COOKBOOK VERSUS PERFORMANCE SIS PRACTICES

Angela E. Summers, Ph.D., P.E, President, and Michela Gentile, Design Consultant, SIS-Tech Solutions

"Cookbook versus Performance SIS Practices," Process Safety Progress, September 2008.

"The Evolution of the Cookbook," 9th Annual Symposium, Mary Kay O'Connor Process Safety Center "Beyond Regulatory Compliance: Making Safety Second Nature," Texas A&M University, College Station, Texas, October 23-24, 2006.

Abstract

A Safety Instrumented System (SIS) is designed to achieve or maintain a safe state of the process when unacceptable process conditions are detected. An SIS is an Independent Protection Layer that is covered by the performance-based standard ANSI/ISA 84.00.01-2004. The risk reduction allocated to the SIS determines its target safety integrity level (SIL). ANSI/ISA 84.00.01-2004 allows a combination of factors to be considered in the verification of the SIL of the SIS. Performance-based practices provide flexibility to users, yet add complexity to the design process, encouraging project teams to reinvent the wheel for even widely used process equipment.

For many engineering applications, prescriptive approaches are favored due to simplicity. These so-called "cookbook" practices were very common in the process industry when ANSI/ISA 84.01-1996 was issued. They are also the backbone of many application standards and recommended practices. The cookbook typically specifies the SIS and maximum proof test interval based on analysis and accepted practice. The user must ensure that the cookbook assumptions are met by the existing equipment and mechanical integrity program. Otherwise, the installed risk reduction may not achieve the expected performance. This paper provides an example of a "cookbook" approach for a simple SIS and illustrates the effect of extending the proof test interval from 1 year to 5 years on its probability of failure on demand.

Introduction

Historically, owner/operators used prescriptive practices to define the safety instrumented system (SIS) requirements. These internal practices were based on experience and industry codes, standards and practices. Internal practices provided the approved equipment technology, architecture, voting, diagnostic expectations, installation details, and maximum proof test interval. Many owner/operators mandated a 6 month to 1 year off-line proof test interval for all SIS devices. These practices were further supported by an approved equipment list, providing the model/version of specific equipment demonstrated to work to the desired reliability in the operating environment.

Due to successful mechanical reliability and preventive maintenance programs, as well as increased profit pressures, many owner/operators extended their maintenance (or turnaround) interval of the process unit. These extensions yielded significant economic returns through increased production and enhanced product quality. While extension of the maintenance interval conflicted with the previously selected proof test requirements, evidence mounted that SIS target integrity could still be achieved, using a combination of off-setting factors. Cookbooks often did not allow adjustment for higher integrity equipment,

additional redundancy, enhanced diagnostics, and on-line testing. The need to tailor the mechanical integrity program to meet required performance caused a shift from prescriptive practices to performance-based practices, starting in the late 1980s and continuing through today.

Cookbook Practices

As early as 1993, CCPS/AIChE published Guidelines for Safe Automation of Chemical Processes [1], which addressed the importance of designing safety systems to meet performance expectations established by a hazard and risk analysis. It also introduced the concept of safety integrity level (SIL) to benchmark SIS performance. SIL was defined by three discrete values related to the probability that the SIS fails to perform as required when needed.

As the SIL is increased from SIL 1 to SIL 3, the performance expectation increases, i.e., the tolerable probability of the SIS failure is reduced. More rigor in the design, operating, inspection, and maintenance practices is required as the SIL increases [2]. The cookbook concept is acknowledged in ANSI/ISA 84.01-1996 [3], where the verification of SIL could be qualitative (comparison to cookbook design) or quantitative. ANSI/ISA 84.00.01-2004 [4] requires a quantitative verification of the SIL.

Prescriptive approaches are still widely used to specify SIS requirements, especially for widely used equipment within a market or an industry sector. “Cookbook” approaches evolve through historical experience and are sufficiently conservative that a wide range of devices can be used to implement the design. Cookbooks generally cover acceptable equipment technology, voting architectures, diagnostic expectations, configuration requirements, and maximum proof test intervals.

During cookbook development, the design should be analyzed to ensure that it fully meets ANSI/ISA 84.00.01-2004. As long as the assumptions behind the cookbook are met by the installation, the SIS design and management are justified by the cookbook. Deviation from any cookbook assumption should be analyzed for its impact on the expected performance.

