Lessons Learned from "Lessons Learned":

The Evolution of Nuclear Power Safety after Accidents and Near-Accidents

Edward D. Blandford and Michael M. May

AMERICAN ACADEMY OF ARTS & SCIENCES

Lessons Learned from "Lessons Learned":

The Evolution of Nuclear Power Safety after Accidents and Near-Accidents

Edward D. Blandford and Michael M. May

Copies of this publication can be downloaded from:
http://www.amacad.org/projects/globalnuclearbooks.aspx.

Suggested citation: Edward D. Blandford and Michael M. May, *Lessons Learned from "Lessons Learned": The Evolution of Nuclear Power Safety after Accidents and Near-Accidents* (Cambridge, Mass.: American Academy of Arts and Sciences, 2012).

Cover image: A hazard sign indicating radiation, with the containment shelter for the damaged fourth reactor at the Chernobyl Nuclear Power Plant, Ukraine, seen in the background, April 24, 2012. © Reuters/Gleb Garanich.

ISBN: 0-87724-094-9

This paper is part of the American Academy's Global Nuclear Future Initiative, which is supported in part by grants from Carnegie Corporation of New York, The William and Flora Hewlett Foundation, The John D. and Catherine T. MacArthur Foundation, the Alfred P. Sloan Foundation, the Flora Family Foundation, and Fred Kavli and the Kavli Foundation. The statements made and views expressed in this publication are solely the responsibility of the authors and are not necessarily those of the Officers and Fellows of the American Academy of Arts and Sciences or the foundations supporting the Global Nuclear Future Initiative.

Please direct inquiries to:
American Academy of Arts and Sciences
136 Irving Street
Cambridge, MA 02138-1996
Telephone: 617-576-5000
Fax: 617-576-5050
Email: aaas@amacad.org
Web: www.amacad.org

Contents

Preface

As countries struggle to meet the electricity demands of their growing populations while also reducing their carbon footprints, many have turned to nuclear energy. The U.S. nuclear energy program may not increase significantly in the coming decades, but other countries, including many developing countries, have plans for rapid expansion. Even after the recent accident at the Fukushima Daiichi Nuclear Power Plant in Japan, the global trend toward expansion of nuclear energy has continued.

While serious accidents like Fukushima, Three Mile Island, and Chernobyl can provide invaluable lessons, the nuclear industry, nuclear regulators, and the research community must study minor incidents and near-accidents as well. These experiences often reveal not only how to decrease the likelihood that the same mistakes will occur, but also how to avoid larger accidents that may be foreshadowed in earlier, smaller incidents.

In this paper, Edward Blandford and Michael May enumerate the lessons from nuclear accidents and incidents, asking whether the nuclear energy community has indeed learned from those lessons. The authors argue that stakeholders must commit to ongoing improvement of their protocols and standards. Each nuclear incident—no matter its size—underlines the importance of pursuing high standards of safety, security, and proliferation resistance.

For more than five decades, the American Academy of Arts and Sciences has played an integral role in nonproliferation studies, beginning with a special issue of *Daedalus* on arms control published in 1960. Today, the Academy's Global Nuclear Future (GNF) Initiative is examining the safety, security, and nonproliferation implications of the global spread of nuclear energy. Through innovative scholarship and behind-the-scenes interactions with international leaders and stakeholders, the Initiative is developing pragmatic recommendations for managing the emerging nuclear order.

The GNF Initiative is supported in part by grants from Carnegie Corporation of New York, The William and Flora Hewlett Foundation, The John D. and Catherine T. MacArthur Foundation, the Alfred P. Sloan Foundation, the Flora Family Foundation, and Fred Kavli and the Kavli Foundation. The Academy is grateful to these supporters and to the authors for advancing the work of the Initiative. I want to express my thanks to the GNF principal investigators: Steven E. Miller, codirector (Harvard University); Scott D. Sagan, codirector (Stanford University); Robert Rosner, senior advisor (University of Chicago); Stephen M. Goldberg, research coordinator (Argonne National Laboratory); and Kimberly Durniak, program officer (American Academy of Arts and Sciences).

Leslie Berlowitz
President and William T. Golden Chair
American Academy of Arts and Sciences

Acknowledgments

We gratefully acknowledge the contributions from experts who reviewed this manuscript: Robert J. Budnitz (Lawrence Berkeley National Laboratory), Scott D. Sagan (Stanford University), and Burton Richter (Stanford University). In particular, we would like to thank Robert D. Sloan (Entergy) for his review of the final draft and his extensive feedback. We also want to thank the organizers of the October 2011 Nuclear Enterprise Conference at the Hoover Institution at Stanford University, where this paper was first presented. The conference brought together participants from several of the communities involved in the nuclear enterprise, and we benefited greatly from participating.

Edward D. Blandford
Stanford University

Michael M. May
Stanford University

Lessons Learned from "Lessons Learned":

The Evolution of Nuclear Power Safety after Accidents and Near-Accidents

Edward D. Blandford and Michael M. May

EXECUTIVE SUMMARY

In this paper, we briefly survey the lessons that emerged from the three major accidents in the history of nuclear power—the Three Mile Island accident in the United States in 1979, the Chernobyl accident in Ukraine in 1986, and the recent Fukushima accident in Japan in 2011—as well as from a few other, less important accidents. To determine what (if any) impact those lessons have had on the course of nuclear power, we consider which measures were adopted to prevent similar accidents from occurring. We conclude with a few observations that might help guide possible future action.

Our survey yields nine general observations:

1. In terms of fatalities and effects on health and environment, and even taking into account rare destructive accidents such as Chernobyl and Fukushima, nuclear power has overall been safer and less environmentally damaging than most other ways of generating electricity. However, there is no way to ensure complete safety in the nuclear industry (or anywhere else), and the rare accidents have been extremely damaging. Learning from every opportunity is essential, but this has occurred spottily, especially across national boundaries. "Safety is hard work," according to Richard Meserve, former chairman of the U.S. Nuclear Regulatory Commission (NRC). "It must be embedded in the management and cultural practices of both operators and regulators; it is an obligation that demands constant attention."[1] This obligation has not always been met.
2. The rare destructive accidents at Fukushima and Chernobyl have had a significant impact on nearby communities due to radioactive contamination of land, groundwater, and the ocean. Long-term evacuations that prevent people from returning to their homes, farms, and businesses have

1. Richard A. Meserve, "The Global Nuclear Safety Regime," *Daedalus* 138 (4) (Fall 2009): 102ff.

a lasting impact on public well-being. While these consequences should not be trivialized, large-scale contamination is not unique to accidents from nuclear power. It occurs across a broad spectrum of human activities ranging from dam failures, to accidents at chemical industrial facilities, to oil spills. Therefore, any efforts to expand regulatory safety goals beyond public health impacts to include off-site contamination should factor in all risks encountered by society, assessing environmental contamination relative to other individual and public health risks.[2]

3. All three of the major nuclear power accidents as well as several of the lesser-known close calls had precursors in previous incidents, although often not at the same location or in the same country. The lessons-learned reviews completed after the accidents have often contained specific useful points. Some of those points have been implemented—that is, the lessons were learned—but others have not been. Not surprisingly, implementation steps that translated into more efficient operations, such as better, more standardized operating procedures, were carried out more often than steps that required immediate expenditures to avoid uncertain disaster, such as better defenses against possible flooding. Further analysis may find other, less obvious correlations.

4. A regulating agency with appropriate power and strong technical competence—one that is well staffed, well funded, and independent of its licensees[3]—is a necessary, though not sufficient, requirement for safety and in particular for the formulation and implementation of lessons learned. Regulatory capture by licensees through either political or administrative processes has been a problem in several countries. Recent decisions (for example, in India and Japan) to remove the regulating agency from the administrative structure of the operating and promoting agency are a step toward greater safety. However, such decisions have been politically challenging to implement. One year after the Fukushima accident, Japan has yet to establish an independent regulating agency because of political bickering between the ruling and opposition parties. India has faced similar challenges. Beyond an effective regulator, however, a culture of safety must be adopted by all operating entities. For this to occur, the tangible benefits of a safety culture must become clear to operators. Regulators must also encourage the identification and reporting of problems to enable effective implementation of corrective action programs. Ensuring both safety and security at nuclear sites is not a matter of simply setting forth regulations to meet known problems.

2. The NRC set safety goals in its Safety Goal Policy Statement, initiated not long after Three Mile Island and released in 1986. These goals are stated in terms of both individual risk and societal risk; they establish a level of acceptable risk in comparison with other types of risk encountered by individuals and society.

3. Licensees are the entities licensed to construct, operate, and otherwise deal with nuclear installations. They are mainly electric utilities but also include nonprofit research organizations, among others.

Rather, it is a continuing and dynamic set of interactions involving regulators, licensees, and other stakeholders, none of which is independent of the others.

