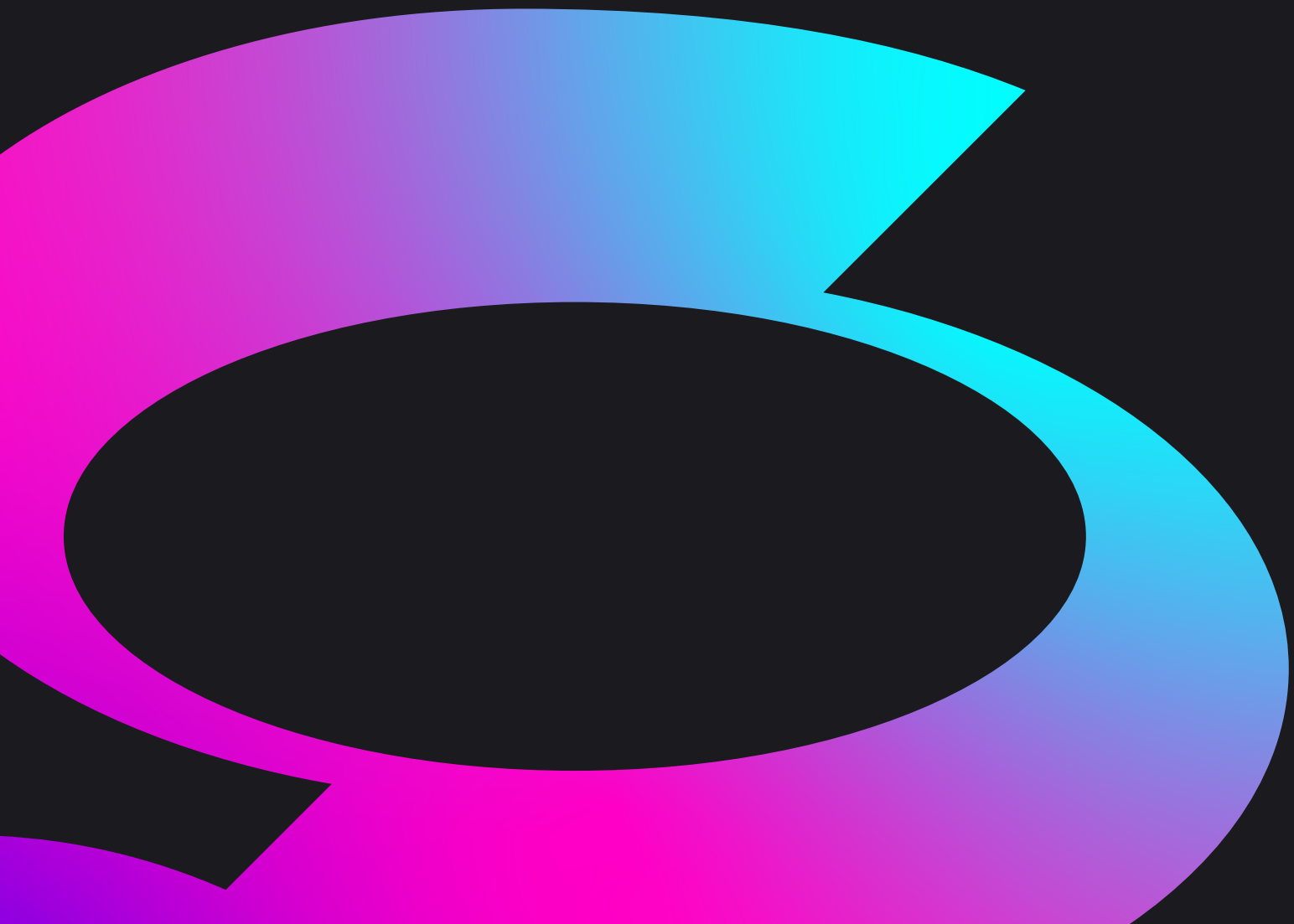
OCTAVE

WHITE PAPER

Who's watching your safety sytem when you're not?



