Optimal Compliance with IEC-61511 Hardware Fault Tolerance Requirements
Photography and audio/video recording is not permitted in any sessions or in the exhibition areas without press credentials or written permission from the Emerson Exchange Board of Directors. Inquiries should be directed to:

EmersonExchange@Emerson.com

Thank you.
Presenters

- Nagappan Muthiah @ “Muthu”
- Justin Clem
Introduction

- IEC 61511 Safety Lifecycle
- Realization Phase - SIL Verification
  - Probability of Failure on Demand (PFD)
  - Hardware Fault Tolerance (HFT)

Optimal Redundancy
What does Safety Lifecycle mean?

IEC-61511 Clause 3.2.76 definition: Necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use.

Analysis Phase
- How safe is my process?
- How much Risk can I take?
- How much safety do I need?

Realization Phase
- How much safety does my design actually have?
- Does my design meet what is required?

Operations Phase
- How do I keep my plant running safely?
Safety Lifecycle – Realization Phase

1. Safety Requirements Specification
2. Perform Conceptual Safety Instrumented Function (SIF) Design
3. Perform Detail SIF design
   - Select Technology
   - Architecture
   - Proof Test Philosophy
4. Safety Integrity Level (SIL) Verification
5. SIL Achieved?
   - Yes: Implement SIF Design
   - No: Improve Design

SIL Achieved? Yes
Implement SIF Design

SIL Achieved? No
Improve Design
SIL Verification

- Failure Rate
- Diagnostic Coverage
- Proof Test Frequency
- Mean Time to Failure (MTTF)

Probability of Failure on Demand (PFD) Requirements

What is missing?
SIL Verification

SIF Conceptual Design

- Failure Rate
- Diagnostic Coverage
- Proof Test Frequency
- Mean Time to Failure (MTTF)

SIF Detailed Design

- Safe Failure Fraction
- Equipment Design
- Failure Modes
- Proven in Use records

Probability of Failure on Demand (PFD) Requirements

Hardware Fault Tolerance (HFT) Requirements
Hardware Fault Tolerance (HFT)

IEC-61511 / ISA-84-2004 Clause 3.2.23
Fault tolerance: Ability of a functional unit to continue to perform a required function in the presence of faults or errors

HFT of 1: Need 2 redundant devices (e.g. 1oo2 Voting)
HFT of 2: Need 3 redundant devices (e.g. 1oo3 Voting)
Safety Instrumented Function - Example

SIF: High pressure in vessel will trip inlet block valve

Layers of Protection Analysis (LOPA) result:
SIL 2 SIF design required

Assumption: Present design complies with PFD Requirements

Redundancy on basis of HFT
Need for Optimal Redundancy

Under Redundant
- IEC-61511: Avoid Design that relies on overly optimistic failure rate data
- IEC-61511: Avoid Design that relies on very high test frequency

Over Redundant
- Increases Spurious trips – Potentially Not Safe!
- Increased Cost
- Increase Personnel risk

Optimal Redundancy
- Comply with IEC-61511 redundancy requirements
Safe Failure Fraction

IEC-61511 Clause 3.2.65.1
Safe Failure Fraction (SFF): Fraction of the overall random failure rate of a device that results in either a safe failure or a detected dangerous failure.

\[ SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}} \]

- \( \lambda^{SD} \) = Safe Detected Failure Rate
- \( \lambda^{SU} \) = Safe Undetected Failure Rate
- \( \lambda^{DD} \) = Dangerous Detected Failure Rate
- \( \lambda^{DU} \) = Dangerous Undetected Failure Rate
IEC 61511 HFT Requirements

IEC 61511 Clause 11 - Table 5

<table>
<thead>
<tr>
<th>SIL</th>
<th>HFT for Smart Logic solvers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SFF &lt;60%</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

IEC 61511 Clause 11 - Table 6

<table>
<thead>
<tr>
<th>SIL</th>
<th>HFT for sensors and final elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
### Selection based on Prior Use

<table>
<thead>
<tr>
<th>SIL</th>
<th>HFT for sensors and final elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1 - 1 = 0</td>
</tr>
<tr>
<td>3</td>
<td>2 - 1 = 1</td>
</tr>
</tbody>
</table>

Clause 11.5.3.1: Appropriate evidence shall be available that the components and subsystems are suitable for use in safety instrumented system.

