KEEP OPERATIONS SAFE

Angela E. Summers, PhD, PE, President
William H. Hearn, PE, Senior Consultant

"Keep Operations Safe," Chemical Processing, August 2008.

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 control system would maintain normal and safe operation, but perfection is impossible in the real world. Latent conditions exist in the equipment, procedures, and personnel training, eventually presenting challenges to safe operation when enough accumulate. Safe operation is achieved through implementation of a risk reduction strategy relying on a wide variety of safeguards to prevent releases of highly hazardous chemicals. Quality design and management are absolutely essential if real risk reduction and incident prevention is to be achieved – not just calculated risk reduction. This paper uses the Shewhart Cycle to introduce the various activities involved in achieving safe operation using instrumented safety systems (ISS). The Plan, Do, Check, and Act phases support the discussion of quality assurance and its application to ISS.

Introduction

Accidents continue to happen because too many owner/operators still use injuries and fatalities as the predominant metric for safe operation. A focus on direct impact can lead to a normalization of loss of containment events and a tolerance for latent weaknesses in process safety management. Knowledge of equipment integrity and management system gaps should not depend on catastrophic events. Injuries and fatalities should occur so infrequently that impact data is meaningless for trending performance.

Accidents often occur when equipment is not properly designed, installed, operated, tested and maintained. Adequate theory and standards are available to ensure process equipment can be operated safely. Preventing errors and improving safety requires a systems approach that reduces the conditions contributing to error. The problem is not bad people and lack of competency; the problem is that the systems governing equipment integrity are not rigorous enough to ensure the required reliability.

A rigorous quality management system must be used to sustain equipment reliability; otherwise, accidents will occur when enough latent conditions accumulate. A proactive approach monitors for behaviors, errors, and failures that are known root causes for process safety incidents. Identifying improvement opportunities is essential to counter this accumulation and minimize risk.

PLAN

Deming believed that 85% of a worker's effectiveness is determined by the system he works within, only 15% by his own skill [1]. 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. The output of planning is a management system of policies, practices, and procedures that seek to identify and control releases of highly hazardous chemicals. Recommended work practices and activities are provided for instrumented protective systems in the CCPS book, Guidelines for Safe and Reliable Instrumented Protective Systems [2] and for safety instrumented systems in ANSI/ISA 84.00.01-2004 [3].

There is no substitute for knowledge [4]. Only a small amount of knowledge can prevent mistakes leading to process hazards. Unfortunately, many owner/operators are losing process knowledge and history as operators and technical staffs retire or simply leave for better jobs. Errors accumulate unless there is continuous analysis and improvement of safety practices. Significant effort is required to counteract loss of expertise, as well as equipment degradation through age and obsolescence.

Internal process knowledge is sustained by a foundation of written process safety information (PSI) covering the process hazards, technology, and equipment. A written design basis should define the PSI for the safety equipment and should be traceable to the process hazards analysis. For safety instrumented systems, the design basis is the hardware and software safety requirements specification [3]. The design basis should be maintained under revision control for the equipment life.

Knowledge evolves over time as research and development yields operational facilities. Real world failures identify weaknesses in actual system performance. Hazard evaluation procedures [5] are used periodically throughout the equipment life to identify and evaluate significant events involving abnormal process operation. The event risk is analyzed qualitatively or quantitatively to determine the causes and potential frequency of occurrence. Independent protection layers are implemented to ensure that 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.

Personnel should be trained in the process safety information associated with their work activities. Personnel must have the skills and knowledge necessary to follow procedures and execute their tasks 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 [2].

Finally, planning must consider security and management of change. Physical and cyber access to the ISS should be restricted using administrative procedures and physical means [2]. Independence assessments should consider data communication and human interface failures. Written procedures should address how to initiate, document, review, and approve changes to ISS other than replacement in kind. Any change to the process and its equipment should be evaluated through a management of change process to identify and resolve any impact on the ISS requirements.

DO

The Do phase implements the systems defined in the Plan phase. From a project perspective, detailed engineering is completed yielding an ISS installation that conforms to the design basis. Detailed engineering includes sufficient information to ensure ISSs are properly specified, constructed, installed, commissioned, operated, and maintained. Equipment installed in ISS should be proven to provide the required performance in similar operating environments.