Performance-based Practices

SISs are covered by the international standard, IEC 61511 [5], which has been adopted in many countries, including the United States, where it is known as ANSI/ISA 84.00.01-2004. SIL is used to establish requirements for various aspects of the SIS lifecycle. ANSI/ISA 84.00.01-2004 has four SILs; however, SIL 4 is strongly advised against in ISA TR84.00.04 Annex J [6] and Guidelines for Safe and Reliable Instrumented Protective Systems Appendix B.4 (CCPS IPS Book) [7]. Inherently safer design or multiple protection layers are recommended to address risk of such magnitude. ISA TR84.00.04 and the CCPS IPS Book provide practical guidance and explanation on ANSI/ISA 84.00.01-2004 requirements.

While ANSI/ISA 84.00.01-2004 provides flexibility, it does not eliminate the need for internal practices, but rather increases their importance. Flexibility can lead to inconsistencies in installation and configuration practices, fault detection and response practices, and proof test facilities. Inconsistency increases the potential for systematic error during long-term operation, especially on sites where personnel are responsible for several process units.

While the standard allows owner/operators to determine how to invest their capital and manage their operating costs, additional capital investment in device redundancy, diagnostic capability, and test/bypass facilities often lowers long term operating costs. Many owner/operators are willing to expend the capital necessary to achieve high reliability installations. However, some owner/operators prefer to

implement systems with lower capital cost and absorb the higher operating and maintenance expenses in the product cost. Fixed cost design/build contracts often increase pressure to shift costs from capital to operating expenses. Prescriptive internal practices help to ensure consistency in the SIS design and management practices across a process facility given an owner/operator's preferences.

Performance-based processes are only as good as the data and information fed into them. Operating experience and historical performance are more essential than ever to the development and verification of the risk reduction strategy. Experience gained in equipment operation yields a greater understanding of normal and abnormal process operation. Equipment integrity in the operating environment is monitored and tracked, allowing design assumptions to be verified. Operating and maintenance history affects two key areas: 1) the risk assessment that identified potential hazardous events and developed the risk reduction strategy and 2) the design basis that reflects the known effectiveness of SIS equipment in the operating environment.

Example of An Approach

Prescriptive approaches are often favored over performance-based due to the apparent simplicity offered by the cookbook. However, the user must understand its assumptions and limitations and ensure that the SIS as designed, operated, tested, and maintained agrees. A cookbook is essentially a recipe with prescribed limits on the ingredients. When the design meets the recipe, the performance of the system is predictable based on past history and analysis. Violate the assumptions and the installed SIS may not meet expectations.

A significant limitation of many cookbooks is the choice of a base architecture. This example considers only a single process variable measurement and single process action. The performance of an SIS is dependent on the sum of its parts. If more process variable measurements are required to detect the unacceptable process condition or more process actions are required to achieve or maintain the safe state, the SIS may not achieve the SIL indicated in this section even if the sensors and final elements are designed similar to that shown in the illustrations and the design meets all other assumptions discussed in this section.

The assumptions for this example:

- SIS is managed throughout it's lifecycle to achieve the required core attributes.
- Equipment is specified to fail to the safe state on loss of power and other support systems.
- Redundant sensors are installed on separate process connections.
- The logic solver is separate and independent of the basic process control system (BPCS) such that failures of the BPCS do not result in simultaneous failure of the SIS.
- Detected failures result in the sensor voting to the trip state. 2oo2 voting degrades to 1oo1 on detected failure. 2oo3 voting degrades to 1oo2 on detected failure.
- The proof test fully validates the required operation of each subsystem and the inspection and preventive maintenance activities are sufficient to ensure the equipment is maintained in the "as good as new" condition.

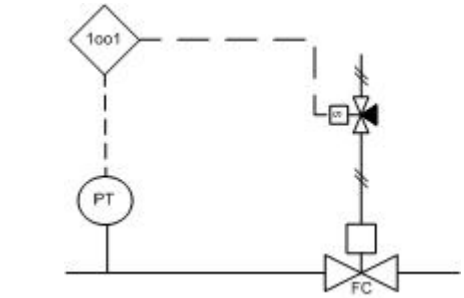
The CCPS IPS Book Appendix D [7] provides more details on the impact of these assumptions on the system performance. This section provides examples of a "cookbook" approach and illustrates how the architecture changes as successively higher SILs are required. The effect of extending the proof testing interval from 1 year to 5 years is presented for a theoretical system implementing one function.

