Safety controls, alarms, and interlocks as IPLs

Angela E. Summers, Ph.D., P.E.
SIS-TECH Solutions
12621 Featherwood Dr. Suite 120,
Houston, TX 77034

Keywords: safety controls, alarms, interlocks, SIS, BPCS, process control, layers of protection analysis

Abstract

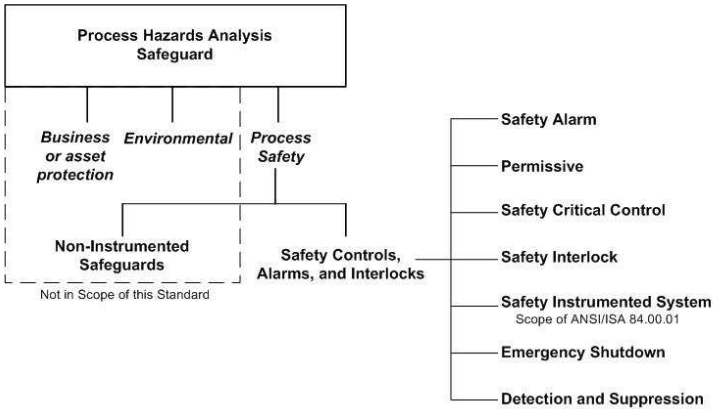
Layers of Protection Analysis (LOPA) evaluates the sequence of events that first initiate and then propagate to a hazardous event. This semi-quantitative risk assessment technique can expose the role that automation plays in causing initiating events and in responding to the resulting abnormal operation. Automation that is specifically designed to achieve or maintain a safe state of a process in response to a hazardous event is now referred to as safety controls, alarms, and interlocks (SCAI).

Guidelines for Initiating Events and Independent Protection Layers addresses four basic types of SCAI: safety controls, safety alarms, safety interlocks, and safety instrumented systems (SIS). This article discusses the design, operation, maintenance, and testing practices necessary for SCAI to be considered as independent protection layers (IPL). It also provides guidance on claiming multiple layers of protection in the basic process control system.

WHAT ARE SCAI?

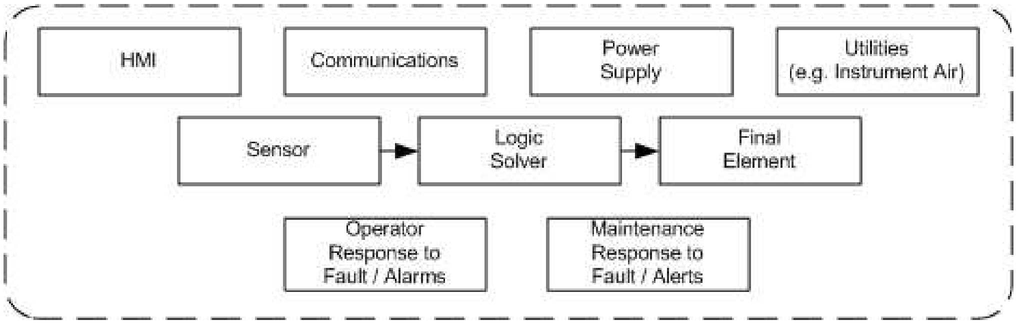
SCAI or Safety Controls, Alarms, and Interlocks are process safety safeguards implemented with instrumentation and controls, used to achieve or maintain a safe state for a process, and required to provide risk reduction with respect to a specific hazardous event (ISA 84.91.01-2012 [1,2]). They are the safety subset of instrumented protective systems (IPS), which are discussed in Guidelines for Safe and Reliable IPS [3]. An IPS is any instrumented system that addresses risk related to health and safety effects, environmental impacts, loss of property and business interruption costs. As shown in Figure 1, there are many terms that can be used to further classify SCAI.

Figure 1. Classification of SCAI (adapted from ISA 84.91.01-2012 [2])


Process Hazards Analysis Safeguard
Business or asset protection
Environmental
Process Safety
Non-Instrumented Safeguards
Not in Scope of this Standard
Safety Controls, Alarms, and Interlocks
Safety Alarm
Permissive
Safety Critical Control
Safety Interlock
Safety Instrumented System
Scope of ANSI/ISA 84.00.01
Emergency Shutdown
Detection and Suppression

As with any IPL, SCAI should be independent of the initiating cause and any other IPL used for risk reduction for a particular hazardous event. To understand its capability in stopping the event, the SCAI function must be clearly identified, for example, what does it detect, what is the setpoint, how does it affect the process, how fast does it need to act, and how does the process respond to its action. Typically, SCAI have sensors to detect the process condition, a logic solver to determine what action to take based on the process condition, and final elements to take action on the process (Figure 2). The decision and action can be manual (e.g., operator response to a safety alarm) or automatic (e.g., via continuous control, interlock, or safety instrumented system [SIS]). SCAI also includes other interconnected equipment, such as human interfaces, wiring, process connections, communications, and utilities, which are necessary in order to achieve the desired functionality and to operate and maintain the SCAI.

