Proposed Abstract for the 2011 Texas A&M Instrumentation Symposium for the Process Industries

Focus Area: Automation – HMI

Title: **Shared Field Instruments in SIS: Incidents Caused by Poor Design and Recommendations for Improvement**

Author: Edward M. Marszal, PE, ISA 84 Expert
Kenexis
edward.marszal@kenexis.com, (614) 643-2451

Introduction

Even though the ISA 84 standard for Safety Instrumented Systems has been in use since 1996, there is still a lot of confusion about a key attribute of good SIS design – specifically separation of basic process control systems (BPCS) and safety instrumented systems (SIS). It could be argued that newer versions of SIS standards have further complicated the issue be specifically allowing combined safety and BPCS applications, given that certain requirements are met. The objective of the standard is not to enforce a complete separation between the systems but to either:

1) prevent a single point of failure from both creating a demand to the SIS to activate while simultaneously preventing the SIS from performing its critical action; or,
2) ensure that the frequency of this sort of single point of failure is low enough that tolerable risk goals are not violated.

The requirements for when sharing BPCS and SIS equipment is acceptable that are presented in the most recent version of the SIS functional safety standard (i.e., ISA 84.00.01-2004 – IEC 61511 Mod) are complex, confusing, and often misunderstood or simply ignored. Understanding when sharing is acceptable is and when it is not is further complicated by the fact that it is a multi-disciplinary effort, requiring knowledge not only of the instrumentation itself, but also of the process to which the equipment is connected. In fact, knowledge of the process and how it responds to BPCS failures is much more important. Verification that sharing BPCS and SIS equipment is acceptable thus requires a detailed analysis of all of the failure modes of the shared equipment along with an assessment of how each of those failure modes affects the process under control.

In the following sections, the author will clearly demonstrate the situations where combined safety and BPCS are not acceptable by providing descriptions of process industry accidents that are the direct result of combined designs. The paper will go on to provide guidelines describing how the systems should have been designed in order to avoid the problems that resulted in the accidents. The highlighting of the areas where combined designs have

historically failed will then result in common sense guidelines for applications where a combined design is acceptable.

Separation Requirements

The IEC/ISA 61511 standard for functional safety of safety instrumented systems has a number of key requirements that define the relationship between BPCS and SIS. These requirements were written to ensure that overall tolerable risk levels are always achieved and to ensure that BPCS failures do not have an adverse impact on the performance of SIS, potentially resulting in risk levels that exceed tolerable risk. The first key requirement is presented in the "Process Hazard and Risk Assessment" section of the standard (Section 8). Clause 8.2.1 presents the requirements for performing the risk assessment that will yield the risk reduction requirements for the SIS. This risk assessment considers the potential causes of unwanted accidents and the non-SIS safeguards that are in place to prevent the accident. An informative note to this clause clearly spells out the considerations that must be made when a single piece of equipment can both create process demands and then fail to respond to those demands.

> *8.2.1 –*
> *NOTE 1 In determining the safety integrity requirements, account will need to be taken of the effects of common cause between systems that create demands and the protection systems that are designed to respond to those demands. An example of this would be where demands can arise through control system failure and the equipment used within the protection systems is similar or identical to the equipment used within the control system. In such cases, a demand caused by a failure of equipment in the control system may not be responded to effectively if a common cause has rendered similar equipment in the protection system to be ineffective … In determining whether the overall design of process and protection layers meets requirements, common cause failures will need to be considered.*

This clause highlights the fact the separation between BPCS and SIS is an important consideration all the way back in the earliest stages of the safety lifecycle. The determination of the risk of a process before SIS risk reduction is applied usually considers the impact that BPCS failures have on the risk. When a required risk reduction to be allocated to the SIS is calculated, the tacit assumption is that the SIS is completely independent from the initiating causes of the hazard and also any other independent protection layers that were credited with reducing risk. If the SIS is not truly independent, this initial risk calculation is no longer valid, and the achievement of tolerable risk is no longer verified.

More requirements for the separation of BPCS and SIS can be found in the "SIS Design and Engineering" section of the standard (Section 11). Clause 11.2.10 contains a specific separation requirement along with an informative note providing more detail.

