LESSONS LEARNED IN AUDITING AUTOMATED SYSTEMS FOR PSM COMPLIANCE

Angela E. Summers, PhD, PE, President, SIS-TECH

Lessons Learned in Auditing Automated Systems for PSM Compliance, 1st Latin America CCPS Conference, featured speaker, Buenos Aires, May 27-29, 2008.

Abstract

While reliance on instrumentation has increased at an incredible pace, resources allocated to design and manage the equipment have declined in many companies, leading to more burden and expectations being placed on fewer and fewer people. Quality instrumented system performance relies on a rigorous management system that minimizes human error and equipment failure potential. This paper focuses on safety instrumented systems and applicable process safety management requirements. Observations from assessments and audits are provided, illustrating poor performing instrumented systems, inadequate operating and maintenance procedures, recordkeeping and retention practices, and out-of-date documentation.

Introduction

The process industry has rapidly adopted automation to improve product quality and production rates, to reduce the potential for operator error, and to decrease manpower requirements. Process industrial automation includes many systems, such as production controls and alarms, safety systems, and mitigation systems. New technology often brings production, product quality, and cost performance benefits. However, new technology also demands more effort and expertise throughout the equipment's installed life. The more programmable electronics that are involved in the equipment's operation, the more prone to systematic flaws the system becomes, which can lead to unpredictable operation. Reliable automation leads to safer operation. Poorly implemented or poorly maintained - automation can lead to significant hazardous events impacting people, the environment, and assets.

A safety instrumented system is a subset of "safety systems" which are covered by OSHA 1910.119 (1). Safety systems are subject to assessment for compliance with specific OSHA process safety management (PSM) requirements, as well as applicable recognized and generally accepted good engineering practices (RAGAGEP). PSM requirements address five general subjects:

- Planning
- Hazard and Risk Analysis
- Design Basis
- Maintenance Procedures
- Operating Procedures

SIS-TECH

12621 Featherwood Drive • Suite 120 • Houston, Texas 77034
Tel: (281) 922-8324 • Fax: (281) 922-4362
www.SIS-Tech.com

Each subject is presented below with references to specific OSHA PSM paragraphs. The highlighted issues and gaps are an amalgam of this author's observations over the last 12 years since ANSI/ISA 84.01-1996 (2) was issued by ISA. If you recognize aspects of your own facility in my observations, consider this confirmation of the reality of what is presented and a challenge for you to overcome.

Planning - PSM (d)(3)(ii), (d)(3)(i)(F), and (d)(3)(iii)

Many facilities do not have any formal work process to ensure equipment complies with RAGAGEP. Mike Marshall, OSHA Directorate of Enforcement Programs, has stated (3) that OSHA's view of the applicability of RAGAGEP is provided in a compliance letter to Lois Ferson, ISA dated 11/29/2005, concerning ANSI/ISA 84.00.01-2004 (4,5). Mr. Marshall stated that the name of any industry practice could be substituted into the letter where it references the S84 standard. Essentially, OSHA expects facilities to identify applicable good engineering practices, or to develop their own, and to demonstrate compliance to those practices. If OSHA identifies practices applicable to the process that the owner/operator did not apply, the owner/operator could be found in violation of the grandfather clause of PSM or the general duty clause of the OSH Act.

> "In support of a Section 5(a)(1) citation, industry consensus standards, such as ANSI/ISA - S84.00.01-2004, can be used as evidence that a hazard is recognized and can feasibly be abated. (4)"

A grandfather clause is included in ANSI/ISA 84.00.01-2004 for safety instrumented systems. Clause 1 y states For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issue of this standard (e.g., ANSI/ISA-84.01-1996), the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner. In 2006, the ISA SP 84 committee published ISA TR84.00.04 (6), a guidance document on ANSI/ISA 84.00.01-2004. It states that there are two essential steps to determine the acceptability of existing equipment under the grandfather clause:

- Confirm that a hazard & risk analysis has been done to determine qualitatively or quantitatively the level of risk reduction needed for each safety instrumented function in the safety instrumented system.
- Confirm by assessment that the existing safety instrumented function has performed as designed and delivers the needed level of risk reduction.'