5. An example of a well-balanced combination of transparency and privacy is INPO (the Institute of Nuclear Power Operations), which was created in the wake of Three Mile Island. Funded and supported by the U.S. nuclear power industry, INPO provides a forum for the ongoing process of learning lessons in the operations area. Operator ratings at the various plants remain private, but results with regard to operating procedures and consequences are public. Because of differing laws, policies, and priorities, however, it will be difficult to extend the concept to the international nuclear power industry despite the fact that what happens in one country usually affects the future of the industry in other countries. In addition, many lessons that do not concern operations must be learned. International cooperation should be broadened beyond participation in INPO and the World Association of Nuclear Operators (WANO) to include, for example, the Electric Power Research Institute (EPRI).[4]
6. In the United States and in some other countries, public fear of radioactivity and the ensuing interventions of often well-informed organizations have been a spur to learning from experience. On the other hand, unswerving ideologically based political opposition has served to decrease transparency and mutual cooperation.
7. Fear and uncertainty surrounding the health impacts of low levels of ionizing radiation have resulted in widespread feelings of worry and confusion particularly, but not only, for those affected by reactor accidents. Therefore, public discourse about the health impacts of low-level ionizing radiation must be carried out in the context of all such public risk to health and safety, so as not to contribute unnecessarily to excessive health concerns.
8. Because so much of the cost of nuclear power is incurred before the first kilowatt-hour is generated, the financial backers, including private and government insurers and guarantors, in theory have considerable leverage over the industry, as does any entity that can delay construction and operations, such as regulators and interveners.
9. There can be a tendency to focus the lessons-learned effort primarily on system failures, sometimes marginalizing system successes. Lessons can also be learned from successes. Severe reactor accidents are extremely rare, and every effort should be taken to abstract key engineered or organizational successes.

If we look at the conclusions drawn from both lessons learned and lessons not learned, we could ask how they might apply in the future and, in particu-

4. WANO is an international advisory body; EPRI is an independent research organization of U.S. utilities.

lar, how they might improve nuclear power safety worldwide. From these questions, we come to another set of observations:

1. Modern reactors (classified as Generation III and III+) use safer designs and can be operated more safely than the ones that have caused major accidents. But it is not clear at present how many of the safest designs will be built. Currently there are more than sixty new reactors under construction and hundreds more in the planning stage. The majority of those under construction are Generation II designs with enhancements over plants currently operating. However, the first sets of Generation III and III+ designs are now being built, and many reactors in the planning stage will incorporate the improved variety.

2. The Fukushima accident was initiated by a "once in a thousand years" external event. A precursor incident at the Le Blayais Nuclear Power Plant in France in 1999 that did not lead to radioactivity release had also been viewed as a "once in a thousand years" flood. These characterizations are misleading. In the case of Fukushima (analyzed in more detail later in this paper), the possibility of this "rare event" had been anticipated and disregarded; moreover, the severity of the nuclear accident was greatly increased by siting, design, and response failures. In addition, rare events occur randomly, and the recurrence rate cannot be counted on. Further, considering the lifetimes and the siting of reactors worldwide, there is a valid statistical basis for taking into account even those events that occur once in a thousand years and spending money to prevent or alleviate the worst consequences.

3. While there was clearly substantial failure in Japan to adequately address external natural events that *should* have been included within the design basis, it is important to recognize that there will always be events, in particular natural events or potential terrorist attacks, that will surprise us (for example, the 5.8 magnitude earthquake in Virginia and the Missouri River flooding, both of which took place in 2011). These types of events are why margin and a defense-in-depth approach to safety are essential to ensuring minimal public risk. The failure at Fukushima was due to an insufficient "tsunami defense-in-depth approach," not a failure of the defense-in-depth philosophy itself. Regulatory reform must always focus on a healthy blend of improving defensive actions, mitigation measures, and emergency response to ensure facility robustness for events we can anticipate and those we cannot.

4. Most serious accidents and incidents have had precursors that could have served as warnings. Mechanisms to facilitate and, where needed, enforce mutual learning have not always been adequate to prevent avoidable disasters, especially from one country to another. Information-sharing, import/export agreements based on safety standards, agreements to facilitate cooperation among regulatory authorities, and the participa-

tion of financial interests such as investors and insurers all have a role to play in improving mutual learning among different states.

5. Improved cooperation will rest most securely on lasting, shared economic interest among vendors, owners-operators, government regulators, and the public. At the same time, the international nuclear power and nuclear fuel cycle markets will become if anything more competitive than they have been. New users with no operating or regulatory experience are entering the market: for example, the United Arab Emirates. Therefore, without considerable government attention and cooperation, the nuclear power industry may not become safer, even though from a purely technical point of view it has the potential to do so by adopting the more advanced Generation III and III+ passive reactor designs.
6. Any plan to deal with emergencies must include an incident command structure with clear lines of communication and well-defined areas of responsibility, including the responsibility to provide timely information to the actors involved and to the public. This plan must include all relevant actors, from top political authorities to the regulators and management structure of the licensee and on to local operators and responders at the scene of the emergency. Reviews of the Fukushima accident have highlighted failures in this regard, but Chernobyl and, to a lesser extent, Three Mile Island also demonstrated the need for improvement.

BACKGROUND

Safety issues associated with nuclear technology first arose during the Manhattan Project, which established the U.S. nuclear weapons program. In 1942, the DuPont company agreed to be the prime contractor responsible for construction of the plutonium production complex, starting at Oak Ridge, Tennessee, and ending up at the Hanford site in Washington State. Nuclear technology spanning the fuel cycle, from enrichment all the way to chemical separation, developed at a remarkable pace, with large material inventory demands and little margin for error.

In fact, it was DuPont chemical engineers working on the B-Reactor at Hanford who formally introduced reactor system hierarchy and the "defense in depth" concept into reactor design and construction.[5] The B-Reactor was the first large-scale reactor built following the successful demonstration of the technology at Oak Ridge with the X-10 pilot reactor. Due to the unfamiliarity of the technology, the DuPont engineers relied on their fundamental understanding

5. William Keller and Mohammad Modarres, "A Historical Overview of Probabilistic Risk Assessment Development and Its Use in the Nuclear Power Industry: A Tribute to the Late Professor Norman Carl Rasmussen," *Reliability Engineering & System Safety* 89 (3) (2005): 271–285.

of industrial chemical plants and implemented several layers of independent "barriers" between the site workers and the hazardous radioactive source. Additionally, the concepts of redundancy and diversity in engineered safety systems were formalized into the reactor design process.

Out of the weapons program emerged a commercial nuclear industry that has undergone many transformations over the last fifty years. In this paper, we focus on the ways the organizations responsible for operating and regulating this industry have learned from operational experience, their own and that of others.[6] Throughout this history there has been a range of reactor events differing in severity. Many of these events have been deconstructed and better understood through root-cause investigations yielding a set of lessons learned. We seek to examine these sets further and develop insights about how the industry and other stakeholders collectively learn from accident experience. Following the three major commercial reactor accidents—Three Mile Island, Chernobyl, and Fukushima—the lessons-learned process was carried out in public and scrutinized by the media. However, there have been less severe incidents and operational anomalies that have received much less attention but have, in some cases, provided invaluable learning experiences. What lessons were learned as compared with lessons that should have been learned and were not? How can this experience inform the future so that we can improve on the past?

Key Stakeholders Involved

The key organizations that are responsible for industry learning include the regulatory and other relevant government authorities, licensees and their shareholders, industry organizations, the media, and citizen groups. Given the potential for severe accidents and the public apprehension over all things nuclear, there is a special need for nuclear installations to demonstrate and maintain higher safety standards than is the industry norm with regard to fossil fuel–based utilities. Thus all stakeholders need to make full use of the lessons-learned process. Additionally, regulatory bodies *and* licensees have to learn from serious accidents. This requires, among other factors, regulatory independence from politics and transparency; we consider these questions insofar as they affect stakeholder groups.

Historically, one of the challenges of establishing effective regulatory bodies has been ensuring the complete separation of the organizations responsible for advancing and implementing the technology from those charged with regulating it, as well as insulating the regulators from political pressures to the ex-

6. Some of this learning was facilitated by EPRI and involved cooperation between utilities and the nuclear industry, leading to advanced reactor designs that took advantage of lessons learned from prior incidents.

tent possible.[7] The two types of agency were originally combined because of heavy federal involvement in the commercial introduction of the technology. Splitting the agencies occurred for different reasons and with different effectiveness in different countries. In 1974, the United States split the Atomic Energy Commission into the NRC and the Energy Research and Development Administration primarily for political and confidence reasons. Other countries such as India and, following the Fukushima accident, Japan have taken initial steps in the same direction.

Private organizations such as INPO and WANO perform important functions and are discussed later in the context of learning from accidents. Members of the public, through nongovernmental organizations and the process of intervention, have also played roles in the lessons-learned process, roles that can vary in the international context.

