BRIDGING THE SAFE AUTOMATION GAP

PART 2

Angela E. Summers, Ph.D., P.E., President, SIS-TECH Solutions

"Bridging the Safe Automation Gap Part 2," 2002 Instrumentation Symposium, Texas A&M University, College Station, Texas, January 2002.

"Bridging the Safe Automation Gap Part 2," Hydrocarbon Processing, May 2002.

In the decade since the release of the PSM regulation, every major industrial standard related to safe automation has undergone revision. API and NFPA standards have been modified to use stronger language and more prescriptive requirements. In 1996, the Instrumentation, Systems, and Automation Society (ISA) released ANSI/ISA 84.01-1996 (1), which is a performance based standard covering the lifecycle of safety instrumented systems (SIS). Internationally, in 1999, the International Electrotechnical Commission released IEC 61508 (2), covering the implementation of safety related systems. In 2002, the 10th anniversary of PSM, the international process industry SIS standard, IEC 61511 (3), will be released.

Much has been done to encourage, guide, and regulate safety through identification and control of procedures and systems installed to achieve safe automation. While industry is indeed safer from a personnel injury risk (i.e. falls, burns, cuts, etc.), significant events continue to occur at an alarming rate. Incident causes can be viewed as safe automation gaps, which must be bridged if a company desires to move from where it is now to safer operation.

This topic is divided into two parts. Part 1 discusses safe automation on a broad perspective examining safety culture, organization and hazards analysis issues. Part 2 focuses on instrumented systems and discusses specification, implementation, operation, maintenance, and management of change.

PART 2: SPECIFICATION, IMPLEMENTATION, OPERATION, MAINTENANCE, AND MANAGEMENT OF CHANGE

The process industry has been using instrumented systems for as long as there has been chemical processing. While the reliance on instrumentation has increased at an incredible pace, the resources allocated to properly specify, implement, and document these systems has declined. This has led to many significant deficiencies in the instrumented system design.

Over the years, this author has seen numerous examples of poor performing instrumented systems, poor operating and maintenance procedures, and inaccurate documentation. The following provides examples of six problem areas that must be addressed in order for plants to achieve safe operation.

Problem 1. General instrumentation Design

Separation

When the SIS logic is implemented in the Basic Process Control System (BPCS), the entire system is viewed by everyone, including operators, technicians, and engineers, as the BPCS. SIS logic can be accessed and changed as easily as BPCS logic, making management of change difficult. When the BPCS program is optimized, unexpected changes to the SIS logic can occur, ranging from a simple incorrect register setting to complete loss of a SIS functionality. Separation of the SIS and the BPCS provides a means for ensuring that access to the SIS is restricted, thus, maintaining SIS functionality.

Poor graphics for operator

HMI graphic software has enabled designers to use a large variety of colors and fonts and to increase the graphic density. This has resulted in some HMI screens having the clarity of mud. It is simply impossible for the operator to quickly review critical information or alarms. In some cases, the operator must page through multiple screens to make diagnosis and take action. When rapid response is required, information retrieval must also be rapid.

Ergonomics

The physical capability of the operator is occasionally challenged by the required field response. In one case, operators were required to go out to the field and run up and down flights of steps to adjust valve settings and to verify process response. In another, the procedure required the operator to manually close multiple, large valves to mitigate a hazardous event. The capability of the operator to rapidly act in hazardous situations is critical for safe automation.

Problem 2. SIS Design

Poor pre-trip alarms

When the pre-trip alarm setpoint is too close to the trip setpoint, the operator does not have time to respond in order to prevent the trip. The pre-trip alarm is a trip notification alarm letting the operator know that the plant is about to shutdown. If the intent is that operations should prevent the shutdown, the pre-trip alarm should provide enough time for the operator to take action. If the setpoint is too close to the trip setpoint, the operator will, in desperation, find a way to bypass the SIS to allow enough time for response.

No first out alarms

Daisy chained inputs do not allow first out indication to be provided to the operator. This reduces the troubleshooting capability and forces the operator to make assumptions about what caused the trip. In the worse case condition, the operator will restart the process to determine whether the trip corrected the process problem or whether the process disturbance has passed. If the process problem is serious and still present, the restart could result in an incident. First out indication is essential for troubleshooting the process.

