CONTINUOUS IMPROVEMENT IN SAFETY INSTRUMENTED SYSTEMS

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

"Continuous Improvement in SIS," American Institute of Chemical Engineers, Process Plant Safety Symposium, 2007 Spring National Meeting, Houston, TX, April 23-26, 2007

Introduction

In the book, Lessons from Disaster, Trevor Kletz states that "listing…human error as the cause of an accident is about as helpful as listing gravity as the cause of a fall. It may be true, but it does not lead to constructive action." When a bridge collapses, the incident investigation report does not say that the incident was the result of the force of gravity. It is understood that gravity is a fundamental property considered in the bridge's design and construction. The incident report will refer to improper steel specification, inadequate support structure, etc. Gravity is not listed as the cause, because it is obvious that given the right conditions all things succumb to gravity.

The process industry has adopted automation to improve product quality and production rates, to reduce the potential for operator error, and to decrease resource requirements. Process automation includes many different instrumented systems, such as process controls, alarms, instrumented protective systems (IPS), and emergency shutdown systems. These systems range from simple hardwired systems to complex programmable electronic systems.

While the latest in instrumentation and controls often requires less support once implemented, the increased complexity may require a significantly greater level of attention during assessment, design, inspection, testing, and maintenance. Unforeseen failures can occur during long-term operation, rendering the system incapable of executing its specified action. This is especially problematic in programmable electronic systems (PESs) due to the large number of potential failure combinations between the various software and hardware elements that comprise the system. PESs also tend to require more frequent upgrades, with the potential for new failures resulting from conflicts with interconnected new and old equipment.

Good design leads to safe operation by anticipating potential errors and failures and implementing means to detect their presence, so that they can be corrected. Good design ensures that the core attributes of independence, functionality, integrity, auditability, reliability, access security, and management of change are addressed consistent with owner/operator requirements. Poorly implemented design can lead to significant hazardous events, involving impact to people, the environment, and plant assets.

Much has been done to encourage, guide, and regulate safety through identification of hazardous events and management of significant risk. However, catastrophic incidents continue to occur around the world. There are common threads woven throughout these incidents that point to cultural issues, where decisions were made that were contrary to what was appropriate for safety.

Developing a safety culture requires that values and policies are converted to practices and behaviors. The policy of "Safe operation is our mission" must be backed with the authority, resources, and

tools necessary to achieve the policy. Everyone from the front-line operator to the board of directors must understand and believe that safe operation is a core operating principle. Periodic audits of actual practices and behaviors should be used to verify that internal practices and procedures are being followed. It should also be clearly communicated that safe operation is rewarded and that unsafe operation is not tolerated.

IPS design is a team effort requiring knowledge and skills from a variety of disciplines. Some of these skills may be rarely used, but when required, high levels of expertise must be available. Massive restructuring and mergers have become commonplace within the process industry. Corporate technical departments that once served as clearinghouses for new technologies and new ideas no longer exist. Responsibility has shifted in many companies from specialized corporate personnel to site personnel, who often find it difficult to maintain the required expertise. In some facilities, there is an increasing reliance on manufacturers and other third party contractors to provide the missing expertise. At the plant site, numerous departments and many different individuals may be responsible for various, yet limited, aspects of safe operation.

Without strong oversight, it is easy for simple slips of reason, errors, loss of knowledge, loss of skill, or bad behavior to become the predominant cause of process safety incidents. A safety and reliability driven culture can only exist when the owner/operator documents the information, practices and procedures necessary to achieve the attributes important to safe and reliable operation. The goal is to maintain the IPS equipment in an “as good as new” condition throughout the process equipment life. To accomplish this, random failures and systematic errors that cause IPS equipment to fail must be identified and corrected, as early as possible.