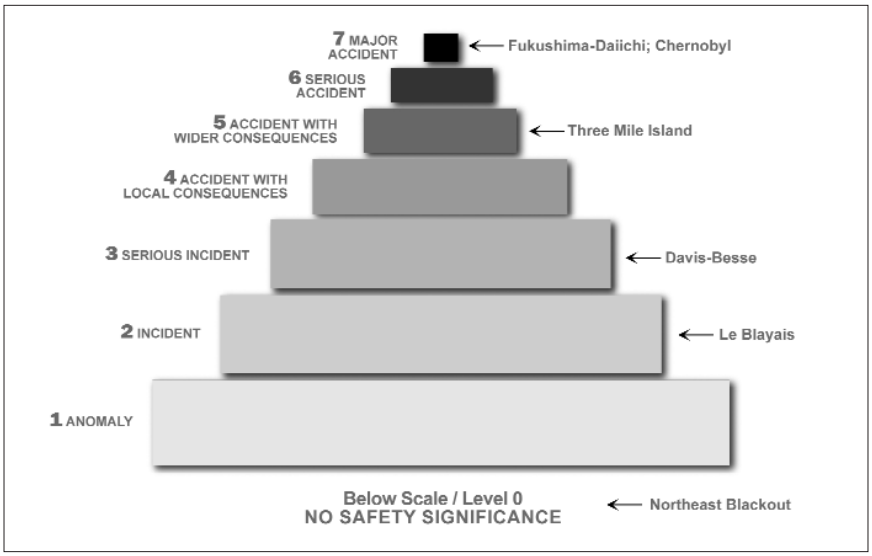
Evaluating Off-Normal Operation

In order to combine into an effective system, both licensee and regulator must constantly learn from *all* modes of operation. Success and failure in nuclear operation are continuums and must be evaluated with equal scrutiny. Success does not mean simply meeting regulatory requirements and maintaining high capacity factors. It is a dynamic process that includes learning. Conversely, failure in plant operation can include routine maintenance all the way up to catastrophic failure. Each aspect enters into a dynamic process of improvement. Success and failure can be measured in such variables as economic, health, and environmental impacts.

In this paper, we discuss events that have occurred since the inception of the commercial nuclear industry. We will loosely follow the qualitative, and therefore somewhat subjective, International Nuclear and Radiological Event Scale (INES) introduced by the International Atomic Energy Agency (IAEA) in 1990; the scale allows events to be rated from "operational anomalies" through "incidents" and all the way to "severe accidents." The INES considers the impact on people and the environment, radiological barriers and control, and defense in depth. Figure 1 indicates where each event considered in this paper lies on the scale. The role of precursor events is especially noteworthy because severe accidents are often the results of earlier anomalies and incidents. Successful identification of these precursors requires initiative, awareness, and operational experience.

7. The NRC is structured to function as an independent agency in which commissioners can be removed only for just cause. In most executive branch agencies, administrators serve at the will of the U.S. president.

Figure 1. IAEA International Nuclear and Radiological Event Scale (INES)



Source: IAEA; used here with permission from the IAEA.

General Assumptions

To focus our discussion, we have made some initial assumptions about the relevant background, including:

- Risk acceptance varies widely around the world. This paper is normative in the sense that it represents a local perspective and is not globally representative.
- It is critical that we differentiate reactor technology and plant operations, as they involve fundamentally different organizations; their relationship varies widely across the globe.[8]
- Initiating events can be broadly classified as *internal* or *external*. Internal events are typically caused by combinations of hardware failures and human errors. External events can be malicious (for example, a terrorist attack) or natural hazards such as earthquakes or tornadoes. Some events that can be internally or externally initiated, like fire and flooding, are often classified as external events.
- The term *near miss*, while not quantified, is used when damaged or deteriorating equipment, human error, or some other factor internal to the state of the reactor or its operation increases the risk of core damage to such a degree that the NRC sends out an inspection team.

8. One NRC spokesperson put this point a different way: "A really good careful driver can probably drive a poorly designed car with no bumpers, but a poor driver can easily wreck a well-designed car." See Joseph V. Rees, *Hostages of Each Other: The Transformation of Nuclear Safety Since Three Mile Island* (Chicago: University of Chicago Press, 1994).

- Lessons are learned from both success and failure. Severe reactor accidents are extremely rare, and every effort should be taken to abstract key engineered or organizational successes.

KEY REACTOR ACCIDENTS, INCIDENTS, AND ANOMALIES

In this section, we review the lessons-learned experience following a range of reactor events. We first focus on major reactor accidents in which the lessons-learned process played out in the public domain and many stakeholders were involved in the process. The location of the reactor accident as well as the reactor technology heavily affects the lessons-learned experience. We then review some less severe reactor incidents and anomalies, which can be of equal interest. Such incidents often reveal the conditions that can lead to more serious accidents.

Reactor Accidents

In each of the following reactor accidents, key organizations such as the IAEA, state regulatory authorities, licensee organizations, and independent commissions initiated formal review processes. We will discuss each accident within the context of the type of initiating event, the major contributor(s) to failure, and the extent of hazard consequence. In the case of Three Mile Island and Chernobyl, the initiating events that caused the accident were *internal* events and were exacerbated by human error. In the case of Fukushima, the initiating event was an *external* event in the form of an earthquake and subsequent tsunami. A common response to nuclear accidents from those outside the country where the accident occurred is a) we don't build our reactors that way, b) we don't operate them that way, and/or c) we understand the governing phenomenology. We keep these three perspectives in mind in the following discussion.

Three Mile Island. This event occurred on March 28, 1979, near Harrisburg, Pennsylvania, when a cooling malfunction and human error caused part of the core to melt in Unit 2 of the Three Mile Island (TMI) Nuclear Generating Station. TMI has two PWR units (pressurized water reactors), both Babcock and Wilcox designs. Unit 1 generates 800 megawatts of electricity (MWe) and was commissioned in 1974; Unit 2 is slightly larger at 900 MWe and began operation in 1978. The accident was initiated by a pilot-operated relief valve (PORV) in the primary system that had become stuck open and was exacerbated by operator action following the initiating event.[9] Unit 2 was ultimately

9. The so-called Rogovin Report disputes the role of operator error as a major contributor to the TMI accident. Instead, it cites inadequate training, poor operator procedures, lack of diagnostic skill on the part of the entire site-management group, misleading instrumentation, plant deficiencies, and poor control-room design. Whatever the cause, some operator actions clearly contributed to the accident. See Mitchell Rogovin and George T. Frampton, Jr., "Three Mile Island: A Report to the Commissioners and to the Public," Nuclear Regulatory Commission, Special Inquiry Group (Washington, D.C.: U.S. Government Printing Office, 1980).

destroyed. Some fission product gas was released a couple of days after the accident, but not enough to cause any detectable dose to local residents above background levels. There were no injuries or adverse health effects. The TMI accident was caused by an internal initiating event and has been rated Level 5, "Accident with Wider Consequences," on the INES. The accident sequence and post-accident forensics are discussed in much greater detail elsewhere.[10]

Following TMI, there were many efforts to conduct comprehensive studies and investigations of the reactor accident. Two weeks after the accident, President Carter established the Kemeny Commission to carry out a technical assessment of what occurred and to make a series of recommendations for the future based on its findings. The NRC created its own inquiry group, headed by Washington, D.C., attorney Mitchell Rogovin. Following the review of the accident, the NRC established a Lessons Learned Task Force charged with suggesting changes to fundamental aspects of basic plant safety policy.[11]

Lessons Learned from Three Mile Island. The Kemeny Commission made a series of recommendations concerning the NRC, the licensees, training, technical assessment, public health and safety, emergency planning, and the public's right to information.[12] Four strong themes emerged from these recommendations and were broadly classified by Joseph Rees as *management involvement*, *normative systems*, *learning from experience*, and *professionalism*.[13] An important recommendation that does not fit under those categories is better human factors engineering (HFE), that is, the engineering that goes into operator-machine interactions. Early control rooms without such HFE modifications placed a much greater burden on operators in an emergency.

- The first key lesson focused on the role of management in operating nuclear power plants. Prior to TMI, many in utility management viewed nuclear plants as assets indistinguishable from fossil fuel–based power generation facilities. Utility executives focused solely on plant output, leaving the challenging day-to-day operations of the plant to others in the company. This situation led to performance objectives that were sometimes inconsistent with the required and expected level of safety.[14]

10. For example, see ibid. and Douglas M. Chapin et al., "Nuclear Power Plants and Their Fuel as Terrorist Targets," *Science* 297 (5589) (September 20, 2002): 1997–1999.

11. U.S. Nuclear Regulatory Commission, "TMI-2 Lessons Learned Task Force Final Report" (NUREG-0585), Washington, D.C., 1979.

12. John G. Kemeny, *Report of the President's Commission on the Accident at Three Mile Island* (New York: Pergamon Press, 1979).

13. Rees, *Hostages of Each Other*.

14. Contrast this mindset with Admiral Hyman Rickover, the "Father of the Nuclear Navy," who famously said: "My program is unique in the military service in this respect: You know the expression 'from the womb to the tomb'; my organization is responsible for initiating the idea for a project; for doing the research and the development; designing and building the equipment that goes into the ships; for the operations of the ship; for the selection of the officers and men who man the ship; for their education and training. In short, I am responsible for the ship throughout its life—from the very beginning to the very end." See "Hearings on Military Posture and H.R. 12564," Department of Defense Authorization for Fiscal Year 1975, 93rd Cong., 2nd sess. (Washington, D.C.: U.S. Government Printing Office, 1974), 1392.