Introduction

You pay a lot of money for your Safety Instrumented System (SIS) and spend a lot on its upkeep. You expect it to always be there for you. To be loyal and to do its job. But can you trust it? Are you really getting your money's worth? Is it doing things you don't know about or not doing things it should? In this paper, we examine many of the necessary administrative tasks associated with managing independent protection layers (IPLs) with particular emphasis on SIS. Some of these tasks are often overlooked, and significant risks exist if they are not done properly.

History

In the 1980s, several major process safety-related accidents occurred that spawned regulatory demand for improved industrial risk management. In response, the ISA convened experts to produce the first version of a standard to address functional safety in modern control systems, known as ISA-84 (1996). Since then, additional standards have been created and repeatedly updated, and then harmonized into international standards IEC 61508, 61511 and others. The result is a large and complex body of knowledge for the design, operation and maintenance of an SIS. Many books and training courses are available for acquiring expertise in this field.

All process industries involving hazardous materials use these systems. Once implemented and operational, SIS owners must track a variety of issues mandated by these standards. This has long been an arduous and error-prone task.

Scope of functional safety

The basics of SIS technology are straightforward, but as with all things engineering-related, the field has its own special jargon. The relevant standards specify the design, implementation, operation and maintenance of:

- Safety Instrumented Systems (SISs) containing multiple
- Safety Instrumented Functions (SIFs) designed to meet a
- Safety Integrity Level (SIL), based on the nature and risk probability of the hazard, and considered as
- Independent Protection Layers, separate from the basic control system.

Some quick definitions are needed to discuss the issue and the potential for improvement.

- Process safety event: What SIS-SIL-SIF-IPL is there?
- Safety Instrumented System (SIS): Hardware and software safety controls on critical process systems, functionally independent of the primary control system but generally linked to it for controlled data exchange.
- Safety Instrumented Function (SIF): A specific control function used to mitigate a hazard, designed in accordance with the SIL rating. An automated equipment trip is an example of a SIF.
- Independent Protection Layer (IPL): A prevention method that is independent of any other such method.
- Safety alarm: An alarm used as an IPL, with a 10% risk reduction credit based on assuming the operator will take a predefined response action. Such alarms must have periodic operator training, suppression control and several other administrative and depiction requirements.
- Process safety time: The amount of time between an initiating event in the process and a hazardous result if a mitigating safety function is not performed.

- SIF design time: The amount of time within which a SIF is designed to successfully complete its mitigating action. The design time must always be shorter than the process safety time. This is sometimes called the "response time" of the SIF.
- SIF demand rate: The assumed frequency that the hazard mitigated by the SIF will occur, and that the SIF will be required to function. The demand rate assumption determines certain aspects of the SIF design.

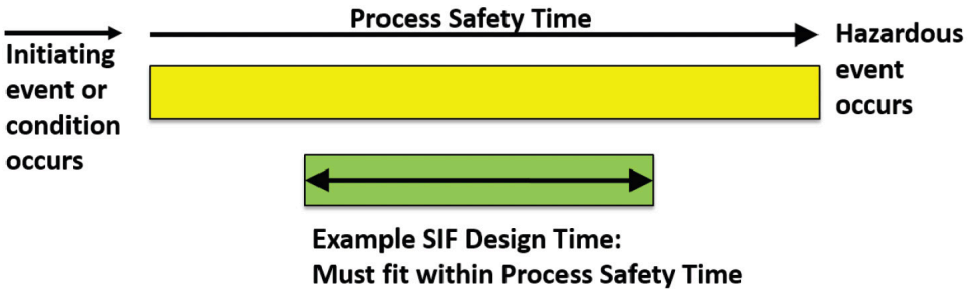


Figure 1: SIF Design Tool

All SISs are designed and managed in a "lifecycle" format. The cycle goes through:

- The initial identification of hazards
- The creation and evaluation of independent layers of protection to mitigate those hazards
- The creation of safety specifications for instrumented protections
- The design of the instrumented protection functions, with an integrity factor determining aspects such as sensor redundancy

Probabilistic risk assessment is involved in all these activities. After the installation and commissioning of the system, the subject of this paper is the operations phase.