The protective management system recommended in the CCPS/AIChE IPS Book encourages the early identification and correction of failures and errors. It provides a framework for the implementation of quality control processes for the development, implementation, and management of a risk reduction strategy that reduces the risk below the owner/operator risk criteria. The protective management system is intended to ensure:

- Protective functions and required risk reduction are identified for each mode of process operation,
- IPSs are designed, installed, commissioned, and validated to meet the design basis,
- IPSs are inspected, tested, maintained, and operated to ensure the equipment operates in an “as good as new” condition,
- The process is adequately protected during periods where the process is being operated with a known IPS failure,
- Changes to the IPSs are evaluated through a management of change process,
- Access to the IPS is controlled administratively and physically, and
- IPS equipment failures and the occurrence of process demands are tracked and periodically assessed to ensure prompt response and resolution of any identified inadequacy.

The Protective Management System

Some owner/operators establish “classes” of IPSs, providing different management systems for safety, environmental, asset and business risks. The management system establishes priority for the implementation of and adherence to the core attributes for each class. The level of rigor employed in the management system is typically based on the event consequence severity and the risk reduction expected

from the IPS. The main difference between IPS and non-IPS is the level of rigor required to support the core attributes, especially management of change, access security, and auditability.

Knowledge-based management systems (see Figure 1) rely on the communication of the owner/operator risk management philosophy to its personnel through broad objectives. It provides maximum flexibility for managing the process risk because each solution can be custom tailored as desired by the individuals involved with the process.

Knowledge-based systems are used throughout the process industry. This system relies on knowledgeable, skilled, and experienced personnel to yield the required human, equipment, and process performance. Knowledge-based systems rely heavily on personnel skills and experience to correctly interpret management goals and implement IPSs. The performance achieved by a knowledge-based system can be highly affected by personnel and organizational changes.

The greatest caveat of a knowledge-based system is the uncertainty of consistent quality workmanship. Without strong oversight, each person's unique perspective on what is the "right" thing to do becomes a variable in process performance. The culmination of numerous independent decisions can erode performance over time. With this management system, verification, assessment and audit activities are very important to ensure personnel behavior matches owner/operator expectations.

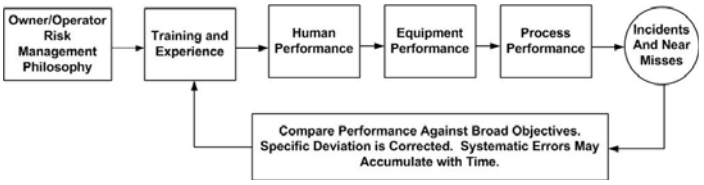

Figure 1. System Relying on Personnel Training and Experience. (adapted From Reason 1997)

The management system illustrated in Figure 2 communicates the owner/operator's risk management philosophy using polices, procedures, and practices. These prescriptive practices cover the human, equipment, and process lifecycles. Personnel knowledge and experience are not as important, because work activities and tasks are of sufficient detail that random variation in personnel knowledge does not significantly influence the work outcome.

This management system is not flexible in managing the process risk, because it dictates the solution. Maintaining the procedures requires discipline. Incremental technology changes can render existing procedures irrelevant. The natural tendency is to allow the behaviors to evolve organically over time, as a mixture of procedures that are followed to varying degrees and on-the-job training that provides the "here's how we actually do it" instructions.

While prescriptive systems require substantial effort to develop and maintain, these systems achieve very consistent performance when personnel are expected to comply with the practices and procedures. Periodic evaluation of practices and procedures is necessary to ensure that they remain up-to-date and relevant to current work expectations and requirements. Work practices and procedures should also be periodically benchmarked against industry published good engineering practices to ensure that internal practices keep pace with industry guidance and requirements.

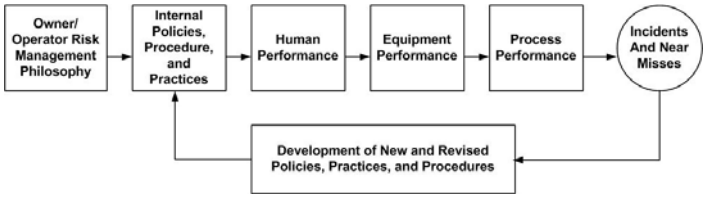

Figure 2. System Relying on Procedures and Practices. (adapted from Reason 1997)

For the management systems represented in Figures 1 and 2, unacceptable deviations are identified through incidents and near misses. Many accidents are complex and often involve multiple errors, lapses, and failures. Very rarely, does a single deviation cause an incident; it is usually the accumulation of deviations over time. Only a small percentage of unacceptable deviations are identified through incidents and near misses.