A grandfather clause evaluation requires a review of existing process safety information, mechanical integrity records, operating records, management system records, and metrics. If the result of the review is satisfactory, the owner/operator may choose to maintain the existing equipment as is. Performance shortfalls and documentation gaps must be addressed with action plans to close those gaps.

While the evaluation is obviously an OSHA expectation, many companies do not actively review existing equipment against current practices. Sometimes, it seems that management views industry practices with disdain, as if somehow this crazy group of people with some ulterior motive wrote impractical things. There is little support for writing internal practices or requiring compliance to industry practices. Instead, support goes to create a 'legal interpretation' that lack of compliance is acceptable.

Yet each time a regulatory or independent investigation board publishes findings, they cite lack of compliance to industry practices. Regulatory and liability expectations are that risk is driven as low as reasonably practicable (ALARP). Since the capital cost of instrumented safety systems is small compared

to process equipment and control system investments, ALARP arguments are typically not applicable to SIS. Further, most industry practices document minimum requirements for the stated application. Owner/operators should demonstrate that deviation from a RAGAGEP meets or exceeds the intent of the practice.

Hazard and Risk Analysis - PSM (d)(2)(i)(E) and (e)(3)(iii)

Hazard and risk analysis is an area where the techniques and software tools have improved substantially since the 1990s. Recognizing the need to capture the latest in techniques, CCPS is releasing an update to Guidelines for Hazard Evaluation Procedures [HEP, 7] in 2008. HEP emphasizes the analysis of hazardous events and the identification and reduction of risk. Identified safeguards should be covered by process safety information, operating procedures, maintenance and test procedures, and training. Residual risk should be addressed with compensating measures and action plans to reduce risk as required.

Every company has a stack of hazard and risk analysis reports, but the quality of this information is often very poor. Analysis reports should be considered official company documents for collecting and distributing information concerning the process hazards and the safeguards used to respond to them. Unfortunately, many facilities treat this analysis as a regulatory burden and assign minimum resources and time to it. An effective hazard and risk analysis identifies events for all intended operating modes and develops strategies for preventing them. A poor hazard analysis may result in inadequate risk reduction through poor definition of functionality or excessive performance claims on safeguards.

Compounding the problem is that collected information is considered a compliance item and it is stored. It is accessible, so every company appears to meet the letter of the PSM requirement. However, most companies do not use the information for any other purpose. Companies are not taking ownership of the hazard and risk analysis. Instead, many complain about the content and overall meaningfulness of the report. The business value of the hazards analysis is the use of report to train people on how deviations from normal operation propagate to process hazards. The risk analysis defines the risk reduction strategy selected to address unacceptable risk. Plant management, engineering, operations, and maintenance must understand this information if they have responsibility for decisions affecting the hazards or risk. Operator and maintenance procedures should include a description of the process hazards where their actions potentially increase risk. The hazards analysis documents should be discussed at Operations' safety meetings.

Management of change reviews and risk analyses routinely miss hazardous events. In some cases, the analysis did not identify the hazardous event because the initiating cause was not identified, the cause was considered non-credible, or the consequence severity was underestimated. The "single jeopardy" only rule that was intended to prevent people from confusing hazardous event causes with protection layers has been inappropriately applied to eliminate the evaluation of legitimate low frequency, multiple jeopardy events. Further, some events have been deemed non-credible due to the required time for event propagation even though similar events have occurred within the process sector. There is a tendency with low frequency events to assume that it cannot happen at particular site; previous experience is discounted as being due to poor luck or incompetence.

