Optimizing Safety Instrumented Systems to Protect Industrial Operations

By Erica Bartlett, Anvil Resource Manager, Control Systems with Linda Ricard

Safety instrumented systems (SIS) are critical to maintaining safe industrial operations involving highly hazardous, explosive, and flammable chemicals such as oil, gas, ammonia, and other toxic gases.

Nowhere is SIS reliability and safety more critical than in our nation's refineries. According to the U.S Energy Information Administration, as of January 1, 2024, there were 132 operable petroleum refineries in the U.S. [1]

With approximately 85% of those refineries built between 50 and 140 years ago and still processing millions of barrels of oil per day, their aging infrastructure requires stringent safety instrumented systems (SIS) to operate safely while maintaining peak production levels. In addition, refinery outages have increased 50% since 2023, adding to the strain of meeting targeted market demand throughput. [2]

As a closed loop cybernetic system independent of the rest of the industrial control networks, safety instrumented systems (SIS) synchronize within a controlled process to provide intelligence and diagnostics on a processing unit's operating systems. The role of SIS is to respond predictably and sometimes quickly during critical events. Its reliable, predictable, and redundant control loop process ensures fail-safe facility operations.

SIS is comprised of sensors embedded within transmitters (i.e., flowmeters, fire dampers), logic solvers, and final control elements (i.e., pressure control valves), that continually monitor multitudes of systems in processing units such as boilers, piping, heaters, and reactors.

The role of SIS sensors is to detect and transmit information on a unit's processing performance to the logic solver. Sensors read and measure pressure, temperature, liquid flow rates, and liquid levels to detect any safety anomalies (e.g., corrosion, vibration, erosion, leakage of hazardous material, flame, smoke, or heat) or inconsistencies in unit operation (i.e., abnormal flow ranges).

These sensors then transmit that information to the logic solver. The logic solver determines whether the process system performs as expected within its calculated operational limits based on its risk failure rates and that the process variables (PVs) are within their expected allowable band. [3]

If the logic solver program meets its requirement that a process unit has exceeded its safe operational limits (SOL) (e.g., high temperature, abnormal flow, or high-pressure readings), it immediately signals the final element to perform the necessary action to put the system back into a safe state, such as closing a flow control valve.

If that fails, the logic solver then initiates safety instrumented functions (SIFs) within the SIS safety interlock system to perform an emergency unit shut down to maintain a specified safety integrity level (SIL). In extreme situations, SIFs will trigger an alarm to initiate an emergency shutdown of either the affected area of a plant so that the rest of the plant can maintain safe operations or shut down the entire plant to avoid a potentially catastrophic event.

To further ensure the integrity of safety instrumented systems, facility owners/operators continue to improve SIS reliability and safety across the spectrum of their industrial operations, including isolating SIS systems from the rest of their industrial controls networks to prevent cyberattacks.

However, this is just one approach to optimizing SIS safety and reliability. Other approaches include conducting ongoing process hazards analysis (PHA) and layers of protection analysis (LOPA) studies to continually uncover areas of SIS vulnerability and implementing advanced safety and diagnostic technologies.

3 Approaches to Optimizing SIS Safety and Reliability

Approach #1: Conduct PHA/LOPA Studies on an Ongoing Basis

A sound SIS management system defines how an owner/operator will assess, design, engineer, verify, install, commission, validate, operate, maintain, and continuously improve their SIS. [4] This entails mapping an SIS reliability plan that begins with some form of a Process Hazard Analysis (PHA) study.

This could be a simple "what if" comprehensive hazard and operability (HAZOP) study, or other qualitative hazard analysis. These studies establish the basis for identifying deficiencies or gaps in layers of protection. The resulting quantitative study from a PHA is commonly known as a LOPA or Layers of Protection Analysis.

As the level of complexity increases, so do risk factors since complexity and risk often go hand-in-hand. As a result, a risk assessment is conducted as part of a PHA to identify potential failures and root causes. This information is then captured and ranked in a waterfall matrix in terms of consequences, such as the probability and severity of failures. The resulting data dictates the strategies that will be required to mitigate the hazards.

