Nuclear Safety

Expect the unexpected

By R. Bruce Matthews

THE *COLUMBIA* SPACE SHUTTLE DISASTER and the near-hit incident involving corrosion of the reactor vessel head at the Davis-Besse nuclear power plant have prompted many in the nuclear power industry and the nuclear weapons complex to focus on the issue of how high-consequence, low-probability accidents can be reliably prevented. This revitalized concern for safety is particularly important for Dept. of Energy's (DOE) national security and environmental management programs because they operate with complex, tightly coupled systems that pose significant hazards.

Such systems are made up of numerous connected and interacting parts that react quickly to completion; once started, the reaction can only be stopped with great difficulty, if at all. Mishandling of special nuclear materials or radiotoxic wastes can result in serious incidents such as an uncontrolled criticality, dispersal of nuclear materials or even an inadvertent nuclear detonation. Because the consequences are so significant, a nuclear incident is not acceptable.

Therefore, work associated with nuclear materials demands a diligent approach to safety. This approach must be integrated with other requirements for safety programs designed to prevent construction, transportation and electrical accidents that can injure individuals but do not necessarily pose a catastrophic risk to the public. The nuclear safety approach must reliably prevent high-consequence accidents, even when other safety indicators are improving.

The nuclear weapons programs managed by DOE have not experienced a major system failure leading to a catastrophic accident, safety performance indicators are respectable and complaints are expressed about the burden of compliance with safety requirements. A logical reaction might be to relax safety requirements and oversight to improve productivity. In fact, DOE is taking steps to improve productivity and efficiency and lower costs by: 1) imiplementing performance-based contracts; 2) streamlining requirements to remove perceived impediments; and 3) decentralizing federal oversight responsibilities to field elements.

These recent changes at DOE stem from desirable intentions, and safety is emphasized as an important objective. The question is whether the emphasis on productivity could lead to a gradual reduction in safety margins that could ultimately result in a major system failure at a defense nuclear facility. In this context, and as a result of testimony received at a series of public hearings, the Defense Nuclear Facilities Safety Board issued Recommendation 2004-1, "Oversight of Complex, High-Hazard Nuclear Operations," aimed at addressing concerns about: 1) DOE's increased emphasis on productivity at the possible expense of safety; 2) the loss of technical competency and understanding at high levels of the organizational structure; 3) the apparent absence of a strong safety research focus; and 4) a reduced central oversight of safety.

Safety Performance

DOE and its predecessor organizations have a long and improving safety performance record in nuclear operations. For example, as shown in Figure 1, lost workday cases at DOE sites are low by national industry standards, and the rate of lost workdays has dropped more than 50 percent during the past 12 years. Similarly, as shown in Figure 2, the number of deaths in the DOE complex has been steadily declining and only four of the 453 accidental deaths in the defense nuclear complex during the past 61 years have been attributed to radiation. These safety performance data suggest that DOE has a good and steadily improving safety record.

However, closer examination of some DOE safety performance data reveals inconsistencies which could counter the conclusion that safety oversight and controls can be relaxed based on DOE's safety

R. Bruce Matthews, Ph.D., *is a member of the Defense Nuclear Facilities Safety Board, which oversees the safe operation of nuclear weapon plants in the U.S. He has more than 30 years' scientific and engineering experience in nuclear technologies with a primary focus on special nuclear materials, weapons plutonium and nuclear reactor fuels. Matthews has a B.S. in Metallurgy from Penn State University, an M.S. in Materials Science from the University of Denver and a Ph.D. in Materials Science from the University of Wales.*

record. Figure 3 compares DOE's lost workday cases with those of the U.S. nuclear industry and National Aeronautics and Space Administration (NASA). When compared with these similar organizations, DOE's safety performance does not look quite as good.

This highlights the fact that decision makers can be misled by incomplete data. For example, DOE's lost workday case incident rates prior to 1990 were nearly 50-percent lower than the early 1990s data shown in Figure 1, indicating that the downward trend after 1990 could be a simple accounting artifact. The apparent downward trend in fatalities shown in Figure 2 looks quite different when one considers only deaths at defense nuclear fatalities since 1975.

Near-Hits

In addition to having a solid worker safety record, the DOE weapons complex has not experienced a catastrophic system failure accident resulting in multiple deaths or major environmental impacts. Nevertheless, review of near-hits related to the weapons complex suggests that this good record is no justification for relaxing vigilance.