The effectiveness of incident and near miss investigations on correcting behavior and ensuring reliable performance is limited if the root cause analysis does not seek to identify the systemic problems. It is normal human behavior for personnel to believe that, due to the complex nature of the event, the incident or near miss is unique. The natural tendency is to focus on personnel errors or equipment malfunction, because these errors or failures are inherently linked to the chain of events leading to the incident. However, effective feedback requires examination of the management system and a determination of how the deviations went unchecked.

Incidents and near misses are lagging indicators of safe operation, because they do not allow the early identification and correction of the individual deviations. In general, by the time a near miss or incident manifests itself, the systemic problems that lead to the event may be (and often are) pervasive throughout the human, equipment, and process systems.

The management system recommended by this guidelines book establishes a set of attributes which are considered fundamental characteristics of a quality IPS management system. The management system (see Figure 3) uses a combination of internal practices and personnel knowledge, skills, and experience to achieve and maintain the core attributes throughout the lifecycle.

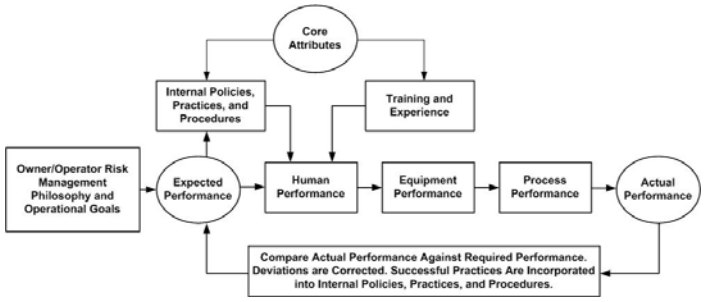

Figure 3. System Relying on Establishing and Monitoring Core Attributes. (adapted from Reason 1997)

The level of rigor used to control and monitor the core attributes affects the actual performance which can be achieved from personnel, the equipment, and the process. Actual IPS performance is monitored through various leading indicators, such as detected faults, dangerous and safe failures, process demands, and personnel conformance to management system requirements. These leading indicators allow an owner/operator to determine more quickly when the operational and mechanical integrity of equipment is insufficient to ensure consistent safe and reliable operation.

Risk management is an area where many technical personnel have limited training and skills, yet personnel are often expected to make risk based decisions with little guidance. Personnel responsible for process safety must understand the hazards associated with the process and the consequences of abnormal operation. Without this knowledge, personnel cannot be expected to make risk management decisions.

The attribute priority and management rigor typically reflect an owner/operator's risk management philosophy and operational goals. These attributes should be an inherent part of internal policies, practices, and procedures and conformance to these attributes should be monitored. The rigor required to maintain the attributes is influenced by the site culture. Lessons learned in applying the attributes should be incorporated into the work processes and requirements so that risk is continuously reduced.

Rather than waiting for an incident to identify a systemic problem, the recommended management system examines the reports and records created during day-to-day activities affecting safe and reliable operation. For example, how many pieces of IPS equipment are behind schedule for proof testing? Why are they behind? Is it a resource limitation or priority issue?

Unlike the incident-driven management systems represented by Figures 1 and 2, the management system proposed by Figure 3 acknowledges that sustainable performance is obtained when:

- Important work processes are documented,
- Personnel with the appropriate skill and training are assigned responsibility,
- Personnel are trained on the work processes,
- Compliance to approved practices is expected and audited, and
- Continuous improvement is considered important to business viability.

Sustainable performance results in decreased business losses, less rework, and higher plant performance. The protective management system is intended to:

- Outline the general work processes and deliverables required to properly manage risk,
- Identify key resource needs and gain management commitment to fulfill these needs,
- Outline the essential criteria for the various decision-making processes that occur throughout the life of a process unit,
- Provide a clear definition of risk criteria in terms of safety, environmental, and economic protection,
- Define an engineering approach to prevent process incidents, especially those that involve the catastrophic release of hazardous chemicals or energy, and
- Incorporate process and equipment reliability goals in terms of on-line time, spurious trip rate and on-line repairs.