Clause 11.5.3.2: The evidence of suitability shall include the following

- consideration of the manufacturer’s quality, management & configuration management systems
- adequate identification & specification of the components or subsystems
- demonstration of performance of components or subsystems in similar operating profiles & physical environments
- the volume of operating experience.
### Selection based on Prior Use

<table>
<thead>
<tr>
<th>Smart SIS Features</th>
<th>Prior Use Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Smart Sensors can detect component failures</td>
<td></td>
</tr>
<tr>
<td>• Smart Sensors can provide both transmitter and process diagnostics</td>
<td>Better data gathering</td>
</tr>
<tr>
<td>• Smart Final Elements - Automates performance monitoring and testing</td>
<td></td>
</tr>
</tbody>
</table>

Examples:
- Rosemount SIS Sensors
- Bettis SIL-PAC
- Fisher FIELDVUE
IEC 61511 Clause 11.4.5: Alternative fault tolerance requirements may be used providing an assessment is made in accordance to the requirements of IEC 61508-2, Table 2 and 3.

### IEC 61508-2: Table 2

<table>
<thead>
<tr>
<th>Safe Failure Fraction</th>
<th>Hardware Fault Tolerance</th>
<th>Simple Device (Type A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;60%</td>
<td>0</td>
<td>SIL1, SIL2, SIL3</td>
</tr>
<tr>
<td>60%&lt;90%</td>
<td>1</td>
<td>SIL2, SIL3, SIL4</td>
</tr>
<tr>
<td>90%&lt;99%</td>
<td>2</td>
<td>SIL3, SIL4, SIL4</td>
</tr>
<tr>
<td>&gt;=99%</td>
<td></td>
<td>SIL3, SIL4, SIL4</td>
</tr>
</tbody>
</table>

### IEC 61508-2: Table 3

<table>
<thead>
<tr>
<th>Safe Failure Fraction</th>
<th>Hardware Fault Tolerance</th>
<th>Smart Device (Type B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;60%</td>
<td>0</td>
<td>Not Allowed, SIL1, SIL2</td>
</tr>
<tr>
<td>60%&lt;90%</td>
<td>1</td>
<td>SIL1, SIL2, SIL3</td>
</tr>
<tr>
<td>90%&lt;99%</td>
<td>2</td>
<td>SIL2, SIL3, SIL4</td>
</tr>
<tr>
<td>&gt;=99%</td>
<td></td>
<td>SIL3, SIL4, SIL4</td>
</tr>
</tbody>
</table>
Design based on IEC 61508

Example Safety Instrumented Function

Simple Device - SFF = 60% to 90% (XV-101)
Smart Device - SFF = 90% to 99% (PT-101)

Single sensor and Single valve can be used for SIL 2
## IEC 61508 Certified Devices

### Smart SIS Features

<table>
<thead>
<tr>
<th>Automated proof testing</th>
<th>Higher SFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial valve stroking</td>
<td></td>
</tr>
</tbody>
</table>

**Examples:**
- Bettis actuators
- DVC6000 SIS Digital Valve Controller

**Third Party Certification:**
- TUV certification assessed per IEC 61508
- exida certification assessed per IEC 61508
Business Results Achieved

Compliance with IEC-61511

Improved Safety and Availability

Efficient Capital Allocation
Summary

SIF Design - Don’t forget HFT Requirements!

Under Redundant Systems – Not Good
Over Redundant Systems – Not Good

Optimal Redundancy
Where To Get More Information

- Dr. Goble (2005), Safety Instrumented Systems Verification: Practical Probabilistic Calculation, ISA
- Emerson Exchange 2013: Improve SIL Verification with the New 2H Approach per IEC 61508 - Dr. Goble - exida
- Emerson Process Management - Smart SIS - Benefits Delivered
  [http://www2.emersonprocess.com/en-US/plantweb/sis/Pages/SmartSISBenefits.aspx](http://www2.emersonprocess.com/en-US/plantweb/sis/Pages/SmartSISBenefits.aspx)
- Contact Email: Nagappan.muthiah@mustangeng.com
Thank You for Attending!

Enjoy the rest of the conference.