MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

20th Annual International Symposium
October 24-26, 2017 • College Station, Texas

Addressing the Challenges of Implementing Safety Instrumented Systems in Multi-Product Batch Processes

Eric P. Steinhauser
eric.steinhauser@albemarle.com
Albemarle Corporation
Pasadena, TX 77501

Abstract

Adapting the requirements of IEC 61511 to a batch system can be frustrating, particularly for multi-product units. While a Safety Instrumented System (SIS) for continuous operation is often a straightforward detect-decide-act loop, implementing a SIS for a batch system may involve multiple safety functions, time- or state-dependence, intricate calculations, or complex installations. Relationships between the SIS elements and the basic process control system (BPCS) must be tightly managed, providing both for the safety of the unit and its ability to operate without spurious trips or other hindrances. These issues are further complicated when multiple products requiring different functions or setpoints are produced in the same SIS-protected batch unit.

This paper will discuss the challenges particular to the design, operation, and maintenance of a SIS in multi-product batch operations and present practical options for successfully resolving the concerns. A key insight into successful adaptation is treating the batch SIS as a "permission" system for the BPCS to operate. Although many items can be addressed through clever engineering practices, sustainable success relies on proactive, robust management of the safety lifecycle.

Background – The Problems of Functional Safety in Batch Processes

Batch operations are ubiquitous in the chemical process industry; even facilities that operate large continuous processes typically include some forms of batch transfers or smaller batch unit operations. Batch reaction chemistry is particularly prevalent throughout the specialty chemicals, fine chemistry, and pharmaceutical sectors. Risk analyses of batch operations may drive organizations towards the use of a SIS to address safeguard gaps and meet risk tolerance criteria.

A safety instrumented function (SIF) for a simple batch process – such as transferring materials between a transportation container and fixed storage – often only requires process variable detection to activate, and is thus independent of any phase sequencing. Design and implementation of these systems resembles those prevalent in continuous operation. See Figure 1 for a basic overfill SIS example.

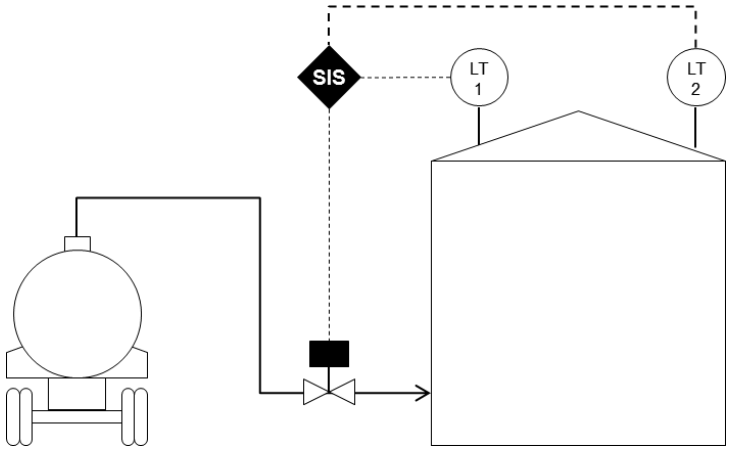

Figure 1: Simple batch SIS installation for level protection of a fixed storage tank

Things can become decidedly more complicated with batch reactions. A typical batch reaction process may include many phases in one vessel, and the potential hazards can vary widely depending on which phase of the batch is being executed. Conditions that are of no concern in an early phase may be extremely hazardous in a later phase, and the SIF required to mitigate a dangerous condition in one phase may be completely different from the SIF required in a subsequent phase. Incorrect sequencing of batch actions or additions may also pose significant hazards.

From a safety standpoint, it might be ideal to segregate the batch phases into different process vessels to eliminate any phase-dependent SIFs. This is not always possible or practical, particularly in the industries in which batch production dominates. New products or revised chemistry is often retrofitted into existing units, and the cost of a SIS is usually far less than installing additional vessels. In addition, as risk tolerance criteria become tighter and the industry-wide understanding and evaluation of reactive hazards improve, there is increased demand to implement safety instrumented systems in existing units.

Further confusing this situation is that in many facilities a single batch unit (reactor and other associated processing equipment) may be used for multiple different products or varieties of a product class. Each recipe or product may have unique safety requirements and thus demand different SIFs or setpoints for a common SIF. Conversion of the equipment between product campaigns can include significant changes in the piping, instrumentation, or vessel configurations that must be accommodated by the SIS.

When phase- or recipe-dependent SIFs are required, then, the resulting overall SIS is far more complex than the basic detect-decide-act loop monitoring a single process variable. Monitoring

of multiple variables (pressure, temperature, flow, etc.) is often required, and the SIS final elements are often spread across multiple process lines or shared with the basic process control system (BPCS). See Figure 2 for an example of this type of batch system.