SIS did not work from installation

A quick inspection of control room consoles will reveal instrument alarms that are being ignored. Talk to maintenance department personnel and they can point to instruments that do not work. Furthermore, inspections of maintenance reports reveal instrumentation that has repeatedly failed. Instead of

investigating whether the specification should be changed, the instrumentation was simply replaced/repaired and returned to service. In extreme cases, operations and maintenance personnel accept the failure and simply ignore or bypass the device. Non-working instrumentation should be investigated as potential near-miss incidents. If the instrument is not needed, remove it.

Start-up difficulties

Incidents are much more likely during start-up than during normal operation. Process startup difficulties can be caused by poor SIS design that requires numerous bypasses or multiple startup attempts to get the process up and running. To eliminate these problems requires thoughtful design and additional logic. Start-up logic must be developed during the SIS design and be thoroughly tested along with the trip logic.

Does not meet SIL

In many cases, the installed SIS is not properly designed to achieve expected performance. For example, the hazards analysis may describe a risk that requires a SIL 2 SIS for successful mitigation, but the installed SIS only achieves low SIL 1. In the worse case that this author has seen, the installed SIS was only 67% available, which does not meet the 90% minimum requirement to be defined as a SIS. Remember that an interlock symbol shown on a P&ID does not mean that the SIS can successfully mitigate the risk.

Inadequate testing frequency

Many SIS designs get installed that are comprised of good devices and adequate redundancy, but simply do not meet the SIL due to inadequate testing. Many plants have complied with the mechanical integrity program of OSHA PSM by stating that they test at turnaround. Unfortunately, a turnaround frequency of three years is unacceptable for many SIL 2 and SIL 3 applications. Consequently, provisions for on-line testing must be considered as part of the SIS design.

Excessive Nuisance Trip Rate (NTR)

Excessive nuisance trip rate can impact the safety of a facility by causing the operators to skip troubleshooting the cause of the trip and to initiate re-start assuming that the trip was false. Furthermore, most nuisance trips result in the activation of other safety systems, such as cascade trips in other units or the lifting of pressure relief valves. Start-up is also required after a shutdown, and industry data has shown that startup is where many incidents occur. Lowering the nuisance trip rate is essential for improving safety and plant uptime.

Problem 3. SIS Operation

Do not know the devices in SIS.

Many operators cannot walk through the process unit and identify which devices are connected to the SIS versus the BPCS. In plants that are serious about SIS access restrictions, these devices are clearly identified using paint or other highly visible methods. This educates operators and maintenance on SIS device location. It also allows operators to quickly assess the status of SIS devices and bypasses during plant walkthroughs.

Do not understand significance of trips

Many operators consider the SIS as the "taking me down" instrumentation, viewing the SIS as the enemy of plant operation. An operator who does not understand the significance of SIS trips is an operator who will not think twice about defeating the SIS. Operators must be trained on what the SIS is intended to prevent in terms of equipment damage and personnel risk. Information leads to informed decisions.

Do not understand what trips the SIS and when

Many operators are unaware of equipment and process operational limits. The operator often does not know when the SIS will trip the process. This is especially a problem with Vendor packages, which often provide general trip notification alarms. The operator must understand what trips the process and why.

Do not know what to do in response to SIS device faults

When the operator receives a SIS diagnostic alarm, the operator must know what to do in response to the alarm. This is substantially more than calling maintenance to repair the device. There must be an identified compensating measure or mitigation plan for maintaining safe operation. This might include control room monitoring of specific control system variables, field monitoring of local process indicators, or initiation of shutdown if repair is not completed within a prescribed period of time.

Problem 4. Bypassing

No procedures for bypassing

There is a lack of adequate SIS bypass procedures. In many facilities, the operators have the authority to bypass the SIS without management of change or supervisor approval. Plant personnel seem to think that since the bypass will only last for a short time period that the risk is acceptable. Personnel must be trained that, when a SIS is placed in bypass, the process is unprotected.