Scenario

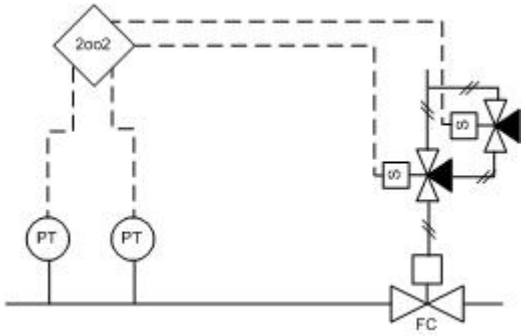
The scenario involves protection of a pipeline from overpressure due to various causes. Pipeline failure could release a large amount of highly hazardous chemicals with a high likelihood of significant harm to people and to the surrounding equipment. A safety instrumented function (SIF) is used to detect high pressure and to isolate the pressure source taking the process to the safe state.

SIL1

Figure 1A provides a simple independent SIL 1 SIF. A single sensor is used to detect the pressure. The logic solver de-energizes a solenoid operated valve (SOV) removing air from the valve actuator, allowing the valve to go to its specified failed closed (FC) position. Figure 1B provides a higher reliability (low spurious trip rate) SIL 1 design by implementing 2oo2 voting for the sensor and SOV. 2oo2 voting SOVs have been proven through decades of use to achieve high integrity and reliability when instrument air quality is good and the SOVs are properly maintained.



A

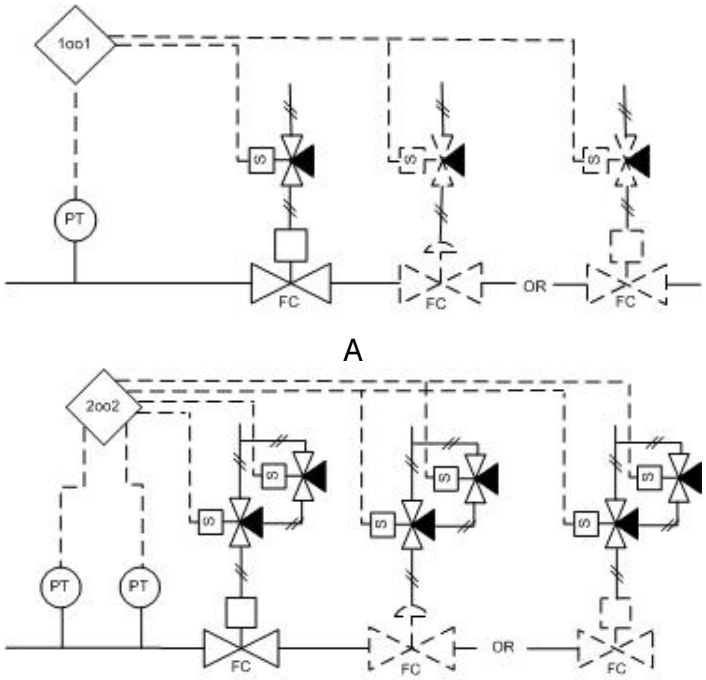


B

Figure 1: Example SIL 1 SIF (A) and High Reliability SIL 1 SIF (B).

SIL 2

Simplex pressure transmitters can be used in SIL 2, given a reasonable test interval and the use of good quality equipment. Figure 2A provides an SIL 2 SIF with an option to use an additional block valve or to share the control valve as a second means of process isolation. The control valve cannot be used, unless it fully meets the SIS design basis (e.g., integrity, independence, leak tightness, response time, etc.). This is illustrated in Figures 2A and 2B by the “OR” and the dashed representation of the control valve and block valve. Figure 2B provides a higher reliability SIL 2 design using 2oo2 voting sensors and SOVs.