- Nuclear weapons have been involved in fires, accidental drops and airplane crashes. In *The Limits of Safety,* Sagan summarizes several unexpected events that have occurred in the nuclear weapons stockpile. Fortunately the weapons failed safe, but the possibility of an inadvertent nuclear detonation cannot be ruled out.
- Fires in nuclear facilities are not uncommon. A major plutonium building fire at Rocky Flats burned nearly 350kg of plutonium, shut down operations for months and exposed 41 workers (Ackland). Fortunately, the contamination released off site was minimal. However, the fire was out of control and more than a ton of plutonium was in the building; a catastrophic dispersal of plutonium was credible and a criticality accident could have occurred.
- Tanks containing highly radioactive wastes "burp" hydrogen and leak radioactive solutions to the ground (Gephart). Again, no catastrophe has occurred, but one cannot know how much longer the aging tanks will provide the required containment protection.
- The weapons complex has not experienced a criticality accident in many years, thanks in part to the strong technical capabilities of the criticality community. However, recent criticality reports from the DOE Occurrence Reporting and Processing System (ORPS) reveal that calculation errors and inaccurate estimates of nuclear materials still occur.

Defense Nuclear Facilities Safety Board

The Defense Nuclear Facilities Safety Board is an independent executive branch agency chartered with providing technical safety oversight of DOE's defense nuclear facilities and activities in order to protect the safety and health of the public and workers.

Social Science Aspects of Safety

Organizational and management literature is rich in safety theory [LaPorte; Perrow; Reason(a); (b); Sagan] and analysis of severe accidents, yet it is short on solid advice concerning nuclear safety and the prevention of high-consequence accidents. Models of safety include risk management, normal accident theory, human error theory and high-reliability organizational theory. In addition, numerous post-mortem analyses of major accidents such as Chernobyl (Medvedev), *Columbia* (Vaughan) and Three Mile Island (Walker) have been published.

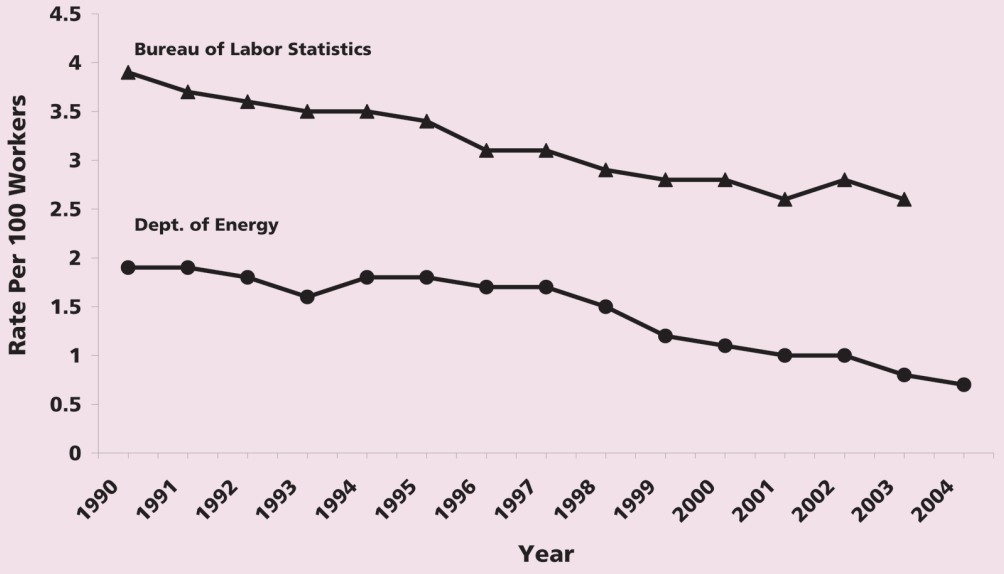
Managing Risks

In *Managing the Risks of Organizational Accidents,* Reason provides a framework to visualize the challenge of managing productivity versus safety risks. He uses a hypothetical protection versus production operating space, whereby an organization may relax

Abstract: *Nuclear weapons development activities require oversight of a unique combination of high-hazard materials and operations. This article explores the importance of organizational structure on preventing high-consequence accidents. The author summarizes social science perspectives of managing high-hazard operations, lessons learned from reviews of major accidents and the engineered approach of using standards to control hazardous activities. This article synthesizes vital safety management attributes with the objective of significantly reducing the likelihood of a high-consequence nuclear accident.*

Figure 1

Lost Workday Cases at DOE vs. National Industry Standards



safety controls to increase productivity until an accident occurs, forcing management to impose more stringent regulatory controls that result in reduced productivity. This cycle, shown in Figure 4, repeats after productivity has declined, operations once again appear to be safe and controls are relaxed until a major system catastrophe causes the enterprise to end in failure.

Simply stated, too high an investment in protection can lead to a business failure, while too much risk-taking can lead to a catastrophic accident. Safely managed organizations consistently exhibit characteristics and attributes that keep them predominantly on the side of the cycle where accidents are less likely to occur. However, real-world organizations sometimes—even if only temporarily—drift to the less-safe side of the cycle and can experience a major accident. Reason's "production/protection" cycle is useful in that it illustrates the importance of balancing the reaction to major accidents. However, the hypothetical diagram is not to imply that good safety is counterproductive. In fact, organizations that have implemented strong safety programs generally find that safety is good for business.

