Quality Assurance in Safe Automation

Angela E. Summers, PhD, PE, President, and William H. Hearn, PE, Senior Consultant
SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120, Houston, TX 77034
asummers@sis-tech.com, www.sis-tech.com

Published in Process Safety Progress (2008).

Adapted from: Quality Assurance in the Management of Instrumented Safety Systems, 1st Latin America CCPS Conference, featured speaker, Buenos Aires, May 27-29, 2008.

Quality Assurance in the Management of Instrumented Safety Systems, American Institute of Chemical Engineers, Process Plant Safety Symposium, 2008 Spring National Meeting, New Orleans, LA, April 6-10, 2008.

ABSTRACT

A perfect process would have no hazards, but perfection is impossible in the real world. Nearly all process units have inherent risk associated with their design and operation. Safe operation is maintained with a risk reduction strategy relying on a wide variety of safety systems. This article focuses on the most common safety systems for managing process deviations during planned operating modes – instrumented safety systems (ISS), such as safety alarms, safety controls, and safety instrumented systems (SIS). Rigorous quality assurance is necessary to achieve real-world risk reduction, so this article follows the Plan, Do, Check, and Act process to discuss quality assurance and its application to ISS. © 2008 American Institute of Chemical Engineers Process Saf Prog 27: 323-327, 2008

Keywords: process hazards, instrumentation, safety instrumented systems, quality assurance

INTRODUCTION

Too many owner/operators have used fatalities as the predominant metric to substantiate safe operation. The Baker report [1] states that this metric is inadequate, because this type of incident should occur so infrequently that it is meaningless as a quality indicator and, since it is what we desire to prevent, it does not provide any feedback to allow corrective action prior to occurrence. The Baker panel suggested adoption of other less-lagging indicators, such as the number of loss-of-containment incidents, injuries, fires, and explosions. CCPS [2] has agreed and has published a recommended list of metrics for process safety incidents.

Preventing errors and improving safety requires a systems approach that identifies and monitors conditions which are precursors to failure. The problem is not bad people and lack of competency; the problem is that the systems governing equipment are not rigorous enough to ensure instrumented safety system integrity.

Quality design and management practices are absolutely essential if real risk reduction and incident prevention – not just calculated risk reduction – is to be achieved. Without effort, latent conditions appear over time causing failures in the safety layers like holes in Swiss cheese. Unless proactive action is taken, the holes will eventually align to present a challenge to safe operation when process deviation occurs.

Only a rigorous quality management system can maintain the integrity expected from ISS. Identifying improvement opportunities is essential to counter latent failure and minimize risk. An active approach evaluates the present state of safe operation by monitoring for behaviors, errors, and failures that lead to releases. This article uses the Plan, Do, Check, and Act process of the Shewhart cycle [3] to discuss the various quality assurance activities necessary to achieve safe operation using ISSs.

PLAN

W.E. Deming [4] believed that 85% of a worker's effectiveness is determined by the system he works within, only 15% by his own skill. Planning results in a set of policies, practices, and procedures that seek to identify key activities and monitor the quality of their execution. Planning ensures that work processes yield equipment that operates consistently in a safe manner, fulfills government and jurisdictional requirements, and meets recognized good engineering practices. Recommended work practices and activities are provided for instrumented protective systems in the CCPS book, Guidelines for Safe and Reliable Instrumented Protective Systems [5] and for safety instrumented systems (SISs) in ANSI/ISA 84.00.01-2004 [6] and ISA TR84.00.04-2005 [7].

There is no substitute for knowledge [8]. A small amount of knowledge can save many hours of work or prevent mistakes leading to process hazards. Knowledge expands when hazard evaluation procedures [9] are used throughout the equipment life to identify and evaluate hazardous events. Knowledge evolves over time as research and development produces operational facilities, yielding real-world experience with process deviations and historical records on performance. Loss-of-containment events identify weaknesses in the risk reduction strategy, leading to the implementation of improved safeguards.

The hazard evaluation must be thoroughly performed and its findings addressed during the lifecycle, so risk is reduced as low as reasonably practicable. HSE [10] identified the three most prevalent causes of risk control system failure as inadequate operating procedures or work execution, plant and process design errors, and hazard and risk assessment errors. HSE analysis of incident data [10] determined that more than one in four hazardous events were missed during hazard and risk assessment. Another incident analysis [11] found that more than one in three incidents that occurred due to process deviations from normal operation were not adequately considered as potential hazards or causes of equipment failure.