- The second key lesson stems from the overly prescriptive nature of the regulatory structure. The normative landscape was made up of an impressive list of documentation, rules, standards, and so on required to build and operate a nuclear plant. This led to unintended consequences: for example, it left operators to believe, sometimes erroneously, that their plants were completely safe as long as the formal safety requirements had been met.[15]
- Third, the Kemeny Commission noted that previous operational experience elsewhere in the fleet had not been learned across the industry. In fact, learning from experience across the industry was viewed as a peripheral activity and not a necessary endeavor. The Commission noted that the dominant hardware failure at TMI, involving the PORV, had occurred in eleven other instances, but this operational experience with Babcock and Wilcox valves had not been shared across the industry.
- Finally, the Kemeny Commission noted an overall lack of professionalism in the personnel who operated the plants. As a result, operating standards had suffered. Interestingly, the Commission also called for a complete restructuring of the NRC and the abolishment of the five-member commission system. Not all of its recommendations were followed, however. The multimember regulatory commission system is well entrenched in a number of areas in the United States, with members named by political authorities but, once confirmed, nominally independent of them. There is no clear consensus on what structure best assures such independence—or, rather, effectiveness in managing an inherently interdependent process that involves many stakeholders.

The NRC conducted its own review of TMI and suggested several improvements in nuclear power plant operations, design, and regulation.[16] This review was performed independently, but it recognized many of the limitations identified by the Kemeny Commission. Some important regulatory changes that the NRC enumerated included the establishment of crucial equipment requirements and the identification of human performance as an integral component of a safe nuclear plant.

Traditionally, the NRC had left plant management strategies to the licensees and had focused most of its effort on plant operations. This gap was largely remedied by the creation of INPO just two weeks after the TMI accident. The creation of INPO is often cited as the major lesson learned from TMI, and for good reason. INPO confounds the expected norm of an organization that improves the safety and reliability of the nuclear industry; that is, INPO is a private regulatory bureaucracy that was set up by the industry itself and is funded

15. Joseph Rees quotes former UC Berkeley Professor Tom Pigford: "The massive effort to comply with the vast body of [NRC] requirements and to demonstrate compliance therewith . . . foster[ed] . . . [the] complacent feelings that all of the work in meeting regulations must somehow insure safety"; see Rees, *Hostages of Each Other*.

16. U.S. Nuclear Regulatory Commission, "TMI-2 Lessons Learned Task Force Final Report."

directly by licensees. Following TMI, it was recognized that the nuclear navy had an extraordinary safety record and perhaps the commercial industry should learn more from the nuclear navy. Indeed, INPO's first CEO was retired Navy Admiral Eugene Wilkinson, who had served under Admiral Hyman Rickover. There are many reasons why INPO has been recognized as a successful organization, and we discuss several of them later in this paper. The fact that INPO interacts at three distinct hierarchical levels within the organization (the worker level, the manager level, and senior management and executive levels) makes it extraordinarily effective. Additionally, the naval influence can be seen in INPO's emphasis on establishing effective self-assessment and corrective action programs.

Chernobyl. In late April 1986, during an experimental systems test at Unit 4 of the Chernobyl Nuclear Power Plant about eighty miles north of Kiev in Ukraine, a sudden power surge caused the plant to become unstable. Attempts to initiate emergency cooling failed, resulting in more severe power excursions. The reactor pressure vessel ultimately failed, and a massive explosion led to huge amounts of radioactive material being released into the environment. The accident, the worst in the history of nuclear power, was largely due to a reactor design that led to an unstable condition during the test as well as to operator error, in part from a lack of adequate information. The ultimate causes were complex and involved several of the reactor's design features, including its lack of secondary containment. Another factor was that under some conditions, the more the coolant water boiled, the more power was generated; and, again, under some conditions, power generation also increased when the control rods designed to shut down the reaction were inserted. The reactor type, a Soviet-designed RBMK, was originally deployed in several Soviet bloc countries but is now found only in Russia; no new models are being built. Several of the design features that led to the accident have been fixed. Much more on the accident can be found in a number of publicly available references covering the sequence of events, the subsequent analyses, and the environmental and health impacts.[17]

Lessons Learned from Chernobyl. Reactors in the United States and the West in general have different plant designs, broader shutdown margins, robust containment structures, and operational controls to protect them against the combination of lapses that led to the accident at Chernobyl. Thus, from a Western perspective, the Chernobyl accident could be dismissed as "different technol-

17. For a generally accepted analysis of the sequence of events, the causative factors of the accident, and a summary of measures to improve the safety of RBMK reactors, see International Nuclear Safety Advisory Group, "The Chernobyl Accident: Updating of INSAG 1," Safety Series No. 75-INSAG-7 (Vienna, Austria: IAEA, 1992), commonly referred to as INSAG 7, as well as references and annexes therein, including to the earlier document, INSAG 1. See also the NRC backgrounder on Chernobyl: http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/chernobyl-bg.html. For a description of the RBMK reactor and more details on safety fixes after the Chernobyl accident, see "RBMK Reactors," http://www.world-nuclear.org/info/inf31.html. For a summary of environmental and health effects, see "The Chernobyl Accident: UNSCEAR's Assessments of the Radiation Effects," http://www.unscear.org/unscear/en/chernobyl.html, including references therein, especially "Health Effects due to Radiation from the Chernobyl Accident" (2008), an authoritative and detailed recent assessment. UNSCEAR is the United Nations Scientific Committee on the Effects of Atomic Radiation.

ogy" run by a completely "different organization." However, the accident demonstrated some lessons that are relevant for different and safer reactor designs.[18]

1. Three crucial elements are containment; effective severe accident management strategies; and perhaps most important, an inherent and/or passive safety function that can respond with no operator action for a set period of time.
2. Chernobyl demonstrated the importance of operator training, already underscored by TMI, and the complementary need for making accurate and timely information about the complete reactor state available to operators. As a result, a "global INPO" was agreed upon, and WANO was established.
3. Precursor incidents that are not damaging in themselves but point to conditions that could lead to a much worse accident must be acted upon. In the case of Chernobyl, the International Nuclear Safety Advisory Group (INSAG 7) noted that "observations made at the Ignalina [Lithuania] plant in 1983, when the possibility of positive reactivity insertion on shutdown became evident, and the event at the Leningrad nuclear power plant in 1975 pointed to the existence of design problems. . . . [T]his important information was not adequately reviewed and, where it was disseminated to designers, operators and regulators, its significance was not fully understood and it was essentially ignored."[19]
4. Another important effect of Chernobyl was the realization that reactor accidents can have a regional impact on environment and health and a global impact on plans for future additions to nuclear power.

The above lessons learned were only partially acted upon, for a variety of reasons. Thus, with respect to Lesson 1, while all new reactors have effective secondary containment features, better passive safety features (as found in so-called Gen III+ plants) have been implemented in only limited cases. The more complicated licensing and higher financial risk associated with such features have slowed their introduction, with most reactor vendors continuing to offer evolutionary reactor designs with active safety systems. In the case of Lesson 2—the provision for better operator training—WANO's lack of real authority has meant that it is devoted mainly to sharing information, a necessary but insufficient feature. Additionally, no effective carrot (for example, through financial incentives) has been established. In contrast, INPO ratings are used by the financial community to assess U.S. utility stocks and by insurance companies to determine premiums. (We discuss this topic further in the next section.) With

18. In what follows, we do not discuss the fixes specific to the RBMK. Those may be found in the references noted above, particularly "RBMK Reactors," which also has a list of currently operating RBMK reactors.

19. International Nuclear Safety Advisory Group, "The Chernobyl Accident."

respect to Lesson 3, precursor incidents are still being overlooked in some cases; we explore this fact in our discussions of Fukushima and Le Blayais. Lesson 4 has, in general, been internalized by established nuclear power users, but it remains to be seen whether it will also be internalized by new users.

Fukushima-Daiichi. The March 2011 large-scale industrial accident at the Fukushima-Daiichi Nuclear Power Plant was the culmination of three interrelated factors: external natural hazard assessment and site preparation, the utility's approach to risk management, and the fundamental reactor design. The Fukushima-Daiichi plant was first commissioned in 1971 and houses six boiling water reactors (BWRs) ranging in size by age.[20] The reactor accident was initiated by a magnitude 9 earthquake on March 11, 2011, followed by an even more damaging tsunami. However, it was the inability to remove the decay heat in the reactor core that led to core meltdown and radioactive release from three units. The plant first experienced a station blackout (that is, loss of all off-site and on-site power) due to flooding of backup critical emergency electrical generation equipment. Following failure of backup water injection equipment, delays in initiating injection of seawater into the reactors using portable pumping equipment led to the fuel overheating. Subsequently, the generation of hydrogen through steam oxidation of the fuel cladding led to chemical explosions causing significant structural damage.

Contamination of surrounding land, groundwater, structures, and vegetation extended to about 10,000 square miles, of which about 250 square miles are contaminated above safety levels, mainly from Cesium-137. Hot spots were identified beyond these areas. Measurements are ongoing; figures are now only approximate and will change. In addition, the cores were cooled by injection of seawater for a period of time before more permanent arrangements could be made. A small but not yet fully known fraction of that seawater, together with some of the core material, was dispersed into the sea. Measurements of the extent of that contamination are also ongoing.

While the direct public health impact of the reactor accident has, to date, appeared to be low, the economic and nearby environmental consequences are severe. Land restoration alone will take more than a decade and perhaps much longer. Nearly as many people have been evacuated as a result of the radioactivity as were displaced by the tsunami and earthquake. The latter of course was far more deadly, causing perhaps twenty thousand deaths. In contrast with the response to the tsunami and earthquake, which has been widely praised, the response to the nuclear accident perhaps worsened the consequences of the accident and showed the responsible authorities as unready to deal with it.