Continuous Improvement

The historian John Lewis Gaddis defines strategy as "the process by which ends are related to means, intentions to capabilities, and objectives to resources" (Alden 1996). The goal of the process industry is no incidents, no harm to people, and no damage to the environment. This goal can only be reached by going beyond compliance and establishing safety as a strategic business value. Success requires alignment of personnel, procedures and equipment, leading to more efficient operating performance.

Operating performance is influenced by the culture of the operating facility. According to Jim Collins in Good to Great: Why Some Companies Make the Leap...and Others Don't (2001), "Culture is leadership, the discipline of people, thought, and action." An organization's safety culture is represented by shared underlying values and assumptions that drive individual behavior and management attitude and expectations concerning individual behavior. In 1993, Great Britain's Health and Safety Commission (HSE 1997) stated the following:

> "The safety culture of an organisation is the product of individual and group values, attitudes, competencies, and patterns of behavior that determine the commitment to, and the style and proficiency of, an organisation's health and safety programs. Organisations with a positive safety culture are characterised by communications founded on mutual trust, by shared perceptions of the importance of safety, and by confidence in the efficacy of preventive measures."

Achieving operating excellence requires that the outcome of the chosen risk reduction strategy meet or exceed expectations in a cost effective manner. Cost effectiveness is often interpreted by front-line personnel as minimum cost, time, and resources with "minimum" being defined by today's budget. Doing more with less generally does not lead to safe or reliable operation and it does not support continuous improvement.

An organization's culture is ultimately driven by what management indicates is important; what is measured; and what is rewarded. Safe operation can only be sustained where it is recognized that the direct costs of an incident represent the tip of an iceberg (Figure 4). Hidden from view are the indirect costs and long-term business damages resulting from unsafe operations.

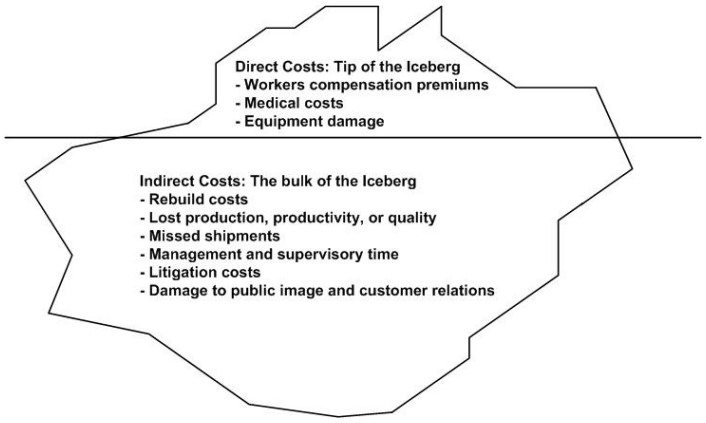

Figure 4. Iceberg Illustrating the Direct and Indirect Costs of Injuries.

When the true cost of an incident is understood, it becomes very clear that being cost effective is much more than simply today's budget. Success requires that personnel believe that investment in reducing risk further is encouraged and rewarded. Market leaders recognize that this investment provides benefits that far outweigh its costs. Operating excellence seeks to prevent incidents, because it is good for business and it is the right thing to do.

Management must establish clear performance expectations and provide the resources necessary to meet expectations. Resource deployment is not about quantity, but about quality, discipline, and rigor. Organizational discipline expects compliance with work processes as the foundation for a safe and reliable culture. The protective triangle (Figure 5) has been used throughout this book to emphasize the

interconnection of people, equipment and work practices required to support a strategy where “ends are related to means, intentions to capabilities, and objectives to resources” (Alden 1996).

Figure 5. Protective Triangle.

Continuous improvement, as shown in Figure 6, ensures that everything ties back together and continues the lifecycle. Performance is monitored and gaps between expected and actual performance are closed in a timely manner. Investments are made to reduce risk further when practical. Continuous improvement evolves the design and management practices to ensure relevance to current needs, consistency with good engineering practices, and the installed equipment is designed, maintained, inspected, tested, and operating in a safe manner.