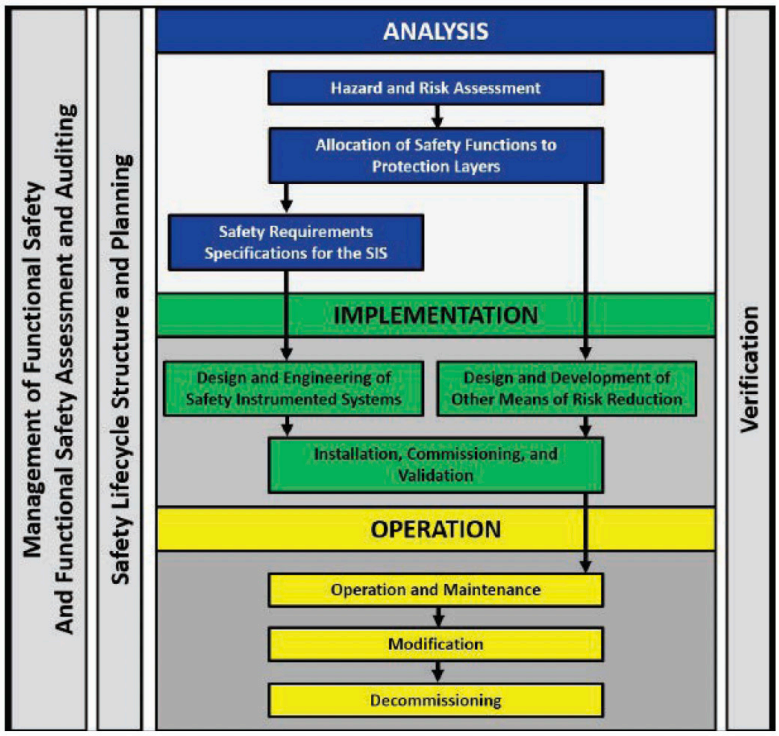


Figure 2: SIS Lifecycle

Ongoing SIS operational requirements, challenges and solutions

During the operations phase, ongoing SIS-related tasks, such as performance monitoring, maintenance, SIF bypassing, management of change, periodic proof testing and ongoing suitability verification, require the attention, time and effort of engineers and technicians.

According to customer feedback, these tasks are often accomplished using inconsistent, error-prone and potentially unreliable methods such as uncontrolled spreadsheets, notes, homegrown applications and manually marked-up drawings and sketches. There is often no organized method applicable to similar SIFs at different sites.

As a result, no "single point source of the truth" exists. The many different operating and maintenance procedures referring to the SIFS may not be consistent with the SIF design. For example, an operating procedure may mention one setpoint for SIF activation, a SIF design document specifies a different one and a maintenance test procedure in the work order generation system has another – it is common for disparate systems to accumulate errors.

Performance monitoring and verification

You must monitor and document that a SIS is performing its function. If you have a comprehensive alarm event analysis solution, such as Octave Tempo Control System Effectiveness (formerly PAS PlantState Integrity) from Octave, then you may already be monitoring all events and changes in connected DCSs and SISs. A solution for the SIS monitoring issue is to record and thoroughly document the activation of any SIF. This includes timestamped records of inputs, activations, outputs and success or failure of the SIF response related to the hazard it mitigates.

SIF performance reports should be automatically created. SIF demand rates were assumed in the design phase and should be verified by actual performance numbers once in service. However, this task is often overlooked in the aftermath of the event that triggered SIF activation. If the demand rate assumption is wrong, the SIF may need redesign (to provide the needed safety) or it may be overly designed, overly complex and scheduled for testing more often than needed. Demand rates for all SIFS should be automatically calculated and tracked for performance and design verification.