Such a cycle of productivity and event-driven safety reactions can be discerned from the history of nuclear weapons activities. The Manhattan Project was followed by an awareness of the health effects of radiation and the possibility of an inadvertent criticality event. The outcome was strict, expert-based guidelines for nuclear materials handling and radiation control. The design and development of new nuclear weapons were accompanied by a period of atmospheric testing, which was subsequently banned in part because of the significant quantities of plutonium released into the environment. The rapid buildup of nuclear weapons during the Cold War led to potential environmental impacts from poor management of radioactive wastes. These safety impacts led to imposition of stringent environmental controls and regulations. Fifty years later, DOE is still working to clean up the radioactive residues from the weapons buildup under the oversight and regulations imposed by DOE, federal and state agencies.

The major plutonium building fire at Rocky Flats led to a

Figure 2

DOE Fatalities 1943 to 2004

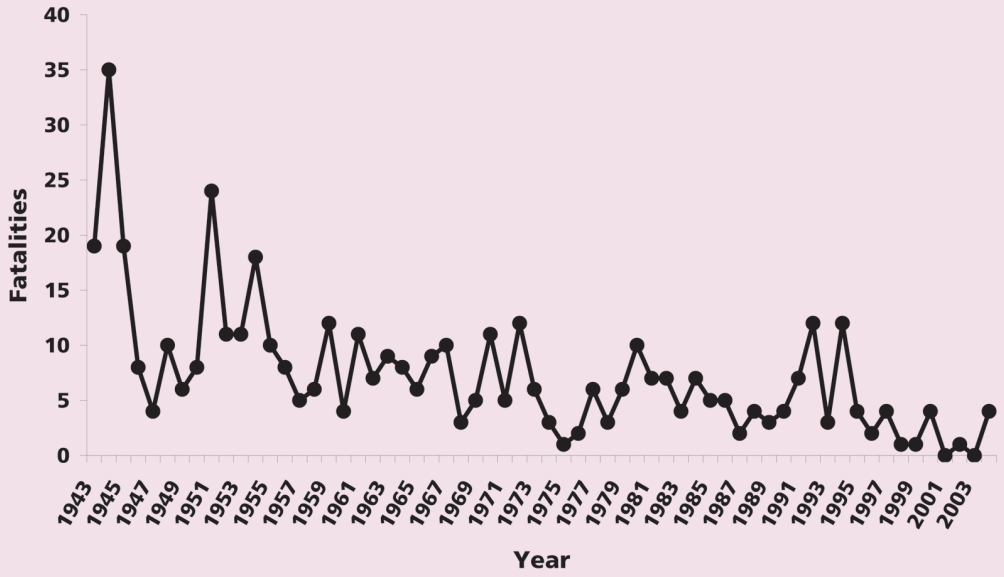
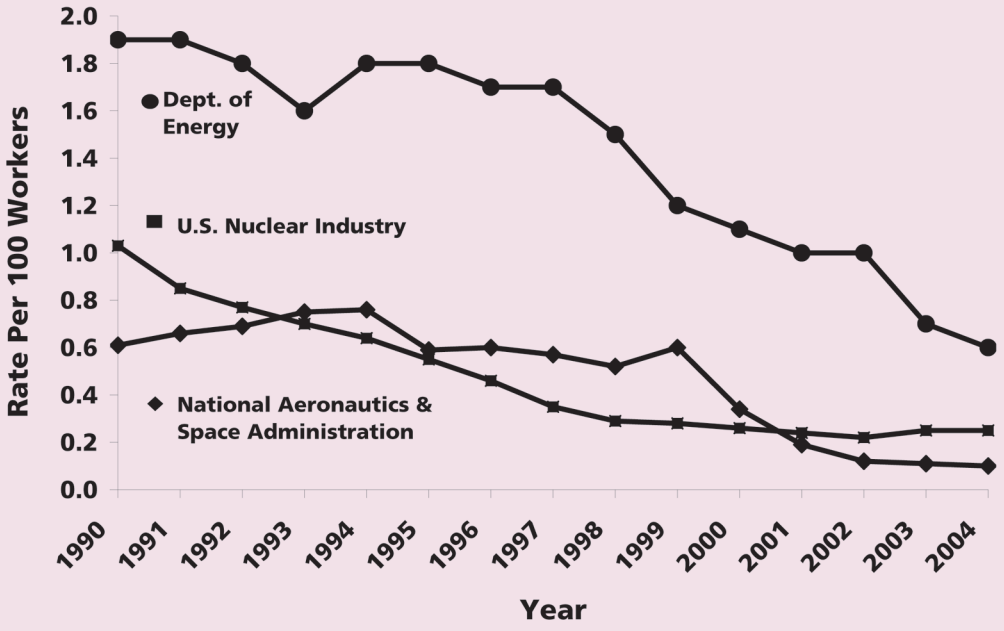