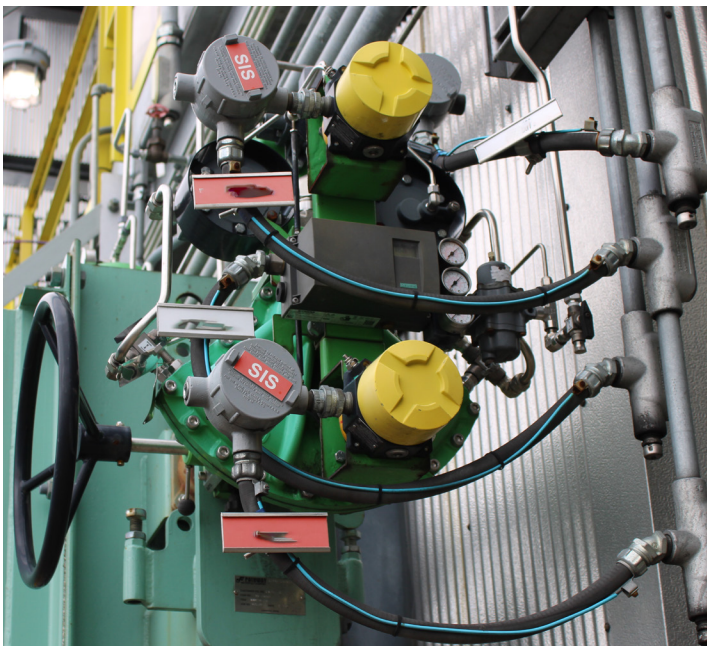
As mentioned previously, if the risk ranking is not acceptable and the consequences still severe, engineers then conduct a Layers of Protection Analysis (LOPA) study. The LOPA report specifies all the safety instrumented function (SIF) safeguards that must be put in place to mitigate the risk, whether an alarm or an automatic system shut down, to meet safety requirement (SR) standards.

The team then recalculates the risk ranking with the added layers of protection. More layers of protection are added until the new risk ranking is acceptable.

After specifying the safety instrumented functions (SIF) and documenting the safety requirements (SR), a safety integrity level (SIL) is then assigned. The probability of a specific SIF failing to perform its required function when called upon is known as the probability of failure on demand (PFD). [5]

As per IEC 61511 standards, SILs are required to protect against specific hazards. As a result, components included in a SIF are SIL compliant and meet safety requirement standards. All LOPA, risk rankings, mitigation strategies, SIF, SR, and SIL information is then captured in the HAZOP's LOPA report.

To maintain the integrity of the SIS architecture, it's important that facility owners/operators continue to perform PHA studies at least every five years. This not only reduces the probability of potential failures which can lead to operational disruptions and increased



safety risks, but it also gives owners/operators the information to help them determine how to safely maintain their industrial assets over time and when to procure long lead items to optimize maintenance schedules or facility turnarounds.

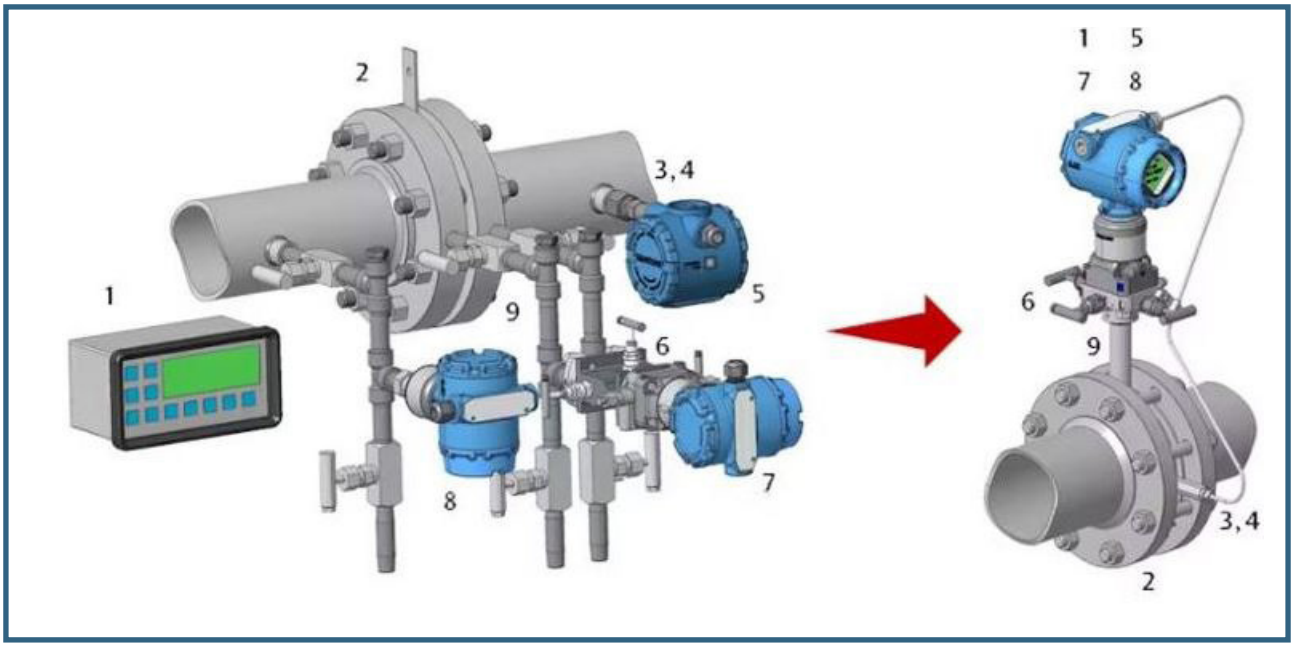
Approach #2: Implement Advanced Technologies for Redundancy in Data

