Safety Management is a Virtue

Angela E. Summers, Ph.D., P.E., SIS-TECH Solutions, LP Houston, TX 77034 USA Phone: 281-922-8324
www.sis-tech.com Sept, 2009 *Process Safety Progress*

Abstract

It is undeniable that safe operation and process reliability are not only compatible, but highly interrelated. Reliable production units rarely have safety incidents, while unreliable ones tend to repeatedly experience abnormal operation. To prevent incidents, personnel, procedures, and equipment must be aligned to facilitate rapid identification and response to failures of the control system and protective safeguards. Safe and reliable performance requires minimization of the root causes that lead to abnormal and emergency operation. The challenges to accomplishing this in a timely manner are considerable, but not insurmountable. This paper discusses various challenges to sustaining safe operation of process equipment. Each challenge is introduced using a Chinese fortune cookie to remind the reader that the barriers against progress are not new but have existed from many years. In most cases, the solutions are also well known and generally required deployment of robust equipment, proven techniques, and competent resources.

> Common sense is not so common.

Common sense is defined in the on-line encyclopedia Wikipedia (1) 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 long-term retention of lessons learned. Retention depends on personnel mentoring and documented internal practices. Common sense should ensure that incidents experienced within the process industry are not repeated. Unfortunately, organizations have been proven to have poor retention of lessons learned. For something to become common sense, it must be understood and openly discussed. Incidents can only be prevented with thorough failure investigation and widespread distribution of findings (2). Preventing incidents requires internalization of root causes followed by continuous effort to ensure that they do not happen again.

> Experience is the name everyone gives to their mistakes

Trevor Kletz (3) 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.” Human error has been a contributing cause to many significant process incidents. The following incidents can be traced to

decisions made by technical, operations, and maintenance personnel. These decisions were made for various reasons and each led to a catastrophic release of hazardous chemicals.

- Flixborough, UK (1974)
- Seveso, Italy (1974)
- Mexico City, Mexico (1984)
- Bhopal, India (1984)
- Pasadena, TX USA (1989)
- Esso, Australia (1998)
- Texas City TX USA (2005)
- Brucefield, UK (2005)

The location of these incidents proves that process safety is an international issue. The range of dates shows that the issue is timeless. Unfortunately, many young engineers naturally believe that incidents prior to their birth are a reflection of old technology and practices. However, while much has evolved, the root causes of human error and equipment failure have not appreciably changed. It is an inevitable that abnormal events will occur during process operation, so inherently safer design should be used to minimize the potential for hazardous events by making the equipment more tolerable to process disturbances.

You will make a change for the better

Experience and knowledge affect what is thought to be prudent and sound practices. Many industrial societies (CCPS, API, ISA, NFPA) have published standards and guidelines addressing good engineering practices for safe design of chemical processes. These societies capture consensus practices, allowing owner/operators to benefit from the collective knowledge of peer companies.
These efforts continue with recent focus on the development of international standards, such as IEC 61511 (US: ANSI/ISA 84.00.01-2004) (4) and consensus practices, such as CCPS's Guidelines for Safe and Reliable Instrumented Protective Systems (5) concerning implementation of instrumented systems to prevent process safety incidents. In recent years, CCPS has published quite a few guidelines books on various process safety topics.
Internal practices should be benchmarked against published guidelines and practices. 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

A key aspect of continuous improvement is a strong safety culture that seeks to drive risk as low as reasonably practicable (6). This culture accepts that the investment should be made to reduce risk until the cost is grossly disproportionate to the benefit gained. Nothing frustrates personnel more than feeling that their recommendations are being dismissed based on capital requirements with little consideration of

technical merit. Over time, a failure to implement causes a steady decline in the design and administrative processes that are intended to look for risk reduction opportunities. The net result is often that there is little business benefit for what may be perceived internally as a significant resource investment.

Benchmarking can be painful, especially if you have not kept up with the latest practices. There are many industrial organizations, as well as coalitions, who are publishing new or updated guidance and practices every year. Keeping up is a challenge and requires resource investment. Making changes to existing systems in response to changes also takes substantial commitment.

Gaps in the safety management system should be addressed quickly, since it serves as the fundamental basis for all lifecycle activities. When the gaps extend to existing equipment, interim measures should be implemented as quickly as possible while long-term solutions are engineered and installed. Concrete achievable action plans are absolutely essential. Consider the development of standardized approaches for common applications (7).