Figure 3

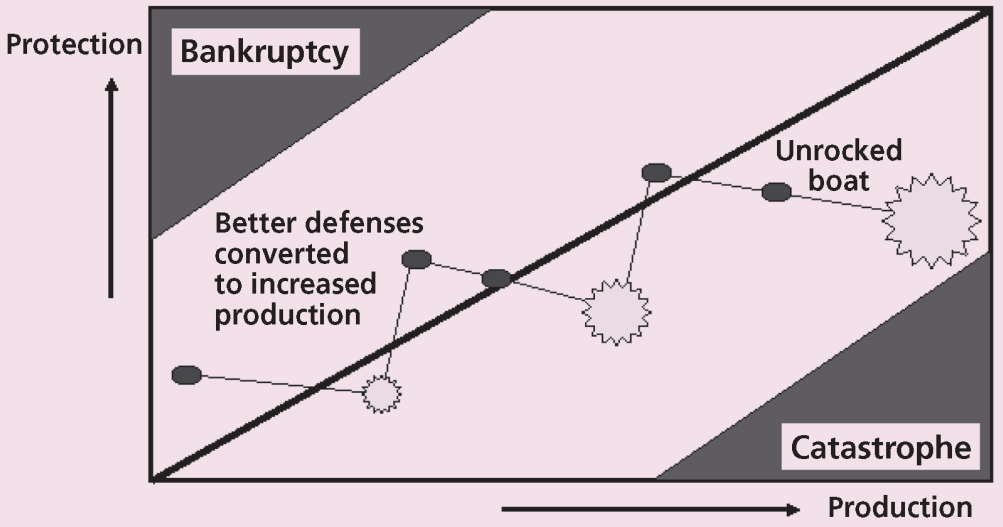
Comparison of Lost Workday Cases: DOE, U.S. Nuclear Industry & NASA



plethora of requirements and regulations that defined boundaries for activities involving nuclear materials handling. An increase in accidents, near-hits and deaths at DOE sites during the mid-1990s resulted in enhanced oversight and rules, as well as orders for hazard identification and control. Recently, DOE has been on a course to modify the organization to improve productivity and efficiency by eliminating redundancy, decreasing oversight and streamlining requirements.

Figure 4

Production/Protection Cycle



Source: Reason.

Normal Accidents

In *Normal Accidents,* Perrow concludes that accidents in large, high-technology organizations are inevitable. Competing priorities, conflicting interests, motives to maximize productivity, interactive organizational complexity and decentralized decision making can lead to confusion within the system and unpredictable interactions with unintended adverse safety consequences. Perrow believes that interactive complexity and tight coupling make accidents more likely in organizations which manage dangerous technologies.

In *The Limits of Safety,* Sagan defines interactive complexity as "a measure . . . of the way in which parts are connected and interact" and "organizations and systems with high degrees of interactive complexity . . . are likely to experience unexpected and often baffling interactions among components, which designers did not anticipate and operators cannot recognize." Sagan suggests that interactive complexity can increase the likelihood of accidents, while tight coupling can lead to a normal accident. Nuclear weapons, nuclear facilities and radioactive waste tanks are tightly coupled systems with a high degree of interactive complexity and high safety consequences if safety systems fail. Perrow's hypothesis is that although rare, the unexpected will defeat the best safety systems and catastrophes will eventually occur.

In essence, normal accident theory says that failures should be assumed and high-risk activities eliminated. Proponents of this theory argue that the catastrophic potential of a nuclear accident is unacceptable and, therefore, nuclear reactors and weapons should be abandoned. Yet, thousands of nuclear weapons exist and hundreds of nuclear reactors operate around the world; one cannot ignore the reality of today's nuclear weapons and the nuclear energy infrastructure and the need to manage high-consequence nuclear activities safely.

The Human Factor

Many social scientists conclude that most minor and major accidents have their origins in human error. In *Human Error,* Reason makes the distinction between active and latent human errors. The impact of active errors, caused by hands-on mistakes, can be immediate localized accidents. Latent errors are more difficult to detect because they can be embedded in the design of facilities and equipment or established in the organizational structure at a time and place that is removed from the work. Designers, safety analysts, decision makers, program managers and even regulators can make judgments that have unintended future consequences. Based on analyses of some high-consequence accidents, Reason concludes that latent errors pose the greatest threat to the safety of complex systems. The problem is that human errors are inevitable and error-free performance is clearly not achievable.