According to Offshore Reliability Database, the overwhelming majority of SIS failures originate in sensors (42%) and final control elements (50%). [6] The reason for the high sensor failure rate is due to the fact that sensors were installed decades ago and are now aging out.

The good news is that as technologies continue to evolve and become more sophisticated, new sensor designs are becoming smaller, smarter, and simpler to install and maintain while still being more reliable and robust.[6] To further reduce false readings, some instruments are now built with redundant transmitters and detectors, resulting in a simple, compact, integrated, single device configuration.

Relying on multiple and independent readings per unit versus a single reading from a potentially faulty transmitter that can produce false readings, the redundant readings in the controlled loop process verifies the accuracy of the information, leading to higher levels of reliability.

For example, Rosemount's 8800 Series Quad Vortex Flow Meter provides four independent flow measurements in a single meter unit versus the traditional multiple meter design for more robust backup capability. [7]



1. Flow Computer
2. Primary Element
3. Thermowell
4. Temperature Sensor
5. Temperature Transmitter
6. DP Manifold
7. DP Transmitter
8. Pressure Transmitter
9. Connection Hardware

Figure 1. Newly designed, compact, and integrated DP orifice flowmeter assemblies reduce leak points by up to 80% from "Improve the Reliability of Safety Instrumented Systems with Advanced Measurement Technologies," by Meha Jha and Julie Valentine, Improve the reliability of safety instrumented systems with advanced measurement technologies | P.I. Process Instrumentation, August 10, 2021.

Besides breakthroughs in SIS process intelligence, there have also been significant advancements in troubleshooting and maintenance diagnostics to monitor the health and performance of sensors, transmitters, logic solvers, and final control elements to detect issues or potential failures early on.

Remote troubleshooting reduces the need for field trips to inspect equipment which could lead to personnel safety issues and increased labor costs.
In addition, taking sensors offline to be calibrated as part of the troubleshooting process may no longer be required as the calibration process can now be done remotely.

It is also important to note that advancements in SIS diagnostics and maintenance also reduce the potential for human error. Now, proof testing can be done online to verify the reliability of the sensor, logic solver, and final control element.

Partial stroke testing, a type of proof testing, is also valuable as an ongoing preventative maintenance procedure to ensure that on/off valves that only operate during an emergency situation or during plant shutdowns will function when needed. The partial stroke testing device works in conjunction with the logic solver to ensure that the test will not adversely affect the process when the valve moves during the test.

The purpose of the test, which may only take seconds, is to ensure that the valve is able to move freely. The device takes measurements of the test and logs it into the logic solver so that the logic solver can determine if there are any issues. If it fails, operators can then develop a plan to replace the valve. [8]

It is important to note that advanced technologies are only as good as the personnel operating the systems. Human error can also cause SIS failures. For this reason, personnel should be thoroughly trained in SIS operation, maintenance, potential common cause failures (CCF), and mitigation strategies.