> *11.2.10 A device used to perform part of a safety instrumented function shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety*

instrumented function, unless an analysis has been carried out to confirm that the overall risk is acceptable.

NOTE When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand for the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared component because if the shared component fails, a demand will be created immediately to which the SIS may not be capable of responding. For that reason, additional analysis will be necessary in these cases to ensure that the dangerous failure rate of the shared equipment is sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered.

This clause sets requirements against the most critical flaw is shared BPCS/SIS components, which is using a single component whose failure simultaneously creates a demand and prevents actions against that same demand. While the clause, at first, categorically disallows this type of design, it then steps back and allows the design if "an analysis has been performed to verify that the overall risk is acceptable."

While this statement seems reasonable on its face, a lot of poor designs have been issued under the auspices of an "analysis" that verifies that the overall risk is acceptable. The problem stems from the quality (or lack thereof) of the analysis that justifies the combination. As will be discussed later in this paper, an analysis justifying combined SIS/BPCS is not a trivial task. The analysis will require assessment of ALL of the failure modes of the shared equipment in a Failure Modes and Effects Analysis (FMEA). This FMEA will consider more than just the control equipment. It will also consider the effect of how the failure will affect the process, and how that process upset might be "fed back" into the control system or SIS.

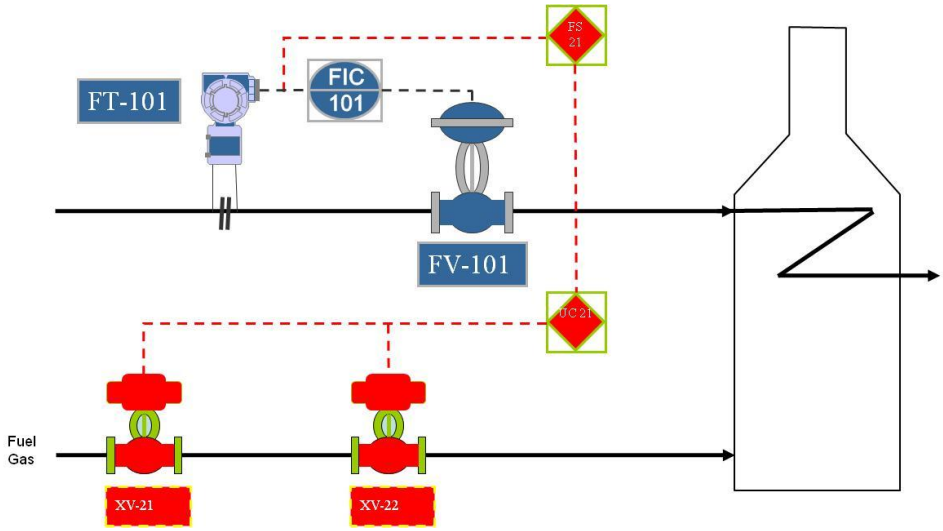
Case Histories

In order to demonstrate why Clause 11.2.10 of the IEC 61511 was written this paper will present two case histories of what can go wrong if separation requirements are ignored. The case histories are real accidents in the process industries that resulted in significant damage to the process. The case histories were specifically selected to demonstrate how use of shared field equipment can directly lead to a demand on a SIS combined with the unavailability of that same SIS, all due to a single component failure.

Case History #1 – Shared Measurement Device

A refiner in the Northeastern United States was operating a fired heater to elevate hydrocarbon feed temperature prior a reactor. In the early 2000's this refiner suffered an incident in this heater related to SIS failure. The incident resulted in a rupture of the process materials that were being heated in the furnace. Figure 1 presents a simplified depiction of the process and equipment related to the incident.

Figure 1 – Fired Heater Simplified Schematic



The fired heater depicted in Figure 1 was operating in a stable fashion for a significant period of time, when a cold spell occurred in the area, dropping the ambient temperature below the freezing point for a significant period of time. During this time period the insulation bag fell off the flow transmitter (via differential pressure) taps, which proceeded to freeze, locking in the pressure at the transmitter diaphragm and effectively isolating it from the process. Soon after, the operational situation of the plant called for a decrease in production rates through the unit, resulting in the flowrate setpoint being decreased. Since the setpoint was lowered below the measured variable (which was now frozen in place) the controller took action to close off the flow control valve in an attempt to decrease the flow. Since the taps of the flow transmitter were frozen, closure of the valves did not change the measurement that the controller received causing the controller to "wind up" and set the controller output (and valve position) to zero – completely stopping flow through the heater passes.