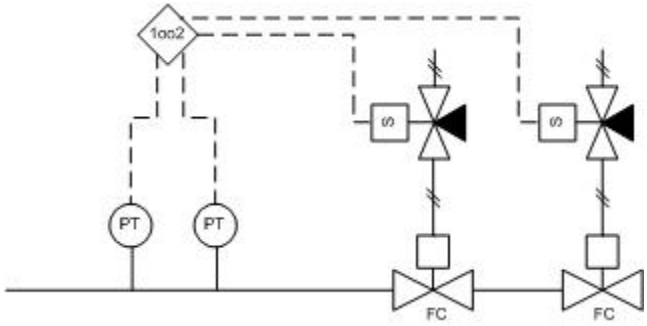
A

B

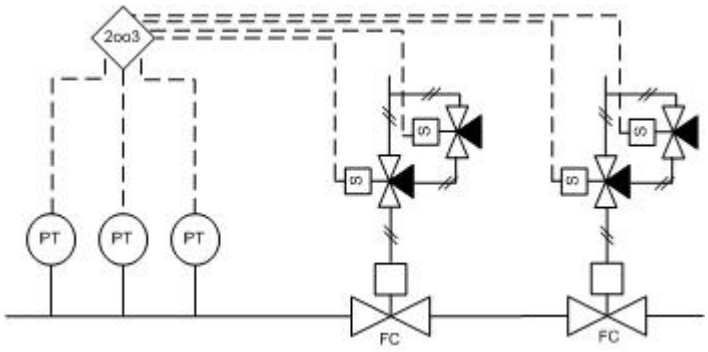
Figure 2: Example SIL 2 SIF (A) and High Reliability SIL 2 SIF (B).

SIL 3

SIL 3 is the highest level of performance typically expected from an SIF in the process industry. For SIL 3, systematic errors must be minimized through the use of fault tolerance. Fault tolerance must be provided in the sensors, logic solver, final elements, and any required support systems. Figure 3A provides an SIL 3 architecture that is fault tolerant against dangerous failures using 1oo2 voting sensors and dedicated block valves. Figure 3B provides a high reliability SIL 3 architecture using 2oo3 voting sensors and 2oo2 SOVs.



A



B

Figure 3: Example SIL 3 SIF (A) and High Reliability SIL 3 SIF (B).

Equipment and Data Selection

A pressure transmitter is used to detect pressure, providing an analog electrical signal. When transmitter faults are detected, the transmitter is configured to drive the output signal to the trip condition. For redundant process measurements, the analog signals are compared. When the signal deviates more than 5%, a deviation alarm is issued, allowing early detection and repair of transmitter problems. Diagnostic coverage factors of 80% and 90% are assumed for the signal comparison in 2oo2 and 2oo3 voting, respectively. The common cause or beta factor for the redundant pressure transmitters is assumed to be 2%.

The logic solver is a trip amplifier that takes an analog signal and changes its output state from energized to de-energized at a preset value of the input signal. It meets SIL 2 as a single device and SIL 3 in a 1oo2 or 2oo3 architecture. Trip amplifiers have been used for many years in various industries and are simple, easy to maintain devices.

Block valves are modeled for simplex and redundant valve cases. The block valves are spring return, fail-closed and are actuated using de-energize-to-trip SOVs. The SOVs are low power and pilot assisted. The beta factor for the redundant SOVs and valves in a clean operating environment is assumed to be 0.1%.

The equipment failure rates are shown in Table 1. The equipment is assumed to be repairable, and the mean time to repair is 72 hours.

Table 1: Equipment Data

Device Type	Failure Rate	
	Dangerous (Per Year) λ^D	Spurious (Per Year) λ^{SP}
Pressure Transmitter	6.67E-03	1.25E-02
Trip Amplifier	1.40E-03	5.10E-03
Solenoid Valve, Low Wattage	1.67E-02	3.33E-02
Block Valve, Ball	1.67E-02	6.67E-03

Analysis

With a proof test interval of 1 year, the illustrated architectures easily meet the SIL requirements (see Table 2). A cookbook design using simple architectures and annual testing can be used to meet the SIL requirements. However, given the reality of less frequent turnarounds, the time and cost involved in proof testing the SIF, and the perceived safety margin provided by redundancy, the natural tendency is to extend the test interval.

If the proof test interval is extended, the performance is significantly affected and the PFD_{AVG} increases. This effect is illustrated in the Table 2, which summarizes the results for the architectures shown in Figures 1 through 3. An important assumption in this analysis is that the equipment failure rate is not affected by the reduction in inspection, preventive maintenance, and / or proof testing. When maintenance is performed less often, the mechanical integrity program may fail to detect and correct incipient and degraded failure, allowing these failures to progress to safe and dangerous failure. Reduced proof testing also decreases the number of times that the mechanical components are moved (exercised), which may increase the likelihood that these components will hang-up or stick, increasing the dangerous failure rate.