Equipment classification considers the core attributes of protection layers, namely independence, functionality, integrity, reliability, auditability, management of change, and access security. To counteract the unknown, owners/operators rely on a defense-in-depth strategy of multiple independent protection layers (IPLs) to lower operational risk [6]. Defense-in-depth also seeks to minimize common cause, common mode and systematic errors that cause multiple layers to fail [7,8]. An independent and separate safety instrumented system (SIS) is an important IPL for ensuring safe and reliable operation.

Detailed design should provide a safety equipment list identifying equipment by a unique designation (e.g., the tag number) and the required mechanical integrity schedule. 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 should be satisfactorily completed prior to the initiation of any operating mode where a hazardous event could occur.

Proof tests are periodically conducted using a written procedure to demonstrate the successful operation of the ISS and to identify and correct deviations from the design basis and equipment specification. Maintenance personnel should be trained on the procedures and understand equipment pass/fail criteria. The proof test interval is chosen 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 consider the inspection and preventive maintenance requirements necessary to maintain the equipment in the "as good as new" condition. ISS proof tests should demonstrate that the mechanical integrity program is maintaining the required equipment performance. Records are fed forward into the Check phase for trending and metrics. Operating procedures should cover the safe and approved methods for interacting with the safety equipment, such as bypassing, manual initiation, and reset. Operations personnel should be trained and tested on the procedures as necessary to ensure correct actions are taken. Operator actions in response to abnormal operation should be recorded and periodically assessed.

CHECK

By what method? Only the method counts [4]. The Check phase applies metrics to assess performance against requirements. Sustainable operation is achieved by focusing on metrics providing real-time indication. Example metrics are provided in Table 1 for the ISS. Additional metrics have been suggested by CCPS [9].

Selecting appropriate metrics to track can seem like an overwhelming task. Sometimes, technical personnel want to measure everything just because they can. Metrics should be carefully chosen, so that just the right amount of meaningful data is collected. All systems involving humans and machines suffer

some degree of variation in output quality. Good metrics drive personnel to do the right thing by identifying and correcting variation outside what is considered acceptable. If the wrong things are measured, the outcome can be negative for process safety. It is unfortunate, but true, that personnel will behave contrary to reason and to the best interest of the company if necessary to "make their numbers."

In the real world, some owner/operators are essentially following the old adage: "Measure with a caliper. Mark with a scribe. Cut with a chain saw." Their process hazards analysis is becoming increasingly quantitative with more factors and modifiers; the verification calculation is reported with multiple significant digits; and the mechanical integrity record simply states "failed."

The real world must come into balance, because the risk reduction strategy is proven by mechanical integrity data. 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. Using probabilistic techniques, the PFDs of specific equipment can be calculated and compared to expectations [7].

The most important things cannot be measured [1]. Consequently, process safety management requires that quality be built into the design and management system. Inspection and periodic proof testing is required to demonstrate that the quality system is rigorous enough to maintain the desired equipment integrity. Maintenance plans should consider how degraded equipment operation will be detected early, so it can be corrected before the equipment fails. Safety equipment must not be run to failure.

The more that is known about the equipment and what is affecting its operation, the better the risk can be managed. For safety systems, the most important thing is knowledge that the equipment will operate as required when called upon. The quality of the installed equipment is limited by the rigor, timeliness and repeatability of mechanical integrity activities, as well as equipment wear-out and degradation.

Confidence in the equipment is gained through periodic inspection and preventive maintenance that maintains the equipment in the 'good as new' condition. Proof tests provide an auditable means to demonstrate proper operation. Near miss and incident investigations should evaluate any identified ISS inadequacy or failure. Spurious trips and process demands should be tracked and compared with expectations from the hazard analysis. The Check phase involves monitoring equipment records and looking for trends indicating design or management gaps that need to be closed.

Failure tracking is essential to close the safety lifecycle. Repeated failures likely indicate that the installed equipment is not capable of meeting the performance requirements. Root cause analysis should be used to determine why metrics are trending in the wrong direction, so action plans can be implemented to improve the management system, equipment, procedures, and personnel training. Special causes and previously unknown causes of failure should be identified and communicated to personnel, ensuring that lessons learned are not hidden in mechanical integrity records. Management of change processes should be used to resolve performance gaps.