Process knowledge is sustained by a foundation of written process safety information (PSI), covering the process hazards, technology, and equipment. Detailed PSI prevents the loss of process knowledge and history as operators and technical personnel move to other units or take different jobs. Continuous analysis and improvement of safety practices is necessary to counteract loss of expertise through retirements, downsizing, and equipment degradation.

Event risk is analyzed to determine the causes and potential frequency of occurrence. Independent protection layers are implemented to ensure that single failures or errors do not compromise safe operation. When the residual risk exceeds the owner/operator risk criteria, additional administrative and engineered safeguards are recommended and implemented to reduce the risk below the criteria. These safeguards include ISSs that achieve or maintain a safe state when unacceptable process conditions occur.

A written design basis should define the PSI for identified safety equipment and be traceable to the hazard and risk assessment. For safety instrumented systems, the design basis is the hardware and software safety requirements specification [6]. The design basis should be maintained under revision control for the life of the equipment and should ensure the following:

- The safety equipment has been proven to work in the operating environment with the required performance.
- The safety system is designed to exceed the risk reduction specified in the risk assessment

However, the most important things are unknown and unknowable [8]. So, many owners/operators rely on a defense-in-depth strategy using multiple independent protection layers to lower operational risk [12]. Defense-in-depth also requires minimization of common cause, common mode, and systematic errors that cause multiple layers to fail [5,12].

Finally, planning must consider security and management of change. Physical and cybernetic access to the ISS should be restricted using administrative procedures and physical means [5]. Common cause assessments should consider data communication failures. Written procedures should address how to initiate, document, review, and approve any changes to ISS other than replacement in kind. Changes to the process or its equipment should be evaluated to determine and resolve impact to the ISS requirements [5].

DO

This phase involves the implementation of the various administrative and engineering safeguards identified during planning. From a project-implementation perspective, detailed engineering must yield an ISS installation that meets the design basis and exceeds the required performance. Detailed engineering includes sufficient information to ensure ISSs are properly specified, constructed, installed, commissioned, operated, and maintained. ISS equipment should be user approved for the intended operating environment through a formal process that considers compliance with appropriate standards, the operating environment, the design basis requirements, and performance history.

Equipment should have prior use in control applications so issues associated with equipment operation and performance can be promptly identified in a continuous service. Lessons learned and operational history provides justification for the selection of safety equipment, which generally operates in a standby mode where failure may only be found through proof test or process demand.

Equipment classification also considers the core attributes of protection layers, namely independence, functionality, integrity, reliability, auditability, management of change, and access security. Detailed design

should provide an ISS equipment list identifying the equipment by a unique designation (e.g., the tag number) and the required inspection and proof test interval.

Validation activities include an input-to-output test of each new or modified ISS to demonstrate and document that the equipment is installed according to the specification and operates as intended for each operating mode. Validation must be satisfactorily completed prior to the initiation of any operating mode where a hazardous event could occur that requires the operation of a new or modified ISS.

Proof tests should be periodically conducted using a written procedure to validate the successful ISS operation and to identify and correct deviations from the design basis and equipment specification. Maintenance personnel should be trained on the procedures as necessary to ensure equipment is maintained in its "as good as new" condition. The proof test interval should be based on the relevant regulatory or insurance requirements, equipment history in a similar operating environment, manufacturer's recommendations, and risk reduction requirements.

Operating plans should support the inspection and preventive maintenance requirements that are necessary to maintain the required equipment performance. ISS proof tests should demonstrate that the mechanical integrity program is maintaining the equipment in the "as good as new" condition. Mechanical integrity program records and trends are fed forward into the Check phase of the quality cycle. Operating procedures cover the safe and approved methods for interacting with the safety equipment, such as bypassing, manual shutdown, and reset. Operations personnel should be trained and tested on the procedures as necessary to ensure that the correct actions are taken.

CHECK

The more that is known about the process and what is affecting its operation, the better the risk can be managed. An HSE study [10] reported that 37% of loss-of-containment incidents resulted from incorrect operator action, due to inadequate operating procedures, deficient process design, inadequate supervision, and ineffective management of change. People performance is limited by the quality of the verification, assessment, and auditing activities. Another 32% of loss-of-containment events [10] were caused by process and safety equipment failure, due to inadequate design and maintenance. Safety equipment performance is limited by the rigor, timeliness, and repeatability of mechanical integrity activities.