Lessons Learned from Fukushima-Daiichi. While learning all the lessons from Fukushima will take time, a number of important conclusions about preventive design, mitigation actions, and emergency response have been drawn by Japanese and international organizations in the year since the accident. Among the many reports, accounts, analyses, and recommendations, we note the following:

20. The smallest and oldest, Unit 1, was 460 MWe, while Units 2 through 5 were 784 MWe. Unit 6 was the newest and was 1,100 MWe.

- Three months after the accident, the Japanese government issued a report to the IAEA Ministerial Conference on Nuclear Safety.[21] In this report, the Japanese government identified twenty-eight lessons (thus far) to be learned from the accident. They include (paraphrased here for clarity and brevity):
  - The expectation of and the preparedness for the onslaught of an enormous tsunami were not sufficient.
  - The design against tsunamis was based on tsunami folklore and remaining traces of past tsunamis, not on adequate consideration of the recurrence of large-scale earthquakes.
  - The necessary backup power supply was not adequately safeguarded.
  - Earthquake and tsunami damage caused the loss of cooling functions, leading to the need to diversify those functions.
  - Accident management measures were inadequate in some cases. The report calls for making those measures legal requirements.
  - Effective training to respond to accident restoration at nuclear power plants as well as to work and communicate with relevant organizations in the wake of severe accidents was not sufficiently implemented.
  - Critical instrumentation needed for dealing with the accident failed.
  - Environmental monitoring was insufficient and not communicated adequately to those who needed this information.
  - Central control, communications, and logistics support were inadequate.

  Many of the recommendations made by the Japanese government require major organizational changes that could be considered country-specific. In particular, recommendations on regulatory independence and emergency preparedness have already been implemented in some countries (although certainly not all). Additionally, many of the recommendations discussed below have not yet reached final approval.
- After a ninety-day review of the Fukushima accident, the NRC's Near-Term Task Force released its findings, including twelve recommendations.[22] It attempted to structure its review activities to reflect insights from previous lessons-learned efforts carried out by the agency. For ex-

21. Nuclear Emergency Response Headquarters, Government of Japan, "Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety–The Accident at TEPCO's Fukushima Nuclear Power Stations" (Vienna, Austria: IAEA, June 2011).

22. Charles Miller, Amy Cubbage, Daniel Dorman, Jack Grobe, Gary Holahan, and Nathan Sanfilippo, "Recommendations for Enhancing Reactor Safety in the 21st Century: The Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident," Nuclear Regulatory Commission, July 12, 2011, http://pbadupws.nrc.gov/docs/ML1118/ML111861807.pdf. The NRC determined that both short-term and long-term task forces should be established, as has been done in Japan.

ample, some post-TMI recommendations considered a number of actions that were proposed for general safety enhancement as opposed to specific safety vulnerabilities revealed by the accident. The NRC Backfit Rule[23] may play an important role in determining which recommendations are ultimately implemented in the United States. The recommendations made by the NRC task force were divided into general regulatory concerns: ensuring protection, enhancing mitigation, strengthening emergency preparedness, and improving the efficiency of the regulatory oversight process of the fleet.

- More recently, an independent investigative committee created in June 2011 by the Japanese government issued its interim report, which sharply reinforced earlier conclusions.[24] In the executive summary of its interim report, the independent investigative committee reemphasized several themes from the earlier report issued by the Japanese government to the IAEA. The summary was particularly explicit in calling attention to failures of communication within the government, between the government and TEPCO (the Tokyo Electric Power Company) headquarters, and among those two entities and the operators in the field. In addition, the organization charged with disseminating radioactivity information to the public, SPEEDI, reported to a different ministry than the one involved most directly in managing the accident; therefore, information did not reach the public or the managers in a timely way.

Key themes emerge from the set of recommendations made by those organizations:

1. Each report acknowledged the need to rely on a defense-in-depth philosophy, with resources allocated to measures that improve system protection, mitigation, and emergency response.
2. The Fukushima-Daiichi accident made global licensees and regulators reevaluate whether their facilities have adequate protection from natural phenomena within the design basis. Additionally, redefinition of the design basis and the way in which external hazards are treated was a constant theme. It has become clear that the recurrence time of rare external events cannot be known with any degree of assurance. Even if it could be, simple calculations show that, given the number of reactor sites around the world, the likelihood of a rare external event at some site at some time over the lifetime of a reactor is relatively high.

23. The Backfit Rule was introduced into NRC rule-making in 1970. A later rule-making change required that a backfit "must result in cost-justified substantial increase in protection of public health and safety or common defense and security."

24. The interim report was issued on December 26, 2011; the full report is to be made available in Summer 2012. Only the executive summary was available in English at the time of this writing; see (Provisional) Executive Summary of the Interim Report, Investigation Committee on the Accidents at Fukushima Nuclear Power Stations of Tokyo Electric Power Company, December 26, 2011.

3. A station blackout in which all on-site and off-site AC (alternating current) power is unavailable has long been known to be a highly vulnerable plant operational mode. Regulators require licensees to demonstrate that the plant can meet an "acceptable" specified duration of time known as "coping time." A plant's coping time varies, depending on the redundancy and reliability of both on-site AC backup and off-site power options. The process is currently performance-based and risk-informed in the United States. However, Fukushima-Daiichi illustrated the importance of adequately defining an acceptable coping time.
4. There were some positive lessons from Fukushima-Daiichi. The effective performance of fission product scrubbing in the wet well, greatly reducing aerosol fission product release, was impressive. We know from data collected by authorities (for example, measurements of the uptake of Iodine-131 in children living near Fukushima) that the overall direct public health impact from the nuclear accident will be relatively small.[25] Soil and water contamination by Cesium-137, however, will cause a lasting decontamination problem, likely making return impossible for many evacuees.
5. The reports recognized the challenges posed by multi-unit accidents as opposed to a single-unit accident such as TMI. NRC safety inspections of the domestic fleet revealed that some sites were underprepared for a multi-unit reactor accident.[26]
6. Assignment of responsibilities, chain of command from the highest relevant authority to the operators on the ground, and communications—issues important in every situation—were a dominant theme in the reports from both the Japanese government and the independent investigative committee. Both recognized the critical communication failures on multiple levels, including the communication between local and central organizations, the communication to the public, and the communication to international organizations and the rest of the world. These operational failures led to unnecessary delays in taking key emergency actions, such as depressurization of and alternative water injection into the primary containment vessel in Units 1 and 3 (for different reasons). Lack of timely communication and gaps in responsibility assignments were pervasive in the relevant organizations in Tokyo as well. Monitoring of off-site radiation levels also failed to be communicated in a timely

25. Per F. Peterson, Testimony to California State Senate Energy Committee Hearing on Nuclear Power Plant Safety, Panel on "Seismic and Secondary Seismic Risks Near Nuclear Power Plants and Spent Fuel Rod Storage Facilities in California," April 14, 2011, http://seuc.senate.ca.gov/sites/seuc.senate.ca.gov/files/04-14-11Peterson.pdf.

26. Evidence of a lack of preparation can be found in inadequate mutual aid agreements. For example, Diablo Canyon Power Plant near San Luis Obispo, California, identified the fact that no memorandum of understanding was in place with the California National Guard for the contingency to supply diesel fuel to the site were the main road to be unavailable. More examples can be found in the NRC investigative report, http://pbadupws.nrc.gov/docs/ML1113/ML11133A310.pdf.

> fashion to responsible authorities. According to Japan's report to the IAEA, "The Japanese Government could not appropriately respond to the assistance offered by countries around the world because no specific structure existed within the Government to link such assistance offered by other countries to the domestic needs."[27]

The Fukushima accident continues to have a major global impact. The three lines of rationalization noted at the beginning of this discussion—we don't build our reactors that way, we don't operate them that way, and/or we understand the governing phenomenology—cannot be used here: reactors of the same design as the ones at Fukushima can be found around the world; operations in Japan are not qualitatively different from those elsewhere; and while the phenomenology involved in the reactor is understood, that involved in such external events as earthquakes and tsunamis is not known precisely enough to permit prediction.

The impact on Japan is the most severe. The entire nuclear industry, which provides more than 30 percent of electrical power for that nation, has come under question; as of this writing (March 2012), only two nuclear reactors are in operation in Japan. This outcome seems to stem at least as much from a loss of trust in the government and industrial institutions involved as from the direct effects of the nuclear accident. By comparison, the tsunami itself caused enormously more deaths and devastation than the nuclear accident, but no similar loss of trust in the relevant institutions has occurred.

The impact is not limited to Japan. Germany has returned to a plan calling for early phaseout of its nuclear reactors, and Italy has reconsidered its decision to deploy nuclear power. The impact in the United States, India, and elsewhere continues to evolve. The exact impact cannot now be assessed, nor is it possible to determine how many of the lessons offered by the Fukushima accident will be learned.

Reactor Incidents

In this section, we review two critical reactor incidents that provide insights into industry learning. Neither incident had health or environmental consequences; but in both instances, the responsible licensee and regulator were caught significantly off guard. In the case of Davis-Besse, the trustworthiness of the industry was brought into question. Criminal charges were filed, and two employees and a former contractor were indicted for hiding key evidence from the regulator.

