA Team Determines:**
1. Overpressure scenario could cause leaks Severity 4
2. Potential Cause of the overpressure is failed control loop
3. Safeguards are DCS Alarm and Relief Valve

**LOPA Team Determines:**
1. Accepts overpressure could cause leaks (S4) [1E-4/yr target]
2. Accepts the potential cause of the overpressure is failed control loop (BPCS Failure)
3. Determines as independent layers the safeguards are relief valve but **not** credit the DCS Alarm due to not being independent

---

**Event Tree (LOPA) Example**

```plaintext
Initiating Event | Existing Protection Layers | Required IPL | Consequence
-----------------|-----------------------------|--------------|-------------
BPCS Failure     | 90%                         | 10%          | Safe Outcome
Freq = 1E-1/yr   | 10%                         | 99.9%        | Safe Outcome
Relief Valve     | 0.1%                        | 0.1%         | Safe Outcome
PFD = 1E-2       |
```

---

**PHA**

**LOPA**

**SIL/GAP Analysis**

**Detailed Design**

**Construction Commissioning**

---

Honeywell Confidential - © 2017 by Honeywell International Inc. All rights reserved.
Risk = Function (severity [without safeguards], frequency)

PHA Team Determines:
1. Overpressure scenario could cause leaks Severity 4
2. Potential Cause of the overpressure is failed control loop
3. Safeguards are DCS Alarm and Relief Valve

LOPA Team Determines:
1. Accepts overpressure could cause leaks (S4) 1E-4/yr target
2. Accepts the potential cause of the overpressure is failed control loop (BPCS Failure)
3. Determines as independent layers the safeguards are relief valve but not credit the DCS Alarm due to not being independent
4. Determine the need for an additional IPL.
Event Tree (LOPA) Example

Risk = Function (severity [without safeguards], frequency)

PHA Team Determines:
1. Overpressure scenario could cause leaks Severity 4
2. Potential Cause of the overpressure is failed control loop
3. Safeguards are DCS Alarm and Relief Valve

LOPA Team Determines:
1. Accepts overpressure could cause leaks (S4) 1E-4/yr target
2. Accepts the potential cause of the overpressure is failed control loop (BPCS Failure)
3. Determines as independent layers the safeguards are relief valve but not credit the DCS Alarm due to not being independent
4. Determine the need for an additional IPL.
Safety Function Example

\[ \text{Risk} = \text{Function (severity [without safeguards], frequency)} \]

PHA Team Determines:
1. Overpressure scenario could cause leaks Severity 4
2. Potential Cause of the overpressure is failed control loop
3. Safeguards are DCS Alarm and Relief Valve

LOPA Team Determines:
1. Accepts overpressure could cause leaks (S4) 1E-4/yr target
2. Accepts the potential cause of the overpressure is failed control loop (BPCS Failure)
3. Determines as independent layers the safeguards are relief valve but not credit the DCS Alarm due to not being independent
4. Determine the need for an additional IPL

<table>
<thead>
<tr>
<th>SAFETY INTEGRITY LEVEL</th>
<th>Demand Mode of Operation</th>
<th>Average Probability of Failure on Demand (PFD)</th>
<th>Availability (%)</th>
<th>Corresponding Risk Reduction Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL-4</td>
<td>$10^{-4}$ to $10^{-3}$</td>
<td>99.99 - 99.999</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>SIL-3</td>
<td>$10^{-3}$ to $10^{-2}$</td>
<td>99.9 - 99.99</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>SIL-2</td>
<td>$10^{-2}$ to $10^{-1}$</td>
<td>99 - 99.9</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>SIL-1</td>
<td>$10^{-1}$ to 10^{-2}</td>
<td>90 - 99</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Safety Requirements Specification
Build and Commission the SIS

- The Logic Solver and field instrumentation must be installed per the SRS. If changes are found to be necessary for a particular SIF, the SRS and all associated documentation / SIL Calculations need to be updated to ensure the functional and availability requirements of the H&RA are still met.

- During the build process Factory Acceptance Testing (FAT) is carried out to ensure the SRS requirements are being adhered to.

- Construction and Commissioning

- SIS safety Validation, sometimes integrated with Site Acceptance Testing (SAT), is the final step to confirm that all components from input instruments to final elements (e.g. block valves). Work per the original intent.
Operate and Support the SIS

- The objective of the ISA 84 clause is: “To ensure the required SIL of each safety instrumented function is maintained during operation and maintenance.”

- SIF operation concerns include training operators in the function of SIF, including:
  - Manual activation.
  - Reset requirements.
  - Actions taken following demand on the system.
  - Training maintenance on how to sustain the full functional performance.
  - Controlling bypass of SIF in such a way that it is not done when risk mitigation is required or compensating measures are provided to substitute for the risk mitigation that is missing while the SIF is in bypass.

- Support concerns include training maintenance in actions which maintain the performance of the SIF including:
  - Proof Testing.
  - Bypass communication with Operations.
  - Allowable component replacements.
  - Post maintenance verification of function.
1. The Safety System design should begin with
   a. SIL Analysis
   b. Safety Manager Drawings
   c. HAZOP or PHA
   d. LOPA

2. T/F: All companies must have the same risk tolerances per ISA S84.

3. The Safety Requirement Specification (SRS) outlines the following:
   a. The Logic Solver
   b. Field Instrumentation
   c. Both A and B
   d. None of the above.
SIS is Engineered Risk Reduction

- A Safety Instrumented System is all the instrumentation together designed to bring the process into a safe state, without relying on mechanical or physical protective devices, following an upset or abnormal operating condition.

- Each SIF (Safety Loop) has an independent SIL rating. SIL rating does not apply to an entire system.

- SIL rating requirement is determined by a hazard and risk assessment.

- A balance of safety, reliability and cost all are considered during the engineering process of a safety instrumented system.

QUESTIONS?