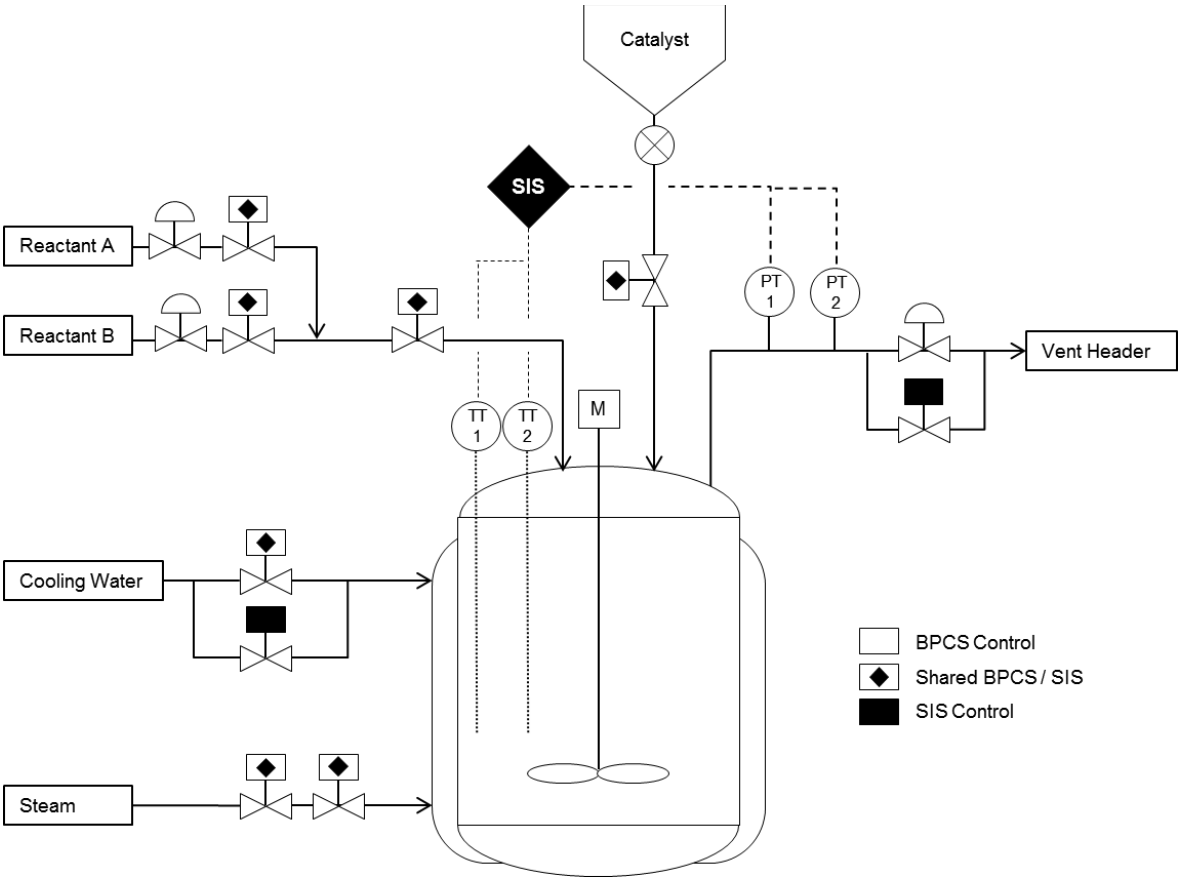

Figure 2: Example of batch reactor SIS requiring multiple process variables and final elements on different portions of the system. Not all valves may be involved in each SIF.

Considerations for Batch SIS Implementation

The need for and use of SIS in batch operations has long been recognized. Batch processes are mentioned several times in IEC 61511-2, and ISA TR84.00.04-2005 includes lengthy discussion of implementing a SIS in batch production [1,2]. Despite this, there is little specific guidance in either standards or literature for the peculiarities of implementing a SIS for multi-product or phase-dependent batch processes.

Ideally, SIFs should be active at all times, use fixed setpoints, and have no dependence on any part of the BPCS. As this is often not possible or practicable for a batch SIS, three major questions must be addressed:

- How will the SIS be aware of what phase the batch BPCS is executing?

- How will the recipe or product selection be communicated to the SIS?
- How will any shared elements between the SIS and BPCS be designed and managed?

One of the earliest treatments of this topic is a 2002 article by van Beurden and Amkreutz that noted the need for phase synchronization and communication of recipe or product and provided some discussion of how that might be accomplished [3]. In 2016, the European groups WIB and NAMUR published a set of recommendations (NE-154) for the application of IEC 61511 to multi-product batch systems [4]. This document is likely the most comprehensive treatment of the subject to date.

Sharing of field elements and the details of BPCS/SIS interaction have received more attention from functional safety experts, and there have been several published examinations about how it might be accomplished and what dangers or limitations are inherent in that approach [5,6,7,8]. This is still a controversial topic, but it seems that the consensus among those who have implemented shared elements is that defense-in-depth redundancy (often 1oo3 or 2oo3) is the appropriate strategy.

It is hoped that this paper will provide some additional rationale behind the guidance and some examination of how the guidelines might be practically applied, including some generic examples and discussion of the burdens a batch SIS places on management systems. Because shared elements can be vitally important to the success of a batch SIS, that topic will be addressed before phase and recipe dependency.

Sharing Final Elements, Permission Architecture, and Permissive SIFs

Automated batch reactor systems typically use BPCS-controlled block valves to provide positive shut-off of material flow. Flow may be further regulated by a BPCS control valve. In instances where a SIF requires the shut-off of some flow, it may be advantageous to use the same block valves that are ordinarily operated by the BPCS. Reasons for sharing valves between a SIS and the BPCS include physical constraints on pipe space, minimization of components / leak points, reduced capital cost, and potentially enhanced reliability of the valve.

The latter point is particularly applicable for batch systems where these block valves are being opened and closed routinely. While not necessarily the same as a formal proof test of the valve, routine stroking of valves provides additional assurance of their ability to perform on demand. (Whether this could be counted as a stroke test or what credit could be applied in SIL calculations is beyond the scope of this discussion.) This additional use and operation of the valve should be taken into account for the determination of appropriate periodic maintenance of the valve and actuator.

Sharing final elements usually induces some trepidation among SIS practitioners, as it goes against the general independence principle. However, as long as a dangerous failure of the final element would not create a demand on the SIS, this approach is acceptable. As noted in clause 11.2.10 of IEC 61511-1, additional analysis is necessary to ensure that the overall risk from sharing components is acceptable in the event of a dangerous failure [1].

In general, it is not recommended that final element sharing be considered for a control valve – the nature of a control valve usually means that a valve or positioner failure could be an initiating event leading to a demand on a SIS. This type of dangerous failure is near impossible to engineer out of the system (redundant control valves are rare). Furthermore, control valves often have poor closure tightness compared to the quarter-turn block valves typically used as on/off valves in batch production. Control valves may need to be included in SIFs that demand certain process lines be opened, such as with opening cooling fluids or vents – functional safety redundancy here is provided by a bypass line around the control valve. This is shown on the cooling water and vent lines in Figure 2.

Dangerous failure of a single automated block valve in a batch system would likely be either a failure to close when required or a spurious opening. Using an appropriate architecture for the shared components can reduce much of the concern and isolate the dangerous failure cases for these valves [6]. Hardware fault tolerance for the block valves (1oo2 or 1oo3) in series significantly reduces the danger from a single stuck or otherwise failed valve or actuator, barring an unaccounted common-cause failure. Spurious opening cases can be addressed through redundancy in control, allowing both the BPCS and SIS to command the valve. Care must be taken with this approach such that a command disagreement sends the valve to the predesignated failure state (1oo2).

A common method for valves is to use a pair of solenoid valves on the pneumatic feed to a valve actuator, or switches in the case of motor-driven valves. The SIS acts on a solenoid valve in series with the ordinary BPCS solenoid and the actuator (See Figure 3). This effectively sets up the SIS as a "permission" system for the BPCS to use the SIS valves during routine operation. This architecture also gives the BPCS the first opportunity to react to a dangerous upset condition, provided the BPCS trip points differ from the SIS, though in many cases this could not be considered a credible IPL.