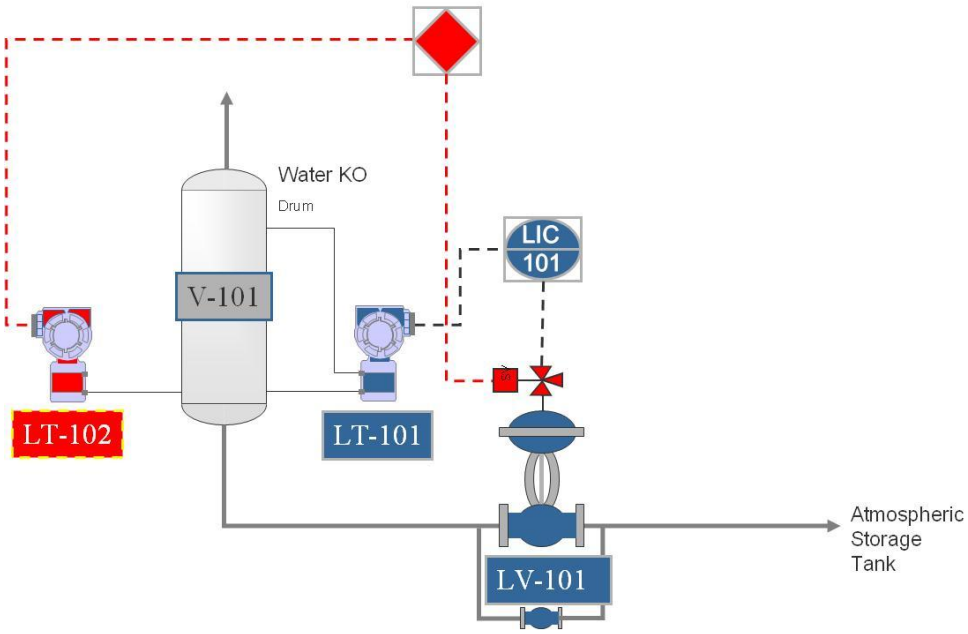
The plant designers foresaw that loss of flow was a dangerous condition and implemented a low flow shutdown which is intended to stop fuel gas to the heater upon detection of low flow. Unfortunately, the same flow transmitter was implemented in this design to take the SIS action. Since the SIS input "appeared" normal, no safety action was taken. Loss of flow through the heater tubes resulted in the tubes overheating beyond the limits of their mechanical integrity. The tubes subsequently ruptured causing release of the flammable hydrocarbons on the process side to be dumped into the firebox which resulted in a large fire in and near the heater firebox. While there was significant damage to the heater and appurtenances (>$10 Million) and a loss of production, luckily there were no injuries.

This accident was caused by the sharing between the BPCS and SIS of a transmitter whose failure caused a demand (i.e., caused heater pass flow to go dangerously low), and simultaneously prevented the SIS from being able to take its action to prevent the accident. This design is a clear violation of clause 11.2.10 of the IEC/ISA 61511 standard. In this case, the SIS was grandfathered to pre-ISA 84 standards, and no analysis of the risk of sharing a combined component was performed.

Case History #2 – Final Element Device

A oil and gas production company in the Middle East was operating a separator vessel in its production process that was intended to measure the interface level between hydrocarbon and water, and drain off the produced water into a sewer system where the water would be treated and re-injected into wells in the oil production formation. Figure 2 presents a simplified depiction of the process and equipment related to the incident.

Figure 2 – Water KO Drum Simplified Schematic



The water knockout drum system depicted in Figure 2 was operating in a stable when processing conditions changed, resulting in a significantly decreased water-make. As a result of the decreased water-make the interface level began to drop. As the interface level in the drum decreased the controller output to the valve decreased, signaling the valve to move toward the closed position. Unfortunately, due to lack of movement of the valve and fouling and build up on and around the plug of the valve, it did not respond the signal to go toward the closed position and was effectively stuck in place. The level continued to decrease below the level of the low-level shutdown. The low level shutdown effectively de-energized the solenoid valve and vented the diaphragm of the control valve, but since the valve is stuck in position, the valve did not move – rendering the safety action ineffective.