Increased risk due to changes in the process equipment operation is also not adequately evaluated. Many production units are now running significantly above the original design capacity. Advances in control system technology have been exploited to the disadvantage of safety to allow process units to run significantly above original design capacity. Some are operating very close to the vessel

maximum allowable working pressure (MAWP), resulting in inadequately sized, weeping pressure relief valves and fatiguing rupture disks. The total process safety time has shrunk to the point where there is often inadequate time for effective operator response or automated system response. Risk has escalated as competitors ramp up production and build larger facilities. Yet, the impact of these process changes is not reflected in the hazards analysis documents.

Significant changes to safety equipment technology, design, and mechanical integrity have occurred over the last 30 years, but these changes cannot be detected within the hazards analysis. Many users are still treating the safeguard evaluation as a check box – do we have some? Yes. There is little assessment of the design and management of the equipment, review of the procedures and documentation supporting the claimed risk reduction, or discussion of actual mechanical integrity results. Each generation of new technology is considered better than the last when experience actually demonstrates the opposite that, while many modern programmable devices have better configuration and diagnostic capability, they tend to fail more frequently than the previous generation.

Design Basis - PSM (d)(3)(i)(H), (j)(6)(i), and (j)(6)(iii)

Written process safety information is often missing for safety systems at many facilities. When it is available, it is often not as-built and misrepresents the current system architecture. An as-built design basis must be available for all safety systems to support management of change, proper validation, and training. For SISs, the design basis includes the safety requirements specification and the verification that safety equipment meets the risk reduction expectations. Detailed engineering must ensure equipment is specified and configured as necessary to achieve the safe state and required risk reduction. Design deviations must be justified to be as safe or safer.

The lines between safety and control became blurred at some facilities when distributed control systems were first implemented. These facilities combined control and safety loops within a single DCS or basic process control system (BPCS). In a few cases, the combined equipment is designed to be fault tolerant, is safety-configured, and is managed as safety. In most cases, the equipment is none of these. There is generally little to no process safety information on the control and safety system design within the combined system. The shared equipment is not included in the mechanical integrity program or management of change process.

Control systems operate in an intermittent or continuous mode, maintaining the process within prescribed process limits. Random and systematic failures that occur throughout the lifecycle are detected as soon as they begin to effect production and product quality. In contrast, safety systems are demand mode (or dormant) systems. That is, they operate only when the process exceeds a specified condition. Inadvertent or deliberate changes to safety equipment are not easily detected during normal operation. Safety system failure is found by demanding that it operate, either by proof test or process excursion. If equipment failure is found through test, an opportunity for continuous improvement is revealed. If it is found through process excursion, an incident may occur. A rigorous and documented management system reduces the potential that human error could defeat safety system operation.

Without a clear defense-in-depth strategy, design and management tends to fall to the lowest common denominator. Everything is eventually managed as control rather than safety, since so much of the combined system is dedicated to control. As a result the potential for common cause is higher in all aspects, including hardware, software, and people. When the same hardware and software is used for control and safety, failures or errors missed in installed equipment and during user approval processes can

become the common cause failure leading to a hazardous event. This is why many facilities choose to implement separate, independent and diverse logic solvers, as discussed in ISA TR84.00.04 Annex F.

Mechanical Integrity - PSM (j)(1)(iv), (j)(1)(v), (j)(2), (j)(3), (j)(4)(i), (j)(4)(ii), (j)(4)(iv), (j)(4)(iii), j)(5), (j)(6)(ii), (l)(1), and (m)(1)

The mechanical integrity schedule is often based on process equipment objectives rather than on the needs of the safety equipment. For example, the proof test interval floats with the unit turnaround schedule with little consideration for how this might impact the equipment integrity. At a minimum, the schedule should consider prior use information, manufacturer recommendations, and risk reduction requirements. The mechanical integrity schedule should consider identified performance gaps, wear-out conditions, or repeated failures during field operation. The proof test schedule should be a reportable 'management focus' metric, ensuring on-time testing and proper allocation of resources. Proof test delay should be approved through a management of change process which considers the risk of safety equipment misoperation.