Figure 2. Example elements required for SCAI successful operation


HMI
Communications
Power Supply
Utilities (e.g. Instrument Air)
Sensor
Logic Solver
Final Element
Operator Response to Fault / Alarms
Maintenance Response to Fault / Alerts

SCAI are complex systems requiring many different devices to operate successfully in order to stop the hazardous event propagation. The logic solver technology is typically implemented using electrical, electronic, or programmable electronic equipment. Older installations may use mechanical switches, which change state based on manipulating pneumatic (or hydraulic) flow and pressure. Field device technology ranges the gamut from simple switches to complex analyzers. While there is no limit on the designer's choice, the technology must provide the desired level of risk reduction in the operating environment and under the user's management system. As technology moves from the drawing board to sustained operation, the proof of integrity must also move from estimated performance to historical operation as evidenced through site mechanical integrity records. Historical demonstration of successful prior use is essential for assuring that installed equipment is fit for service.

The ability of SCAI to achieve the desired functionality and the claimed risk reduction is limited by the performance achieved by the installed equipment. Each SCAI device has distinct failure modes and has a failure rate that contributes to the overall SCAI performance. For this reason, equipment is selected based on its expected capability in the operating environment, but the SCAI is judged by the cumulative capability of the system. The actual level of risk reduction achieved should be substantiated by mechanical integrity and human reliability data. The records associated with any SCAI should confirm that the equipment operates as specified during all intended operating modes. Failure tracking and analysis is important to verify hazards and risk analysis assumptions and to support continuous improvement.

SCAI PRACTICES

According to Guidelines for Initiating Events and Independent Protection Layers, SCAI specifications should consider:

- Functional requirements.
- Configuration, installation, and maintenance requirements to achieve and sustain the claimed performance.
- SCAI Failure modes, means used to detect these failure modes, and expected system and operator response to detected failure.
- Compensating measures required to continue safe operations with faulted SCAI
- Conditions required to safely bypass the SCAI (includes override or manual operation) and any compensating measures to be in place during bypass.
- Conditions required for safe reset of the SCAI.

SCAI equipment should be sufficiently robust to withstand the actual stresses of the operating environment and provide the required integrity and reliability. Some technologies used in control applications may not be acceptable for SCAI due to inadequate installation history, poor in service reliability/integrity, or unpredictable/erratic behavior. For example, wireless technology as defined by ISA 100.11a [4] is not generally considered an acceptable technology for executing SCAI, but may be used for monitoring, status or diagnostic communication [5].

An equipment list should be maintained which identifies SCAI equipment by a unique designation, such as a tag number or equipment ID that is traceable to the mechanical integrity requirements necessary to maintain the required integrity and reliability throughout its life. Mechanical integrity includes a variety of activities, such as inspection, calibration, preventive maintenance, repair/replacement, and proof testing.

Inspections and proof tests are conducted as necessary to identify and correct equipment deficiencies. Visual inspection and preventive maintenance may need to be conducted frequently when equipment is installed in harsh process and environmental conditions. Inspection and proof test are performed according to a procedure that ensures that the required operation is demonstrated to the degree feasible under safe conditions. Typical information recorded includes as found/as left conditions, the tester, when tested, the procedure and equipment used, and calibration records.

It is inherently safer to implement SCAI equipment such that it takes the safe state action on failure rather than fails to an alarm (or dangerous) state. Examples of failures to consider are loss of signal, out of range values, loss of communications, power failure, instrument air failure, and loss of other utilities. If it is intended to continue operation of the process with out-of-service SCAI equipment, the risk should be assessed and compensating measures should be provided to address increased risk. Out-of-service periods should be tracked and minimized to the degree possible through equipment design and maintenance practices.

Documented procedures, training, and auditing ensure effective management of change control for the hardware and software. As with any IPL, SCAI are only bypassed (e.g., suppressed or setpoint changed) with administrative approval and after deployment of any necessary compensating measure. Administrative approval may involve formal MOC, bypass control procedures, or special operating procedures.

Information about SCAI should be included in operating procedures, since the operation of SCAI affects the process and often requires that the operator take action. When programmable electronic systems are used, management of change and access security procedures are needed to ensure that changes to the embedded software and application program are reviewed and approved. Any change potentially affecting SCAI should be examined to determine the requirements for validating the functionality prior to the SCAI being placed in service. Access to engineering interfaces should also be controlled to reduce human error and prevent compromise of the system.

BPCS VERSUS SIS

The type of equipment and the design and management practices used to implement SCAI limits achievable performance. SCAI can be implemented using basic process control system (BPCS) or safety instrumented system (SIS) equipment. To be counted as IPL, SCAI are designed and managed to achieve an order-of-magnitude risk reduction (PFD ≈ 0.1). Because of the typical design and management of BPCS equipment, SCAI implemented with BPCS equipment is limited to an order-of-magnitude risk reduction. Higher claims (e.g., PDF < 0.1) can be supported by a SCAI designed and managed in compliance with IEC 61511.

