Functional Safety: Don’t Pay the Cost for the Wrong Reason!

JC Ogleby: Control System Lead
5th May 2016
SIS Design and Engineering

“The primary purpose of today is to demonstrate the criteria for establishing the design criteria for Safety Instrumented Systems as an independent protective layer and hence prevent harm, loss of containment and/or economic loss”.

Word cloud with terms like safety, system, software, requirements, instrumented, hardware, application, failure, test, see, IEC, integrity, etc.
SIS Design and Engineering

- Independent Layers of Protection [IPL]
  - Three step process
    - IPL Rules
      - Effective,
      - Independent
      - Auditable
  - Types of IPL
    - Preventative
      - Prevent the significant consequence event
    - Mitigating
      - Reduce the risk of a significant consequence event; and
      - Permit a less significant consequence event
SIS Design and Engineering

- Functional Safety
  - Objective
    - “Freedom from unacceptable risk of physical injury and/or damage to the health of people either directly or indirectly [through damage to property or to the environment]”
  - Achieving functional safety
    - Functional Safety is achieved when every specified instrumented protective function is executed and the level of performance integrity required of each function is achieved
    - Functional safety cannot be determined without considering the system as a whole and the environment within which it interacts. Functional safety is inherently end-to-end in scope
SIS Design and Engineering

- Benchmark Guidance and Engineering Standards
  - Technical Standards
    - BS EN 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems
    - BS EN 61511 Functional safety - Safety instrumented systems for the process industry sector
    - BS 7639 Code of practice for instrumentation in process control systems: installation design and practice
SIS Design and Engineering

- HSE Operational Guidance
  - The Storage of Flammable Liquids in Tanks [HSE Books- ISBN 0 7176 1470]
  - Out of control-Why control systems go wrong and how to prevent failure [HSG 238]
  - Proof Testing of Safety Instrumented Systems in the Onshore Chemical / Specialist Industry
  - Principles for proof testing of safety instrumented systems in the chemical industry
  - Operator Response within Safety Instrumented Systems in the Chemical (Onshore), Oil & Gas (Offshore), and Specialist Industries
  - Management of instrumented systems providing safety functions of low / undefined safety integrity
  - Managing competence for safety-related systems Part 1: Key guidance
  - Managing competence for safety-related systems Part 2: Supplementary material
  - Human factors: Alarm management
SIS Design and Engineering

- Industry Guidance
  - EEMUA 191 Alarm Systems A Guide to Design,
  - EEMUA 201 Process plant control desks utilising Human-Computer Interfaces
  - EEMUA 222 Guide to the Application of IEC 61511 to safety instrumented systems in the UK process industries
  - IChemE Using risk graphs for Safety Integrity Level (SIL) assessment - a user-guide for chemical engineers
  - CCPS Layer of Protection Analysis: Simplified Process Risk Assessment
  - CDOIF Demonstrating prior use of elements of a safety instrumented function in support of BS EN 61511
SIS Design and Engineering

- Functional Safety: Management
  - Life Cycle Step: Design and engineering
    - The objective of the requirements of this step is to design one or multiple SIS to provide the safety instrumented function[s] and meet the specified safety integrity level[s] in accordance with BS EN 61511

    - The design of the SIS shall take into account human capabilities and limitations and be suitable for the task assigned to operators and maintenance staff

    - The SIS shall be designed in such a way that once it has placed the process in a safe state, it shall remain in the safe state
SIS Design and Engineering

- Principle Design Philosophy

  - “The focus of your safety instrumented system design must be on excellence”.
  - “Don’t let the fear of cost prevent you from taking advantage of good engineering practice”:
    - It costs you, if it doesn’t work
    - It costs you, if it works when it shouldn’t
  - Therefore:

  "When purchasing real estate the three most important selection criteria are location, location, location. When purchasing a Safety Instrumented System, the three most important selection criteria are diagnostics, diagnostics, diagnostics."
Functional Separation

- BPCS and SIS separation
  - The basic process control system shall be designed to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised.
  - A device used to perform part of an instrumented protective function shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety instrumented function.
SIS Design and Engineering

- SIS Operating Modes
  - Demand mode
    - Definition
      - Where a specified action [for example, closing of a valve is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS]
  - Continuous mode
    - Definition
      - Where in the event of a dangerous failure of the safety instrumented function a potential hazard will occur without further failure unless action is taken to prevent it
      - NOTE 1 Continuous mode covers those safety instrumented functions which implement continuous control to maintain functional safety
SIS Design and Engineering