Bypass management

SIFs must be capable of being fully or partially bypassed. Many different methods accomplish this, but they must be rigorously controlled. Bypass design is usually for testing or, in some cases, for special operating modes such as startup. Bypassing a SIF introduces additional risk during operation. Special interim procedures may be required during bypass. It is essential that a bypass cannot be missed or forgotten, and yet such things have occurred.

The state of all SIF bypasses should be automatically monitored and made easily visible by operators and staff. Detailed reports on all SIF bypasses, such as their frequency and duration, should be automatically created.

Visualizing risk and exposure

Risk increases when SIFs are bypassed, when testing is occurring or overdue and when other IPLs (such as the control loop in the basic process control system or particular alarms) are unavailable. Historically, determining the risk level of a process because of one or more IPLs being out of service has been impractical or even impossible. Should these conditions occur simultaneously, the plant may be operating in a significantly higher risk condition than intended. In such conditions, the familiar safety model showing that "the holes in the slices of Swiss cheese are lining up" is applicable and accidents are more likely to occur.

If IPL status is automatically monitored to show when they are unavailable, out of service, overdue, bypassed or otherwise compromised, the risk level can be displayed on a dashboard, included in automatic reporting or generate immediate notifications.

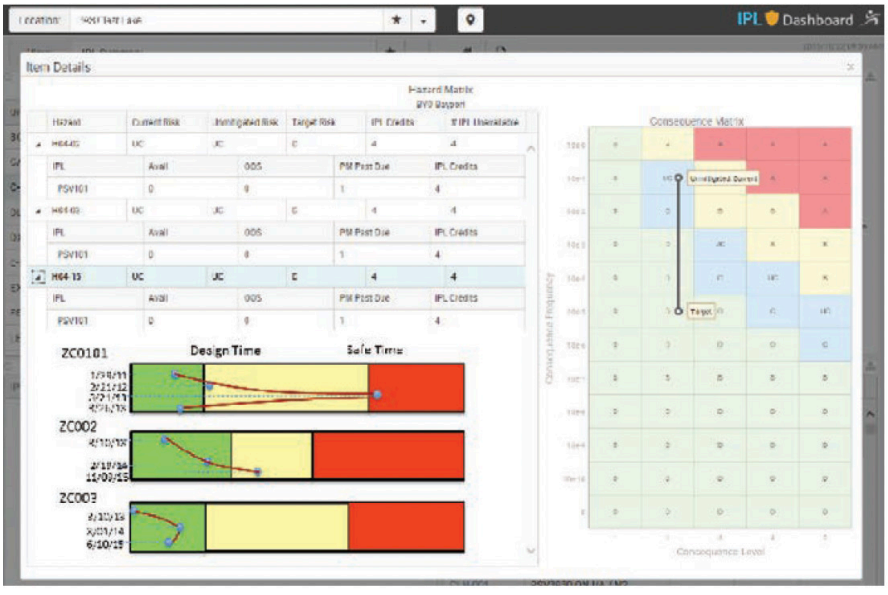


Figure 3: Example of an IPL dashboard using using Octave Tempo Safety System Performance (formerly PAS IPL Assurance)

SIF periodic testing

It is mandatory in both the standards and regulations that SIFs are periodically tested, including the inputs, logic and outputs. This includes verifying that the operator can correctly see the SIF activations. Some of the design assumptions, such as demand rate, determine the frequency of testing. Testing is expensive because of both technician costs and lost production.

Many wait until a scheduled outage for SIF testing, a practice that increases the outage duration and the lost production. This also consumes technical and maintenance resources during turnarounds, potentially delaying other tasks.

Some SIFs are tested online. There is a risk of full SIF activation during online testing. Additionally, this practice is often accompanied by reduced rate operation and hence lost production. Testing should not be done more often than necessary. Feedback on the actual demand rate compared to the assumed rate in design can often lengthen the test interval. There is another technique made possible and practical by closely monitoring and documenting every SIF activation that can lower the frequency of testing.