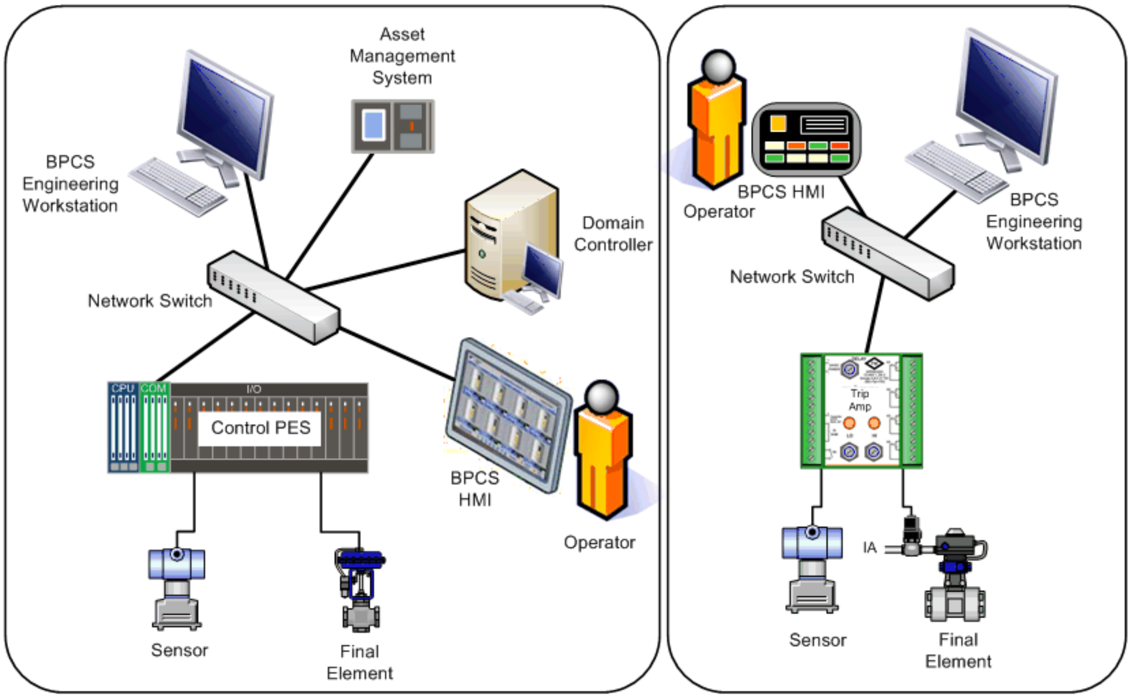
SCAI claimed as IPL are limited to PFD = 0.1, unless they are designed and managed per IEC 61511. IEC 61511 describes the conditions necessary to allow two BPCS loops to be credited for the same hazardous event with an overall claim of PFD = 0.01. IEC 61511 identifies independence and separation of non-SIS (including control, diagnostics, and SCAI) and SIS as a critical requirement; otherwise the implementation must meet the full requirements of IEC 61511.

BPCS

Type

BPCSs are most commonly implemented in pneumatic control loops, programmable logic controllers (PLCs), distributed control systems (DCS), discrete control systems (e.g., on/off, relay), and single loop controllers (Figure 3).

Figure 3 ***Examples of BPCS using PES and Trip Amplifier Technology***



Practices

The design and management of BPCS is usually focused on ensuring that it can reliably perform the control functions that maintain normal operation, such as proportional-integral-derivative and batch (or sequential) controls. The response to detected faults and momentary loss of communication is generally continued process operation using the last "good" value. Failure of the BPCS in executing normal control functions is one of the leading causes of hazardous events. A BPCS is also capable of executing other functions such as alarming and process shutdown when special design and management practices are followed.

Performance Capability

A BPCS's performance is limited by its hardware and software design. Most BPCS have little online redundancy in the input/output cards (I/O) or in the CPU and have limited diagnostic coverage of these components. When redundancy is available, it is generally a backup processor that does not operate until internal diagnostics (typically not themselves redundant) detect a problem. Redundant BPCS are generally composed of hot standby or hot swappable processors, which significantly limits the potential performance claim.

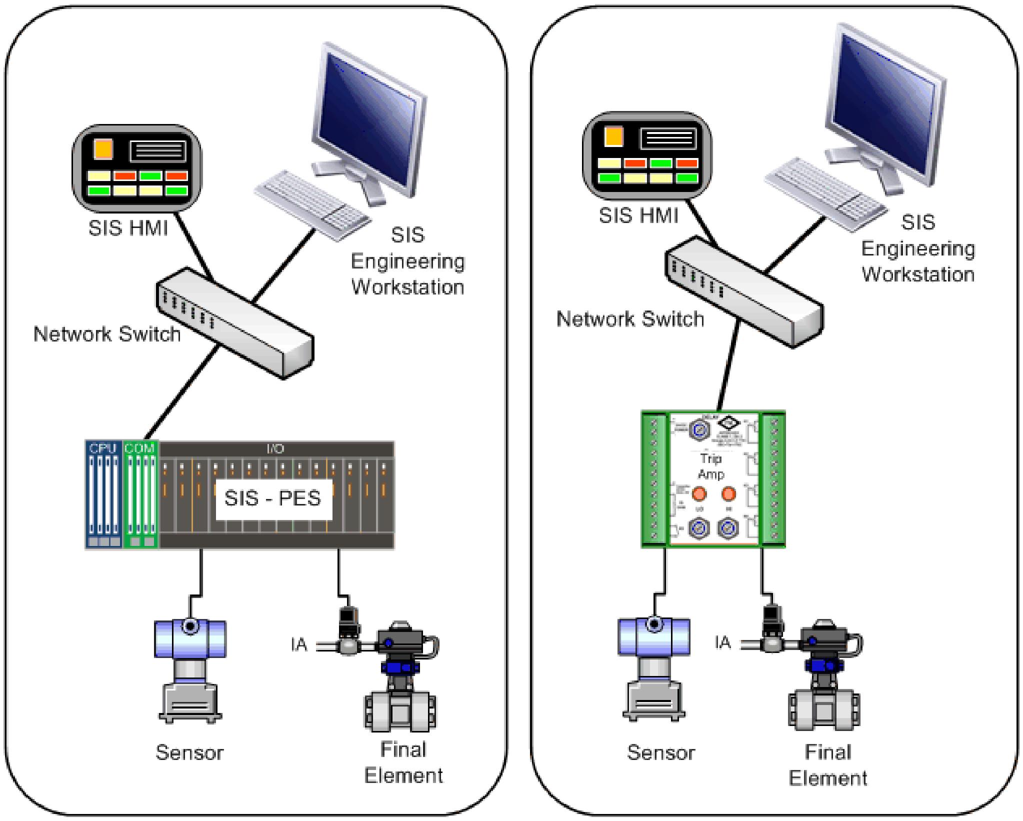
With multiple devices required to operate correctly, individual devices within the SCAI usually need to achieve an installed performance an order of magnitude better than the required system performance. For example, if it is desired to claim that a BPCS loop achieves a PFD = 0.1, the BPCS controller would need to have a PFD < 0.01. Industry data (ISA TR84.00.04 [6] and PDS Data Handbook, 2010 [7]) does not support a PFD < 0.01 claim for controllers that are not designed and managed in compliance with IEC 61511. The typical design and management practices associated with BPCS equipment limit its risk reduction capability to one order of magnitude per logic solver (e.g., controller).