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 are not 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 staying on budget represents the ultimate challenge for many owner/operators. To succeed, continuous improvement must be more than another initiative. It must 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.

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 decision makers refuse to acknowledge safety gaps. Risk assessment can become skewed with credible safety recommendations and concerns being dismissed without appropriate consideration.

Sustaining a culture that respects the process risk and seeks to reduce it further is perhaps one of the greatest challenges facing industry. Risk exposure tends to lead to risk acceptance and increased tolerance of process upsets and loss of containment events. Erroneous assumptions concerning equipment

and procedure robustness can lead to complacency and an acceptance of increased risk. Often, this is done in the absence of dependable documentation, information, data, or a rigorous mechanical integrity program. 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.

Avoid the trap of "ignorance is bliss" and embrace "knowledge is power." Effective safety planning must be supported by detailed hazard analysis and the application of sound judgment and common sense approaches. Hazard awareness supports the development of a sound risk reduction strategy that ensures safe operation. Execution requires technical expertise and practical field experience.

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

Market leaders recognize that the benefits of safety investment far outweigh its cost. While some safety benefits are measurable, many do not acknowledge the loss prevention savings when incidents are prevented. These savings should be tracked to demonstrate return on investment. Detailed cost tracking often highlights that the asset loss and re-build costs are only the tip of the iceberg.
An organization's culture is ultimately driven by what management indicates is important; what is measured; and what is rewarded. A strong safety culture expects ownership and accountability for process equipment performance. Personnel must believe investment in reducing risk further is encouraged and rewarded. Operating excellence occurs in an environment that supports continuously reducing the potential for incidents, because it is good for business and it is the right thing to do.

> Failure is a dress rehearsal for success.

Improving equipment integrity requires a culture that values maintenance. Safety equipment should be included in a mechanical integrity program that emphasizes rigorous inspection, maintenance, and proof testing. Inspection and preventive maintenance should be performed at regular intervals to sustain the equipment reliability and ensure that it is fit for service.
Equipment can fail at any time (8), so periodic proof tests are used to demonstrate through a witnessed test that equipment is operational and capable of acting as required. Proof tests are covered by operation and maintenance procedures that ensure the test is done correctly, consistently, and safely and the equipment is returned to a fully operational state after maintenance is completed. 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. Safe operation encourages the identification and resolution of process reliability and equipment performance gaps.

Be definite now, worry about precision later.

Don't get lost in the numbers. All quality control processes need metrics (9). 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 attempting to track too much. Safe operation is not about setting targets, it is about taking action to ensure (4) that:

- Safety equipment 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 safety equipment failure,
- Access to safety equipment is controlled administratively and physically, and
- Safety 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 (10) 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?

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

Industry leaders recognize that investment in resources and safety equipment to prevent process incidents is essential to achieve the lowest lifecycle cost. Unfortunately, there are many who lag behind. Without care and attention, incidents invariably happen when the "wrong conditions" occur at the "wrong time." All owner/operators must realize that the management of safety risk is an inherent part of process design and operation and that demonstration of safe operation is required for their license to operate.
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. To succeed, safety must be a business value. Achieving it is a virtue.

References

1. http://en.wikipedia.org/wiki/Common_sense, accessed June 4, 2009.
2. Summers, Angela, "Fault Management Analysis," *Process Safety Progress*, pages 204-207, November 2001.
3. Kletz, Trevor, *Lessons from Disaster: How Organizations Have No Memory and Accidents Recur*, Institution of Chemical Engineers, United Kingdom (1993).
4. *Guidelines for Safety and Reliable Instrumented Protective Systems*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York (2007).
5. ANSI/ISA 84.00.01–2004, International Society of Automation (ISA), Research Triangle Park, NC, (2004).
6. Summers, Angela, ""Safe Automation through Process Engineering," *Chemical Engineering Progress,* pp. 41-47, December 2008.
7. "Cookbook versus Performance SIS Practices," *Process Safety Progress*, 27(3), pp. 260-264, September 2008.
8. "Random, Systematic, and Common Cause Failure: How do you manage them?" *Process Safety Progress*, December 2006.
9. "Safeguard Safety Instrumented Systems," Chemical Engineering Progress, pages 85-90, November 1999.
10. Guidelines for Pre-Start-up Safety Reviews, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York (2006).