CHALLENGES TO CONTINUOUS IMPROVEMENT OF SAFETY SYSTEMS

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

"Continuous Improvement and Existing Safety Systems," 10th Annual Symposium, Mary Kay O'Conner Process Safety Center Symposium, Texas A&M University, October 24-25, 2007.

"Continuous Improvement in SIS," Texas Chemical Council, 2007 Annual Meeting, Galveston TX, June 4-7, 2007.

Introduction

Safe operation requires the identification and implementation of a practical risk reduction strategy that addresses potential process safety incidents. Achieving operating excellence requires the chosen risk reduction strategy to 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 controlled by today's budget. Unfortunately, doing more with less generally does not lead to safe or reliable operation and it does not support continuous improvement.

The historian John Lewis Gaddis defined strategy as "the process by which ends are related to means, intentions to capabilities, and objectives to resources" (Alden 1996). 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.

The following discussion highlights some of the issues facing owner/operators when attempting to align personnel, procedures, and equipment to achieve cost-effective and safe operating performance. Each issue is presented using simple and practical thoughts toward life, collected from fortune cookies consumed during the development of the new CCPS book, Guidelines for Safe and Reliable Instrumented Protective Systems.

Common sense is not so common.

Common sense is defined in the on-line encyclopedia Wikipedia as "Some use the phrase to refer to beliefs or propositions that in their opinion they consider would in most people's experience be prudent and of sound judgment, without dependence upon esoteric knowledge or study or research, but based upon what is believed to be knowledge held by people in common." Common sense relies on experience and depends on the long-term retention of lessons learned. Retaining common sense requires personnel mentoring and supervision, supported by written internal practices,

Common sense should ensure that incidents experienced within the process sector are not repeated. However, Trevor Kletz in Lessons from Disaster: How organizations have no memory and accidents recur (1993) 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 lack of on-going training concerning previous events.

Experience is the name everyone gives to their mistakes

Trevor Kletz states in Lessons from Disaster 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, "The accident was the result of the force of gravity." It is understood that gravity is a fundamental property that the design must consider. The accident 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. Similarly, it should be recognized that given the right conditions all things succumb to human error.

Human error has been a contributing cause to many significant process incidents. The following incidents could be traced to decisions made by technical, operations, and maintenance personnel. These decisions were made for various reasons, but each led to a catastrophic release of hazardous chemicals.

- Flixborough (1974)
- Seveso (1976)
- Mexico City (1984)
- Bhopal (1984)
- Pasadena (1989)
- Texas City (2005)

While we should learn from these incidents, time makes them seem less relevant. There are engineers working today who were born after the Mexico City and Bhopal incidents. They naturally believe that these incidents are a reflection of the technology and practices of the time. However while technology has evolved, the root causes of these incidents, especially the human factors, have not been eliminated. The date and location of the incidents is irrelevant. Engineers must realize that the potential for incidents is an inherent part of the process design. Without focused effort, incidents invariably occur. Inherently safer design minimizes the potential for hazardous events.

You will make a change for the better

Experience and knowledge affect what is thought to be prudent and sound practices, necessitating periodic update of internal practices. Over the last few years, numerous industry practices have been issued to capture consensus practices, allowing owner/operators to benefit from the collective knowledge of a particular peer group. Good engineering practices, such as the new CCPS book, Guidelines for Safe and Reliable Instrumented Protective Systems, and ANSI/ISA 84.00.01-2004, provide consensus approaches for preventing process safety incidents.

Internal practices should be benchmarked against published practices, as well as the practices of market sector peers or other process industry companies. Gap analysis should be conducted to determine whether existing equipment is designed, maintained, inspected, tested, and operated according to currently accepted practices. Based on observed performance and benchmarking information, action plans for improvement should be developed and implemented.

Your pain is the breaking of the shell that encloses your understanding

Benchmarking can be painful, especially if you have not kept up with the latest practices. ANSI/ISA 84.01 was issued in 1997 and the 2004 release is already under maintenance by the international committee. If you are just getting started, you are entering a territory where there is as much bad information as there is good. Segregating the bad from the good is probably the most painful aspect of implementation; mistakes are relatively easy to make unless you apply a heavy dose of common sense. Practical guidance is provided in ISA TR84.00.04 - Guidance on the Implementation of ANSI/ISA 84.00.01-2004 and CCPS - Guidelines for Safe and Reliable Instrumented Protective Systems.

Although it feels like a roller coaster now, life will calm down.

Aristotle declared that a man obtained a virtue when he habitually made the choice of the golden mean between the two extremes. For safety, this often represents the choice between being so risk tolerant that the process is operated in what might be perceived by others as a reckless manner or being so risk averse that one can no longer operate the process. Cost effective decisions cannot be made by waiting for problems to occur before taking action to improve. Reducing risk where practical (or when deemed necessary by experience) should be the habitual choice and considered the common sense choice.