Davis-Besse Reactor Vessel Head Degradation. The Davis-Besse Nuclear Power Station in Oak Harbor, Ohio, closed down on February 16, 2002, for routine refueling and maintenance. During inspections, a refueling outage team discovered serious material flaws in the control rod drive mechanism located in

27. Nuclear Emergency Response Headquarters, Government of Japan, "Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety."

the upper reactor pressure vessel. Davis-Besse has a single PWR of 889 MWe, a Babcock and Wilcox design first commissioned in 1978. The penetrations were made of Alloy 600, which is a common material used to fabricate various parts and components in nuclear power plants and which has historically been susceptible to primary water stress corrosion cracking.

The extent of the pressure vessel corrosion, known as wastage area, was found to be approximately the size of a football. In some regions, instead of the original six-inch-thick reactor head, only the remaining three-eighths-inch stainless steel cladding inner liner made up the primary system pressure boundary. If the liner had failed, the plant would have undergone a loss of coolant accident and would have required activation of the emergency core cooling system to bring the reactor to acceptable standby conditions. With the degradation occurring so close to the control rod penetrations, there was also considerable concern about the reactivity shutdown capability of the plant following a breach in the vessel.

In 2006, two former employees and a contractor were indicted after being criminally prosecuted for a series of safety violations and intentional cover-ups. While Davis-Besse was most affected, this incident represented a management failure on the part of the licensee (FirstEnergy), the NRC, and INPO. Consequently, the entire PWR fleet in the United States was strongly affected. The degradation of the Davis-Besse upper reactor pressure vessel head was ultimately rated Level 3 on the INES, classified as a "Serious Incident."

Lessons Learned from Davis-Besse. Immediately following Davis-Besse, the NRC established a Davis-Besse Lessons Learned Task Force in order to better understand how such a failure in regulation could occur. On September 30, 2002, the task force reported its findings to a senior management review team.[28] The report included fifty-one recommendations for actions that the NRC should take; all but two were ultimately approved by the commission. The recommendations were divided into four categories: (1) assessment of stress corrosion cracking; (2) assessment of operating experience, integration of operating experience into training, and review of program effectiveness; (3) evaluation of inspection, assessment, and project management guidance; and (4) assessment of barrier integrity requirements.

The task force revealed that certain operating experiences from other countries, involving similar reactor pressure vessel penetration nozzles, were not widely known within the NRC and the U.S. nuclear industry. In some cases, these experiences were erroneously determined to be inapplicable to PWR plants in the United States.[29]

The fundamental issue—better understanding of the governing phenomenology behind stress corrosion cracking in the nickel-based alloy nozzle—has

28. For the final report, see U.S. Nuclear Regulatory Commission, "Davis-Besse Reactor Vessel Head Degradation," Lessons Learned Task Force Report, 2002, http://www.nrc.gov/reactors/operating/ops-experience/vessel-head-degradation/lessons-learned/lltf-report.html.

29. Ibid.

plagued the industry. In Spring 2003, just a year after the Davis-Besse incident, apparent boron deposits were detected at the lower reactor pressure vessel head of South Texas Project Unit 1, near two bottom-mounted instruments. While this degradation was unexpected, the advancements made in visual examination of Alloy 600 components following the Davis-Besse incident contributed greatly to locating these flaws.

In the case of Davis-Besse, the key regulatory and operational stakeholders involved failed on organizational, management, and technical grounds. There had been a number of indicators of corrosion, but they were not acted upon, probably because continued production was prioritized over safety. The deceit and resultant cover-up efforts weakened public confidence in the industry, representing a low point in the history of U.S. commercial reactor operations. Unexpected degradations such as those at the South Texas Project will continue to occur; it is the licensee's resultant actions that matter.

Le Blayais Flooding. Le Blayais Nuclear Power Plant is a complex of four 900-MWe PWRs built from 1981 to 1983 alongside the Gironde marine estuary, the outlet for the river Garonne to the Atlantic Ocean in southwestern France. Major floods have been recorded in the area for centuries. EdF, the owner-operator, had put in place sea walls ranging in height from 4.75 to 5.2 meters[30] and had taken other precautions prior to the December 1999 incident. In the month before the incident, the plant's annual safety report announced a plan to increase the height of the sea walls to 5.7 meters in the following year, though EdF delayed construction.

On the night of December 27, 1999, a combination of high tide, high waves driven by winds up to 200 kilometers/hour (160 mph), and intense rain resulted in flooding and the loss of most power supplies, shutting the plant down. Diesel backup generators started up, maintaining power to Units 2 and 4 until some supply was restored. In Unit 1, one set of the two pairs of pumps in the Essential Service Water System failed due to flooding; if both sets had failed, the safety of the plant would have been endangered. In both Units 1 and 2, flooding put part of the Emergency Core Cooling System out of commission.[31]

Because some pumps and generators continued to operate, cooling was maintained and the safety of the plant was not impaired. It was a close call, however, rated as Level 2 on the INES. The incident had an impact on both EdF and political authorities, especially local ones.

30. These are measured from NGF, a sea-level standard used in France.

31. Our account draws from Jean-Marie Mattéi, Eric Vial, Vincent Rebour, Heinz Liemersdorf, and Michael Türschmann, "Generic Results and Conclusions of Re-Evaluating the Flooding in French and German Nuclear Power Plants," Eurosafe Forum, 2001, http://www.eurosafe-forum.org/files/semb1_7.pdf; http://vert-estuaire-charentais.over-blog.com/article-27345494.html (accessed March 21, 2011); A. Gorbatchev, Jean-Marie Mattéi, Vincent Rebour, and Eric Vial, "Report on Flooding of Le Blayais Power Plant on 27 December 1999," Institute for Protection and Nuclear Safety, 2000; Eric de Fraguier, Presentation on "Lessons Learned from 1999 Blayais Flood: Overview of EdF Flood Risk Management Plan," March 2010, http://www.nrc.gov/public-involve/conference-symposia/ric/slides/th35defraguierepv.pdf.

Lessons Learned from Le Blayais Flooding. EdF and various advisory committees conducted a review that lasted seven years and focused mainly on the effects of combinations of adverse events, such as those that led to the Le Blayais flood. As a result of the review, protection against floods was upgraded at most French nuclear plants considered to be at risk, including higher dikes and seawalls, better sealed doors and closures, and a stricter protocol for protective action upon warning.[32] A continuing assessment of the possible effect of climate change was also provided for. The total cost was estimated at €110 million.

EdF appears to have learned some of the important lessons from the incident and has set up a continuing review process; however, it is unclear what other countries have learned from the Le Blayais incident. While TEPCO faced a far worse situation at Fukushima in the wake of the Tohoku earthquake, some of the lessons from the Le Blayais experience were relevant. Most notable among these were improving the protection of backup power supplies (about which TEPCO had been warned by the Japanese regulatory authority) and establishing and rehearsing a clear protocol to deal with flooding. In the United States, the Fort Calhoun Nuclear Generating Station on the Missouri River (about twenty miles north of Omaha, Nebraska) was surrounded by water up to a level of nearly 1,007 feet above sea level in June 2011. The protective berms and walls were 1,009 feet above sea level; the NRC had mandated an increase to 1,014 feet, which had been contested for a time by the operator, Omaha Public Power District. Similar water levels had been reached in 1952; levels just short of 1,000 feet have been reached several times since.[33]

Flooding is only one potential external initiator for accidents, but it is an important one given that nuclear plants are frequently located near large bodies of water. Flooding risks are also of particular concern because they are susceptible to a "cliff edge" effect: that is, the safety consequences of a flooding event can increase greatly with a modest increase in the flooding level.[34] These incidents and other lesser ones show two common features: the maximum design basis flood in some countries is uncomfortably close to floods that recur on a regular basis, and climate change is likely to affect the recurrence pattern of high waters and high winds. This preliminary examination raises the question of whether flood protection should again be reviewed and should be a major part of protecting any new installation.

32. For a summary, see de Fraguier, "Lessons Learned from 1999 Blayais Flood."

33. Peter Behr, "A Nuclear Plant's Flood Defenses Trigger a Yearlong Regulatory Confrontation," *The New York Times*, June 24, 2011, http://www.nytimes.com/cwire/2011/06/24/24climatewire-a-nuclear-plants-flood-defenses-trigger-a-ye-95418.html?pagewanted=all. Also, see http://www.forbes.com/feeds/ap/2011/07/27/general-ne-missouri-river-flooding-nuclear-safety_8587449.html.

34. This observation was made in the NRC's near-term task force report on insights from the Fukushima-Daiichi accident.

Reactor Anomalies

In this section, we look at a reactor event that would be classified as an anomaly or abnormal occurrence rather than an accident or incident. As mentioned earlier, anomalies and reliability indicators are very important, as they often serve as precursors for much larger incidents. The NRC recognizes this fact and is required to provide an annual report to Congress about each abnormal occurrence for the fiscal year. The NRC defines an abnormal occurrence as an unscheduled incident or event that the regulator determines to be significant from the standpoint of public health or safety.

Northeast Blackout. On August 14, 2003, the largest blackout in the history of North America left fifty million people across southeastern Canada and the northeastern United States without power. About six months later, after a three-month investigation, a U.S.-Canada task force determined that a combination of human error and equipment failures was the root cause of the blackout.