Further, many facilities no longer perform frequent routine inspection and preventive maintenance of safety equipment. Advances in instrumentation have been taken as a license to extend all activities, including proof testing to turnaround by relying heavily on equipment diagnostics to detect failure. Probabilistically, this is acceptable philosophy, as long as the mechanical integrity program maintains the equipment in the "as good as new" condition. But in some facilities, the concept has been taken too far. It is assumed that equipment diagnostics are sufficient, so no other inspection, preventive maintenance or testing is performed.

There are several problems with this concept. The failure must have been identified previously for diagnostics to cover it. Internal diagnostics suffer from a high degree of common cause and systematic error. Safety equipment manufacturers generally do not provide means for testing internal diagnostics, so it is not possible for the user to prove that each diagnostic is functioning as required. Equipment diagnostics rarely cover peripherals, process connections, or support systems. Excessive diagnostic coverage claims extend the calculated proof test intervals, increasing the probability of the equipment being run to failure.

Safety equipment maintenance is often not prioritized. Management does not seem to understand that the out-of-service time is a higher risk period. This is especially true when compensating measures consist of shifting responsibility for safe operation onto a busy operating crew. This compensating measure seldom achieves equivalent risk reduction. After all, the operator's principle duty is production, not process safety management.

Proof test procedures are inadequate or missing for many types of safety system equipment. Many owner/operators assume that a trained technician knows how to test equipment. However, a proof test demonstrates the operation of equipment according to a design specification written to address an identified process hazard. While the technician may understand how to perform basic tasks, a detailed proof test procedure is needed to ensure adequate demonstration that the equipment works as specified for every anticipated operating mode, e.g., the pass/fail criteria for normal, alarm, and trip conditions. The technician must also understand how to judge whether the installed equipment will continue to operate in the "as good as new" or "fit for purpose" condition until the next proof test.

In many facilities, bypasses obtain easy approval without planned and documented compensating measures. Bypasses allow processes to continue to operate while safety equipment is out of service awaiting maintenance. Bypasses are sometimes allowed to remain in place for an extended time period

without management of change approval. At some facilities, the view is that any bypass period is okay as long as someone approves it. In the majority of facilities, operations is notified about the temporary bypass. However, the total time in bypass is not tracked and extended bypass is not covered by management of change in many facilities. Repeated repair or bypass is not tracked and trended.

Many facilities expend significant resources on maintenance. However, many mechanical integrity programs are failing because of the poor quality of the investigation and tracking of repeated failure. Proof tests must demonstrate that equipment is maintained in the "as good as new" condition. Procedures should clearly state the pass/fail criteria so failures can be properly classified. Maintenance records should be tracked and trended based on technology and operating environment. Failures on demand and spurious operation should be recorded and investigated to identify the root cause, so measures can be taken to reduce occurrence.

Pre-start-up safety review - PSM (i)(2)(i)

The pre-start-up safety review (PSSR) is an area where many facilities have improved since the 1990s. Many companies now use an extensive checklist covering major process equipment and controls. However, there is still an inadequate evaluation of the safety system documentation, procedures and training. The PSSR assesses:

- New or modified equipment is installed and demonstrated to operate per design intent;
- Adequate procedures are in place;
- Appropriate hazard analysis or management of change reviews have been conducted and their recommendations addressed; and
- Training of affected personnel has been completed.

Additional information about the PSSR can be found in CCPS Guidelines for Performing Effective Pre-Startup Safety Reviews (8). For safety instrumented systems, the PSSR is the same as the ANSI/ISA 84.00.01-2004 Stage 3 functional assessment.