Random Events

Even with excellent safety performance indicators, organizations can be misled by ignoring random events that occur too infrequently to benefit from traditional performance measurement and improvement programs. Fortunately, major high-consequence accidents in nuclear operations are rare and have not occurred for decades. In *Fooled by Randomness,* Taleb addresses the role of low-probability events in the stock market—observations that offer interesting parallels to nuclear safety.

Taleb discusses how savvy investors protect themselves from the rare event (or alternatively take advantage of the rare event). An investor may have a long string of profitable investments, but this does not necessarily mean that the individual is good; s/he may just be lucky. Luck is not an acceptable nuclear safety strategy. Safety experts would do well to adopt the belief of the 18-century Scottish philosopher David Hume that severe skepticism is the only defensible view of the world.

This view is clarified by the so-called black swan problem: "No number of observations of white swans can allow the inference that all swans are white, but the observation of a single black swan is sufficient to refute that conclusion." A black swan—which can be a metaphor for a high-consequence/low-probability accident—is a random event that has a significant impact, a very low probability and a surprise effect. Nuclear safety organizations would do well to take the possibility of a "black swan" seriously.

Perrow's hypothesis is that although rare, the unexpected will defeat the best safety systems and catastrophes will eventually occur.

Because thousands of nuclear weapons exist and hundreds of nuclear reactors operate around the world, one cannot ignore the reality of today's nuclear weapons and the nuclear energy infrastructure, and the need to manage high-consequence nuclear activities safely.

High-Reliability Organizations

A somewhat different view of accidents emerged from research conducted by a group at the University of California-Berkeley (LaPorte; Roberts; Rochiln). This group spent many hours observing and analyzing the factors leading to safe operations in nuclear power plants, aircraft carriers and air traffic control centers. The researchers found that high-reliability organizations place a high cultural value on safety; effectively use redundancy, flexible and decentralized operational decision making; and exhibit a continuous learning and questioning attitude. Proponents of the high-reliability viewpoint conclude that effective management can reduce the likelihood of accidents and avoid major catastrophes if certain key attributes characterize organizations managing high-risk operations.

Following is a synthesis of some of the most important such attributes:

- *Extraordinary technical competence* is required among operators, scientists, engineers, managers and decision makers so they understand the safety consequences of their work.
- *Flexible decision making* during times of action is important. During normal operations, technical standards and waivers are controlled by a centralized technical authority; during emergencies, rapid decision making is transferred to the local site.
- *Processes reward the discovery and reporting of errors.* Processes are also in place to prompt reporting, evaluation, tracking, trending and corrective action.
- *Equal value is placed on reliable production and operational safety.*
- *A sustaining institutional culture is present.* This culture demonstrates steadfast political will, the transfer of knowledge, ongoing analysis of future impacts, the remediation of failures and persistent leadership.

High-reliability organizations manage systems that depend on complex technologies and pose the potential for catastrophic accidents, but experience fewer accidents than industrial averages. High-reliability organization theory is valuable because it develops the importance of some key organizational attributes that should reduce risks of latent human errors, but the ideas tend to be values rather than engineered solutions.

Engineered Aspects of Safety

Social scientists and organizational theorists tend to assume that the technical basis and formality of safety is active in organizations which manage high-hazard operations; consequently, they do not comment on the importance of the engineered aspects of safety. No discussion of avoiding high-consequence accidents is complete without including the technical and engineering aspects of safety. Engineered safety processes that are designed to eliminate system and human failures include regulatory compliance-based safety, formality of operations, performance-based safety and integrated safety management.

Regulatory Compliance

Both the Nuclear Regulatory Commission (NRC) and DOE use established codes and standards to design nuclear facilities. Technical specifications are implemented to define and control the safe operating envelope. DOE has developed a base of nuclear facility directives and authorizes operation of its nuclear facilities under regulatory requirements embodied in 10 CFR Part 830, Nuclear Safety Management (2004).

Part A of the rule requires contractors to conduct work in accordance with an approved quality assurance plan that meets established management, performance and assessment criteria. Part B requires development of a safety basis that 1) provides system-

atic identification of hazards associated with the facility; 2) evaluates normal, abnormal and accident conditions which could contribute to the release of radioactive materials; 3) derives hazard controls needed to ensure adequate protection of workers, the public and the environment; and 4) defines safety management programs needed to ensure safe operations.

Regrettably, it sometimes appears that compliance with paper requirements is the primary goal of safety management, regardless of cost, risk or benefit. The perception is that compliance with complex and redundant regulations and requirements has become expensive and fails to improve safety. Furthermore, civil or even criminal penalties can be levied for noncompliance. That may be, yet DOE and its contractors have spent nearly a decade scaling back requirements. The prevention of a high-consequence nuclear accident depends on promulgating a robust set of safety standards that are inviolate. All things considered, formal regulations, rigorous and independent oversight, and redundancy in safety systems and components are essential elements for nuclear safety.