Nine nuclear power plants tripped in the United States: eight plants lost off-site power, and one plant was in an outage. The maximum amount of time until power was available to the switchyard for any plant was six-and-a-half hours. While all on-site emergency diesel generators performed as designed, this event was significant due to the number of plants affected by the outage and the unexpected amount of time without off-site power.

Lessons Learned from the Northeast Blackout. The NRC immediately took action following the blackout incident by issuing a regulatory summary reminding licensees that they are required to comply with their technical specifications relative to inoperability of off-site power. The NRC also issued a generic letter titled "Grid Reliability and the Impact on Plant Risk and the Operability of Off-site Power."[35] It required licensees to submit information in four areas: (1) use of protocols between the plant and the transmission system operator (TSO) or independent system operator (ISO) and the use of transmission load flow analysis tools to assist plants in monitoring grid conditions to determine the operability of off-site power systems; (2) use of plant protocols and analysis tools by TSOs to assist plants in monitoring grid conditions for consideration in maintenance risk assessments; (3) off-site power restoration procedures; and (4) losses of off-site power caused by grid failures at a frequency equal to or greater than once in twenty site-years per regulation.

The NRC and the Federal Energy Regulatory Commission (FERC) have held joint meetings annually since the blackout incident to ensure that adequate progress has been made in raising loss of off-site power capabilities of the domestic fleet.[36] Licensees and the NRC are routinely in communication with TSOs and ISOs in order to anticipate potential issues. The NRC also developed improved operator examination and training programs that gave operators prac-

35. http://www.ferc.gov/eventcalendar/Files/20060403161019-nrc-gl200602.pdf.

36. The capabilities of U.S. nuclear plants to deal with serious situations increased greatly following the 9/11 terrorist attacks. While these changes were targeted toward specific extreme external threats such as airplane attack and large fires, the plants' defenses, mitigation capabilities, and emergency response capabilities have greatly improved.

tice in communicating with grid operators. The relationships among FERC, the North American Electric Reliability Corporation (NERC), the NRC, and domestic licensees appear to be proactive and will be further examined as the NRC recommendations from Fukushima are implemented.

SOME KEY OBSERVATIONS

What can be taken away from the foregoing retrospective survey of the more serious nuclear accidents and near-accidents, and from the lessons learned—and not learned—from those events? A few observations emerge.

On the record of the past fifty years, nuclear power has an edge over other forms of providing energy both in terms of limiting day-to-day adverse health and environmental effects, including greenhouse gas emissions, and in terms of the frequency and toll of major accidents. Table 1 makes this point clear.

Table 1. Main Sources of Electricity in the World and Their Morbidity and Greenhouse Gas Emissions Per Unit of Electricity Produced

Source (% of world use, 2007)	Deaths per terawatt-hour	Tons of greenhouse gas emissions per gigawatt-hour (life)
Coal (42%)	161 (U.S. average is 15)	800–1,400
Gas (21%)	4	300–500
Hydro (16%)	0.1 (Europe)	Small–100
Wind (<1%)	0.15	Small–50
Nuclear (14%)	0.04	Small–50

Table generated by authors using data from *Key World Energy Statistics 2009* (Paris: International Energy Agency, 2009), 24; Peter Burgherr and Stefan Hirschberg, "Comparative Risk Assessment of Severe Accidents in the Energy Sector," International Disaster and Risk Conference, August 25–29, 2008, Davos, Switzerland; http://www.cna.ca/english/pdf/studies/ceri/CERI-ComparativeLCA.pdf; http://pia.sagepub.com/content/early/2011/10/29/0957650911424699.abstract?rss=1; Benjamin K. Sovacool, "Valuing the Greenhouse Gas Emissions from Nuclear Power: A Critical Survey," *Energy Policy* 36 (2008): 2940–2953; Alfred Voß, "Energy and Universal Sustainability–An Outlook," Institute for Energy Economics and the Rational Use of Energy, International Materials Forum 2006, Bayreuth, Germany; Bert Metz, Ogunlade Davidson, Peter Bosch, Rutu Dave, and Leo Meyer, eds., *Climate Change 2007: Mitigation of Climate Change*, Intergovernmental Panel on Climate Change (Cambridge: Cambridge University Press, 2007).

The low morbidity is due to several factors, but two stand out:

- Most casualties and other health and environmental effects stem from the extractive and transportation industries. Because the same amount of electric power can be obtained from about 200 to 300 tons of uranium ore as from 3 to 4 million tons of coal or similarly large quantities of gas or oil, these effects are inherently less severe for nuclear power than for the main hydrocarbon sources of electricity.
- The nuclear power industry has from the start been aware of the need for a strong and continued emphasis on the safety culture, although in the early years that culture was not sufficiently informed by experience.

Nuclear plants have such low levels of emissions because no combustion is involved in nuclear electricity generation. Emissions are generated only during construction, installation, mining, refining, enrichment, transportation, and decommissioning. In addition, the smaller tonnage to be mined, transported, and processed lowers emissions from nuclear plants. The actual amount of greenhouse gases generated depends on how the energy is obtained for each of the steps listed above; it is also dependent on the techniques used to make the concrete needed for nuclear facilities.

Despite all these advantages, nuclear accidents will always be possible, including major accidents that could have serious consequences and a considerable impact on public opinion. The knowledge of how to improve nuclear safety comes from experience—and sometimes that means the experience of accidents, close calls, and routine problems. The process of learning can be viewed as a continuing investment in both the political and financial future of the nuclear industry. It has to be considered as part of the base levelized cost of power, reaching every part of the process of providing nuclear power, from qualification of materials such as concrete and steel to operations. Fortunately, most of our knowledge has come from research and day-to-day learning, not from major accidents. The process of learning, however, must be ongoing, not only for nuclear power but for all complex engineered systems that have the potential to cause major disasters.

All three of the major nuclear power accidents (TMI, Chernobyl, and Fukushima) as well as several of the lesser-known close calls had precursors in previous incidents, although often not in the same country. The lessons-learned reviews that followed most of these events usually made specific useful points. Some of those points were implemented—the lessons were learned—but often they were not. Not surprisingly, implementation steps that translated into more efficient operations, such as better, more standardized operating procedures, were carried out more often than steps that required immediate expenditures to avoid uncertain disaster, such as better defenses against possible flooding. Further analysis may reveal less obvious correlations.

A regulating agency with appropriate power and strong technical expertise —well staffed, well funded, and independent of its licensees—is a necessary, though not sufficient, requirement for safety; in particular, it would formulate

and implement lessons learned. Regulatory capture by licensees through either political or administrative processes has been a problem in several countries. Recent decisions (in India, for example) to remove the regulating agency from the administrative structure of the operating and promoting agency is a step toward greater safety. Beyond an effective regulator, however, a culture of safety must be adopted by all operating entities. For this to occur, the tangible benefits of a safety culture must become clear to operators.

In the United States and some other countries, public fear of radioactivity and the ensuing interventions of often well-informed organizations have been a spur to learning from experience. But in countries where the responsible nuclear organizations, governmental and private, were insulated from criticism, learning has been slower. Learning from experience is never an easy process, especially when it takes place in a very public, very critical arena. Nevertheless, transparency has enhanced that process. Transparency helps learning in all three groups: the owners-operators, the government regulators, and some of the intervening organizations. Transparency must be conditional, however: the early critical give-and-take that leads to improvements in design, materials, and operation will not be done frankly and effectively if not done in private.

INPO, funded and supported by the U.S. nuclear power industry, is an example of a well-balanced combination of transparency and privacy; it provides a forum for the ongoing process of learning lessons related to nuclear operations. Operator ratings at the various plants remain private, but results with regard to operating procedures and consequences are public. INPO was started in the United States as a result of the TMI accident, which, as discussed above, resulted from design deficiencies, lack of understanding of some fundamental phenomena, and errors in operating the reactor. Design features prevented any significant release of radiation, but the financial loss was so significant that the industry and its financial backers were moved to cooperate with regulators in establishing and maintaining much improved operator training, operations standards, and operations staffing. The resulting rating of the operators is kept confidential within the industry so that criticism can be uninhibited and action can be taken in a timely manner without fear of misinterpretation. On the other hand, actual performance results, including all incidents, are made public. Expert management in the owner-operator sector has been essential to establish and maintain quality of operations. In addition, dealing with reactors during abnormal conditions requires well-thought-out procedures, clearly established lines of authority, and on-site personnel who are competent and authorized to make tough decisions.

Because so much of the cost of nuclear power is incurred before the first kilowatt-hour is generated, the financial backers, including private and government insurers and guarantors, in theory have considerable leverage over the industry, as does any entity that can delay construction and operations, such as regulators and interveners. That leverage can be obvious, as when the European Reconstruction Bank refused to put money into older Chernobyl-type reactors and insisted on safer Western-style models; but it must work with a reg-

ulating and monitoring institution to preserve the investments. Recognition of the need for a strong, competent, and independent regulator has not come easily to most countries and is not always and everywhere accepted in practice to this day. In particular, independence joined with the resources sufficient to maintain competence faces continuing tensions from operators (and, in democracies, their representatives in government), which need to make a profit or at least stay within budget while maintaining market share, and also from government budgeters, who have to work with limited resources.

LOOKING TO THE FUTURE

In examining the above conclusions and looking to the future of nuclear power worldwide, we come to another set of observations.