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 [4].

Even when good people apply adequate theory and standards, there are always lessons to be learned. The act phase involves the actions taken in response to trends in metrics and to continuous improvement opportunities. The Act phase is the opportunity for an owner/operator's safety culture to shine and for risk to be driven as low as reasonably practicable.

Continuous improvement is incorporated in PSM through a concept often called "grandfathering," where the owner/operator determines and documents that the existing equipment is designed, maintained, inspected, tested, and operated in a safe manner. An assessment of the existing safety system should demonstrate that the design and management practices meet or exceed the intent of current good engineering practices and the process requirements. Outdated or under-performing equipment should not be hidden under the cloak of grandfathering.

Identified gaps should be addressed with action plans for closing the gap, compensating measures implemented until the gap is closed, and an implementation schedule created. Plans should be periodically assessed to see if 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 installed equipment. To be successful, action plans should be communicated to affected personnel so they understand and commit to it.

The most important things are unknown and unknowable [4]. So, management must work continually on the system, measure what can be measured meaningfully, and move forward with improvement activities. Continuous improvement counteracts the accumulation of latent conditions that present potential safety challenges and weaken protection layers. Improving long-term operational effectiveness often takes time. Operating plans should consider how residual risk will be managed during the transition. The ISS operating and mechanical integrity basis should be reviewed and updated, as necessary, to ensure 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. New information identifies the need for new metrics which point to additional improvement opportunities.

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 used to verify that actual performance exceeds expectations established in the hazard analysis and design basis. Performance gaps should be closed with action plans that reduce risk and prevent accidents.

REFERENCES

1. Deming, W. Edwards, Out of Crisis, MIT Press, (1986).
2. Guidelines for Safe and Reliable Instrumented Protective Systems, American Institute of Chemical Engineers, NY, (2007).
3. ANSI/ISA 84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Instrumentation, Systems, and Automation Society, NC, (2004).
4. Deming, W. Edwards, The New Economics for Industry, Government, Education, 2nd Edition, MIT Press, (2000).
5. Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples, American Institute of Chemical Engineers, NY, (1992).
6. Layer of Protection Analysis: A Simplified Risk Assessment Approach, American Institute of Chemical Engineers, NY, (2001).
7. ISA TR84.00.02, Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques, Instrumentation, Systems, and Automation Society, NC (2002).
8. ISA TR84.00.04, Guidelines for the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511), Instrumentation, Systems, and Automation Society, NC (2005).
9. CCPS/AICHE, “Process Safety Leading and Lagging Metrics,” proposed metrics for review published on AICHE website (Jan 2008).

Table 1 Example Metrics Related to Instrumented Safety Systems

Lifecycle Step	Example Metric
Hazard Analysis	Total number of hazard and risk analysis scheduled during defined interval
	• Number completed
	• Number behind schedule
	• Percentage hazard and risk analysis behind schedule
	• For those behind schedule, total number of days behind schedule
Design Basis	Total number of safety equipment
	• Number of equipment with as-built documentation
	• Number of equipment with redlined or missing documentation
	• Percentage of equipment with redlined or missing documentation
Mechanical Integrity	Total number of inspections scheduled during defined interval
	• Number of inspections on-schedule but incomplete
	• Number of inspections completed
	• Number of inspection behind schedule
	• Percent on-time for inspection
	• Percent behind schedule for inspection
	• For completed, number of successful inspections
	• Percentage of successful inspections
	Total number of equipment tests scheduled during defined interval
	• Number of tests incomplete
	• Number of tests completed
	• Number of test behind schedule
	• Percent on-schedule for test
	• Percent behind schedule for test
	For completed tests:
	• Number of tests with “as found” within equipment specification
	• Number of tests with “as found” outside equipment specification (i.e., failed dangerously, failed safe, or degraded state)
	• Percentage of tests within equipment specification
	• Percentage of tests outside equipment specification
	Total number of safety equipment
	• Total number of failures found by diagnostics
	• Total number of failures found by inspection and testing
	• Total number of failures requiring equipment repair or replacement
	• Total number of failed equipment returned to service within allowable repair time
	• Percentage of equipment returned to service within the allowable repair time