

Best Practices in Safety

By James Belke

EPA Chemical Emergency Preparedness and Prevention Office

May 2000

At Crossroads, we recently received the question: "Please give me some good sources to obtain information on best safety practices, regardless of industry. Our organization is attempting to revamp our safety culture and is trying to locate companies to research and possibly emulate."

Such a straightforward question deserves an answer in kind, and in a two-paragraph response, I attempted to briefly provide the writer with some sources of information and organizational examples of safety excellence that might be useful. But any short answer to this question belies the decades of human experience and volume after volume of written information that have contributed to defining industrial "best safety practices." Additionally, the question raised the concept of safety culture, which is itself an entire sub-discipline within the overall rubric of safety practice about which much has been written. So in this article I thought I would set the stage for future articles that will explore some specific aspects of "best safety practices" and "safety culture" in more depth, or at least scratch the surface a little deeper than I did in my response to the questioner.

It is useful to step back a bit and discuss some background information. Many modern industrial activities are highly complex, and organizations may necessarily engage in a wide range of "risky" activities in the course of their objectives. These risks exist either because certain materials, processes, or endeavors have inherently hazardous characteristics, thereby precluding the absolute elimination of all risk, or because it would be prohibitively expensive or inefficient to eliminate all hazards, and the risk of those hazards can be managed so that the benefits of the endeavor outweigh its risk over the long term. Such activities may include working with highly toxic, flammable, or explosive chemicals, operating processes at extremely high temperatures and pressures, working with high-energy electrical, mechanical, chemical or nuclear systems, or subjecting workers to a variety of other occupational hazards.

While most readers in this forum will rightly assume I'm referring to the chemical and petroleum industry, its not just chemical manufacturing plants and oil refineries which do these sorts of things. Other organizations, such as the mining industry, power generating utilities, the marine shipping trade, the military, government agencies such as NASA and DOE, and others have also routinely and (usually) successfully engaged in activities that contain some element of risk to workers, the environment, or the public. In order to be successful, these organizations must be able to manage such risks. The methods used to do this have evolved, and continue to evolve, out of the aggregated knowledge and experience arising from these various different risky endeavors into a body of operating practice that can loosely be termed "best safety practices."

This is perhaps an oversimplified explanation for a process which has been punctuated along the way with drastic examples of failure, such as the toxic chemical release at Bhopal, the nuclear meltdown at Chernobyl, and the Challenger space shuttle incident, to name a few. But the examples of success, while generally either less well-known or taken for granted by the public, are a testimony to our ability to successfully manage risk. For example, as an engineer, I often marvel at how commercial airline travel - an endeavor which combines an incredible amount of technical sophistication, human expertise, and organizational skill - is now routinely done with such minimal risks that it has become an indispensable facet of our everyday life. Yet in spite of this marvel, most people (including me on occasion!) feel an infringement of their rights if their flight is delayed for one hour.

So the term "best safety practices" as I use it here encompasses a wide range of meaning and is not necessarily restricted to one particular industry. Furthermore, the particular set of practices adopted generally varies from industry to industry and indeed may be called by different names, and may even vary from facility to facility within the same industry. For example, "process safety management" is the term used in the chemical industry and in OSHA and EPA regulations to describe a widely-accepted set of industrial best safety practices. The Department of Energy, on the other hand, refers to an additional set of guidelines termed "conduct of operations." But both sets of practices contain many common elements, and their respective purposes are basically the same.

Generally speaking, using best safety practices means to systematically apply programs, policies or actions that have been shown through logic and experience to eliminate or minimize industrial risks and prevent accidents from occurring. Examples of best safety practices include performing systematic analyses of process hazards, following written operating procedures to perform hazardous evolutions, designing and operating equipment and systems within specified safety limits, maintaining equipment in good operating condition, systematically reviewing equipment or system changes for safety

implications, and using properly trained and qualified staff to operate equipment and systems, to name just a few.