SIS

Type

SIS are most commonly implemented using discrete control systems (e.g., on/off relay) and programmable electronic systems (Figure 4).

Figure 4 ***Examples of SIS using PES and Trip Amplifier Technology***



Practices

The design and management of the SIS ensures that it can reliably take action to achieve or maintain a safe state of the process to stop propagation of the hazardous event. In the process industrial sector, the term SIS applies to instrumentation and controls designed and managed in accordance with international standard IEC 61511 [8].

Use of programmable electronic systems (PES) requires diagnostics on input and output cards to detect stuck-on (or stuck-off) conditions and on the main processor to detect a stuck (or locked-up) program execution. These diagnostics are necessary for the programmable electronic system to meet the minimum requirements for SIL 1 (PFD < 0.1).

A PES relies on software embedded and application to execute the internal and user functions of the system. This software is patched, upgraded, and updated under a revision control system that ensures adequate testing and validation. Changes to embedded software require full system validation (ISA TR84.00.03 [9]), while changes to the application program must be tested based on their traceable impact to the system (IEC 61511[8]).

Data communication and engineering interface to PES should be separated from other credited SCAI where possible. Any interconnections that can compromise performance should be protected with firewalls and strict access security provisions.

Diagnostics are not required for hardwired logic solvers, such as relays or trip amplifiers, which have low failure rates and well-defined failure modes. Hardwired logic solvers are separate and diverse from other control systems and are not vulnerable to cyber security risks or data highway corruption.

Performance Capability

While it has many prescriptive requirements, IEC 61511 is fundamentally a performance-based standard that requires the establishment of the safety integrity level (SIL). The target SIL is normally determined using some type of risk assessment. For example, a layer of protection analysis (LOPA) determines the PFD that the SIS needs to meet in order for the event risk to be reduced below the risk criteria. The required PFD establishes the target SIL. Table 1 shows the relationship between SIL and the PFD ranges.

Table 1. Safety Integrity Level Relationship to PFD and Risk Reduction (CCPS, 2013)

SIL Level	PFD is greater than:	But less than:	Risk Reduction
SIL 1	0.01	0.1	1 order of magnitude
SIL 2	0.001	0.01	2 orders of magnitude
SIL 3	0.0001	0.001	3 orders of magnitude

When claiming SIL 2 and 3, the standard has minimum redundancy requirements to protect against systematic errors. Redundant devices and signal paths using independent sensors, controllers, or final elements to provide the same function may be necessary to ensure SIL 2 and are required to ensure no single points of failure for SIL 3.

THE 4 SCAI AND LOPA

SCAI are instrumented safeguards identified during the hazard identification and risk assessment that are necessary to achieve risk reduction related to a potential process safety event. As discussed earlier, SCAI can be referred to by many other names – the key to the identification is the function's purpose with regard to the event. This article divides SCAI into four types of systems: control, alarms, interlocks, and SIS [5].

IEC 61511 restricts the PFD claim that can be made for a BPCS loop to ≥ 0.1, while the PFD claim for SIS can be < 0.1 for SIL 1. This limit is due to the higher potential for systemic errors to impact the performance of the BPCS during its life. The functional safety management system of IEC 61511 goes beyond typical process safety management practices and requires rigorous assessment, verification, validation, and change management for any activity potentially impacting the SIS. For the purposes of LOPA, both are given the rounded value of 0.1. Regardless of the PFD performance claim, SCAI must be under an appropriate mechanical integrity program that includes documentation, procedures, and administrative controls (ANSI/ISA 84.91.01 [2]).

