hargrove
controls & automation

Safety Instrumented Systems - Common Misconceptions

Instrumented Protective Systems (IPS) contain controls, alarms, and interlocks, known as Instrumented Protective Functions (IPFs), that are used to reduce risk of harm to personnel. A Safety Instrumented System (SIS) is an IPS that follows a cradle-to-grave life-cycle, specified in the ANSI/ISA-61511 and IEC-61511 standards. An SIS has one or more Safety Instrumented Functions (SIFs), which are IPFs that have been credited with more than one order of magnitude of risk reduction in a given hazard scenario. SIFs are given minimum risk reduction targets of >10, >100, >1000, or >10000, termed Safety Integrity Level (SIL) 1, 2, 3, or 4.

Instrument-based controls have been used for hazard risk reduction for many decades. The formal process for defining, implementing, and managing an SIS has been around for well over two decades. Details of the SIS life-cycle are well understood by many in the process industries; however, there are still misconceptions.

hargrove | SIS - Common Misconceptions

Here are a few common SIS misconceptions from a service provider's perspective:

1. Slap together a "SIL 2 rated" transmitter, "SIL 2 rated" logic solver, and "SIL 2 rated" valve and we are good to go for SIL 2 (or 1 or 3). No!

SIL performance is for an entire integrated SIF and requires clearing three hurdles:

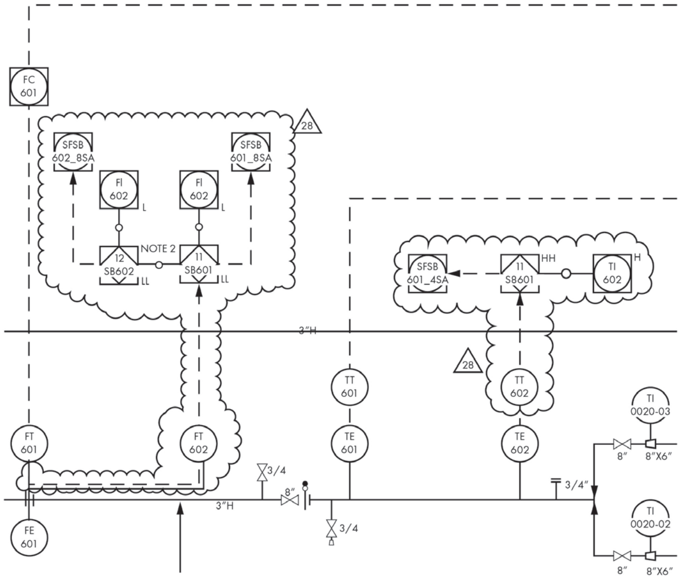
- PFD / RRF calculation result per the target SIL
  - o This is the requirement for a SIL Verification calculation, aka SIL calc.
- Hardware Fault Tolerance (HFT) requirements per the target SIL
  - o This is a requirement for the ability to tolerate a device failure via the use of redundancy, per tables in ISA-61511, or alternatively, in its umbrella standard, IEC-61508.
- Systematic Capability for the target SIL (SC1 through SC4)
  - o "Rated" in the context above refers to the systematic capability (SC) of the device or system.
  - o SC is a measure of suitability for use in a SIS application.
  - o SC alone does not guarantee suitability or SIL performance in specific applications.

Takeaway: SIL performance is a lot more than just combining device certificates.

2. DCS-based, PLC-based, or hardwired safety alarms or interlocks have no special requirements, since they are not in a SIS. No!

- OSHA PSM requires the use of Recognized and Generally Accepted Good Engineering Practice (RAGAGEP) for IPFs. The ISA-84.91.01 standard clarifies this intent:
  - o Requirements apply to all IPFs, i.e. all Process Safety Controls, Alarms, and Interlocks (PSCAI) used to reduce risk of harm in a hazard scenario, including:
    - - Unique identification
    - - Best practice specification, design, and installation
    - - Periodic maintenance and testing as part of a mechanical integrity program
  - o These are a subset of the requirements in the SIS life-cycle.
  - o Safety Instrumented Systems are a subset of PSCAI. Scope covers IPFs having a risk reduction claim greater than 10.
- A new standard, ISA-84.91.03, is in development to define a life-cycle for PSCAI having risk reduction claims not more than 10, so these non-SIS interlocks will likely gain more attention.

Takeaway: All instrumented systems used for hazard risk reduction need special attention to ensure that they continue to deliver the performance assumed in the risk analysis. Not just SIS.



3. Just doing a SIL calc and getting a good result means we are following the SIS standard. No!

OSHA PSM requires using RAGAGEP for management of IPFs. Many methods may be considered RAGAGEP, but OHSA has explicitly recognized the ISA-61511 standard (formerly numbered ISA84) as RAGAGEP.

There is a lot more to the standard requirements than SIL calcs. SIL calcs are intended to support minimization of random device failures. The rest of the life-cycle is intended to reduce systematic failures, primarily human error.

Major steps in the life-cycle include:

- SIS life-cycle planning
- Hazard and Risk Assessment
- Allocation of SIFs to protection layers
- Safety Requirements Specifications (SRS)

- Design and engineering
- Installation, commissioning, and validation
- Operation and maintenance
- Modification
- Decommissioning
- Functional Safety Assessment (FSA, Stages 1-5)

Takeaway: OSHA PSM requires following RAGAGEP. ISA-61511 is RAGAGEP. Compliance with ISA-61511 means that all mandatory requirements in the life-cycle are met. Not just SIL calcs.