Encouraging improvement while managing change and cost represents the ultimate challenge for many owner/operators. To succeed, continuous improvement must be more than another initiative. Initiatives have a defined beginning and an ending. Continuous improvement exists for the life of the process equipment; it must become part of the culture of a facility, beginning at the highest management level and continuing to the front-line operator. Safe and reliable operation must be a shared value that is supported by management with adequate resources and tools.

No one is ever too old to learn, but many people keep putting it off anyway.

There are many excuses given for not modifying existing practices or adopting new ones:

- 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.

The key aspect of continuous improvement is charting the course to achieve it. When changes are proposed, these changes should be carefully considered and when practical implemented. Nothing frustrates personnel more than feeling that their recommendations are being dismissed by managers with little consideration for its technical merits. Repeated analysis without follow-through results in personnel losing interest in the necessary activities. The rigor of the design and administrative processes may decline as a result, providing little business value for what can be a significant resource investment. Concrete achievable action plans are absolutely essential.

The essential conditions of everything you do must be choice, love, and passion.

Balancing safety and reliability goals is a delicate and complex act. Limited resources, including budgets, equipment, personnel, expertise, and time must be allocated to safety and production goals. Production

goals are easy to define and measure. Success is positive, reliable, direct, and continuous. It is immediately reinforcing. Safety goals have a more uncertain outcome. Safety often has a high relevance after event, such as an incident or near miss. The metrics are noisy and can be deceptive.

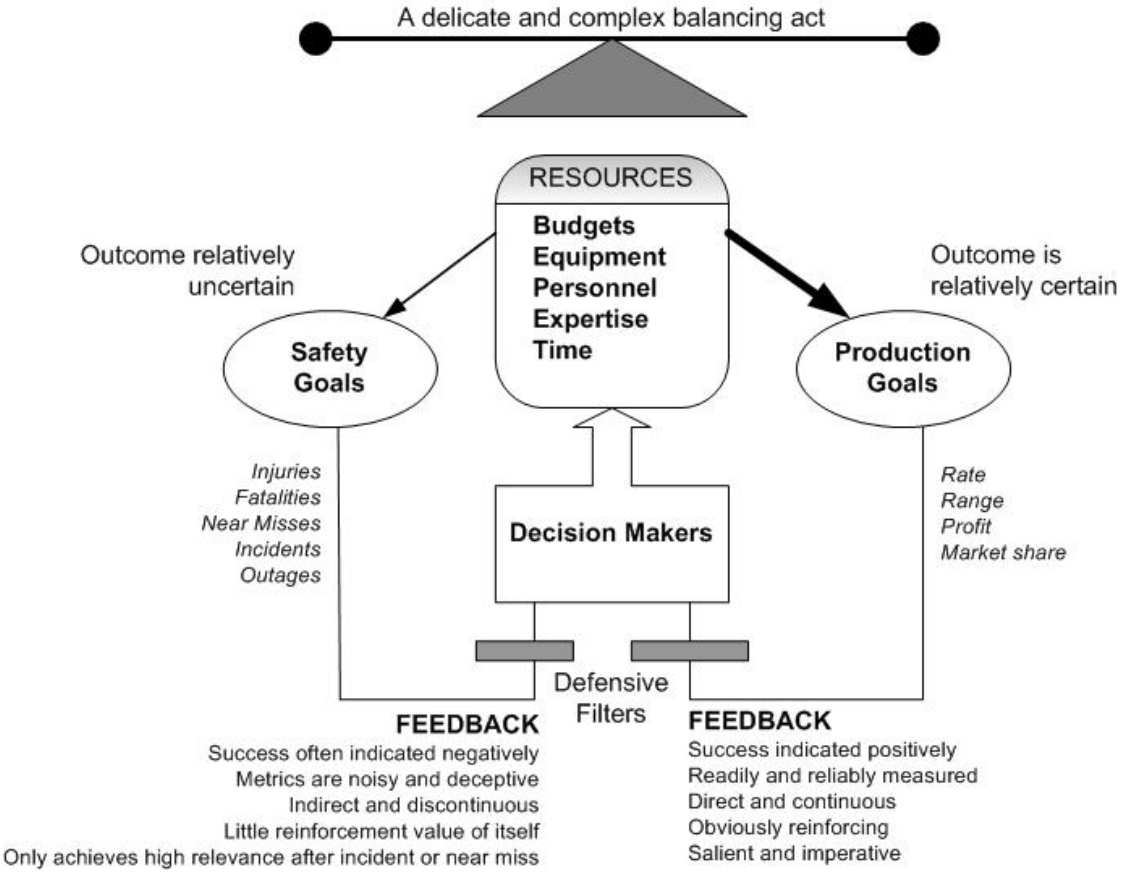

Figure 1. Decision Making Process (adapted from Reason 1990)

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.