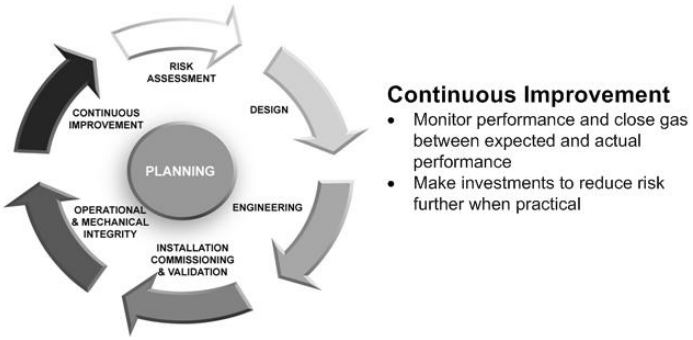

Figure 6. Continuous Improvement in the Lifecycle.

Finding The Balance

Balancing safety and production goals can be a tenuous, delicate and complex act. It is undeniable that safety and production are compatible. It is indisputable that investments in safety yield long-term benefits. However, these benefits are not as obvious nor do they produce the rapid results associated with production investments, which generally have a high certainty of providing a measurable, positive effect within a short time frame.

For protection and safety, many of the benefits are less tangible. When successful, the IPS is blamed for a process outage; when it fails, it is blamed for the incident. The hazard and risk analysis describes the hazardous event prevented by the operation of each instrumented protective function (IPF). When an IPF operates as required, the IPF should be given credit for the event avoided by its successful operation, including potential fatalities, injuries, environmental releases, equipment damage, and financial losses. Also, the IPF should be credited when fault tolerant against spurious failure design prevents a safe IPF failure from taking spurious action on the process.

Figure 7 provides a summary of the decision making process, illustrating how available resources must be allocated across safety and production goals. Decision makers often have defensive filters which affect the receipt and interpretation of information (Reason 1990). Today's business climate puts pressure on personnel in a variety of forms, such as production forecasts, budget cuts, resource reductions, or colleague retirement.

In the absence of a strong safety culture, production and budget pressure can result in a culture of denial where the decision maker's defensive filter refuses to acknowledge any evidence that does not support production or budget plans. Risk assessment can become skewed with credible safety recommendations and concerns being dismissed without appropriate consideration. Erroneous assumptions concerning equipment and procedure robustness lead to complacency and an acceptance of increased risk. Often, this is done in the absence of dependable documentation, information, and data, or a rigorous mechanical integrity program.

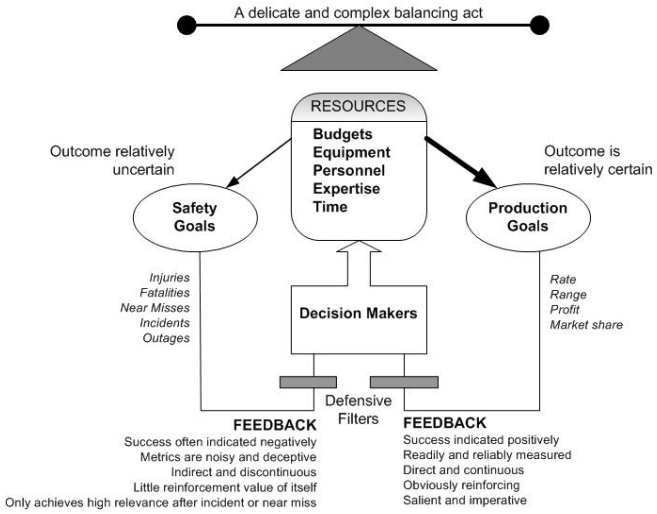

Figure 7. Overview Illustrating the Complexity of the Decision Making Process. (adapted from Reason 1990)

Good engineering practices should be applied in preventing process safety incidents. Internal practices should be benchmarked against those of market sector peers or other process industry companies. Periodic gap analysis should be conducted to determine if existing equipment is designed, maintained, inspected, tested, and operated in a safe manner. Based on observed performance and benchmarking information, action plans for improvement should be developed and implemented.