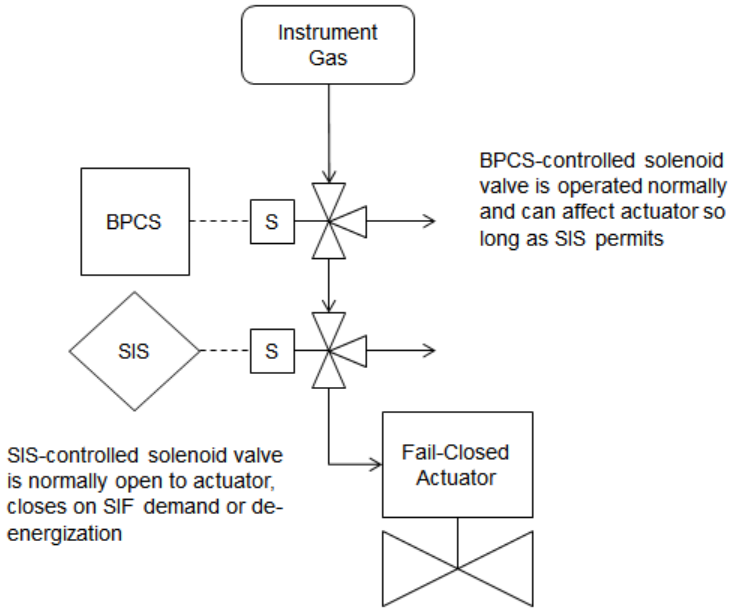

Figure 3: Double-solenoid option for sharing a shut-off block valve with BPCS and SIS

The permission arrangement shown in Figure 3 allows for the creation and use of permissive SIFs, which serve to prevent an action or progression in a batch sequence unless a set of prerequisite conditions have been met. For example, a permissive SIF may prevent addition of catalyst to a reactor prior to the charge of a heel of material in which the catalyst will be mixed, or disallow the transfer of a high-pressure reactor to another vessel until the reactor has been depressured (See Figure 4). These are ordinary features of a batch control system that may be elevated to the SIS if the scenario is of sufficiently high risk. When determining the required SIL for a permissive SIF, there are at least two initiating events to consider – operator attempt to open the valve, and a batch control system failure calling for the valve to open.

A unique feature of permissive SIFs is that they do not have traditional final elements that act to return a process to the safe state when an upset is detected. The permissive SIF's success is not determined by the action of a valve or motor – rather, it is determined by its ability to prevent an action. Permissive SIFs act on the SIS-controlled solenoid valve or switch each time the permissive SIF is activated, and this needs to be considered in the reliability or maintenance plan for that SIS element. Proof testing for permissive SIFs will necessarily involve an attempt to operate the valve(s) or other equipment to which the SIS should be denying operability. This test should be managed under controlled conditions that will not proceed to a hazard in the event of failure. The lack of traditional final elements also removes that aspect from SIL determination calculations; the failure rate of the solenoid or switch would be included, but not the actuated valve.

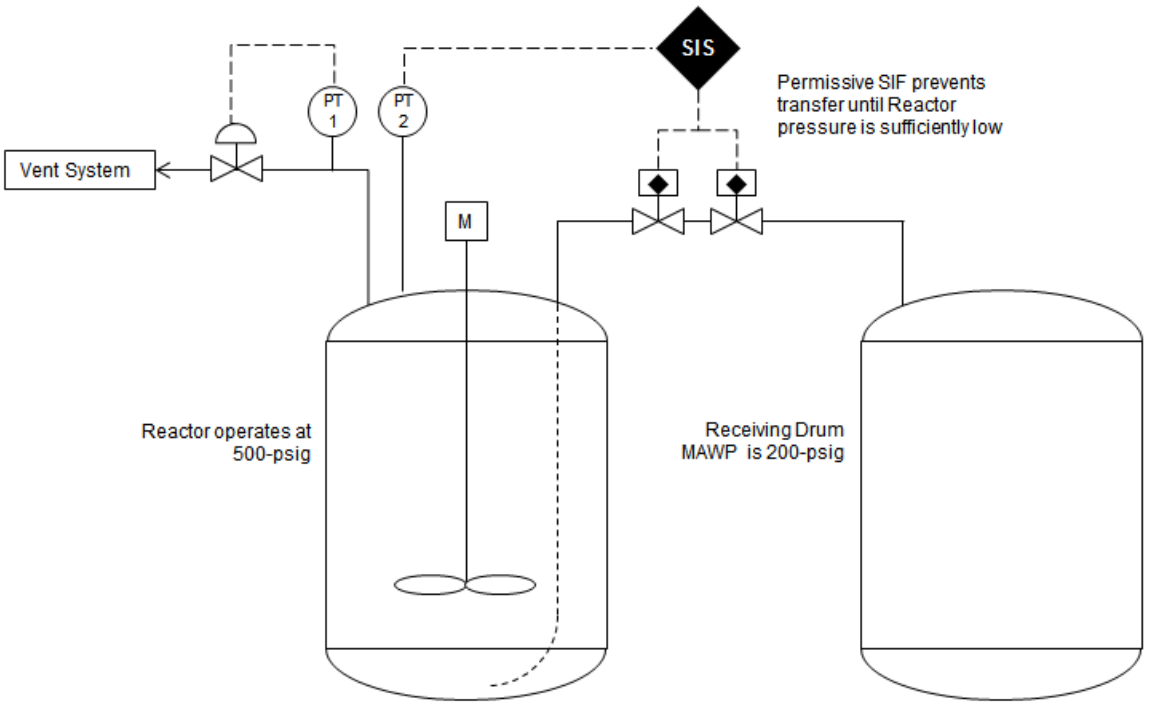

Figure 4: Permissive SIF arrangement to prevent inadvertent overpressure during transfer

In practice, permissive SIFs can be an effective means to provide additional assurance that particularly hazardous situations do not arise, particularly when the process safety time for the hazard scenario is short or the secondary consequences of a mitigated hazard are undesirable. The conditionality of the SIF can be a drawback and makes it less robust compared to standard reactive SIFs – the discussion about phase dependency later in this paper will address that point more directly. A comprehensive failure analysis of the batch control system should be completed before committing to a permissive SIF, especially for routes in which the SIS can be spoofed, fooled, or otherwise bypassed to defeat the withdrawal of permission. For significant hazards, a combination of permissive and reactive SIFs may be appropriate and provide additional segregation of protection layers. In the Figure 4 high-pressure transfer case, an additional valve triggered by a high-pressure detection on the receiving drum could be another SIF independent of both the BPCS and reactor SIS.

Sharing Instrumentation

As with final elements, there may be many reasons for wanting to share instrumentation between the BPCS and a SIS. This is frequently less concerning than with the final elements, particularly for batch systems in which high hazard scenarios often include non-BPCS-related initiating events. Sharing of process instruments between the SIS and the BPCS also requires an overall hazard evaluation under IEC 61511-1 Clause 11.2.10 [1]. Common-cause failure is a major consideration in this hazard evaluation, particularly as the process connection needs to be included in the evaluation of instrument failure rates. When modifying existing batch systems for a SIS, the placement of multiple instruments on a single nozzle or instrument tee may be a significant issue.