1. *Modern reactors are of safer designs and can be operated more safely than the ones that have caused major accidents. But it is not clear how many of the safest designs will be built.* Most reactors being built today are of the Gen II+ design and are significantly safer than the RBMK design involved in Chernobyl and the Mark 1 BWR design involved in Fukushima. With the Gen II+ design, both the reactor vessel and the spent fuel are under two layers of containment. Even safer designs, such as the Gen III and Gen III+, feature more passive cooling systems, which can keep all fuel cool for days without electricity or high-pressure water injection, among other improvements. As of this writing, it is unclear what the future reactor mix will be. An interesting question is whether new reactor users will buy modern designs while existing users will mostly extend the lifetimes of their existing designs.
2. *The Fukushima accident was initiated by a supposedly "once in a thousand years" event and was considerably worsened by faulty design and siting as well as operational and management response. The precursor incident at the Le Blayais Nuclear Power Plant in France had also been viewed as a "once in a thousand years" event. Nevertheless, given how many of the current nuclear sites are subject to rare major external events, and considering the lifetimes of modern reactors, there is a clear statistical basis for taking into account even very rare events and spending some money to prevent or alleviate their consequences.* Reactor lifetimes today are roughly in the sixty-year range, which is 6 percent of the "thousand years" postulated for the recurrence time of the Tohoku tsunami. In addition, there are a number of sites subject to locally rare floods. Since a serious nuclear accident anywhere affects the nuclear industry everywhere, the industry should look at a much higher probability of problems than is implied in the "once in a thousand years" viewpoint. The cost of the Fukushima

accident is estimated to be somewhere between $30 billion and $100 billion; if about a billion dollars had been prudently spent on the precautions that have been identified since the accident (and that we summarized above), some of the worst consequences of the accident could at least have been mitigated. While tsunamis are not the only possible external source of disaster, and while prioritization in allocating limited resources is always necessary, a new look must be taken at rare but potentially catastrophic events as well as the precautions that could be useful and economically justifiable in dealing with such events.

3. *The failure at Fukushima was due to the lack of a sufficient "tsunami defense-in-depth" approach, not a failure of the defense-in-depth philosophy in general.* The Fukushima accident cannot be attributed solely to an inadequately sized seawall. Rather, the accident followed a series of failures, including failures in plant defensive actions, mitigation efforts, and emergency response. Accounting for every potential event that falls within the tails of the respective probability distributions is an unmanageable approach. Appropriate reform should focus not solely on defensive actions but on a robust blend of improved defensive actions, mitigation efforts, and emergency response procedures.
4. *Mechanisms to facilitate and incentivize mutual learning may not be adequate to make best use of lessons learned and prevent avoidable disasters.* The present mechanisms are unsystematic and do not have enforcement or incentive features. They include the efforts of vendors to build safer reactors, the general availability of lessons learned from particular accidents and near-accidents, and awareness of the worldwide cost of a nuclear accident anywhere. At the institutional level, the two active organizations are the IAEA and WANO. The IAEA produces reports and submits protocols for adoption by its nation-members. It has major responsibilities in other areas (for example, safeguards against military use of civilian facilities), and it does not have the personnel, budget, or authority required to set and enforce safety standards (should any be agreed upon). WANO focuses on reactor operation, an essential—but not the only—ingredient of safety. Its main activity in that regard is information sharing. INPO, the U.S. counterpart to WANO, is quite effective. But it is a confidential and cooperative U.S. industry effort that seems difficult to replicate on a worldwide basis, at least without major changes.
5. *Improved cooperation will rest most securely on lasting shared economic interest among vendors, owners-operators, government regulators, and the public. At the same time, the international nuclear power and nuclear fuel cycle markets will become, if anything, more competitive.* No solution to this problem is in sight. Elements of a solution might include the following factors:

- Some form of an import/export agreement, such as what the Nuclear Suppliers Group now uses to monitor weapons-sensitive materials and components, might be effective. Those efforts rest on an agreement at the state level; the same would be true of a safety-oriented agreement. If there were such agreement among states, one could envisage that any vendor wishing to export reactors or other potentially dangerous nuclear facility would need a license certifying that the design meets modern safety standards. With only a few international reactor vendors, implementation of such an agreement seems feasible.

- Reactor design is not the only safety consideration. Siting, construction practices, and operations also enter the mix in essential ways, as do accident management, regulatory review, and lessons-learned feedback. Agreement at the state level that would strengthen cooperation among regulatory authorities—perhaps even setting standards for independence of those authorities—would be a positive step. There is no clear consensus on what structure best assures such independence—or, rather, effectiveness in managing an inherently interdependent process that involves many stakeholders. A conversation that would take into account national precedents and institutions is needed before any attempt is made to discuss standards.

- Finally, investors and insurance companies have strong incentives to avoid serious accidents. Liability for insurance companies is generally limited, leaving investors and taxpayers to take losses. In most countries, investment comes partly from government and partly from bond sales. Investment represents a potential source of leverage to avoid accidents; however, to date it has not been harnessed toward effective action because of a lack of knowledge and because nuclear-related investments may make up only a small part of the portfolios.

Contributors

Edward D. Blandford is a Stanton Nuclear Security Postdoctoral Fellow at Stanford University's Center for International Security and Cooperation; he also serves as an adjunct Research Assistant Professor in the Department of Chemical and Nuclear Engineering at the University of New Mexico. His research at Stanford involves advanced nuclear reactor designs, with an emphasis on safety, security, emergency preparedness, and international safeguards. Other research interests include nuclear reactor thermal-hydraulics in support of the safety of nuclear installations, probabilistic risk assessment, best-estimate code verification and validation, and material degradation management. Previously, he worked as a project manager in the Steam Generator Management Program at the Electric Power Research Institute (EPRI), where he managed thermal hydraulics–related research and development activities.

Michael M. May is Professor Emeritus (Research) in the School of Engineering at Stanford University, where he is also a Senior Fellow in the Freeman Spogli Institute for International Studies. He is former Codirector of Stanford's Center for International Security and Cooperation and is Director Emeritus of the Lawrence Livermore National Laboratory. He has held a number of government advisory positions, was a member of the U.S. delegation to the Strategic Arms Limitations Talks, and is a Fellow of the American Physical Society and the American Association for the Advancement of Science. May received the Distinguished Public Service and Distinguished Civilian Service Medals from the Department of Defense as well as the Ernest Orlando Lawrence Award from the Atomic Energy Commission, among other awards. His current research interests are in nuclear security, energy, environment, and terrorism, and in the relationship between nuclear weapons and foreign policy.

The Global Nuclear Future Initiative of the American Academy

There is growing interest worldwide in civilian nuclear power based on the recognition of its potential for meeting increased energy demands. But the spread of nuclear technology, in the absence of rigorous safety regimes, presents unique security risks, including the potential proliferation of weapons capabilities to new states and to subnational and terrorist groups.

The Academy's Global Nuclear Future Initiative is working to prevent this dangerous outcome by identifying and promoting measures that will limit the security and proliferation risks raised by the apparent growing global appetite for nuclear energy. The Initiative has created an interdisciplinary and international network of experts working together to devise and implement nuclear policy for the twenty-first century.

To help reduce the risks that could result from the global expansion of nuclear energy, the Initiative addresses a number of key policy areas, including the international dimension of the nonproliferation regime, the back-end of the fuel cycle, and the security of nuclear facilities and materials. Each of these areas has specific challenges and opportunities, but informed and thoughtful policies for all of them are required for a comprehensive solution. We also recognize that "game changers," developments that could have a tremendous impact but cannot be extrapolated from current trends, could influence the course of events and should be identified and included in our deliberations.

American Academy of Arts and Sciences

Selected Publications of the American Academy

"Nuclear Collisions: Discord, Reform & the Nuclear Nonproliferation Regime"
Steven E. Miller, Wael Al-Assad, Jayantha Dhanapala, C. Raja Mohan, and Ta Minh Tuan

"The Back-End of the Nuclear Fuel Cycle: An Innovative Storage Concept"
Stephen M. Goldberg, Robert Rosner, and James P. Malone

"Game Changers for Nuclear Energy"
Kate Marvel and Michael May

"Nuclear Reactors: Generation to Generation"
Stephen M. Goldberg and Robert Rosner

"Shared Responsibilities for Nuclear Disarmament: A Global Debate"
Scott D. Sagan, James M. Acton, Jayantha Dhanapala, Mustafa Kibaroglu, Harald Müller, Yukio Satoh, Mohamed I. Shaker, and Achilles Zaluar

"Multinational Approaches to the Nuclear Fuel Cycle"
Charles McCombie and Thomas Isaacs, Noramly Bin Muslim, Tariq Rauf, Atsuyuki Suzuki, Frank von Hippel, and Ellen Tauscher

"On the Global Nuclear Future," vols. 1–2, *Daedalus*, 2009–2010

"Science and the Educated American: A Core Component of Liberal Education"
Edited by Jerrold Meinwald and John G. Hildebrand

"Science and the Media"
Edited by Donald Kennedy and Geneva Overholser

"Do Scientists Understand the Public?"
Chris Mooney

To order any of these publications please contact the Academy's Publications Office.
Telephone: 617-576-5085; Fax: 617-576-5088; Email: publications@amacad.org