The interface level continued to drop until hydrocarbon began to leave the separator vessel and enter the produced water system. While the produced water system is intended to receive some degree of hydrocarbon, the system was completely overwhelmed with

hydrocarbon which accumulated and began to flash into vapor. Some of the vapors made their way to atmospheric vents and found a source of ignition, which resulted in a flash-back and explosions. The explosions resulted in significant equipment damage (>$1 Million) and significant lost production.

This accident was caused by the sharing between the BPCS and SIS of a final element (i.e., the valve) whose failure caused a demand (i.e., allowed excessive flow out of the separator vessel and subsequent release of hydrocarbon to the water system), and simultaneously prevented the SIS from being able to take its action to prevent the accident. As with the previous example, this design is a clear violation of clause 11.2.10 of the IEC/ISA 61511 standard. For this process, no attempt had been made to make the SIS compliant with IEC/ISA 61511 so no risk analysis of the combined system was performed.

Assessing Shared Field Equipment

In general, shared field equipment in combined SIS/BPCS service is strongly discouraged. Complete physical and functional separation of safety instrumentation from control instrumentation has been encouraged in a number of technical guidance documents going back to the AIChE Center for Chemical Process Safety's *Guidelines for Safe Automation of Chemical Processes* and before. Also, some safety related standards that employ instrumentation – such as NFPA standards for fired heaters and nuclear industry standards specifically mandate a complete physical and functional separation. The stance requiring separation is at least as safe as, and usually safer than, complicated schemes that employ combined devices, and this position also requires significantly less effort to assess safety because the protection layers and initiating events are all completely independent. In the experience of the author, the level of effort in justifying combined systems (when done properly) can be prohibitively expensive, and in many cases more costly than the redundant equipment!

If shared field equipment is to be employed, it is required to be subjected to a risk analysis that results in a determination of whether or not tolerable risk is still achieved considering the combined equipment. This analysis should take the form of a Failure Modes and Effects analysis (FMEA) of the shared equipment items. The FMEA proceeds by listing out all of the shared components (or shared functionality) of a system. Next, all of the failure modes of that equipment should be listed. For field equipment this will usually amount to a handful of modes, but if logic solvers are shared this could means thousands as each function that the logic solver performs would need to be considered as an "equipment item". For each failure mode, the effect of that failure on the process needs to be developed and documented. This analysis must assume that other safeguards fail in order to determine the ultimate consequence. Additionally, the assessment needs to determine if the primary failure resulting in the disabling, or unavailability, of an associated safeguard. Figure 3 presents a typical analysis using this methodology.

Figure 3 – Shared Component Analysis

Device	Failure Mode	Effect	Safeguards	Notes
LV-101	Fail open	Valve fully open	Overfill interlock failed	Single point of failure
	Fail closed	Valve closed	No shared interlock	
	Fail in place	Pathway open to completely drain vessel if input rate drops	Overfill interlock failed	Single point of failure
	Bypass open	Pathway open to completely drain vessel	Overfill interlock failed	Single point of failure

The lines where the notes column states "Single Point of Failure" are violation of the hardware portion of IEC/ISA 61511 clause 11.2.10. In these cases a further supplemental analysis would need to justify that the shared component is acceptable. In essence, it would need to be determined that the frequency of failure of the device is so low that its risk is tolerable, similar to making the device its own *continuous-mode* SIF.

Conclusions

In general, shared field equipment in combined SIS/BPCS service is strongly discouraged but the SIS functional safety standards for the process industries allow combination under certain circumstances. While combination is allowed, there are requirements that must be made when combined systems are undertaken – and these requirements need to be given significant consideration. The analysis required of shared components is complex and time-consuming and often done poorly or ignored at the peril of the facility owners and stakeholders. In order to ensure adequate safety, a documented and verified FMEA should be performed to ensure that devices do not simultaneously place demand and causes SIS unavailability, and in situations where they do – quantitative analysis needs to confirm that the frequency is sufficiently low.