Potential cost savings in SIF testing

By documenting every SIF activation and the SIF components involved with timestamped records, the trip occurrence can be taken as full or partial credit for a test. The next testing date can, therefore, be reset to be relative to the actual SIF activation. SIF proof testing cost and impact can be significantly reduced.

Cost reduction estimation

The cost savings from using this method are straightforward to estimate.

Cost of proof testing for a typical system:

- One DCS, one SIS, implementing 200 SIFs
- 100 are tested annually, 100 are tested every two years, for 150 total tests per year
- Testing requires an SIS technician, a field technician and a board operator (usually brought in on overtime for the testing) at a total cost of $3,000 per day
- Estimate four SIFs can be tested/verified per working day, or $750 per test

Annual cost of testing is (150 x $750) = $112,500

Potential cost savings:

A successful documented trip, with the automated analysis, constitutes a valid proof test of the SIF. For the system described:

- Of the 150 SIFs tested each year, assume 20% (30) activate in operation sometime before the required proof test
- The date of the fully documented trip resets the one-year or two-year testing interval

- (Note: the reset order can be automatically generated to the maintenance system)
- Cost savings is 30 x $750 or $22,500 each year

In some cases, a much-reduced test scope may still be needed depending on the SIF configuration and some elements of component redundancy.

Monitoring and reporting

An ideal solution would provide for both online dashboards and automatic periodic reports/notifications related to SIS performance. The following desirable capabilities are based on SIS end-users regarding real-world problems and issues.

- Assure the safety system is functional
  - Automatically notify appropriate personnel of failures
  - Bypass management, SIS availability and risk assessment
- Verify accurate SIL determination
  - Document process demands and SIF failures at every activation
  - Improve accuracy of validation testing; “proof test” at process conditions
  - Automatically calculate the SIF demand rate for verifying the design
- Complete documentation of all safety functions and testing
  - Forecast maintenance for testing plans
  - Provide audit evidence as required by IEC 61508 and IEC 61511
  - Minimize the cost of demonstrating compliance
- Bypass management
  - Report bypass status at any time or scheduled
  - Analyze bypass activity, frequency and duration
  - Determine risk level based on current IPL status
- Post-trip start up
  - Immediately understand individual SIF condition post-event
  - Assess any change in risk level
  - Enable quicker and safer return to operation
- Customizable dashboard – a unified view of safety-critical devices
  - Safety system and safety device assessment
  - IPL service status
  - PM maintenance status
  - Web interface and mobile-enabled

Putting a solution together: configuration data for each SIF

An automated solution requires putting together information from several sources. The point structure related to all SIFs is the starting point. This may already be available if the end-user has a comprehensive alarm analysis software package.

The additional SIF information includes:

- Cause and effect matrix: existing design basis of SIF
- Event mapping: link SIF activation, success or failure verification, bypass, un-bypass, test and similar control system logged events that correspond to functions in the matrix
- SIF data: design time, process safety time, testing interval, risk, consequence, severity and SIL level, etc.

The information is used to analyze each SIF's performance. Desirable analyses and reports will track the following:

- SIF activations
- SIF design time vs. process safety time
- Current SIF bypasses, percent of time in bypass or available
- SIF demand rates
- Historical or test performance

