Session No. 518

Architecture-Based Safety Instrumented Systems

Glenn Young, C.S.P.
Owner
Glenn Young & Associates, LLC PSM Consulting

The process safety consensus standards for safety instrumented systems (SIS)[1] were originally developed in the aerospace and nuclear industries. For these industries, failures were both highly visible and unacceptably expensive.

The standards were intended to provide assessment, evaluation, and target reliabilities for instrumented systems that served a safety function. To be an instrumented system, the system must consist of:

- One or more sensors (such as a temperature, pressure, or flow sensor, for example)
- One or more logic elements (such as a dedicated programmable logic controller for example)
- One or more actuated elements (such as a pneumatic valve or relay for example)
- The connections between these elements

To be an SIS, the system must additionally serve a safety instrumented function (SIF), as opposed to a purely control function. An example of a control function might be a steam controller to a distillation column reboiler that increases or reduces the steam flow based on the temperature demands of the distillation column. The SIF that the same system might provide is to automatically shut off the steam to the reboiler if a safe maximum temperature is ever exceeded. In this example, the same instrumented system provides both control and safety functions. The SIF, however, is what determines whether or not the system is a safety instrumented system; no SIF, no SIS.

Consensus standards and recognized and generally accepted good engineering practices require analysis of the SIS[2] to determine its existing reliability. This is most commonly done using semi-quantitative risk analysis techniques, such as layers of protection analysis (LOPA).[3] LOPA has by this date achieved good penetration of the process industries, is well understood, and is well accepted by management teams. In cases where LOPA is insufficient or is inappropriate, more quantitative analysis methods, such as event tree or fault tree analysis, are often used. In conjunction with the corporate risk tolerance, analysis can determine whether or not the existing SIS has sufficient reliability.

---

[1] HSE-PES (*Programmable Electronic Systems in Safety Related Applications, Parts I & II*).
[2] ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) (*Functional Safety: Safety Instrumented Systems for the Process Industry Sector*), ANSI/ISA-84.01-1996 (*Application of Safety Instrumented Systems for the Process Industries*), IEC-61508 (*Functional Safety - Safety Related Systems*).
[3] AIChE-CCPS (*Layers of Protection Analysis, Simplified Process Risk Assessment*).

For analysis calculations, any specific instrument loop with no safety integrity level (SIL) rating is assumed to be reliable to within an annual failure rate of 1 in 10 years (0.1). This rate is for "on-demand" safety instrumented systems with an expected demand of one challenge per year. For systems with significantly more frequent challenges or that must operate continuously, additional calculations are required.[4]

If the existing SIS has adequate reliability, the exercise is completed. If, however, additional reliability is needed to achieve tolerable risk, three options are available to increase the reliability:

1. Use more reliable parts
2. Add redundancy
3. Test and calibrate more frequently

These options may be used singly or in conjunction to increase reliability. Obviously, the last of the three options is the most expensive route, since the cost is recurring.

The reliability analysis is intended to generate a required SIL.[5] The SIL defines the expected probability of failure on demand (PFOD) for the SIS. Commonly accepted SIL definitions are:

- SIL-1: PFOD of between 0.1 and 0.01 (The system would be expected to operate correctly for 10 of 10 demands, but would be expected to fail on demand at least 1 time in 100 demands.)
- SIL-2: PFOD of between 0.01 and 0.001 (The system would be expected to operate correctly for 100 of 100 demands, but would be expected to fail on demand at least 1 time in 1,000 demands.)
- SIL-3: PFOD of between 0.001 and 0.0001 (The system would be expected to operate correctly for 1,000 of 1,000 demands, but would be expected to fail on demand at least 1 time in 10,000 demands.)

Additional (higher reliability) SIL levels are available, but are typically never required in the process industries. The reason that such high reliabilities are rarely required in the process industries is that the hazards are typically much less than those for the aerospace and nuclear industries. This is an important point, and will be referred to again.

Up to this point, the process industries have typically been able to comply with the safety instrumented systems standards. The analysis tools are in place, understood, and mature in their use; the SIL levels are clearly defined, and clearly relate to the corporate risk tolerance tables. The final step of the SIS standards, however, is field implementation and verification.