Perhaps the most common reason is simply the desire to have all field instrumentation visible and available to operators. In many existing batch systems, particularly reactors, the use redundant instrumentation has been a standard practice, and there is often a resistance to cede any instrumentation to the SIS without retaining some view of it. A potentially significant benefit of this practice is that it can be used to increase diagnostic coverage and provide for a more rapid response to failed instruments and restoration of the system. System alerts can be crafted to notify operators or supervisors of excessive deviation between the SIS instruments and BPCS instruments monitoring the same process variable. Batch systems are generally more easily halted and restored upon diagnosis of an issue than in a continuous process. When this approach is taken, part of the operating plan should be a definition of what deviation is unacceptable and what the response plan will be (see IEC 61511-1 Clauses 11.3 and 16.2.2) [1]. Response plans could include immediate shutdown or temporary degraded operation.

Shared field instruments should be considered first as SIS elements that the BPCS is allowed to view as a courtesy. This is frequently done using a signal conditioner or repeater, which effectively splits the transmitter signal to both systems. Any such equipment that interacts with the instrument or instrument-to-SIS signal must be included as part of the SIS and a potential failure path for each SIF. Data may also be transmitted directly from the SIS programmable logic controller (PLC) to the BPCS, but this adds some complexity to the SIS design and may affect the scan rate of the instrument data. Transmission of instrument data from the BPCS to the SIS should not be considered.

Figure 5 shows how this instrument sharing may be accomplished. Two temperature elements may occupy the same thermowell, one dedicated to the SIS and the other to the BPCS. The signal from the SIS instrument may also be repeated to the BPCS for informational purposes. The same may be done with two pressure transmitters on one instrument tee. This arrangement presents potential issues with common cause failure that must be addressed if failures of PIC-1A or TIC-1A can lead to a hazardous upset condition triggering a SIF including PT-1B or TT-1B. The use of another instrument on a separate process connection allows for greater redundancy and SIS reliability, as shown in Figure 6. The addition of an extra instrument tee for PT-1C and another thermowell for TT-1C allows the SIS to have 1oo2 architecture for both pressure and temperature while remaining largely independent of the BPCS pressure and temperature control systems. For non-fouling batch systems, such an arrangement serves to maximize SIS reliability while minimizing the need for additional system modifications. A 2oo4 architecture including two elements in both tees or thermowells is also possible and would reduce the possibility of spurious trips. In the event of a dangerous failure of the element shared with the BPCS for control, the system reduces to a 2oo3. This approach can be costly and adds complexity to the system.

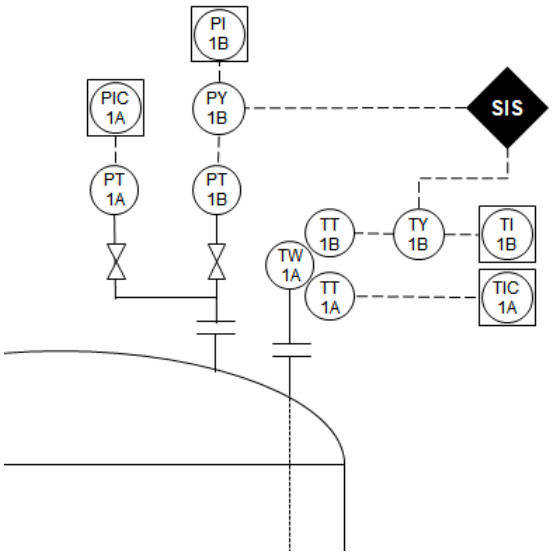

Figure 5: BPCS and SIS sharing instrumentation. Repeating signals is rarely concerning, but the common cause failure of sharing tees or thermowells can be problematic.

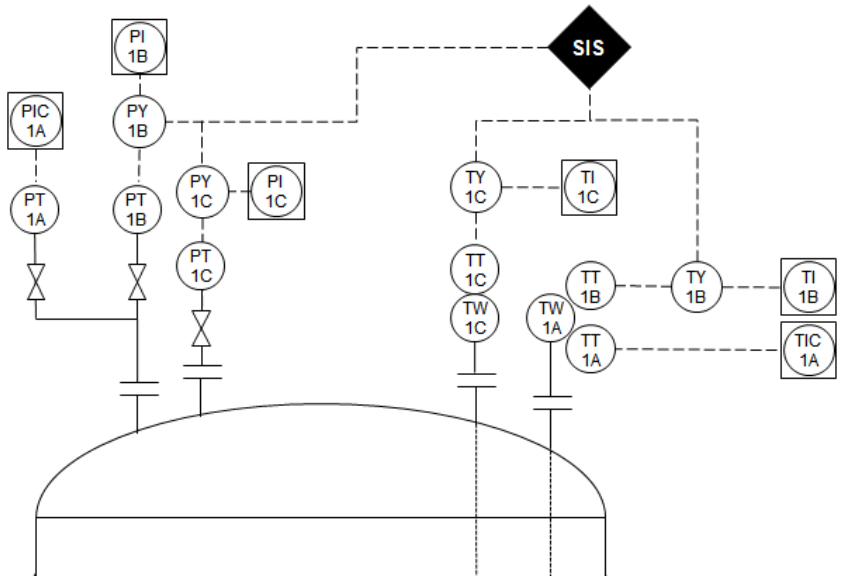

Figure 6: Adding an extra instrument tee and thermowell allows for greater SIS instrument independence from the BPCS loops and increases SIS reliability.

Phase Dependency and Synchronization of BPCS and SIS

Phase dependency is a thorny issue for a batch SIS, as it creates a specific avenue for a SIF to be disabled and unavailable to act on a true process upset demand. This disabling will occur every batch, and the SIF must be re-enabled every time it might be needed. As mentioned previously, the ideal safety solution might be to segregate these steps into different process vessels. This is

especially true for runaway reactive hazard scenarios where a SIF would be triggered on a particular temperature during a reaction, but the batch requires heating to a higher temperature prior to reaction initiation or afterwards in a distillation (see Figure 7). Phase-dependent SIFs should be due to process-specific concerns and setpoints. Any SIFs that are designed around equipment limits (level, pressure, or temperature) should be enabled at all times and have no phase dependency or disabling conditions.