Understanding History

A series of catastrophic chemical incidents occurred during the 1970s and 1980s. These incidents are so legendary that they are often referenced by city only: Flixborough (1974), Seveso (1976), Mexico City (1984), and Bhopal (1984). They were catastrophic incidents that awakened the world to chemical industry risk. These incidents are summarized in Lees Loss Prevention in the Process Industry.

The first process safety regulations were issued in Europe in the 1970s in direct response to the impact on the communities of Flixborough and Seveso. Nearly a decade later, the tragedy caused by the Mexico City explosion and the Bhopal chemical release resulted in process safety regulations being issued

in the United States and many other countries. Industrial societies responded worldwide by publishing numerous codes, standards, and practices on a variety of process safety topics.

Unless you understand history you are doomed to repeat it. Despite these incidents occurring more than three decades ago, the errors and root causes for these incidents still exist today. Trevor Kletz discussed this problem in his book, Lessons from Disaster: How organizations have no memory and accidents recur (Kletz 1993). He presents numerous cases where an incident occurs and is repeated just a few years later. Kletz finds that organizations have poor memory due to many factors, such as insufficient failure investigation, inadequate communication and distribution of investigation findings, lack of information retention and little training concerning previous events.

A safety culture does not rely on balance sheet improvements to justify IPSs. It understands that the potential for incidents is an inherent part of the process design and that, without focused effort, incidents invariably occur.

Benchmarking Current Status

The owner/operator should understand how internal practices compare with recognized and generally accepted good engineering practices. This is often referred to as benchmarking and establishes the owner/operator's position with regard to industrial and market peers. This is often the most painful part of the continuous improvement process, as it tends to shed light on the shortfalls and inadequacies of the protective management system as a whole.

Some owner/operators will likely find that their companies are not aligned with practices documented in various good engineering practices. When unacceptable risk is identified, an action plan should be established with short-term and long-term measures sufficient to reduce the risk below the owner/operator risk criteria. Investments to improve safety and reliability of the process operation yield long-term economic returns.

Defining Gaps

An increasing number of owner/operators are finding themselves operating within a regulatory framework which often does not provide prescriptive requirements. Instead, the requirements are a moving target based on the somewhat fuzzy concept of "good engineering practice." Keeping up and complying with the basic requirements concerning process safety and IPSs can seem taxing enough. How does an owner/operator move forward with continuous improvement when it seems that even the immediate goals are a moving target? To some, it may seem challenging enough just to maintain the status quo; let alone to embrace more changes.

Continuous improvement operates on the principle that finding failures and errors is the beginning of a learning process. Minimizing their reoccurrence requires an understanding of how these failures or errors developed. Continuous improvement, as well as the application of good engineering practice, should be viewed as an on-going process rather than an endpoint. Work processes, information, resources, and skills should be analyzed periodically to identify weaknesses that limit performance and to recommend improvements, as necessary. Information systems, whether computerized or manual, should provide personnel with up-to-date information in a format that is easy to understand. Information should be revision controlled, yet accessible.

Many factors affect IPF performance expectations and the designs used to attain them, such as the economy, market trends, and technology, along with legal and political issues. A strong safety culture expects ownership and accountability for safe and reliable performance of the process equipment over its life. Management should support periodic evaluation of the existing equipment to determine that it is designed, maintained, inspected, tested, and operating in a safe manner.

Changes in operability, functionality, reliability, or maintainability expectations may require the implementation of different design/or management practices. Proof test, failure investigation, alarm, trip, audit reports, etc. provide valuable insight into personnel and management system performance. Operating excellence requires that the root causes of unacceptable process reliability and equipment performance be identified and resolved. Improving equipment mechanical integrity requires a culture that values maintenance.