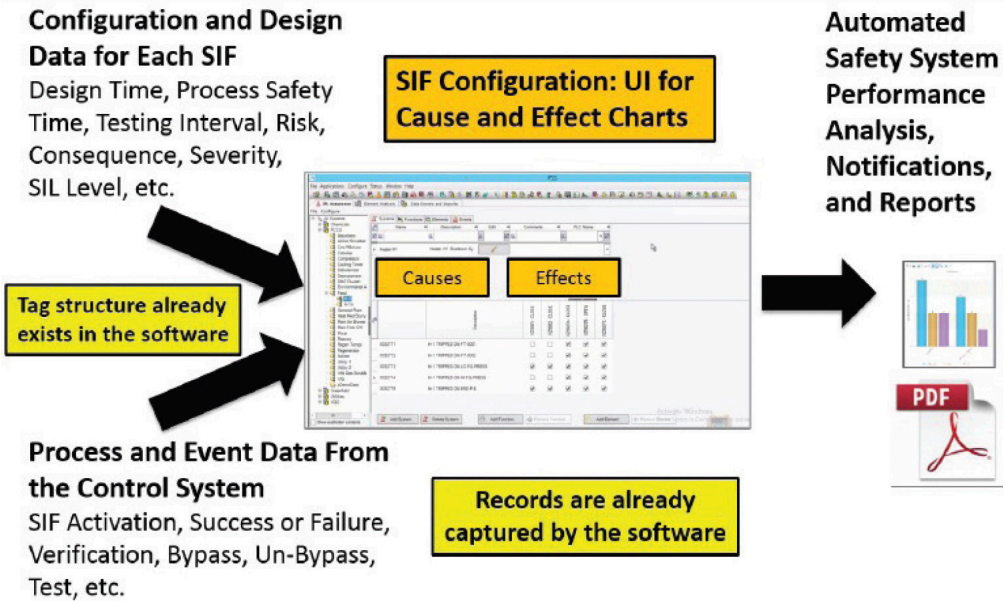


Figure 4: SIF Configuration using Tempo Safety System Performance

Conclusion

Modern plants incorporate a complex SIS technology governed by complicated standards and regulations, containing operational administrative requirements. Compliance with those requirements involves significant work by knowledgeable engineers and technicians. The accuracy of that work is important and yet much of it is often overlooked or accomplished using inconsistent, time-consuming and error-prone methods. You cannot just trust that everything is going well with your SIS.

This report has described all the desirable features of an automated mechanism to address the many issues associated with SIS ownership. Owners of these systems could build such software themselves, a time and resource-intensive effort. Tempo Safety System Performance (formerly PAS IPL Assurance) from Octave addresses this need through automation and offers significant cost savings. It automates the tasks associated with management of safety systems, ensures accuracy, compliance and improves productivity by providing up-to-date knowledge of SIS status and provides notifications when problems arise. SIS performance is monitored and reported. Cost savings related to SIS testing can be significant and are easily documented.

For additional information on Tempo Safety System Performance, please visit Octave.com

About the author

Bill R. Hollifield

Retired Principal Alarm Management and HMI Consultant

Bill is a retired principal consultant responsible for work processes and intellectual property in the areas of both Alarm Management and High Performance HMI. He is a member of the ISA SP-18 Alarm Management Committee, the ISA-SP101 HMI Committee, The American Petroleum Institute's API RP-1167 Alarm Management Recommended Practice committee, and the Engineering Equipment and Materials Users Association (EEMUA) Industry Review Group.

Bill has multi-company, international experience in all aspects of Alarm Management and HMI development. He has 28 years of experience in the petrochemical industry in engineering and operations and an additional 18 years in alarm management and HMI software and services for the petrochemical, power generation, pipeline, pharmaceutical and mining industries.

Bill is co-author of *The Alarm Management Handbook*, *The High Performance HMI Handbook*, and The Electric Power Research Institute (EPRI) Guidelines on Alarm Management for both Power Generation and Power Transmission.

Bill has authored several papers on Alarm Management and HMI and is a regular presenter on such topics in such venues as API, ISA and Electric Power symposiums. He has a BSME from Louisiana Tech University and an MBA from the University of Houston.

In 2014, Bill was made an ISA Fellow.

About Octave

Octave is a leader in enterprise software, turning data into decisive action and intelligence into your edge. Our software solves for and simplifies complexity, from the design and build to operations and protection of people, property and assets – for any scope, at any scale. For decades, we've partnered with customers to sharpen performance, elevate efficiency and amplify results. From factory floors to entire cities, our solutions are tuned to scale up what's possible from day one onward.