SIS in bypass and no one knew it

When bypasses are routinely used, someone will eventually put something in bypass and forget about it. This is especially true if the bypass is physical (e.g., jumper) and no alarm is provided. If the plant does not require authorization or bypass logs, there is no paper trail for what is in bypass. When a SIS is placed in bypass, there must be an intermittent, recurring alarm until the SIS is returned to service.

Plant management said to ride out upsets in bypass

When pressed, operators will relate episodes where they were told to place the SIS in bypass in order to run closer to the trip setpoints and to allow the operator to ride out upsets. The operator and plant management must understand what the SIS is designed to prevent and what will happen if it does not function when required. Armed with this knowledge, it is more difficult to simply ignore the risk. An very effective impediment is to require management authorization and sign-off for bypassing.

Problem 5. Testing and Inspection

Not doing inspection or testing at defined testing frequency

An informal survey of various operating companies revealed that less than 25% of safety critical instrumentation actually gets tested at the frequency that the instrumentation should be tested. The only

way to determine whether a SIS device is functional is to test it or have a process demand that requires that the device functions. The new SIS standards require that the testing frequency be defined that is necessary to achieve SIL. If the required testing frequency is 12 months, the testing should be performed every 12 months not 14 months, 18 months, or 3 years.

Incomplete testing

The entire SIS loop must be functionally testing at a frequency sufficient to achieve the SIL. However, in some plants, the difficulty associated with testing the final element has resulted in the plant personnel deciding that they will test "what can be tested" without process interruption. This typically means that the block valves are not tested until turnaround. However, the entire hazards analysis was directed at determining the safe state condition for the process, which involves the closure of the block valve. If this is not going to be tested, there is no need to even discuss SIL.

Inadequate or no testing procedures

Too many people feel that the cost associated with writing SIS testing procedures cannot be justified. As mentioned in Part 1, some managers think that if they have to tell a technician what to do that they need a new technician. This is not about the technician's capability or training. It is about being able to predict SIS performance, which means that the functional test of the SIS should be performed the same way each time. Testing procedures should also state the approvals and notification requirements for removing and returning a device to service.

Not documenting testing during turn-around

A lot of information is lost during a turn-around. For example, significant buildup in process taps or valve seats are cleaned without any notation in the maintenance record. The reality is that what can be tested in the allocated turnaround period is what is tested and little documentation is retained on what actually got tested, cleaned, or repaired.

Incomplete functional testing after modification

The SIS is often modified and, as long as it appears to be working, the SIS is assumed to be functional. However, the only way to make sure that the "simple" modification did not impact the operation of other safety functions within the same SIS is to test all potentially affected logic.

Problem 6. Management of Change

Everyone needs to understand what triggers a management of change review and why tracking these changes are important. For the SIS, change tracking is done to ensure that the SIS functionality is maintained. The SIS devices are typically less than 15% of the total instrumentation, but the SIS can keep the plant from running and if it fails to perform can allow the hazardous incidents to propagate into equipment damage and/or personnel impact.

CONCLUSION

The Chemical Process Industry must be willing to look honestly at their safe automation policies, design practices, and operational philosophy. The problems discussed in this paper cut across industry, affecting large, public corporations and small, private companies. No process operation is immune.

Plant operation must be examined critically to look for opportunities to reduce risk. This examination must be substantially more than listing safeguards in a hazards analysis. It must consist of a detailed review of the safeguard design, operation, and maintenance from an engineering and human factors approach. Moreover, hardware, such as instrumented systems, cannot be viewed as the only required component for safe operation. Plant personnel must understand the risk that the instrumented systems is designed to prevent and how the instrumented system mitigates the risk. They must understand the actions required when the instrumented system is not functioning and that maintenance must put high priority on the repair of these systems. Finally, plant management must emphasize that instrumented systems are important to plant operation and must be protected. Only through our protection of these systems can these systems protect the plant, yielding true safe automation.

REFERENCES

Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA 84.01-1996, “Application of Safety Instrumented Systems (SIS) for the Process Industry,” Research Triangle Park, NC (1996).

International Electrotechnical Commission (IEC), IEC 61508, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems,” Geneva, Switzerland (1999)

International Electrotechnical Commission (IEC), IEC 61511, “Functional Safety: Safety Instrumented Systems for the Process Sector,” Geneva, Switzerland (expected 2002).