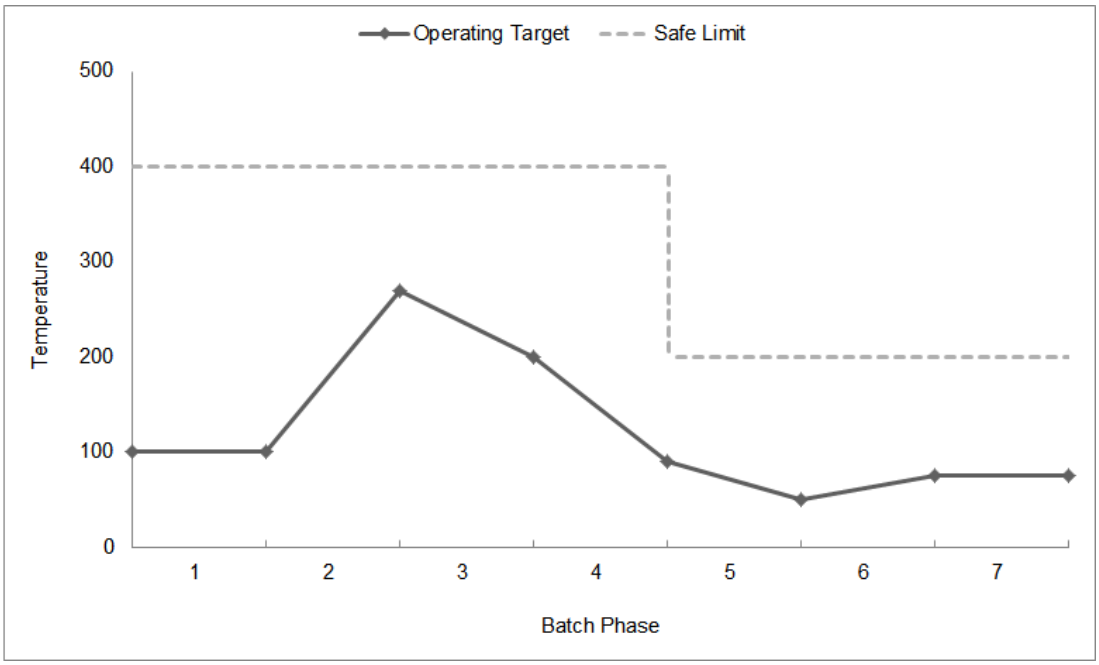

Figure 7: Batch temperature profile showing need for a phase-dependent SIF. The batch is always intended to be operated under the safe temperature limit, but Phases 2-4 will operate the batch temperature above the safe limit for Phases 5-7.

Where phase dependency is unavoidable, the SIS logic controller must be able to detect what batch phase is ongoing. Contrasted with recipe synchronization, phase synchronization requires constant input and evaluation throughout the batch. There are two general strategies for implementing phase detection in a SIS: direct process sensing and BPCS signaling.

Direct process sensing requires the SIS to monitor a broader range of process variables and use a logic set to determine if a specific SIF is applicable at that moment. This has the advantage of better segregating BPCS and SIS function than the BPCS signaling strategy. Many phase-dependent SIFs will be permissive SIFs that require some process-sensing component to function.

Each process sensing element that is involved in phase detection for either enabling or disabling a SIF becomes a safety critical component. Therefore, it must be included, tested, and maintained as part of the SIS. Failure rates for these components and any logic arrangement must be accounted for in the SIL determination calculations.

Particular care should be taken with the use of any discrete, "ON/OFF" process sensors such as valve limit switches or level switches to enable or disable SIFs. Reliable, timely function of these components is often suspect, and diagnostic coverage is limited. When switches (particularly valve limits) are needed to implement process-sensing phase dependency, the BPCS signaling strategy should be considered as either a replacement or an augment.

BPCS signaling requires a level of communication from the BPCS to the SIS. This is often through a "flag" system that indicates what phase is active. Flag systems like this are common when batch programs have to interact with other concurrent programs in a BPCS, and extending that signaling to the SIS from the BPCS is often trivial. Van Beurden and Amkreutz detail several ways this can be done [3].

As with any BPCS dependency for the SIS, a thorough hazard analysis is required to understand how the communication could fail, what the consequences would be, and what redundancies or back-checks are available. NE-154 Clause 9.2 offers a thorough list of items to consider and tackle when adopting the BPCS signaling (termed "BPCS Triggered" in NE-154) method. It also recommends excluding the BPCS-to-SIS signal-generating equipment from SIL determination calculations in favor of implementing a strict "failure avoidance" administrative control strategy validated by hazard analysis [4]. (While excluding the signal requirements from the SIL calculations may be sensible per IEC 61511, it has the perverse effect of understating the PFDavg compared to the direct process sensing option.)

A combination of both strategies is also possible and offers an opportunity for the SIS to determine if the BPCS-signaled phase intention matches with the process state known to the SIS (van Beurden and Amkreutz refer to this as a "plausibility check") [3]. In the event of a mismatch, the SIS may place the batch into a predetermined safe state until the issue is resolved and the batch is reset. This scheme offers additional safety assurance at the expense of higher likelihood of a spurious shutdown, but it may also make particular sense when differentiating different phases solely through continuous process variable measurement is difficult or requires a large set of information.