Safety Controls

These normally operate to support process control (or regulatory control) and prevent process excursions by taking action to maintain the process in the normal operating range. These controls are not typically designed or managed in accordance with IEC 61511, so they may also be referred to as BPCS IPL. The risk reduction claimed for a safety control (which does not conform to IEC 61511) must not be greater than 10 (IEC 61511 Clause 9.4.2). In LOPA, a risk reduction factor of 10 or PFD = 0.1 is used.

Safety Alarms

These initiate an alarm that requires that the operator take action in accordance with a response procedure to stop the hazardous event propagation. The risk reduction claimed for a safety alarm (which does not conform to IEC 61511) must not be greater than 10 (IEC 61511 Clause 9.4.2). The safety alarm includes not only the alarm but also the interfaces and final control elements used by the operator to take the required action. Refer to ANSI/ISA 18.2 [9] and IEC 61511 for additional guidance related to the instrumentation and control design. Operator reliability in responding to the alarm should also be considered in making claims for safety alarms. Operator knowledge of required actions and the capability to take timely action should be validated using tests, drills, or simulated environments. When these conditions are met, a risk reduction factor of 10 or PFD = 0.1 is used in LOPA.

Safety Interlocks

These take automatic action to achieve or maintain a safe state of the process when a process variable reaches a defined limit outside the normal operating envelope. When an interlock is not designed and managed in accordance with IEC 61511, it may also be referred to as a BPCS IPL. The risk reduction claimed for a safety interlock (which does not conform to IEC 61511) must not be greater than 10 (IEC 61511 Clause 9.4.2). With proper design and management, a risk reduction factor of 10 or PFD = 0.1 may be used. When the safety interlock is designed and managed per IEC 61511, it is an SIS.

SIS

These consist of instrumentation and controls designed and managed in accordance with IEC 61511 that take action to achieve or maintain a safe state of the process in response to a process demand. Unless the BPCS equipment is designed and managed per IEC 61511, the SIS equipment must be independent and separate from the BPCS equipment to the extent that the safety integrity of the SIS is not compromised (IEC 61511 Clause 11.2.4). SIS are typically designed to operate in low demand mode but may operate in high demand/continuous mode.

The ISA84 committee has developed a series of complementary technical reports to provide guidance and practical examples related to various SIS topics and applications. Three of these technical reports, ISATR84.00.02 [11], ISATR84.00.03 [9], and ISATR84.00.04 [6], provide a comprehensive overview of the SIS lifecycle and associated requirements.

LOPA APPROACH A VERSUS APPROACH B

In the initial LOPA guideline [12], two approaches were presented for considering the BPCS in LOPA. Approach A allowed the identification of BPCS as providing an IE or an IPL, while Approach B provided the basis for additional analysis of BPCS design and management.

Whether choosing Approach A or B, special consideration should be given to situations where low-demand mode functions are implemented in a BPCS. It is inherently safer to implement low-demand mode functions in a separate and independent SIS that is specifically designed and managed for safety interlocks. Furthermore, some application-specific practices require that safety interlocks be implemented in an independent SIS.

Approach A

The key criteria are (1) the initiating cause is not related to the failure of BPCS equipment and (2) the BPCS IPL is properly designed and managed to claim one order-of-magnitude risk reduction. This approach takes the position that a single BPCS loop failure invalidates all other functions that could be implemented in BPCS. It is used for LOPA because its rules are clear and conservative. It provides a high level of protection against common cause failures between the BPCS implementing control loops that can initiate an event and the SCAI implementing protection layers to prevent the event.

Approach B

This approach potentially allows a maximum of two loops within BPCS to be identified for the same scenario (i.e., cause-consequence pair). Approach B assumes that each BPCS is designed and managed such that it is capable of supporting the specified function and is sufficiently independent from the other such that the likelihood (probability) of simultaneous failure is low enough to support another order-of-magnitude risk reduction. Approach B requires that the analyst be knowledgeable in the BPCS design architecture, has adequate data available on the actual performance of the BPCS, and understands how to identify and account for common cause failures between the different automation layers.

Analytical Approach

LOPA is not the best tool for detailed evaluation of whether the BPCS architecture can support two loops. Analysis and test data should demonstrate that the two particular BPCS are designed and managed in a manner such that the two BPCS loops, in combination, can achieve the overall performance claim of ≈ 0.01/year. Consider use of advanced quantitative analysis techniques, such as fault tree analysis, to ensure that common cause (including systematic errors) is assessed fully. Since a BPCS failure could result in the simultaneous loss of control and safety protection, carefully examine the independence and separation of the BPCS executing the control loops and the SCAI. When strict independence is not maintained, the analysis can become quite complex necessitating higher expertise and knowledge of automation design.

At a minimum, the system analysis should include [5]:

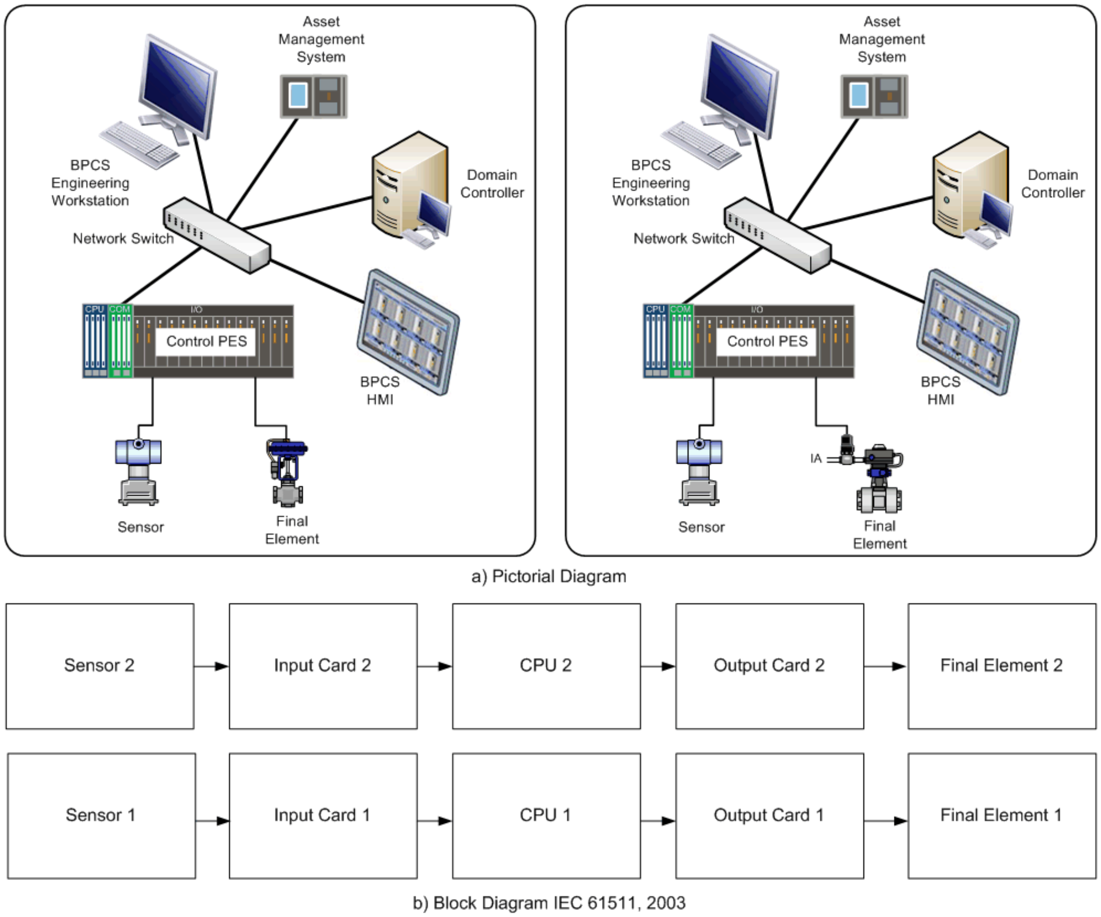
- Assessment of potential common cause, common mode, and systematic failures between the BPCS IE and IPL or the two BPCS IPLs to determine that their impact is sufficiently low as compared to the performance claim.
- Written specification covering all functions within the system, for example, instrument diagrams, P&IDs, loop diagrams, functional specifications.
- For the Generic Data approach to validation, the assessment of previous historical performance of the BPCS logic solver, input/output cards, sensors, final elements, human response, etc. (note: manufacturer information must be examined critically to ensure that it applies to situations similar to a particular installation).
- For the Site-Specific Data approach to validation, evaluation of inspection, maintenance, and test data over a significant period to demonstrate that the system achieves the performance claim.
- Assessment of access security measures for hardware and software.
- Management of change and revision control for the hardware and software, including setpoints, fail configuration, and operator overrides.

Approach B – Example Configurations

Two independent and separate BPCS controllers can be implemented such that there is no communication (or interconnection) between the two BPCS loops (e.g., IEC 61511). This architecture is an inherently safer design, as it is physically separate as well as independent, so it provides a high degree of protection against data corruption and inadvertent software changes.

This architecture can theoretically achieve the 0.01 PFD claim for the overall performance of the two BPCS loops if the two systems are designed and managed according to good engineering practices (Figure 5).

Figure 5. Illustration of two BPCS functions credited for the same scenario per IEC 61511 (Adapted from Figure 2, IEC 61511, 2003)