By what method? Only the method counts [8]. The Check phase applies metrics to the work processes to provide a standard means for assessing performance against requirements. Sustainable operation is achieved by focusing on metrics which provide predictive performance indication on a real-time basis. Example metrics are provided in Table 1 for the ISS. Additional recommended metrics have been published by CCPS [2].

Selecting appropriate metrics to track can seem like an overwhelming task. Good, properlyimplemented metrics drive personnel to do the right thing. Always ensure that the intent of the metric is understood rather than simply managing the metric itself. Most metrics focus on schedules, which are not indicative of work quality. A proof-test schedule can be set at an unreasonably long interval or testing can be performed inadequately, creating an illusion where the metrics indicate a well-maintained system while equipment is failing in the field. A focus on the percentage of success or failure of various activities can lead to

normalization of some failures, which is unacceptable for ISS. Any piece of failed ISS equipment represents a hole in the risk reduction strategy; a single bad metric may impact multiple layers and/or events. It is unfortunate, but true, that personnel will behave contrary to intent, if necessary to "make their numbers."

In the design and engineering phases, it is easy for the process hazards analysis to become a quantitative exercise in an environment of high data uncertainty. It is also easy for the verification to turn into a numerical juggernaut where simple ISS designs turn into complex gambles based on assumed performance. For operating facilities, the challenge is making sure that the mechanical integrity record states more than "broken," "not working," or "failed," e.g., record the equipment condition, failure mode, and failure cause.

The risk reduction strategy is proven by mechanical integrity data, which demonstrates that the ISS can achieve the performance assumed during the process hazards analysis. The risk reduction provided by a piece of equipment is the inverse of its probability of failure on demand (PFD). The PFD is calculated as the number of times the ISS has failed dangerously divided by the total number of times the ISS has been challenged. Consideration should also be given to out-of-service periods where equipment has failed and is awaiting repair or is bypassed for maintenance and testing. Using appropriate metrics, the actual performance of specific equipment can be compared with prior assumptions [5].

Repeated failures indicate that the mechanical integrity program is inadequate. Failure tracking is essential for quality assurance during the safety lifecycle. Existing ISS performance should be periodically assessed by tracking and trending equipment performance. Root cause analysis is used to determine why metrics are trending in the wrong direction, so that actions plans can be implemented to improve the mechanical integrity schedule, equipment installation, maintenance procedures, and personnel training.

Near-miss and incident investigations should clearly identify any ISS inadequacy or failure. Spurious trips and process demands should be tracked and compared with expectations in the hazard analysis. Management-of-change processes should be used to improve the equipment or systems, to resolve performance gaps.

Continued safe use of existing equipment or systems is considered "grandfathering" in process safety management (PSM) where the owner/operator determines and documents that the existing equipment is designed, maintained, inspected, tested, and operating in a safe manner. This requires an assessment of the existing design and management practices against current good engineering practices and process requirements. The review should determine whether the existing ISS is operating per the design basis and the current management system is sufficient to yield the required risk reduction.

ACT

"What is a system?" A system is a network of interdependent components that work together to try to accomplish the aim of the system. A system must have an aim. Without an aim, there is no system. The aim of the system must be clear to everyone in the system. The aim must include plans for the future. The aim is a value judgment [8].

The Act phase involves the actions taken in response to metrics and to continuous-improvement opportunities. It is the opportunity for the owner/operator's safety culture to shine and for risk to be driven as low as reasonably practicable. Action plans should define a path forward, milestones, and timelines. Plans should be periodically assessed to determine whether there is a need to accelerate the schedule or broaden the plan objectives. For example, a planned ISS upgrade may be accelerated when the manufacturer withdraws support for the equipment. To be successful, action plans should be communicated to affected personnel so that they understand the plans and commit to implementation.

Personnel should be trained in the process hazards associated with their work activities. Personnel must have the skills and knowledge necessary to perform their work with the desired quality, so minimum job-entry skills and knowledge should be specified. When on-the-job training is required, the training program should address how the skills and knowledge are developed in a timely and safe manner and how progress is measured [5].

The most important things cannot be measured [4]. Continuous improvements are necessary to stay ahead of latent conditions that present potential safety challenges and weaken protection layers. Implementing an upgrade that is aimed at improving long-term operational effectiveness takes time to complete, depending on the complexity and degree of change involved. As the ISS is changed, operating plans and targets should address compensating measures necessary to maintain safe operation during any period of increased risk. The ISS operating and mechanical-integrity basis should be reviewed and needed revisions implemented to ensure that equipment, procedures, and personnel training remain in sync with modifications.