Formality of Operations

Rigorous attention to formality of nuclear operations is required and any form of unauthorized reduction in formality must be avoided. Work in nuclear facilities must be authorized by line managers and executed according to procedures. The particulars can range from detailed procedures that are read and executed in a stepwise fashion for high-consequence operations such as nuclear weapons disassembly to research procedures which define the hazard and controls and operating boundary conditions.

Good procedures are necessary but not always sufficient. In *Friendly Fire,* Snook coined the term "practical drift" to describe the situation in which the daily practices of workers deviate from requirements as time passes. Safety controls tend to address worst-case scenarios. Yet, most day-to-day activities are routine and, therefore, do not appear to require a full set of controls. In response, workers develop practical approaches to work that they believe are more appropriate. However, when abnormal conditions require the rigor and control of the process as originally planned, these practical approaches are insufficient and accidents or incidents can occur. As a result, a lengthy period without a serious accident can lead to erosion in formality—it is easy to forget hazards that rarely occur.

Performance-Based Safety

Developed to reduce human error, performance-based systems use formal processes to identify, track and correct at-risk work practices that could potentially result in accidents. The idea is that the correction of small problems will prevent big problems caused by active human errors. Indeed, some organizations using employee-driven, behavior-based safety processes have reported impressive declines in incident and accident rates.

However, except to the individual, most reportable incidents and lost workday cases are relatively inconsequential, and they generally involve human error. A common assumption is that if human error can be eliminated, organizational safety will be ensured. On the other hand, the use of performance metrics can be misleading and can actually increase the likelihood of a system accident if controls and oversight are inappropriately relaxed in response to an organization that appears to be operating safely. In fact, the frequency of these types of accidents reveals little about the likelihood of a system accident. For example, NASA's safety performance data before both the *Challenger* and *Columbia* shuttle explosions did not indicate an impending safety problem.

This is not to say that tracking and improving safety performance at the individual level is unimportant; on the contrary, eliminating injuries is extremely valuable in terms of both human resources and productivity gains. However, performance-based safety is not necessarily correlated directly with the prevention of large system failures.

Safety Management

Integrated safety management (ISM) is basically a common-sense, systems engineering approach to performing work safely. ISM is based on controlling hazards to ensure that work is performed safely by: 1) planning the work; 2) identifying hazards associated with the work; 3) applying approved controls to mitigate the hazards; 4) performing work within the controls; and 5) employing continuous feedback and improvement. The success of ISM depends on its proper implementation at the activity, facility and institutional levels [DOE(d); DNFSB].

ISM also considers organizational aspects with the following set of principles that guide management on the safe performance of work:

1) Line management is directly responsible for the protection of the public, the workers and the environment.

2) Clear and unambiguous lines of authority and responsibility for ensuring safety shall be established and maintained.

3) Personnel shall possess the experience, knowledge, skills and abilities that are necessary to discharge their responsibilities.

4) Resources shall be effectively allocated to address the organization's safety, programmatic and operational considerations.

5) Before work is performed, associated hazards shall be evaluated and an agreed-upon set of safety standards and requirements shall be established.

6) Administrative and engineering controls to prevent and mitigate hazards shall be tailored to the work being performed and associated hazards.

7) The conditions and requirements to be satisfied for operations to be initiated and conducted shall be clearly established and agreed upon.

While sound in concept, ISM can be difficult to implement and does not explicitly deal with uncertainties and random incidents. While uncertainty cannot be eliminated, the likelihood of a nuclear accident can be reduced through rigorous attention

A lengthy period without a serious accident can lead to erosion in formality—it is easy to forget hazards that rarely occur.

A worker in the plutonium facility at Lawrence Livermore National Laboratory (LLNL). LLNL plays a large role in the stewardship of the nationals nuclear weapons arsenal and in finding ways to safely dispose of surplus plutonium components.

PHOTO COURTESY DOE

to identifying hazards, eliminating and/or controlling risks, and maintaining safety systems.

High-Consequence Accidents

Unfortunately, catastrophic system accidents do occur, and looking for patterns and common factors leading to these failures can be useful. Investigations of the *Challenger* (Vaughan), Three Mile Island (Walker), Chernobyl (Medvedev) and Tokia-Mura (LANL) accidents revealed common root causes in technical, organizational and human factors issues.

The results of these investigations support the normal accident school of thought by revealing that organization complexity and productivity motives can lead to high-consequence accidents. To prevent incidents from escalating to major accidents, responsible managers and operators must have the in-depth technical understanding and experience needed to respond safely to abnormal events. The human factors embedded in an organization's safety structure are clearly as important as the best safety management system, especially when dealing with emergency response.