A need for improvement may be identified through various management system activities. Continuous improvement processes should include periodic examination of overall available information to identify, trend, and correct systematic problems. A gap analysis (stage 5 functional assessment) is performed to compare the observed IPS performance to the expected performance. The gap analysis should determine that:

- Equipment is operating according to design intent,
- Safety, operating, maintenance, and emergency procedures are appropriate for competency and risk reduction expectations,
- Hazard and risk analysis or management of change recommendations are addressed in a timely manner, and
- Training of relevant personnel is adequate for current expectations.

Significant issues may be identified during the analysis. Management system failures are often reflected in multiple performance metrics. Systematic problems may be identified, such as poor adherence to policies, procedures, and practices or insufficient inspection and preventive maintenance. If IPS equipment is not maintained, it is likely that other equipment is suffering from the same inadequate maintenance. The cumulative maintenance deviations, whether intentional or unintentional, may cause a breakdown of multiple protection layers.

Team effort is often needed to evaluate IPS requirements and performance. Some organizations establish a formal structure where identified personnel participate as site representatives on a core team. The core team evaluates changes in the good engineering practices and makes recommendations for modifying internal practices.

Whenever work processes are modified, a shift in emphasis often leads to changes in the way team members think about and perceive the process, its associated risks, and various protection layers and IPSs. This shift may result in recommendations for additional risk reduction or IPS. These recommendations and other continuous improvement efforts complete the lifecycle moving the process toward safer and more reliable operation.

Determining Path Forward

The key aspect of continuous improvement is charting the course to achieve it. Over time, various options will be presented to upgrade hardware, software, or human interface systems. Proposed changes should

be reviewed using a management of change process to identify how the change affects other functions or systems. Areas for improvement should be addressed with an action plan, which typically prioritizes recommendations based on consequence severity and risk gap.

Action plans should define objectives, milestones, and timelines. Action plans should be periodically assessed to determine whether there is a need to accelerate the schedule or broaden its objectives. For example, a planned IPS upgrade may be accelerated when the manufacturer withdraws support for critical equipment. To be successful, action plans should be communicated to affected personnel so they understand it and commit to it.

Implementing upgrades aimed at improving long-term operational effectiveness takes time to complete, depending on the complexity and degree of change involved. As the IPS is changed, operating plans and targets should consider any additional risk borne by the process during the transition. Once the design basis changes are underway, the operating and mechanical integrity basis should be reviewed and needed revisions implemented.

There are many barriers to improvement, including:

- Poor data integrity and quality,
- Poor information availability and consistency,
- Lack of broad understanding of facts and procedures,
- Poor or missing internal practices and procedures,
- Poorly understood compliance expectations,
- Inadequate revision control or notification of changes, and
- Lack of comprehensive training on data, information, procedures, and practices.

To overcome these barriers, personnel throughout the organization must be held accountable. Continuous improvement must be part of an organization's culture, beginning at the highest management level and continuing to the front-line operator. Personnel should feel that safe and reliable operation is an institutional value and that they won't lose their jobs or be held back for speaking out. Front-line personnel must believe that continuous improvement is supported by all levels of management. They should also know that employment is conditional on safe work performance.

A continuous improvement culture requires that all personnel understand the importance of following approved practices and procedures. To succeed, personnel must be aware of the potential risk and be committed to do what is necessary to maintain and continuously improve operational and mechanical integrity. The path forward encompasses many detailed tasks, but generally includes the following:

- Assign responsibility and hold personnel accountable,
- Audit to ensure practices and procedures are followed,
- Question norms and reduce risk further when practical,
- Integrate business and process safety goals,
- Track performance, address bad actors, and celebrate success, and
- Learn and remember.

References

Excerpt from CCPS/AICHE, *Guidelines for Safe and Reliable Instrumented Protective Systems*, New York (2007).

Alden, Edward, "Comment And Analysis: Five Fraught And Futile Years - Why America must align aims and reality," www.ft.com, Financial Times (2006).

Collins, Jim, *Good to Great: Why Some Companies Make the Leap . . . and Others Don't, Harper Business*, New York (2001).

Health and Safety Executive, *Successful Health and Safety Management*, HSG 65, 2nd edition, HSE Books, Great Britain (1997).

Reason, James, *Human Error*, Cambridge University Press, Cambridge United Kingdom (1990).