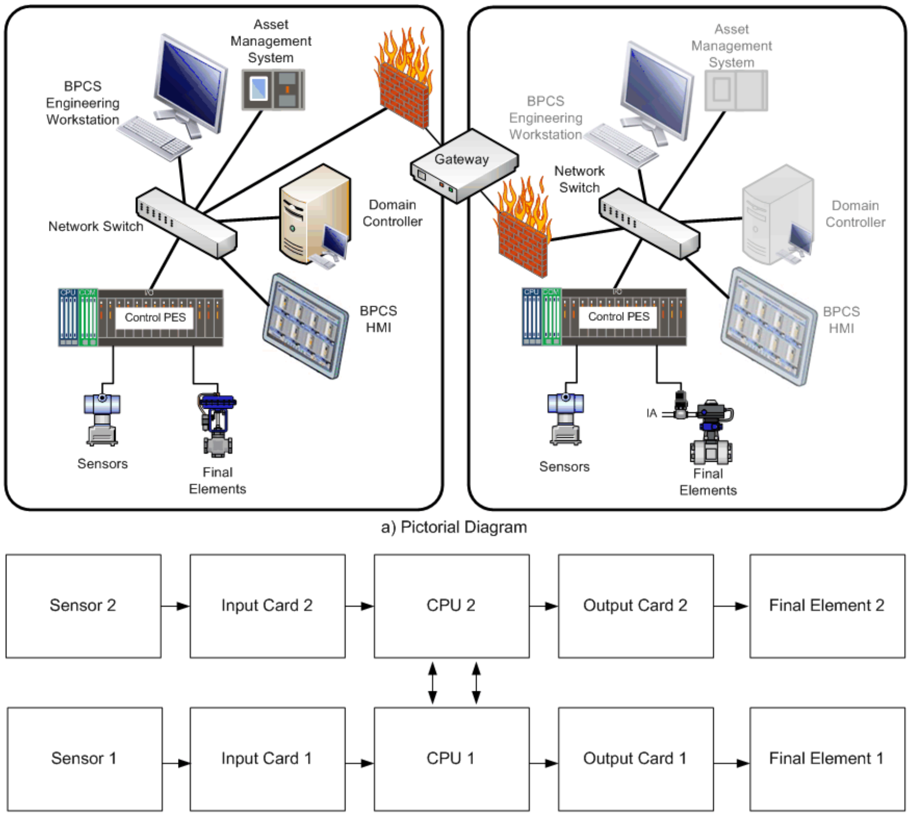


a) Pictorial Diagram

b) Block Diagram IEC 61511, 2003

CCPS IPS [3] recognized that the controllers could be functionally separate while safely sharing information. An example of this architecture (Figure 6) consists of separate controllers that communicate in a secure manner using firewalls and communication controls. When the controllers share data or interfaces, integrity of the two BPCS loops must be assured with rigorous management of change and access control. Ensuring cyber security and software/data integrity necessitate special design and management practices (ISA TR84.00.09 [13] and ANSI/ISA 99 [14]. This architecture can also theoretically achieve the 0.01 PFD claim as long as the two systems are designed and managed according to good engineering practices.

Figure 6. Illustration of two BPCS functions credited for the same scenario per CCPS IPS (Adapted from Figure 4.7 [3])



a) Pictorial Diagram

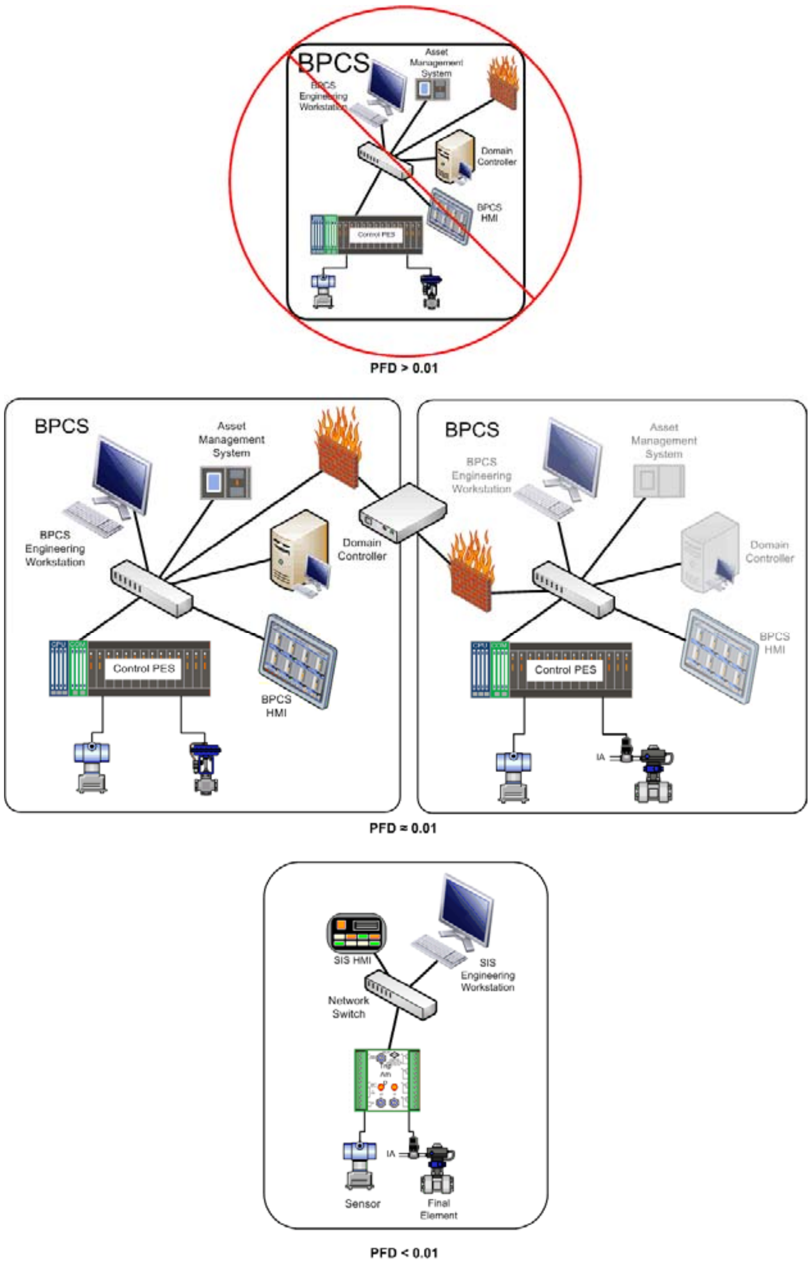
b) Block Diagram, Guidelines for Safe and Reliable Instrumented Protective Systems, 2007