Decision makers struggle against natural defensive filters, which tend to sieve out negative information and only push forward positive information. 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.

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. Market leaders recognize that the benefits of this investment far outweigh its costs. Personnel must believe investment in reducing risk further is encouraged and rewarded. Operating excellence seeks to continuously reduce the potential for incidents, because it is good for business and it is the right thing to do.

The greatest pleasure in life is doing what people say you cannot do.

A strong safety culture expects ownership and accountability for safe and reliable performance of the process equipment over its life. Effective safety planning must be supported by detailed hazard analysis and the application of sound judgment and common sense approaches. Execution requires technical expertise and practical field experience. Having a culture that respects the process hazard is critical. In some process market sectors, sustaining an appropriate level of respect is perhaps one of the greatest challenges. Exposure to risk tends to lead to risk acceptance. The statement, "We have vapor cloud releases all the time and no one gets hurt," has been made in this author's presence too many times.

Operational discipline is essential to ensuring proper consideration of continuous risk reduction. Technology evolution should not be considered an excuse to ignore the importance of separation, hardware fault tolerance, and a rigorous mechanical integrity program in minimizing the impact of common cause. Instead, it should be viewed as a means to obtain better performance. When a set of options is available, the right choice is generally the one that takes action to reduce risk; it is not the one that accepts additional risk.

Failure is a dress rehearsal for success.

Safety equipment should be included in a mechanical integrity program that emphasizes rigorous inspection, preventive maintenance, and proof testing. In II spection and preventive maintenance should be performed at regular intervals to maintain the equipment in the "as good as new" condition. Since a device can fail at any time during its life, periodic proof tests are performed to demonstrate the equipment functionality. Proof tests provide evidence that your mechanical integrity program is adequate through a witnessed demonstration of the safety equipment operation.

Proof tests are covered by operation and maintenance procedures that ensure the test is done correctly, consistently, and safely and the device is returned to a fully operational state after test. Each test serves as an opportunity for personnel to see the equipment in action and to validate the procedures associated with its operation. Failures found during testing indicate gaps in the mechanical integrity program, necessitating root-cause investigation and corrective action. Operational excellence requires that gaps in process reliability and equipment performance be identified and resolved. Improving equipment mechanical integrity requires a culture that values maintenance.

Be definite now, worry about precision later.

Don't get lost in the numbers. All quality control processes need metrics. The level of precision required in establishing the metric must be balanced with the level of precision possible in the monitoring of the metric. It is easy to get bogged down in all the factors that can be considered. Safe operation is not about setting targets, it is about taking action. The focus should be to ensure that:

- Protective functions and required risk reduction are identified for each mode of process operation,
- 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.

Do what you can with what you have, where you are.

Continuous improvement is often incremental. Problems are identified through various activities during the process operating life and addressed through management of change activities. For existing equipment, it should be demonstrated and documented that the equipment is designed, inspected, maintained, tested, and operated in a safe manner. This affirmation is incorporated in the pre-startup safety review (PSSR), which is conducted after the installation of new or modified equipment. The PSSR asks the questions:

- Is the equipment operating according to its design basis,
- Have hazard and risk analysis or management of change recommendations been adequately addressed,
- Are the safety, operating, maintenance, and emergency procedures up-to-date, and
- Are relevant personnel trained on how changes affect equipment operation and procedures?

Conclusion - The man on top of the mountain did not fall there.

Defining and maintaining a comprehensive risk reduction strategy takes effort. To reach the top of the mountain, owner/operators should:

- 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, celebrate success, and
- Learn and remember.

Continuous improvement does not have a defined beginning or end, because safety is an everyday thing. Safety isn't supposed to be easy. If it was, there would be no need for volumes of practices and guidelines to get it right. There would be no need for public relations campaigns involving barbeques, t-shirts, and posters. To succeed, safety must be a business value. Achieving it must be considered a virtue.

References

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

Kletz, Trevor, Lessons from Disaster: How Organizations Have No Memory and Accidents Recur, Institution of Chemical Engineers, United Kingdom (1993).

Mannan, Sam, Lee's Loss Prevention in the Process Industries, Volumes 1-3, Elsevier Butterworth-Heinemann, United Kingdom (2005).

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

"Functional safety: safety instrumented systems for the process sector," International Electrotechnical Commission, IEC 61511, Geneva, Switzerland (2003).

"Guidelines on the implementation of ANSI/ISA 84.00.01–2004," ISATR84.00.04, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, (2006).

Guidelines for Safety and Reliable Instrumented Protective Systems, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York (2007).