SUMMARY

Deming believed that experience by itself teaches nothing and that data without context is meaningless. Information gained from experience must be interpreted against a framework of expected behavior, equipment design, and operating performance. But experience is not always the best teacher. Without an understanding of the underlying root causes, raw data can be misinterpreted, creating a flawed view of reality. Only data understood within its proper context provides a solid foundation for safe operation.

Accidents are prevented when safety issues are approached from a quality perspective. The Plan, Do, Check, and Act phases are essential to maintaining safe and reliable operation. A management system supported with metrics should be used to establish targets and monitor performance against policies, practices, and procedures. Periodic gap analysis should be used to verify that actual performance matches the expectations that have been established for the safety equipment. Gaps should be closed with action plans that reduce risk and prevent accidents.

LITERATURE CITED

1) Baker, J., The Report of the BP US Refineries Independent Safety Review Panel (2007).
2) CCPS/AICHE, "Process Safety Leading and Lagging Metrics," proposed metrics for review published on AICHE website (Jan 2008).

3) W.A. Shewhart, *"Economic Control of Quality of Manufactured Product/50th Anniversary Commemorative Issue", American Society for Quality.* ISBN 0-87389-076-0 *(1980).*
4) W.E. Deming, *"Out of the Crisis", MIT Center for Advanced Engineering Study.* ISBN 0-911379-01-0 *(1986).*
5) *Guidelines for Safe and Reliable Instrumented Protective Systems*, American Institute of Chemical Engineers, NY, (2007).
6) ANSI/ISA 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, Instrumentation, Systems, and Automation Society, NC, (2004).
7) ISA TR84.00.04, *Guidelines for the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511)*, Instrumentation, Systems, and Automation Society, NC (2005).
8) W.E. Deming, *The New Economics for Industry, Government, Education,* Second Edition, MIT Press, (2000).
9) *Guidelines for Hazard Evaluation Procedures*, *Third Edition*, American Institute of Chemical Engineers, NY, (2008).
10) Findings From Voluntary Reporting of Loss of Containment Incidents 2004/05, Health and Safety Executive (2005).
11) Loss of Containment Incident Analysis, HSL/2003/07, Health and Safety Laboratory (2003).
12) *Layer of Protection Analysis: Simplified Process Risk Assessment*, American Institute of Chemical Engineers, NY, (2001).

Table 1 Example Metrics Related to Instrumented Safety Systems (ISS)

Lifecycle Step	Example Metric
Hazard Analysis	Total number of hazard and risk analysis scheduled during defined interval
	o Number on schedule/behind schedule
	o Percent on schedule/behind schedule
	o For those behind schedule, total number of days behind schedule
Design Basis	Total number of ISS
	o Number with as-built documentation
	o Number with out-of-date or missing documentation
	o Percent with out-of-date or missing documentation
Mechanical Integrity	Inspections: Total number of ISS inspections scheduled during defined interval
	o Number on-schedule/behind schedule
	o Percent on-schedule/behind schedule
	For completed inspections:
	o Number passing/failing inspection criteria
	o Percent passing/failing inspection criteria
	Corrective Maintenance: Total number of ISS work orders during defined interval
	o Number passing/failing specification criteria
	o Percent passing/failing specification criteria
	Proof Tests: Total number of ISS tests scheduled during defined interval
	o Number on schedule/behind schedule
	o Percent on schedule/behind schedule
	For completed tests:
	o Number passing/failing test criteria
	o Percent passing/failing test criteria
Degraded Operation	Total number of ISS that are out of service (e.g., bypassed, disabled, or overridden) during any operating mode where the hazard exists during defined interval
	o Total hours out of service per ISS
	o Number out-of-service that are beyond specified repair time
	o Percent out-of-service that are beyond specified repair time
	For out-of-service ISS beyond specified repair time:
	o Number approved/not approved by MOC
	o Percent approved/not approved by MOC
Process Performance	Total number of start-ups (defined beginning of process operation)
	o Number involving ISS operation
	o Percent involving ISS operation
	Total number of process shutdowns during defined interval (consider breakdown by operating mode)
	o Number due to ISS operation (process demand or spurious)
	o Percent due to ISS operation (process demand or spurious)
	o Percent caused by abnormal operation
	Total number of safety alarms during defined interval
	o Number of standing or nuisance alarms
	o Number of safety alarms due to process demand