When both loops are implemented in the same BPCS (Figure 7), the shared equipment is generally insufficient for crediting the two BPCS loops for the same hazardous event. The CCPS LOPA book [13] indicated that the BPCS CPU had at least two orders of magnitude better performance than the field devices. More recent field data demonstrates that the failure rate of a typical BPCS logic solver is greater than 0.01/year [7]. In fact, industry and manufacturer data indicates a random hardware failure rate for typical BPCS equipment (such as DCS/PLCs) in the range of 10^{-5}/hr to 10^{-6}/hr (ISA TR84.00.04-2012 Appendix F.2.1), so the BPCS performance is equivalent to many other electrical, mechanical, or programmable electronic devices. Therefore, it is difficult to substantiate that a single BPCS qualifies for Approach B with a claimed failure rate of ≈ 0.01/year without advanced quantitative techniques.

When the two loops share equipment or support systems that can cause the dangerous failure of the integrated BPCSs, the resulting integrated system should be analyzed as a single BPCS. A BPCS architecture that uses a primary and hot backup controller is not sufficient for crediting as two independent controllers due to potential common cause failure. For example, a hot backup controller shares common equipment with the primary controller, such as the backplane, firmware, diagnostics, and transfer mechanisms. A hot backup controller improves operational reliability by reducing the likelihood of spurious process shutdown by a factor of perhaps 2 to 3, but it is not sufficient for claiming a dangerous failure rate ≈ 0.01/year.

Thus, designing a PE controller to achieve a PFD less than 0.01 requires advanced diagnostics, fault tolerant architectures, and rigorous software controls. Manufacturer claims regarding an individual device is not sufficient to justify sharing the device between two BPCS IPL or between BPCS IPL and BPCS IE for the same hazardous event. IEC 61511 Clause 11.5 provides criteria and considerations for achieving this level of performance. Normal and customary BPCS practices will not meet these requirements.

Figure 7. Illustration indicating what is necessary to achieve PFD ≤ 0.01 in a single controller



SUMMARY

SCAI are an important subset of the process safety safeguards used to reduce the risk of hazardous events. The instrumentation and control systems need rigorous design and management practices to ensure that they are available when rare hazardous events begin to propagate. There are many words that can be used to identify, describe, define, or otherwise classify SCAI. As a rose is a rose, if it is an instrument or control, is process safety related, and is required for risk reduction, it is SCAI.

When considering use of BPCS for SCAI, the first thing to remember is that risk reduction is not free. It requires effort. Getting an order of magnitude risk reduction from the BPCS is hard. The independence and reliability requirements impose rigorous design and management practices, focusing on eliminating single points of failure and human error. The typical design and management practices associated with BPCS equipment limit its capability to one order of magnitude per logic solver (e.g., controller) [8]. The potential for systemic error also limits the risk reduction claim in any scenario to a maximum of two orders of magnitude for two (or more) independent BPCS controllers [3]. When claiming more than one order of magnitude from a single controller in a scenario, the controller must be designed and managed as a SIS in accordance with IEC 61511 [8].

7. References

[1] A.E. Summers, Safety controls, alarms, and interlocks as IPLs, 9th Global Congress on Process Safety, San Antonio, TX, 29 Apr to 1 May 2013

[2] ANSI/ISA 84.91.01 (2012), Identification and Mechanical Integrity of Safety Controls, Alarms and Interlocks in the Process Industry. Research Triangle Park, North Carolina, 2012.

[3] CCPS, Guidelines for Safe and Reliable Instrumented Protective Systems, Wiley, Hoboken, New Jersey, 2007.

[4] ANSI/ISA 100.11a (2011), Wireless system for industrial automation: Process control and related applications, Research Triangle Park, NC, Print.

[5] CCPS, Guidelines for Initiating Events and Independent Protection Layers, Wiley, Hoboken, New Jersey.

[6] ISA TR84.00.04, Guidelines for the Implementation of ANSI/ISA84.00.01-2004 (IEC 61511 Mod), Research Triangle Park, North Carolina, 2012.

[7] SINTEF, Reliability Data for Safety Instrumented Systems Data Handbook, Trondheim, Norway, Gruppen, 2010.

[8] IEC 61511, Functional safety instrumented systems for the process industry sector, Geneva, Switzerland, 2003.

[9] ISA TR84.00.03, Guidance for Testing of Process Sector Safety Instrumented Functions (SIF) Implemented as or Within Safety Instrumented Systems (SIS), Research Triangle Park, North Carolina, 2012.

[10] ANSI/ISA 18.2, Management of Alarm Systems for the Process Industries, Research Triangle Park, North Carolina, 2009.

[11] ISA TR84.00.02, Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques, Research Triangle Park, North Carolina, 2002.

[12] CCPS (), Layer of Protection Analysis: Simplified Process Risk Assessment, Wiley Hoboken, New Jersey, 2001.

[13] ISA TR84.00.09, Electrical/Electronic/Programmable Electronic Systems (E/E/PES) for Use in Process Safety Applications Security Protection Layers and Considerations Related to SIS, Draft 7.4, Research Triangle Park, North Carolina.

[14] ANSI/ISA 99.00.01, Security for Industrial Automation and Control Systems, Research Triangle Park, North Carolina, 2007.