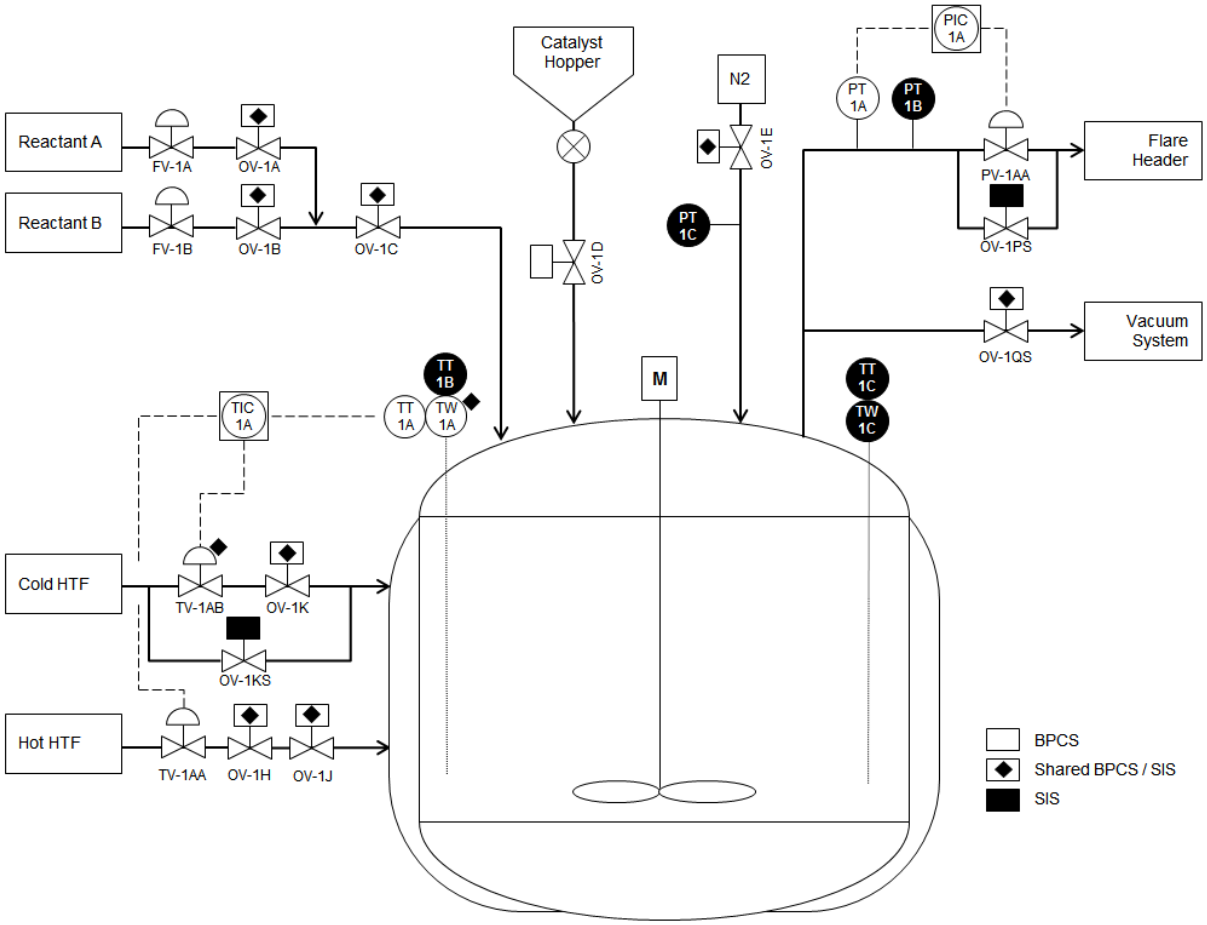

Figure 8: Batch Reactor with multiple SIFs and phase dependency

Consider the fictional batch reactor system shown in Figure 8. During the addition of Reactant B, the temperature is controlled to about 300°F at high pressure. There is danger of a runaway decomposition during this process if the temperature exceeds 520°F, which is a possibility if the reactor loses cold heat transfer fluid to the reactor or the reaction mass is too rich. The SIF will have the following characteristics:

- Trip at 370°F (1oo2 TT-1B and TT-1C)
- Stop the addition of all reactants (Close OV-1A, OV-1B, OV-1C)
- Demand maximum cold HTF flow (Open OV-1KS, OV-1K, TV-1AB)
- Shut off any hot HTF flow (Close OV-1H, OV-1J)
- Open the reactor vent to the flare system (Open OV-1PS)

The 370°F SIF needs no phase dependency. There is another scenario of concern, however, when a vacuum distillation is performed on the reaction mass at the end of the batch process. If the distillation temperature exceeds 285°F at the typical vacuum condition, much of the reaction solvent could flash off and cause the remaining heel to become unstable. Hazard analysis demands a SIL-1 SIF to prevent this condition from occurring. Because the vacuum-phase SIF setpoint is

below the reaction-phase SIF, it will be phase dependent and only be enabled during the vacuum phase. This second SIF will have the following characteristics:

- Enabled when reactor pressure is below 10-psig (1oo2 PT-1B, PT-1C)
- Trip at 275°F (1oo2 TT-1B, TT-1C)
- Shut off hot HTF flow (Close OV-1H, OV-1J)
- Close off the reactor vent to the vacuum system (Close OV-1QS)
- Break vacuum with plant nitrogen (Open OV-1E)

In the Figure 8 example, the phase dependency can be adequately enabled by process detection, and BPCS communication is not required for success. That is not the case for the fictional process shown in Figure 9:

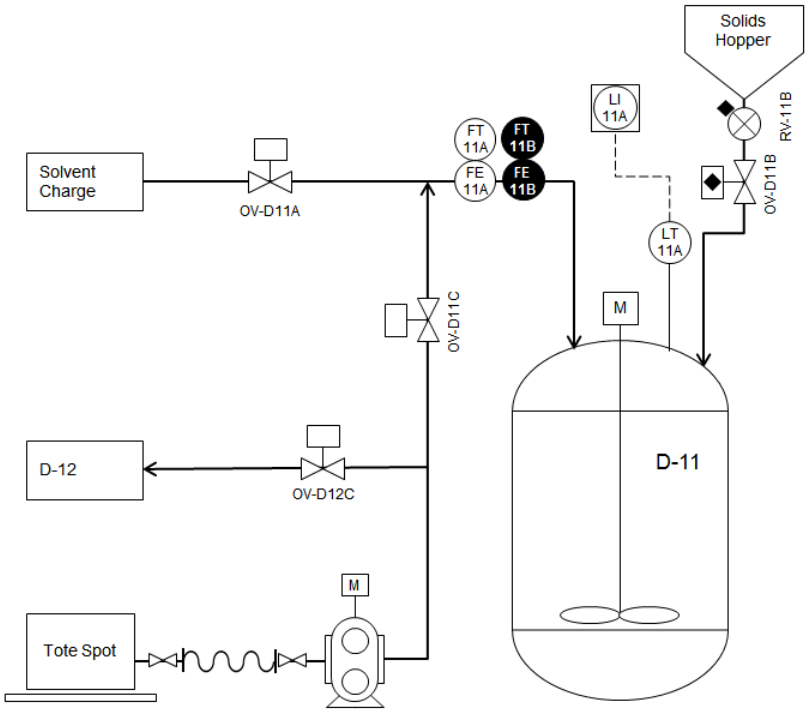

Figure 9: Permissive SIF for a slurry mixing system requires BPCS Signaling strategy

A dispersant is required to be added from a tote spot to a slurry being made in mixing drum D-11. Clumping of the solids is possible even with agitation and can damage the downstream equipment, so a permissive SIF is needed to ensure the addition of the dispersant agent prior to solids charge. Because the tote charge system is used for multiple additives and multiple vessels, the SIS cannot easily follow the sequence of batch phases without tracking valve positions and history. Instead of such a complex process detection scheme, a BPCS signaling strategy will be employed to inform the SIS of the current batch phase. The SIS ensures that the batch phase progression proceeds per design and then verifies the addition through a totalizing flowmeter (FE-11B), which must be reset at the beginning and end of the phase.

Recipe Dependency

Most of the preceding sections are applicable to any batch system, whether designed for single product, capable of making different grades of a similar product, or used for multiple different products that may have minimal similarity. When a SIS is needed for a multi-product unit, however, the SIS design must accommodate the flexibility of the unit without sacrificing functional safety. What form this takes largely depends on the frequency and scale of process changes between recipes. As with phase dependency, recipe-dependent SIFs should be due to process-specific hazards, and SIFs that are designed around equipment limits should be invariant.

The need for recipe dependence should be challenged during the design of any such SIF, particularly if the recipe changes are frequent and do not involve rearrangement or disconnection of equipment. Piping redesigns can eliminate some of the need, particularly by forcing reactants through common headers that can be shut off regardless of product selection and source. Allowing SIS actions to be global rather than recipe-specific can also be advantageous. There is usually no particular harm in a SIF demanding the closure of valves that are not currently involved in the process (either from a phase- or recipe-dependence standpoint). These would be considered "courtesy" actions by the SIS and do not need to be included in the SIL calculations where they are not important to the success of a SIF for a given initiating event. Where there are multiple possible initiating events with a common process variable upset, the SIS may make a common action that covers all the possibilities without regard to which initiating event occurred.