Operating procedures - PSM (f)(1)(i), (f)(1)(ii), (f)(1)(iv), and (g)(1)(i)

In many facilities, the operator is considered an important safeguard in addressing abnormal operation, whether action is taken in response to an observation, indication, or alarm. Unfortunately, too many companies support this very significant decision with procedures directing the operator to execute shutdown "if deemed necessary." When "deemed necessary" is not defined, significant uncertainty is introduced in the operator actions. Will the action be a correct and timely one? Operator training must include recognizing specific process safety and health hazards, managing abnormal and emergency operation, and following safe work practices applicable to job tasks. This becomes even more important when the operator is providing 'compensation' for failed or bypassed safety equipment.

Most facilities have excellent quality control procedures covering the production process. The influence of ISO quality standards is readily apparent. Operators are generally well-trained on the existing operating procedures, even on facilities where deviation from procedure is common. The gap is that the procedures do not cover everything they should. So, while it is widely acknowledged that human error is one of the leading causes of process safety incidents, this awareness has not resulted in detailed safe operating procedures. In many facilities, operator procedures do not adequately cover:

- Potential hazardous events

- ISS description (e.g., how it detects and acts to stop the event) and expected process response if system acts as planned
- Operator action if the ISS fails to function
- What actions to take when equipment failures are detected
- What actions to take in response to alarms
- What to do when the system does not act as expected
- When to execute (e.g., never exceed, never deviate condition) manual shutdown.
- Conditions required for safe startup
- Reporting expectations for abnormal events including safety alarm, interlock, and SIS activation.

Detailed procedures are essential for safe operation, but human error cannot be completely eliminated. W. Edwards Deming, widely regarded as the father of quality control, believed that 85% of a worker's effectiveness is determined by the system he works within, only 15% by his own skill. Procedures can rarely substitute for fail-safe design, but instead should be considered a supplement to good design. Good procedures and equipment in the hands of a competent and trained operator is a recipe for success. Good safety equipment that is well maintained allows the operator to concentrate on production rather than covering equipment shortfalls.

Conclusion

Owner/operators must implement a management system with work processes and metrics that ensure safety equipment operates consistently in a safe manner and fulfills government and jurisdictional requirements. This requires a comprehensive program for identifying and integrating the latest good engineering practices, such as ANSI/ISA 84.00.01-2004, into work processes. Internal practices and procedures should clearly define expectations, so task quality is achievable, whether performed by the best, average, or somewhat distracted employee.

Recommended work processes and activities are provided for instrumented protective systems in CCPS Guidelines for Safe and Reliable Instrumented Protective Systems (9) and for safety instrumented systems in ISA TR84.00.04. The following should be collected and maintained for the life of the equipment:

- Hazard and risk analysis reports
- Design basis documents
- Operation, testing, and maintenance procedures
- Inspection, proof test, and maintenance records
- Failure reports (e.g., trip reports and equipment failure reports)
- Near miss and incident investigation reports
- Management of change records
- Training records
- Audit reports

References

OSHA, "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents, 29 CFR Part 1910." Federal Register 57, 36, Washington, DC (1992).

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

Mike Marshall, OSHA Directorate of Enforcement Programs, 2007 Center for Chemical Process Safety (CCPS) technical steering committee meeting, Salt Lake City, Utah (2007).

OSHA, correspondence, Richard Fairfax, Director, Directorate of Enforcement Program, to Lois Ferson, Manager of Standards Services, Instrumentation, Systems and Automation Society, DEP/GIE/SMK, dated November 29, 2005.

ANSI/ISA 84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Instrumentation, Systems, and Automation Society, NC (2004).

ISA TR84.00.04, Guidelines for the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511), Instrumentation, Systems, and Automation Society, NC (2005).

Guidelines for Hazard Evaluation Procedures, 3rd edition, American Institute of Chemical Engineers, NY (2008).

Guidelines for Performing Effective Pre-Startup Safety Reviews, American Institute of Chemical Engineers, NY (2007).

Guidelines for Safe and Reliable Instrumented Protective Systems, American Institute of Chemical Engineers, NY (2007).