Two recent events—the near-hit at the Davis-Besse nuclear power plant and the *Columbia* space shuttle disaster—seem to be prototypical of normal accidents. Lessons learned from both events have been thoroughly analyzed and discussed in reports from the Columbia Accident Investigation Board (CAIB) and the Davis-Besse Lessons-Learned Task Force.

The Davis-Besse group found both technical and organizational causes for that near-hit. Technically, leaking boric acid that had dried onto the hot reactor vessel was apparently not considered to be a significant corrosion problem. Despite that assumption, leaking boric acid resulted in a six-inch deep corrosion cavity in the carbon steel vessel head; only the stainless steel cladding remained as a pressure vessel boundary for the reactor core. Organizationally, neither the reactor operator self-assessments nor NRC oversight identified the buildup of boric acid deposits as a safety issue.

A major finding of CAIB was that poor organizational structure can be just as dangerous to a system as technical and operational failures. The investigation report identified organizational causes of the shuttle accident. One key finding was that high-risk organizations can become desensitized to deviation. Foam strikes during shuttle launches had occurred many times with no apparent consequence. This so-called "normalization of deviance" involves organizational acceptance of frequently occurring abnormal performance.

Another lesson learned was that past successes may be the first step toward future failure. More than 100 successful shuttle missions with numerous debris strikes per mission had reinforced confidence that foam strikes were acceptable. Such success can lead to a "we have always done things that way and never had problems" approach to safety. The investigation board also stressed that leaders must demand minority opinions and healthy skepticism. Management acceptance of minority opinions regarding O-ring seals and foam strikes might have avoided both of the shuttle explosions. Perhaps the simplest but most profound principle in the report is that safety efforts must focus on preventing—not investigating—mishaps.

Safety Attributes

One objective for delving into the background information on complex, high-hazard organizations is to identify an optimum set of primary attributes and secondary characteristics needed to safely manage operations involving nuclear weapons and nuclear materials. At the highest level, the responsible organization needs to maintain excellence in science and technology, nuclear safety standards and performance assurance in addition to ensuring a proactive safety attitude, reliable nuclear facilities, adequate safety resources and public trust and confidence. The collective insights gained from the social science perspectives and engineered approach to managing hazardous activities, along with lessons learned from major accidents, can be synthesized to identify the following essential attributes for safely managing nuclear operations.

Technical Excellence

Nuclear safety requires a fundamental understanding of nuclear science and engineering. Operators, managers and safety overseers must have in-depth understanding of both the safety and technical aspects of the mission, and the organization must sustain its focus on nuclear safety research and testing. Technical excellence means that safety analyses are based on sound engineering with a solid foundation of physics, chemistry and nuclear technologies.

Safety Standards

Clear, concise technical safety directives that are based on sound engineering principles and are centrally developed, controlled and verified are an essential foundation for safe nuclear operations. Rigorous and inviolate technical safety standards must be applied to high-consequence operations. These safety directives encompass quality assurance, nuclear facility safety basis (documented safety analysis and hazard controls which provide reasonable assurance that a nuclear facility can be operated safely), safety management and radiation protection standards.

Performance Assurance

Competent, robust and frequent oversight is required to assess compliance, evaluate performance, ensure accurate reporting and maintain operational awareness. A performance assurance program should be established to predict and prevent accidents using realistic performance indicators, trend analysis and rapid correction of issues.

Safety Attitude

Fundamental to a good safety attitude is proving that no safety problem exists before work begins. Senior leaders must be equally committed to the value of safety and productivity and must not give mixed signals about the importance of safety. A questioning attitude and constructive skepticism that challenges conclusions must be encouraged at all levels of the organization.

Operational Reliability

Robust nuclear facility safety systems are independent, redundant and diverse, but not overly complex. Redundant safety structures, systems and components must be designed into nuclear facilities and safety margins must be carefully maintained. Nuclear facilities must be built in accordance with robust designs, engineered safety features and defense in depth using codes and standards that clearly control the safety operating envelope.

Safety Resources

Safety issues and productivity must have equal priority for funding and schedule allocations. Modern infrastructure and new facility construction must be maintained. Sufficient organizational redundancy must exist to independently manage and oversee safety performance.

Conclusion

System failures are rooted in complex interactions between engineering failures and human factors. Random events can trigger a complex set of interactions that could lead to an unanticipated nuclear accident. Generally speaking, the more information available, the more confidently an outcome can be predicted; however, one cannot confidently predict the likelihood of a nuclear accident using statistics based on trends in industrial accidents. Furthermore, regardless of how safely the organization operates, if failure is too costly to bear, the organization cannot decrease safety diligence.