- SIS Operating Modes
  - Demand mode
    - Probability of failure on demand

<table>
<thead>
<tr>
<th>Safety integrity level (SIL)</th>
<th>Target average probability of failure on demand</th>
<th>Target risk reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>(\leq 10^{-5}) to (\leq 10^{-4})</td>
<td>&gt;10,000 to (\leq 100,000)</td>
</tr>
<tr>
<td>3</td>
<td>(\leq 10^{-4}) to (\leq 10^{-3})</td>
<td>&gt;1000 to (\leq 10,000)</td>
</tr>
<tr>
<td>2</td>
<td>(\leq 10^{-3}) to (\leq 10^{-2})</td>
<td>&gt;100 to (\leq 1000)</td>
</tr>
<tr>
<td>1</td>
<td>(\leq 10^{-2}) to (&lt;10^{-1})</td>
<td>&gt;10 to (\leq 100)</td>
</tr>
</tbody>
</table>

- Frequency of dangerous failures of IPF
SIS Design and Engineering

- Random Hardware Component Failure
  - Safe failure fraction

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

SIS Design and Engineering

- Architectural Example: Proven in Use-Component Selection
  - Are these instruments suitable for my application?
SIS Design and Engineering

- Architectural Example: Proven in Use-Component Selection
  - Are these instruments suitable for my application?
SIS Design and Engineering

- Are these instruments suitable for my application, cont’d?

SIL 3 Capability:

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated without "prior use" justification by end user or diverse technology redundancy in the design.

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD\textsubscript{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

* FIT = 1 failure / 10^9 hours
SIS Design and Engineering

- Proven in Use vs Prior Use
  - Manufacturer approved
  - User approved
  - Component integrity
    - The proper application of reliability engineering principles, across the lifecycle, is the key to continuous improvement in both facility safety and operating efficiency
    - Reliability and continuous improvement is not just a program, it is about establishing a culture
SIS Design and Engineering

- Architectural Examples
  - Per IEC 61511
    - PE Logic Solver
      - Moore Ind STA IL2 certified SFF 93%

![Image of SIS Design and Engineering](image-url)

<table>
<thead>
<tr>
<th>SIL</th>
<th>Minimum Hardware Fault Tolerance</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>
<tr>
<td>4</td>
<td>Special requirements apply (see IEC 61508)</td>
</tr>
</tbody>
</table>

Figure 4 IEC 61511 Minimum HFT PE Logic Solvers
Diagnostics Coverage

- Scope and meaning
  - Not all things called “Diagnostics” are counted as such in the analysis of an IPS
    - Diagnostics conducted manually, are considered tests and therefore are not applicable
    - Do not consider diagnostics that only reside within the device itself
  - Diagnostics are not the same as functional testing
    - Compare sensor or final elements
      - BPCS and IPS components
      - Two or more IPS components
  - Diagnostic must provide notification of fault to the Operator
  - A defined Operator response must be recorded
    - Priority
    - Action required
    - Near miss reporting
SIS Design and Engineering

- Diagnostic Coverage
  - Example

**Which measurement is true?**
- 2oo2 Operate
- 1oo2 Shutdown
SIS Design and Engineering

- Diagnostic Coverage
  - Example

Which measurement is true?
- 2oo3 Operate
SIS Design and Engineering

- Diagnostics Coverage
  - Diagnostic Techniques
  - Detection of component failures is done by two different techniques classified as reference or comparison
  - Reference diagnostics
    - Can be achieved with a single circuit. The coverage factor of reference diagnostics will vary widely with results ranging from 0.0 to 0.999
    - Reference diagnostics take advantage of predetermined characteristics of a successfully operating PES
      - Measurements of voltages, currents, signal timing, signal sequence, and temperature can be utilized to accurately diagnose component failures
SIS Design and Engineering

- Diagnostics Coverage
  - Diagnostic Techniques
    - Detection of component failures is done by two different techniques classified as reference or comparison
  - Comparison diagnostics
    - Comparison diagnostics require two or more circuits. The coverage factor depends on implementation but results are generally good with most results ranging from 0.9 to 0.999
    - Comparison diagnostic techniques depend on comparing data between two or more PES units
      - If a failure occurs in the circuitry, processor or memory of one PES, there will a difference between data tables in that unit when compared to another unit. Comparisons can be made of input scans, calculation results, output read back scans, and other critical data
Conclusion

- Integrated value engineering solution [Demonstrated RRF]
- Robust, fit for purpose scalable SIS and tiered control system solution
- Fully integrated asset management traceability, reduced cost of ownership
- Operational resource competency demonstration

“Persons, departments or organizations involved in production support and safety life-cycle activities shall be competent to carry out the activities for which they are accountable”.

- Increased value engineering and process optimisation capability

- However, if you get it wrong!
SIS Design and Engineering-Not!

How the Process Hazard Analysis explained it
How the Project Leader understood it
How the Hardware Engineer designed it
How the Software Engineer wrote it
What the Business group thought they were getting

What was documented
What was installed
What it cost
How it was supported
What risk reduction factor was actually delivered