Well, I hope I have convinced you of the enormous breadth of this important subject. There is certainly way too much ground to cover in any one article. My intention here is only to lay the foundation for future articles, where I will go into more specific detail on various aspects of best safety practices, and will provide some literature references for those who desire more in-depth information. I'll also review the concept of "safety culture," which is a fascinating philosophy toward human and organizational behavior change; if successfully implemented, it can dramatically reduce injury and accident rates. Stay tuned....

Best Practices in Safety - Introduction (Part 2)

By James Belke

EPA Chemical Emergency Preparedness and Prevention Office

June 2000

Best Safety Practices are a Component of Loss Prevention

As I indicated in my last article, there are a number of different terms used to describe best safety practices. These include process safety management, risk management, integrated safety management, safety management system, and other terms and variations. While most literature on best safety practice relates to the operational aspects of plant management, it is important to recognize that there are important loss prevention decisions which take place before ground is ever broken on a new chemical plant. Among these are facility siting, plant design, choice of technology, and plant capacity. Each of these decisions have important safety implications. For example, a small-capacity, geographically remote process facility usually has less potential for catastrophic loss than a large facility located close to or within a major urban area. But such decisions are rarely made with safety alone in mind. They also involve important economic considerations. A large, single-stream process facility may achieve significant economies over its smaller counterpart, while transportation and labor costs may be minimized by locating the plant closer to a population center.

In any case, I'm not going to address these non-operational loss prevention decisions. While they are important parts of an overall loss prevention strategy, once these decisions are made, they generally cannot be made over again without great expenditure. Much has been written to encourage inherently safer design, and few would dispute that choosing a fail-safe design alternative at the outset is preferable to virtually any other safety practice. Nevertheless, it is often not economically feasible to redesign the entire plant or even one unit process to adopt some newer, safer design alternative.

Fortunately, there are other means besides the choice of facility siting and design that are available to plant management and workers to prevent accidents and control losses. And in this and future articles, I will usually limit the discussion to those safety practices that are under the control of plant management at an existing facility.

Systems of Best Safety Practice

There are numerous systems that place the generic best safety practices into different categories. OSHA's Process Safety Management standard and EPA's Risk Management Program describe a dozen or so accident prevention elements. Similarly, the American Petroleum Institute stipulates 11 recommended practices in API RP 750, *Management of Process Hazards*. The Center for Chemical Process Safety articulates 14 management guidelines in its *Technical Management of Chemical Process Safety*. The Department of Energy lays out 18 guidelines in *Conduct of Operations Requirements for DOE Facilities*. And there are many other ways to slice the pie. All of them are simply different ways of combining and categorizing related safety practices, so I'll feel free to borrow a little from each of my favorites and make up my own hybrid system for the purposes of these articles. In my next article, I'll reveal my new system, and start discussing its specific elements.

Literature on Best Safety Practices

Last month I promised to provide some literature references for those who are interested in learning more about best safety practices, so its time to start meeting that promise. Fortunately, if you are interested in these topics, there is a great deal of literature. Probably the most comprehensive work on the overall topic of industrial loss prevention is *Loss Prevention in the Process Industries* by Frank P. Lees (2nd edition, 1996). This 3-volume set covers virtually every aspect of the field, operational and non-operational alike, and in great detail. It also provides an unsurpassed bibliography (the third volume contains a 500-page listing of references to other literature in the field). This work is essential reading for anyone seriously interested in chemical process safety.

Best Practices in Safety - Part 3

By James Belke

EPA Chemical Emergency Preparedness and Prevention Office

August 24, 2000

Introduction

In my last article I wrote about the numerous systems of best safety practice, and I promised to borrow from them to create my own. Not because I think I can improve on what smarter people have done - indeed, I think that OSHA PSM, for example, is a fine system for categorizing related best safety practices. However, probably due to my early career in nuclear safety, I sometimes group things a bit differently and perhaps in a somewhat simpler fashion. There's really not much point in arguing about what system is better, since regardless of what system you use, it's important to remember that its various elements are generally not independent from one another; a significant interrelationship usually exists between each of them, and all of the elements need to work well together, or accidents can happen.