Consider Figure 10. Mixing drum D-90 mixes Reactant X with either Solvent A, B, or C depending on which product line is currently active. The drum could be overfilled by any of the four possible sources. While the SIS could be designed to know which solvent line is active during the product campaign, a global shutoff of the fill valves is a simpler solution. This global SIS action covers four distinct initiating events and thus should be evaluated as four different SIFs. The success of closing OV-90AS would have no effect on halting an overfill event due to a failure of the flowmeter controlling the dose of Reactant X.

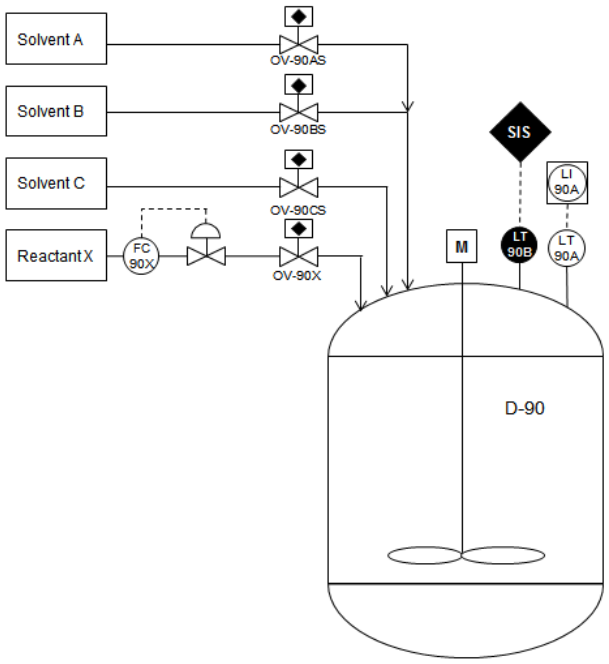

Figure 10: Overfill scenarios for a mixing drum are recipe dependent.

When there is a distinct need for recipe-dependence, the recipe dependence needs be set at the beginning of each batch. This largely eliminates direct process sensing from being a viable recipe-detection strategy. Instead, either the BPCS signaling route needs to be utilized, or there must be an independent means to designate the recipe selection.

If product changes are infrequent and involve significant turnaround activity, an appropriate strategy may be a SIS program reset and verification of the program / product match during an operational readiness check or pre-startup safety review. Especially when coupled with another BPCS-SIS recipe verification prior to each batch (with a trip to safe state in case of a mismatch), this is an excellent way to handle a multi-product batch SIS.

BPCS signaling is probably the easiest way to indicate what recipe the SIS will use when enabling or disabling certain SIFs or setpoints. It may be useful for the BPCS-SIS communication to include a verification check in which the SIS indicates to the BPCS what recipe it has engaged. When there is a mismatch, the BPCS should default to an idle safe state. This has the obvious drawback of being very reliant on both a human-machine interface for selection of a particular recipe and the successful transmission of that selection to the SIS. When there are significant additional human factors in the execution of the batch (e.g., selection of the right drum to charge or which hose to connect), the BPCS signal strategy may not be acceptable. Again, a thorough hazard analysis is required to justify the selection of a BPCS signaling strategy without an independent verification.

A “field switch” strategy is also possible with recipe selection, in which a physical switch or dial system is engaged to signal to the SIS which recipe is intended. This can then be compared to the selection in the BPCS, or it can be used to inform both BPCS and SIS of recipe selection (see Figure 11). This might be a good option for more frequent recipe changes, particularly if it must

also be confirmed through a human-BPCS interface that engages a different operator from the one who set the field switch. As with any electromechanical component involved in the SIS, the field switch needs to be a safety critical component, incorporated into SIL calculations, and included in the SIS maintenance plan.

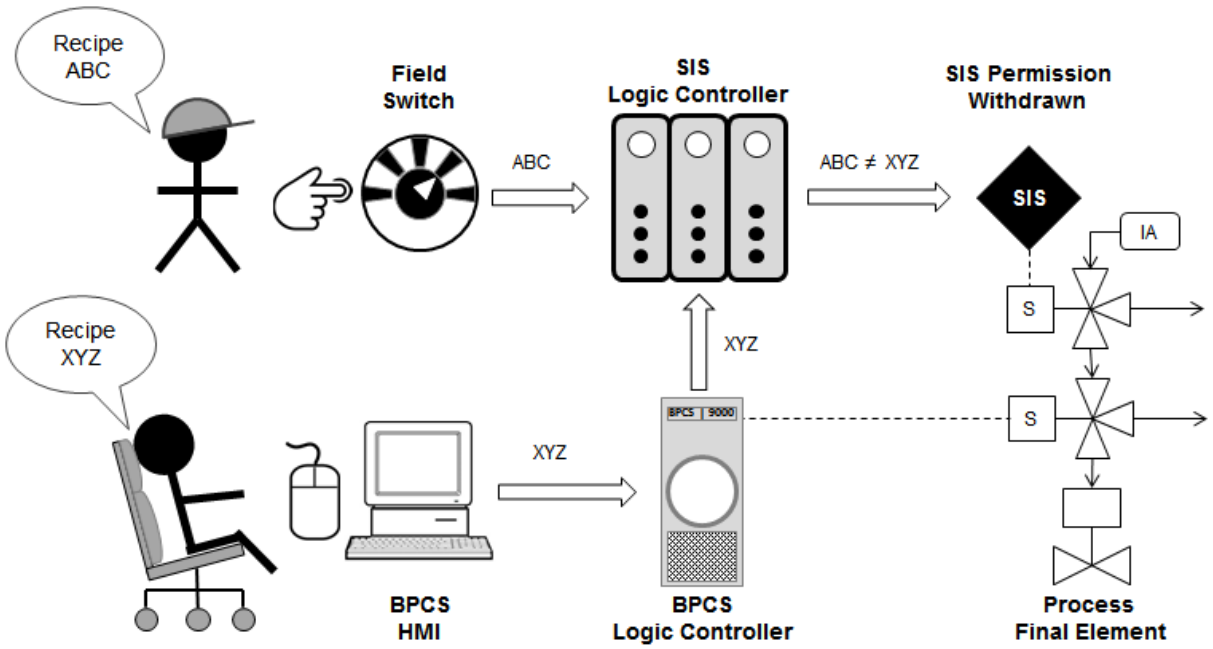

Figure 11: Using a field switch for two-factor authentication of batch recipe. If there is a mismatch, the SIS can withdraw permission for batch operation and hold a safe state.

