Reducing the human error impact on Safety Instrumented system (SIS)

Purdue Process Safety & Assurance Center
December 5, 2019
Your presenter

• Siemens Director for Process Safety (I&C)
• ISA 84 voting member
• 25 years of Process Industry experience
• ISA course developer/instructor (BMS and SIS)
• Electrical Engineering (OSU)
• Descendent of Cyrus McCormick

Charles M. Fialkowski, CFSE
Charles.Fialkowski@siemens.com
Safety Instrumented System (SIS)

A system composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when pre-determined conditions are violated.

How much safety do we need? How do we design it? How do we keep it safe?
How much safety do we need? (Risk Reduction)

Risk inherent in the process

Tolerable Risk Level

SIS  Other  Alarms  BPCS

Process

Risk
**ANSI/ISA 61511**: Functional Safety:

Safety Instrumented Systems for the process industry sector, 2018

- 1996 - 1st edition of ISA 84
- 2004 - ISA 84 (IEC 61511 Mod)
- 2016 – 2nd edition of IEC 61511

Applied to ensure the functional safety requirements are met.

Addresses 2 concepts:

- SIS safety life-cycle
- Safety integrity levels (SILs).
### Safety Instrumented System Performance

What standards can we use to help with this?

Decide how much safety performance you need, and design to meet it

<table>
<thead>
<tr>
<th>Safety Integrity Level (SIL)</th>
<th>Probability of Failure on Demand (PFD)</th>
<th>Risk Reduction Factor (1/PFD)</th>
<th>Safety Availability (1-PFD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>(\geq 0.0001) to (&lt; 0.001)</td>
<td>(&gt; 10,000) to (\leq 100,000)</td>
<td>(&gt; 99.99) to (\leq 99.999)</td>
</tr>
<tr>
<td>3</td>
<td>(\geq 0.001) to (&lt; 0.01)</td>
<td>(&gt; 1,000) to (\leq 10,000)</td>
<td>(&gt; 99.9) to (\leq 99.99)</td>
</tr>
<tr>
<td>2</td>
<td>(\geq 0.01) to (&lt; 0.1)</td>
<td>(&gt; 100) to (\leq 1,000)</td>
<td>(&gt; 99) to (\leq 99.9)</td>
</tr>
<tr>
<td>1</td>
<td>(\geq 0.1) to (&lt; 1)</td>
<td>(&gt; 10) to (\leq 100)</td>
<td>(&gt; 90) to (\leq 99)</td>
</tr>
</tbody>
</table>
Control system failure – Root Causes

From ‘Out Of Control’
(A compilation of incidents involving control systems) by the United Kingdom Health and Safety Executive (UK HSE)
Safety Design Lifecycle (ANSI/ISA 61511, Clause 6)

**Analysis Phase**
- How much safety do you need?
  - Hazard and Risk Assessment
  - Allocation of Safety Protection Layers
  - Safety Requirements Specification (SRS)

**Realization Phase**
- How do you design it?
  - Design and Development of SIS
  - Installation, Commissioning and Validation

**Operational Phase**
- How do you keep it safe?
  - Operation and Maintenance
  - Modification
  - Decommission
Analysis Phase
How much safety do you need?

Hazard and Risk Assessment

Allocation of Safety Protection Layers

Safety Requirements Specification (SRS)

HAZOP

LOPA

SIF List

SRS
  Hazards
  IPLs
  SIFs
  SIL

Cause & Effect Diagram
Realization Phase
How do you design it?

Conceptual Design of SIS
(Select Architecture, SIL Verification)

Design and Development of Safety Instrumented System

Installation, Commissioning and Validation

SIL Verification Report

SRS
Hazards
IPLs
SIFs
SIL

C&E Matrix

Cause and Effect
(Engineering Tool)

(Online Engineering viewer)
Operational Phase
How do you keep it safe?

Operation and Maintenance

Modification

Decommission

SIS HMI Viewer

Operator Log
First Out
Sequence of Events

SIS Engineering Tool
Compare Reporting
Change Documentation

SIS Engineering Tool
Configuration Report

Unrestricted © Siemens AG 2018
Integrated safety lifecycle tool

✓ Documentation
✓ System Validation
✓ Design and Engineering
✓ Installation and Commissioning
✓ Operation and maintenance
✓ Modifications (MOC)
Minimize human errors
✓ Intuitive (Cause & Effect)
✓ Automated logic generation
✓ Common interface (engineering and HMI)
✓ Easy troubleshooting
Installation and commissioning

Integrated Documentation

✓ Validation Reports
✓ On-Line Changes
✓ Bypass Management
✓ First out identification
Operations and maintenance

HMI Visualization

- System diagnostics
- Alarm management
- MOC documentation
- Sequence of Events (SOE) reporting
- Maintenance override
Questions and Answers