Generic Components of Best Safety Practice Systems

Whether you choose to call it a system of best safety practice, process safety management, accident prevention, risk management, the basic elements of comprehensive safety programs generally include the following:

1. **Management System.** The overall administration of a facility's safety program is the responsibility of management. While individual elements of best safety practice are often referred to as "management systems," we also refer to the overall structure within which each of these individual elements are placed as a "management system". The overall management system includes all of the safety program elements, policies, and practices, and is itself just one part of management's many other responsibilities (e.g., fiduciary, production planning, etc.). Management specifies facility organizational structure, provides resources to accomplish tasks, defines authorities, responsibilities, and accountability for various positions, sets operating standards and communications policy, and establishes goals and plans for safety. Obviously, many of these policies impact more than safety alone. An important point to remember is that managers set the tone for the entire facility. Good leaders demonstrate that the top level of the

company is committed to safety, and instill that commitment in all other organizational levels by establishing a "safety culture." Providing strong leadership is at least as important as implementing the technical aspects of a particular safety element. There are numerous references devoted to the subject of management in general, and management of chemical process safety in particular. One excellent reference for the latter is *Guidelines for Technical Management of Process Safety* (AIChE/CCPS, 1989).

- 2. Hazard Identification and Control.** This involves a systematic evaluation of hazards, and the steps necessary to control, mitigate, or eliminate those hazards. By "hazards" I generally mean chemical process hazards, as opposed to the garden-variety industrial hazards (slips & falls). Hazard identification and control are arguably the most important components of any process safety system. If you don't recognize a hazard, then avoiding it is simply a matter of luck. Most hazards, however, are well-known, and are documented in technical literature. Today it is rare that an accident is caused by some completely new or unforeseen phenomenon. Realistically, most accidents occur because of a failure to properly control or mitigate a recognized hazard. There are a number of different accepted methods for conducting a hazard analysis, such as the Hazard and Operability Study (HAZOP), Failure Mode and Effects Analysis (FMEA), the What-If analysis, and others. An excellent reference on this topic is *HAZOP and HAZAN* (Kletz, T., 4th edition, 1999).
- 3. Operating Procedures.** - These are step by step instructions for doing things. Operating procedures are vitally important because they help ensure that the proper actions are taken in the correct sequence every time a task is conducted. They are nearly always written (or sometimes displayed on a computer monitor). Operating procedures should cover all phases of plant operation, including routine operations, abnormal or non-routine operations such as plant startup and shutdown, and emergency operations. The development of effective operating procedures is not trivial. There are numerous considerations, such as equipment design information, technical data, safety information, operator experience, human factors (which influence style, format, and complexity, etc.), regulations, operating policy, and others. Operating procedures should be reviewed and updated periodically and after a system change to ensure they reflect the current condition of the plant. A good reference covering the topic is, *Guidelines for Writing Effective Operating and Maintenance Procedures* (CCPS/AIChE, 1996).
- 4. Equipment and System Status Control.** This is a pretty broad category. In my system, it includes practices related to instrumentation and control systems, alarms, operator shift routines, round sheets, log keeping, and other ways to

monitor and control equipment and process conditions to ensure that they are maintained within safe ranges. Speaking of safe ranges, this category also includes keeping the necessary process information up-to-date, such as design temperatures, pressures, and flows. It also includes any special measures used to verify system status (e.g., verifying valve and switch positions prior to starting a process unit). Since system status control frequently involves the interface between man and machine, human factors play a significant role in this area. For example, more and more facilities are using computerized distributed control systems for process control. While remarkable for the amount of information they place at the fingertips of a control room operator, these systems can also cause "information overload" if not set up appropriately. A related human factors issue involves the use of alarms. Alarms are important features used to alert operators that some parameter or condition is approaching a limit or has fallen outside a specified range. But many parameters may vary widely, so at what point should the alarm go off? The alarm threshold should be set high enough so that it tells the operator that a problem may exist, but not so high that its too late to do anything about it. This can be a tricky balance. A computerized control system can sometimes cause a proliferation of alarms. I've seen several control rooms where the alarm thresholds were set so low that alarms were sounding nearly all the time, usually when nothing was going wrong. This can "immunize" the operator against the alarm, and potentially lead to an unsafe situation.