Table 2: PFD_{AVG} at different test intervals

Required SIL	Case	PFD_{AVG} @ TI=1	PFD_{AVG} @ TI=3	PFD_{AVG} @ TI=5	$MTTF^{SP}$ @ TI=1
SIL 1	A	2.10E-02	6.25E-02	1.04E-01	17.4
PFD_{AVG}: 1.0E-02 to 1.0E-01	B	2.83E-02	8.38E-02(1)	1.39E-01	112.5
SIL 2	A	4.41E-03	1.48E-02	2.73E-02	10.3
PFD_{AVG}: 1.0E-03 to 1.0E-02	B	3.54E-03	1.41E-02	2.97E-02	56.2
SIL 3	A	3.34E-04	2.67E-03	7.24E-03	8.5
PFD_{AVG}: 1.0E-04 to 1.0E-03	B	6.95E-04	5.84E-03	1.60E-02	56.2

(1) While technically within the SIL 2 range, this value would not meet SIS-TECH's internal practice when states that the number must be less than 8.00E-02 unless approved by a senior manager.

The shaded cells indicate cases that do not meet, or only marginally meet, the required SIL. When the proof test interval is extended to 3 years, only the simple SIL 1 architecture (1A) meets the PFD_{AVG} requirements. At 5 years, none of the architectures meet the PFD_{AVG} requirement.

As would be expected, the MTTFSP (mean time to failure spurious) achieved by the Case B architectures (e.g., high reliability) is longer than the simple architectures (Case A). The drawback of the high reliability architectures is the larger number of devices involved in achieving the safe state, which yields a higher PFD_{AVG}. However, the SIL 2 Case B architecture illustrates how the diagnostic coverage can reduce the impact of the larger number of devices. The diagnostics provided for the input sensors reduces the PFD_{AVG} by allowing detection of degraded operation. The PFD_{AVG} for the high reliability case is improved over the low reliability case even with the larger number of devices.

From an operating expense standpoint, the redundant architectures yield benefits from two perspectives. First, the operators get redundant process measurements, making system indication more reliable. Second, from a maintenance perspective, the 2oo2 SOVs can be maintained and tested on-line. The architecture significantly reduces the frequency of spurious closure of the block valve due to fuse, wiring, or coil failure In some processes, block valve closure could block-in a pump or compressor, potentially causing other process hazards and damaging the equipment.

Conclusions

For many years, engineers have followed prescriptive practices to achieve SIL 1, 2, or 3. These cookbook practices provided specific recipes for achieving certain performance levels. Cookbooks define the acceptable equipment technologies, voting architectures, diagnostic expectations, configuration requirements, and maximum proof test intervals. Cookbooks should be sufficiently conservative to ensure the claimed SIL for the range of application of the cookbook.

The analysis illustrated the pronounced effect extending the proof test interval on the PFD_{AVG} for a very simple SIF. All of the recipes provided in the example met the claimed SIL at annual proof testing. None met the claimed SIL at 5 year proof testing.

References

Guidelines for Safe Automation of Chemical Processes, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York (1993).

Gentile M. and Summers A.E., "Random, Systematic, and Common Cause Failure: How Do You Manage Them?" Process Safety Progress, Vol. 25, No. 4, New York (2006).

"Application of Safety Instrumented Systems (SIS) for the Process Industry," Instrumentation, Systems, and Automation Society, ANSI/ISA S84.01-1996, Research Triangle Park, NC (1996).

"Functional safety: safety instrumented systems for the process sector," Instrumentation, Systems, and Automation Society, ANSI/ISA 84.00.01-2004, Research Triangle Park, NC (2004).

"Functional safety: safety instrumented systems for the process sector," International Electrotechnical Commission, IEC 61511, Geneva, Switzerland (2003).

"Guidelines on the implementation of ANSI/ISA 84.00.01–2004," ISATR84.00.04, Instrumentation, Systems, and Automation Society, Research Triangle Park (2005).

Guidelines for Safety and Reliable Instrumented Protective Systems, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York (2007).