Safely managing the enduring nuclear weapon stockpile, fulfilling nuclear material stewardship responsibilities and ensuring the availability of nuclear energy are missions with a horizon far beyond current experience and, therefore, demand a unique organizational structure. Because of the potential risks and importance of the nuclear missions, maintaining public trust is an additional and essential attribute. That trust requires respect for public safety and health as evidenced by an excellent safety record, effective external oversight, a positive safety attitude and public information sharing programs.

Conservative engineering of safety systems is necessary yet not sufficient to ensure safe nuclear operations. Social science considerations are equally important. Organizations can provide added risk reduction by implementing the attributes of highly reliable organizations. To avoid random accidents, organizations must not rely on luck, must not be fooled by success and must always prepare for the worst by expecting the unexpected. ■

References

Ackland, L. *Making a Real Killing: Rocky Flats and the Nuclear West.* Albuquerque, NM: University of New Mexico Press, 1999.

Bureau of Labor Statistics (BLS). Injuries, Illnesses and Fatalities Program. Washington, DC: U.S. Dept. of Labor, BLS.

Columbia Accident Investigation Board (CAIB). "Columbia Accident Investigation Board Report." Arlington, VA: CAIB, 2003.

Defense Nuclear Facilities Safety Board (DNFSB). "Integrated Safety Management." DNFSB/Tech 16. Washington, DC: DNFSB, June 1997.

Dept. of Energy (DOE)(a). Computerized Accident/Incident Reporting System (CAIRS). Washington, DC: DOE, Office of Environment, Safety and Health, ES&H Corporate Reporting Databases. <http://www.eh.doe.gov/cairs>.

DOE(b). "Containers Found with Masses Exceeding Allowed Values." ORTS-YSO-BWXT-2005-004. Washington, DC: DOE, Occurrence Reporting and Processing System.

DOE(c). "Misinterpretation and Misapplication of Available Information Results in Criticality Working Requirement Violation." ED-BNFL-AMWTF-2004-0032. Washington, DC: DOE, Occurrence Reporting and Processing System.

DOE(d). Safety Management System Policy. Policy 450.4. Washington, DC: DOE, Sept. 15, 1996.

Gephart, R.E. *Hanford: A Conversation about Nuclear Waste and Cleanup.* Columbus, OH: Battelle Press, 2003.

Krause, T.R. *Employee-Driven Systems for Safe Behavior.* New York: Wiley, 1995.

LaPorte, T.R. "High Reliability Organizations: Unlikely, Demanding and At Risk." *Journal of Crisis and Contingency Management.* June 1996: 60-71.

Los Alamos National Laboratory (LANL). *A Review of Criticality Accidents.* LA-13638. Los Alamos, NM: LANL, 2000.

Medvedev, G. *The Truth about Chernobyl.* New York: Basic Books, 1991.

National Aeronautics and Space Administration (NASA). "Safety Program Status Reports 1980-2003." Washington, DC: NASA, Office of Safety and Mission Assurance.

Nuclear Energy Institute (NEI). "World Assn. of Nuclear Operators 2003 Performance Indicators for the U.S. Nuclear Industry." Washington, DC: NEI.

Perrow, C. *Normal Accidents: Living with High-Risk Technologies.* Princeton, NJ: Princeton University Press, 1999.

Reason, J.(a). *Human Error.* New York: Cambridge University Press, 1990.

Reason, J.(b). *Managing the Risks of Organizational Accidents.* Aldershot, U.K.: Ashgate Publishing Ltd., 1997.

Roberts, K.H. "Some Characteristics of One Type of High Reliability Organization." *Organizational Science.* 1(1990): 160-176.

Rochiln, G.I. "Reliable Organizations: Present Research and Future Directions." *Journal of Crisis and Contingency Management.* June 1996: 55-59.

Sagan, S.D. *The Limits of Safety.* Princeton, NJ: Princeton University Press, 1993.

Snook, S.A. *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq.* Princeton, NJ: Princeton University Press, 2000.

Taleb, N. *Fooled by Randomness.* New York: Random House, 2001.

Vaughan, D. *The Challenger Launch Decision.* Chicago: University of Chicago Press, 1996.

Walker, J.S. *Three Mile Island: A Nuclear Crisis in Historical Perspective.* Berkeley, CA: University of California Press, 2004.

Acknowledgments

The author would like to acknowledge the input of James J. McConnell, Chief of Defense Nuclear Safety for the National Nuclear Security Administration in developing this article. The views expressed are solely those of the author and no official support or endorsement of this article by the Defense Nuclear Facilities Safety Board or the federal government is intended or should be inferred.

Perhaps the simplest but most profound principle . . . is that safety efforts must focus on preventing—not investigating—mishaps.