5. ***Maintenance Program.*** Under the rubric of maintenance, I include practices intended to keep equipment and systems in good working order. This includes preventive, periodic, or corrective maintenance, as well as equipment testing (e.g., pressure vessel hydrostatic testing, equipment vibration analysis), tracking material history, pre-startup safety reviews, lockout/tagout programs, and mechanical integrity inspections. A very important part of the maintenance program which deserves its own mention is "management of change." Management of Change is a term of art that describes those policies and practices intended to ensure that equipment and process modifications are implemented safely. A number of major accidents have resulted from process changes that were implemented without due consideration of all of their consequences. A good reference for this topic is *Management of Change in Chemical Plants - Learning from Case Histories* (Roy E. Sanders, Butterworth/Heinemann, 1993).
6. ***Training Program.*** When serious accidents occur, inadequate training and operator error are often named as primary causes or contributing factors. As I've written before (see "Recurring Causes of Recent Chemical Accidents." Paper published in *Proceedings of the International Conference and Workshop on*

Reliability and Risk Management, 1998), I think that these causes are probably exaggerated somewhat. But whether or not that is true, everyone will agree that effective training is vitally important to safe plant operations. There are a variety of different ways to provide personnel with the necessary knowledge, skills, and experience to safely perform job tasks. Commonly-used training techniques include On-the-Job Training (OJT), conventional classroom education, computer-based training, emergency drills, certification programs, oral and written examinations, and others. Many governments have recognized the importance of training by enacting regulations requiring employees to meet certain minimum training standards. In the United States, training requirements contained in OSHA regulations such as the PSM and HAZWOPER standards are pretty familiar by now. In my opinion, an under-used form of training in industrial plants is the emergency drill. Drills allow operating teams to practice the response to an emergency or unusual situation, hopefully without risking the dire consequences that could result in an actual emergency (I say "hopefully" because drills can result in actual emergencies if the drill gets out of hand). Many companies don't like to run drills too frequently, if at all, because they interrupt operations and place stress on equipment and processes. Simulators do a lot to compensate, but there is often no substitute for the real thing. If an operator has never practiced responding to unusual or emergency situations, it is more likely that they will make a mistake when things really do go wrong.

7. ***Performance Monitoring System***. This includes all methods intended to provide feedback to management and workers to detect problems or deviations that could lead to equipment or system malfunctions. There are lots of ways to monitor performance. These can include formal audits and inspections, using metrics that track the performance and trends of process and management systems, conducting investigations of minor incidents and near misses to identify and correct their causes before a major problem occurs, and others.
8. ***Emergency Response Plan*** - The practical manager knows that in spite of his best efforts to operate safely, accidents may still occur, and it is prudent to have a plan to respond to them. Both OSHA and EPA require hazardous industrial facilities to have emergency response plans. For a very small facility, that plan might only consist of immediately contacting the local fire department and/or hazardous materials response unit. Larger facilities usually have more detailed, comprehensive emergency plans that often involve using employees to perform previously assigned response functions in the event of an emergency. An excellent reference for planning of this type is *Guidelines for Technical Planning for On-Site Emergencies*, (CCPS/AIChE, 1995).

Conclusion

This article was intended as a short introduction and overview of what is generally meant by the term "best safety practice." As I have repeatedly pointed out, that term is synonymous with several others, so don't be overly confused by the proliferation of terms. Also, readers should recognize that the generic systems described here are just that - generic. Individual industries and companies adapt these practices or develop their own to accommodate differences in hazards, technology, facility size, managerial preference, and other factors. If you are looking for information on best practices to address a particular type of industry or process, your best bet may be to review technical papers that are published in the proceedings of various technical conferences, or to contact industry trade associations or consultants that may specialize in safety engineering. The references cited here should give you a start in that direction, if only by providing additional, more specific literature references.