4.SIL certificates are required for SIF devices. No!

- SIL certificates document Systematic Capability (SC1 through SC4) of the device. SC is a measure of suitability for use in a SIS application.
- The intent of the SC requirement is to reduce systematic failures, primarily human error in design, manufacturing, operating procedures, or other relevant factors.
- The main factors in determination of SC include the manufacturer's quality system and documentation.
- A key part of the SC requirement is to ensure that suitability of selected devices are considered in the context of the application and operating environment.
- A certificate is "nice to have." It is not a requirement in the standard and it does not guarantee suitability or SIL performance in specific applications.
- Devices must be justified for use in a SIS. Certificates combined with application-specific justifications are one option; "prior use" is another.
- Some companies choose to require certificates for SIS devices. Finding certified devices can be an issue in some cases.

Takeaway: SIS devices must be qualified for each specific application, but certificates are not required.

5. SIL calcs are just a back check that can be done well into a project's Detailed Design Phase. Risky!

- Despite the risks, this often happens.
- SIL verification calculation inputs include sensor, logic solver, and final element failure rates, voting arrangements, proof test intervals, diagnostics, and other parameters to estimate the SIF Probability of Failure on Demand (PFD) or Risk Reduction Factor (RRF). (RRF = 1 / PFD).
- SIL calc outputs include the RRF Result, maximum test interval, and assumed use of diagnostics.
- Iterative changes to calculation inputs may be needed to achieve the required PFD and desired test interval. Discussion may be extensive in some cases.
- Calc results impact hardware requirements (e.g. device redundancy), operations (test support, response to detected faults), and maintenance burdens (inspection, maintenance, and test frequencies).
- Changes to required hardware in a SIS can impact project cost, design effort, and schedule.
- Delaying SIL calcs to a Detailed Design phase carries tacit acceptance of cost and schedule risks.
- Gaps or inconsistencies in a LOPA or other basis documents may create a need for review, discussion, and possible revisions. This process can be time consuming, so the documentation should be reviewed as early as possible.
- Timing of the hazard analysis and SIF requirements definition needed for SIL calcs is usually set by the end user, out of the contractor's control.

Takeaway: Do preliminary hazard analysis, SIF definition, and SIL calcs as early as possible to establish hardware designs and O&M impacts. Address questions and issues as early as possible.

6. Sharing a control valve between BPCS and SIS layers in a hazard scenario is ok if the SIS has its own solenoid. Maybe.

- If SIFs are defined using the LOPA methodology, credited IPFs must be independent, since LOPA math is based on an assumption of independence.
- If possible, sharing of components between IPFs in a hazard scenario should be avoided. In some cases, sharing of a device may be acceptable, if an analysis is done that shows the overall risk to be sufficiently low.
- Analysis of sharing between IPFs may be done as a supplement to a LOPA or as an alternate method. Typical methodologies are the use of Fault Tree Analysis (FTA) or multiple SIL calcs combined in an event tree.
- Some companies have an internal standard requirement that forbids device sharing, or that mandates a deeper analysis of potential sharing issues by a SIS authority.

Takeaway: Device sharing among IPFs in a hazard scenario should be avoided but may be ok if a detailed analysis demonstrates risk to be sufficiently low.

7. There is no need for SIS logic solver proof testing if no changes were made since the last test. No!

- The SIS standard, ISA-61511, defines a proof test as "a periodic test performed to detect dangerous hidden faults in a SIS so that, if necessary, a repair can restore the system to an 'as new' condition or as close as practical to this condition."
- Dangerous hidden faults can occur at any time. Proof testing of the SIF sensors, logic solver, and final elements must be done periodically at intervals not more than the assumption in the SIL calc.
- SIS logic solvers are designed for high reliability. They have extensive diagnostics, which reduce the dangerous failure rate. The logic solver contribution to an overall SIF PFD is usually very low in comparison to the sensors and final elements.
- In a SIL calc, it's usually possible to use a logic solver test interval equal to the site turnaround interval so that offline testing can be done.

Takeaway: Periodic proof testing of all devices in a SIF, including the logic solver, must be done per requirements in the SIL calc. No skipping of tests.

8. A SIF can have some sensors or final elements wired to a BPCS and communicated to the SIS. No!

- This would mean that an IPF having a risk reduction claim greater than 10 would be implemented at least partially in a BPCS.
- Per the SIS standard, ISA-61511, "If the risk reduction claimed for a BPCS protection layer is > 10, then the BPCS shall be designed and managed to the requirements within the IEC 61511 series." This never happens. Standard PLC and DCS equipment is not designed in accordance with the IEC-61511 / IEC-61508 standards.
- SIF devices must be wired to a SIS. Data can be communicated to other systems as needed, via hard wiring or soft links.
- A SIF has one or more final element actions required to bring the process to a safe state. These must be wired to a SIS. In some cases, the SIF will take additional actions that support non-safety goals (e.g., operations, equipment protection). These additional actions may be in a BPCS and connected to the SIS via hard or soft connections.

Takeaway: All devices used in a SIF that are needed to bring the process to a safe state must be wired directly to a SIS.