Approach #3: Isolate Safety System Logic Solver

Although the majority of SIS failures are confined to sensors and final control elements, SIS logic solvers can be the biggest safety risk if connected to the rest of the industrial control network.

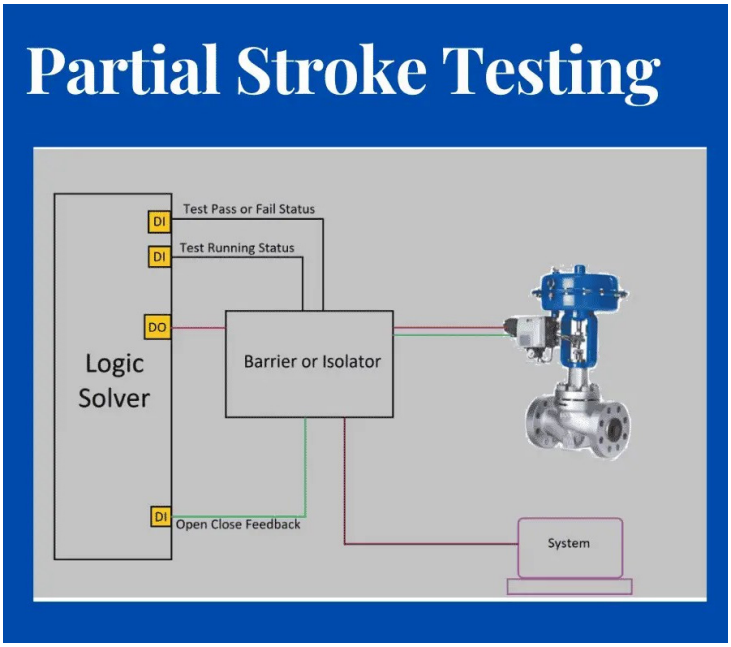


Figure 2. Installing a partial stroke testing device (PSD) in a SIS final control element for automated ON-OFF valve operation improves the proof test requirement from "Partial Stroke Testing Device (PSD) in SIS Final Control Element.".

This would leave safety-critical functions like SIS wide open to an accidental intrusion or potential cyber-attack as demonstrated with the Triton event of 2017 where hackers deployed malware against a petrochemical plant's safety systems.

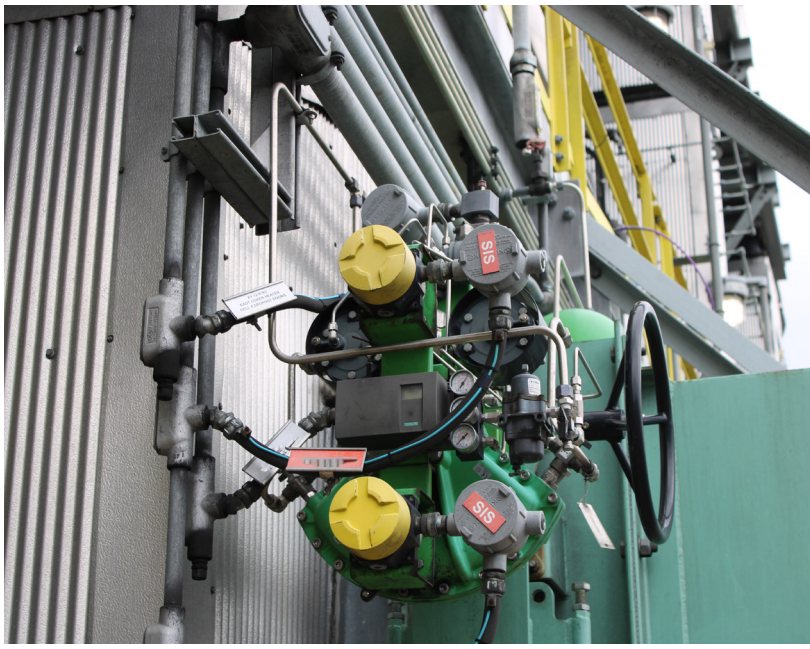
Triton reprogrammed the SIS controllers to initiate a safe shutdown when application code between redundant processing units failed a validation check, automatically shutting down the industrial process. [9] Triton is known as the "Killer Code" and the world's most murderous malware [10] and is the world's first SIS cyberattack where attackers deployed a new Industrial Control System (ICS) attack framework to cause operational disruption to critical infrastructure. [11]

Following the event, the FBI deemed Triton as a deadly new industrial cyberweapon that threatens our nation's energy sector. Even the Department of Homeland Security has expressed concerns over the fact that "emerging SIS solutions present more risk from varying degrees of integration of safety functions with control networks, as opposed to isolation from them." [12]

For this reason and to prevent system-wide safety shutdowns, it is critical to isolate SIS logic solvers and remote engineering workstations that program and configure SIS from the main industrial network by creating dedicated SIS networks.