Managing Batch Conversions and Turnarounds

Compared to many continuous processes, batch units are frequently taken offline for routine maintenance, cleanouts, conversions between product campaigns, or other business reasons. Startup and shutdown is a natural part of batch activity, and in a facility with multiple batch units, such turnaround and conversion activities are often routine and part of the normal day-to-day work for operations and maintenance personnel. When safety instrumented systems are integrated into the batch units at this type of facility, it is incumbent on the facility management to ensure that the routine turnarounds and conversions do not impair the functional safety of those units. This is even more important when relatively few units are equipped with a SIS and employees may not have the same day-to-day awareness of the SIS.

While none of these are unique to batch systems, there are several functional safety concerns that are heightened with frequent maintenance and product conversions:

- Impairment of SIS instrumentation or final elements
- Unauthorized modification to SIS-related equipment
- Unauthorized modification to SIS-protected processes
- Normalization of deviant SIS behavior

Successfully combating these challenges requires a vigorous management systems approach for the operation / maintenance, modification, and decommissioning phases of the safety lifecycle. While Clauses 16-18 of IEC 61511-1 provide the general outline and requirements for effectively navigating these phases, unfortunately there is not any particular silver bullet strategy for these concerns.

One of the easiest things a facility can do to begin to address these challenges is to clearly label and identify SIS-related equipment. Despite the best efforts and intentions, things will be accidentally damaged in the process of performing work in a plant – the worst possible outcome is that it is not reported or fixed. A unique color painted on instrument housings, valves, conduit, and other items can help call attention to the criticality of SIS equipment (many facilities use "safety yellow," but this has a tendency to be overused such that it loses meaning).

Training plays an essential role in the turnaround management system. Instrument technicians and craftsmen must be well-trained on the procedures for servicing and testing SIS instrumentation and final elements. Operations and maintenance personnel must be aware of what safety instrumented systems are installed in the plant, that they are clearly labeled, and that it is extremely important that SIS-related items not be impaired, changed, or otherwise tampered with unless done so with explicit authorization and change control. When contract or temporary maintenance is employed at a facility, training can be a challenge. Site onboarding instruction and even the permit-to-work system may need to include mention of site SIS protocols for maintenance work and reporting abnormal events.

A strong change control / management of change system is vital for any hazardous process, but the system only works effectively when changes are recognized and processed through the system. This fact is yet another reason why training is such an important element of the overall management system. In a facility with a strong process safety culture and management of change program, getting changes authorized and documented is usually of less concern than ensuring that those changes are appropriately vetted. That the change control procedure and workflow should incorporate functional safety review whenever any part of the SIS is changed is both obvious and required as part of the IEC standard. Less obvious – though recognized in the standard – is the need to consider the effects of changes in non-SIS equipment or with the general protected process. Multi-product units are vulnerable to problems with these types of changes, particularly when one process requires a SIF and another does not. Unless all changes associated with the batch equipment are analyzed for functional safety impact across all processes utilizing the equipment, a gap could lead to latent issues with the SIS.

Change control is also particularly important for project commissioning and decommissioning work. If project approvals and management systems do not directly interface with the operational management of change system, they must be similarly equipped to evaluate functional safety concerns when installing, modifying, or removing equipment. Many batch processes are ephemeral in the life of the batch unit – a campaign runs once for a few months, and then never again. When this is the case, it may be better from a systems management standpoint to rely primarily on equipment-based SIFs that are largely independent of the active process. The major concern with equipment-based SIFs is that instruments and valves that are

good for one set of process fluids and conditions may not be appropriate for the next. Suitability of equipment for each process must be strictly evaluated when commissioning a new process that will rely on an existing SIF and SIS equipment. Decommissioning may also pose a danger if there is a call to remove SIS-related equipment that is shared among SIFs for multiple processes.

Well-written, comprehensive, checklist-style procedures help ensure that those activities are done in the proper manner, especially for unit conversions. Conversion procedures should include an operational readiness review (or pre-startup safety review) that accounts for the functional safety needs of the unit. Proof testing prior to startup (whether turnaround or conversion) is an ideal practice and provides the best assurance against an undiscovered impairment of the SIS. Proof testing needs, procedures, etc. will depend on each individual unit, what the SIFs are, and what was done to the unit during the preceding work.

A final concern with frequent batch unit transitions is that abnormalities with the SIS can become normalized rapidly. A small error of installation may require operators to initiate a brief bypass during the beginning or end of a batch. Unless this is recognized as a problem, such a deviation may be repeated multiple times each shift and will soon become the normal operating method. This can lead to further deviation from safe state when a true hazardous condition arises, and operators may begin to lose confidence in or actively distrust the SIS. Facility managers should promote a questioning and reporting culture that encourages rapid reporting of these types of concerns along with their resolution.

Conclusion

Successful implementation of safety instrumented systems in multi-product batch units often requires consideration of many items that are simply not present in a traditional continuous detect-decide-act SIS. This makes them more complex, which in turn makes their proper design and operation even more difficult. Six general principles are offered as guidance to successfully design and implement a robust SIS with the flexibility to provide functional safety to a batch unit:

1. Anything the SIS depends on must be managed as part of the SIS.
2. Challenge and minimize phase and recipe dependency.
3. Minimize BPCS to SIS communication. Use two-factor verification where possible.
4. Use permission architecture to allow BPCS safe state operation.
5. Consider permissive SIFs to avoid hazardous conditions.
6. Batch unit turnarounds and process conversions must be tightly managed.

References

[1] IEC. *Functional safety: Safety instrumented systems for the process industry sector* – Parts 1-2. IEC 61511. International Electrotechnical Commission, Geneva, 2015.

[2] ISA. *Example implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)*. ISA-TR84.00.04-2005 Parts 1-2. International Society of Automation, Research Triangle Park, NC, 2005.

[3] Van Beurden, Iwan and Amkreutz, Rachel. (2002, August). Emergency batch landing. *InTech*, pp 30-32.

[4] WIB/NAMUR Ad-hoc Working Group. *Functional safety in batch processes.* NE-154. Interessengemeinschaft Automatisierungstechnik der Prozessindustrie, Leverkusen, Germany, 2016.

[5] Stack, R.J. (2009). Evaluating non-independent protection layers. *Process Safety Progress*, *28*, pp 317–324.

[6] Boudreaux, Mike. (2011, February 10). Field device sharing between control and safety systems. [Blog post]. Retrieved from http://www.emersonprocessxperts.com/2011/02/field_device_sh/

[7] Marszal, Ed and Hawkins, Gary. (2012, April). When can the process control system, safety system share field devices? *Control Engineering*, *59*(4), pp 22-26.

[8] Marszal, Edward M. and Weil, Christopher P. Implementing protective functions in BPCS and combined systems. [Whitepaper]. Kenexis Consulting Corporation.