The consensus standards and good engineering practice require[6] that the installation of a SIS be verified in the field as meeting its reliability target. Such verification, if done properly, involves frequent testing and calibration of the SIS that includes fully functional checks. A fully functional check involves:

- Creating the actual condition for the sensor that would create the demand on the SIS (not just an isolated bench test of the temperature, pressure, or flow)
- Verifying that the logic responded correctly to the signal

---

[4] ISA (*Safety Integrity Level Selection, Systematic Methods Including Layer of Protection Analysis).*
[5] ISA (*Safety Instrumented Systems: Design, Analysis and Justification, 2nd Edition*).
[6] AIChE-CCPS (*Guidelines for Safe Automation of Chemical Processes*)

- Verifying that the actuated element functioned (the actual valve opened/closed or that the actual relay/breaker tripped/actuated)
- Verifying that the actual connections between the sensor, logic, and actuated element functioned as designed

Most process industries do not have the luxury of taking expensive process equipment off line to do such checks. Isolating individual elements of the SIS and testing in isolation do not provide adequate proof of the system's function.

Further, there can be actual hazard involved in performing fully functional checks. To actually bring a large and expensive turbine and compressor train up to over-speed trip status can risk real and very expensive damage.

Finally, even if fully functional testing is performed and documented, without chi-square testing or equivalent statistical analysis, there is no way to verify that the test results obtained are statistically significant and not due to random chance.

For these reasons, many in the process industries are opting to use architecture-based safety instrumented systems rather than reliability-based ones. This idea has a proven history in the process industries, driven primarily by insurance carriers.

At one time, boiler explosions were common and expensive. In response, the insurance carriers demanded that boilers be fitted with an independent, low-level trip switch that would shut off the heat source on low-low level condition in the boiler. This architecture-based solution has a proven track record of eliminating boiler explosions that are now extremely uncommon.

At one time, fired equipment explosions were common and expensive. In response, the insurance carriers demanded that fired furnaces and boilers be fitted with a double-block-and-bleed gas shutoff. This architecture-based solution has a proven track record of eliminating gas explosions in fired equipment.

At one time, steam turbine over-speed failures were common and expensive. In response, the insurance carriers demanded that larger steam turbines be fitted with both mechanical and electronic redundant high-speed trips. This architecture-based solution has a proven track record of eliminating steam turbine failures.

Following this proven and effective strategy, many companies are opting to implement architecture-based safety instrumented systems in response to SIL calculations. The architecture-based model has much to recommend it including:

- Reduced recurring costs of field verification (SIL reliability is assumed, based on the architecture, unless field experience contradicts the assumption.)
- Clear guidance on what is required for a given SIL requirement (The SIL architecture incorporated in the corporate SIS guidance document specifies the required configuration.)
- A long-time and proven precedent for architecture-based hazard reduction from the insurance industry
- The ability to move at a later date to full compliance with the safety instrumented systems consensus standard when resources are available without additional hardware expenditures

- The ability to implement the safety instrumented systems standard without expensive training for existing instrument personnel

One question, of course, is whether or not regulatory agencies would consider an architecture-based safety instrumented systems program to be fully compliant with the consensus standards. There is no way to reliably predict what any individual compliance officer might decide, but with the precedents from the insurance industry, the case for architecture-based systems is certainly strong. Further, the SIS architecture typically used by architecture-based programs is generally more restrictive than that allowed for reliability-based programs, and an extra layer of safety is provided by the requirements. Overall, companies using the architecture-based method feel that the reliability they achieve is at least comparable to and often better than that achieved with weaker architecture and field reliability measurements.

Examples of typical reliability-based and architecture-based SIL systems are found in Exhibits 1 and 2 below:

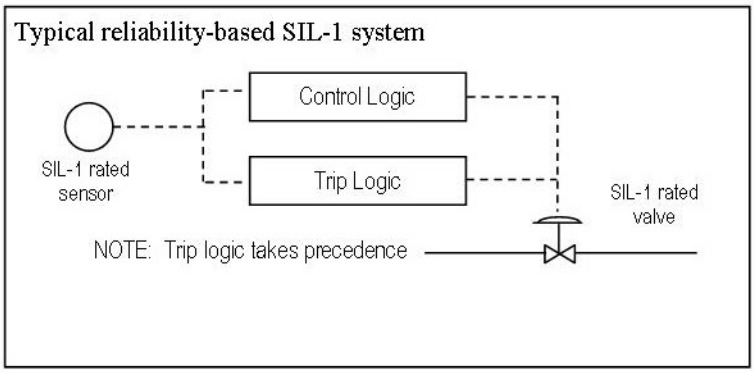

Exhibit 1. Reliability -Based SIL-1

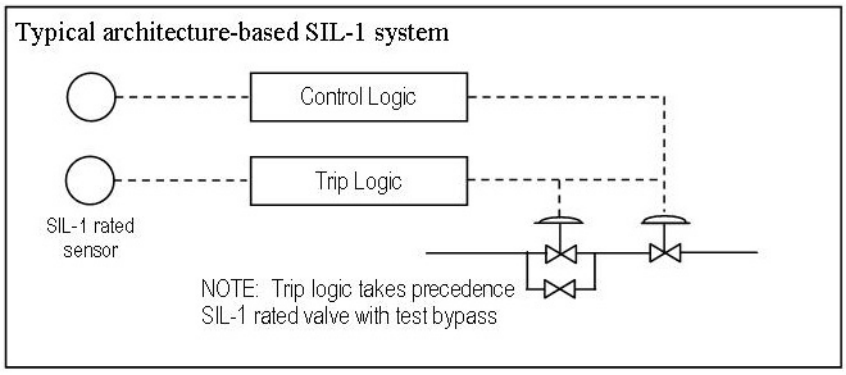

Exhibit 2. Architecture-Based SIL-1

Only SIL-1 systems are depicted here because typically the process industries do not require SIL-2 or SIL-3 reliabilities. If higher than SIL-1 ratings are required, then either the LOPA is being performed incorrectly, the tolerable risk is set too tightly, or the process has unusual hazards.

A fair rule of thumb is that, "Industry-standard hazards require no more than industry-standard safeguards." This means that if SIS analysis shows furnace gas trips, turbine over-speed

trips, or boiler low-level trips as SIL-1 or higher ratings, the analysis is wrong. These types of trips have operated successfully and safely for decades throughout the process industries without specific SIL ratings.

Architecture-based SIL systems require additional attention if (and only if) they are found to be non-functional or are so far out of calibration that they would not have functioned if called on to do so. Any such occurrence is typically treated as a PSM-near-miss incident and given full investigation, including root-cause analysis, to determine why the system was not functional. If successive testing and calibration fail to remedy the problem, the next SIL level up is typically implemented.

Summary

Architecture-based SIS makes sense for the process industries because:

- The hazards of the process industries are lesser than hazards found in the aerospace and nuclear industries where the consensus standards originated.
- The architecture-based hazard control model has a very long and successful history, based on insurance industry requirements.
- The architecture-based control model allows for future conversion to full reliability-based compliance without additional hardware expenditure.
- The implementation requires less training for existing personnel.
- The implementation requires less modification of existing testing, calibration, and design procedures.

Bibliography

American National Standards Institute (ANSI)/International Electrotechnical Commission (IEC). 1998. IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems 61508*. Nnew, NY: ANSI/IEC.

_____. 2003. IEC 61511, *Functional Safety—Safety Instrumentation Systems for the Process Industry Sector*. New York, NY: ANSI/ IEC.

American National Standards Institute (ANSI)/International Society of Automation (ISA). 2004. ANSI/ISA-84.00.01-2004 (IEC 61511, Mod. Parts 1-3). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector.* New York, NY: ANSI/ISA—IEC.

American Petroleum Institute. 2001. API-RP 14C, *Recommended Practice for Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms.* Washington, D.C.: American Petroleum Institute.

_____. 1987. API-RP 556, *Recommended Practice for Instrumentation and Control Systems for Fired Heaters and Steam Generators.* Washington, D.C.: American Petroleum Institute.

Center for Chemical Process Safety (CCPS). 1993. *Guidelines for Safe Automation of Chemical Processes*. New York: Wiley and American Institute of Chemical Engineering (AIChE).

_____. 2001. *Layer of Protection Analysis, Simplified Process Risk Assessment*. New York: Wiley and American Institute of Chemical Engineering (AIChE).

Gruhn, Paul and Harry Cheddie. 2006. *Safety Instrumented Systems: Design, Analysis and Justification.* 2nd Edition. Triangle Park, NC: ISA—The Instrumentation, Systems, and Automation Society.

Health and Safety Executive (HSE). 1987. *Programmable Electronic Systems in Safety Related Applications, Parts 1 & 2*, (PES). Norwich, U.K.: HSE.

Marszal, Ed & Eric Scharpf. 2002. *Safety Integrity Level Selection - Systematic Methods Including Layer of Protection Analysis*. Triangle Park, NC: ISA—The Instrumentation, Systems, and Automation Society.

National Fire Protection Association (NFPA). 2004. NFPA 85, *Boiler and Combustion Systems Hazard Code.* New York City, NY: National Fire Protection Association.