Additional considerations to safeguarding the safety system logic solver from malicious or accidental breaches is applying secure-by-design approaches (NIST SP 800-160) and other security measures such as access controls for authorized users to include:

- Firewalls
- Specific and secured laptops for additional SIS programming
- Sign in security credentials
- Specific access cards, like badge readers, into locked buildings housing logic solvers
- Key switches for locked cabinet
- No blue tooth functionality in the logic solver



Summary

The Triton attack shed light on vulnerabilities in industrial facility safety systems. As a result, increasing the reliability and integrity of SIS in processing plants such as refineries and advanced manufacturing facilities requires a rigorous and multi-pronged approach.

Conducting meticulous risk and process hazard analyses to uncover deficiencies and gaps in protection and developing a subsequent SIS management reliability plan is just the first step. To properly maintain safety levels to meet industry standards requires ongoing analyses, such as PHAs, to fully ensure the reliability

and predictability of SIS network operations.

Further ensuring accuracy through redundant SIS sensor readings on unit performance and processes also requires upgrading to the most advanced intelligence and diagnostics technologies in multivariable sensors. Finally, advanced electronics can only do so much to protect plant processes from a security breach. As new SIS solutions come to market, they may present more risk if integrated into other safety functions within industrial control networks.

SIS networks provide continual and redundant process intelligence and maintenance diagnostics. This can become a potential point of vulnerability if the information is shared across other ICS networks or if the SIS network is not installed or maintained properly. Therefore, it is critical to implement dedicated SIS networks independent of other ICS networks to protect the mission-critical data and to maintain the safety lifecycle of the SIS.

By keeping their SIS networks separate from other industrial control networks, owners/operators will have peace of mind knowing that they are safeguarding their operations from potential cyberattacks or accidental intrusions. In addition, by conducting ongoing HAZOPS studies and proof testing, owner/operators will also have peace of mind knowing that they are maintaining the health and safety lifecycle of their SIS long term.

REFERENCES

1 "U.S. Energy Information Administration, Independent Statistics and Analysis," Frequently Asked Questions (FAQs) - U.S. Energy Information Administration (EIA), January 1, 2024.

2 "Rise in refinery outages, tighter supplies pushing up US fuel prices," by Shariq Khan, Rise in refinery outages, tighter supplies pushing up US fuel prices | Reuters, September 21, 2023

3 "Application of Safety Instrumented System (SIS) approach in older nuclear power plants," by Elnara Nasimi and Hossam Gabbar, Application of Safety Instrumented System (SIS) approach in older nuclear power plants - ScienceDirect, May 2016

4 "Understanding SIS Industry Standards," by Robert I. Williams, PE, Understanding SIS industry standards - Control Engineering, May 14, 2013.

5,6,7 "Improve the Reliability of Safety Instrumented Systems with Advanced Measurement Technologies," by Meha Jha and Julie Valentine, Improve the reliability of safety instrumented systems with advanced measurement technologies | P.I. Process Instrumentation, August 10, 2021.

8 "Partial Stroke Testing Device (PSD) in SIS Final Control Element," www.electricalvolt.com, Partial Stroke Testing Device (PSD) in SIS Final Control Element.

9 "Attackers Deploy New ICS Attack Framework 'Triton' and Cause Operational Disruption to Critical Infrastructure," by Alisa Esage, Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure, December 15, 2017.

10,11 "Triton is the World's Most Murderous Malware, and it's Spreading," by Martin Giles, San Francisco Bureau Chief, MIT Technology Review, Triton is the world's most murderous malware, and it's spreading | MIT Technology Review, March 5, 2019.

12 "LOGIIC Safety Instrumented Systems Project," Science and Technology, U.S. Department of Homeland Security, CSD-LOGIIC-ISP | Homeland Security, August 2, 2024.