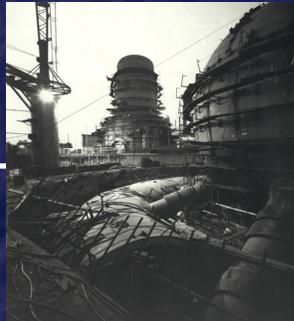
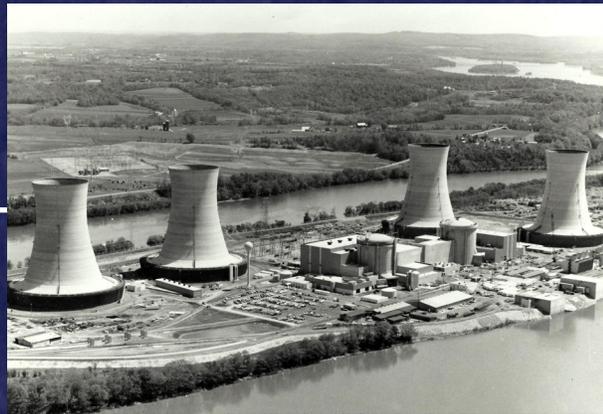


No Undue Risk

*Regulating the Safety of Operating
Nuclear Power Plants*



Acknowledgments

The U.S. Nuclear Regulatory Commission would like to thank the following people who shared their time and experience to make this document possible:

William Ruland

Brian Sheron

Jim Wiggins

Marc Dapas

Tim Collins

Richard Correia

Tom Murley

Mark Salley

Roger Mattson

Frank Miraglia

David Notley

For more information contact Thomas Wellock at thomas.wellock@nrc.gov

Contents

CONTENTS	iii
Figures	v
NO UNDUE RISK: REGULATING THE SAFETY OF OPERATING NUCLEAR POWER PLANTS	1
Introduction	1
PART I: REGULATING OPERATING REACTORS IN THE 1960s AND 1970s	1
The Creation of the Nuclear Regulatory Commission	3
Risk Assessment—The Reactor Safety Study	4
The Three Mile Island Unit 2 Accident	5
PART II: REGULATORY CHANGES INFLUENCING REACTOR DESIGN	6
The NRC Moves Toward Risk-Informed Regulation	6
Reactor Oversight	6
Severe Accident Policy Statement	7
Maintaining Safety: The Maintenance Rule	8
License Renewal	9
PART III: HARDWARE CHANGES	10
INITIATING EVENTS	10
Anticipated Transient Without Scram	10
Station Blackouts	11
MITIGATING SYSTEMS	12
Fire Safety	12
Containment Building Sump Performance	13
Auxiliary Feedwater Systems	15
BARRIER INTEGRITY	16
Combustible Gases in the Containment Building	16
Containment Pressure Relief Performance	17
CROSS-CUTTING AREAS	17
Human Performance	17
Safety Culture	19
THE FUKUSHIMA DAI-ICHI ACCIDENT	21
Conclusion	22

Figures:

Figure 1:	The design and construction of the Loss of Fluid Test (LOFT) reactor at Idaho’s National Reactor Testing Station (now called Idaho National Laboratory) raised questions about the adequacy of Emergency Core Cooling Systems to cope with a loss-of-coolant accident and led to controversial hearings	2
Figure 2:	In 1975, the first NRC Commission meets with President Gerald Ford. Pictured from left to right are Richard Kennedy, Marcus Rowden, William Anders (Chairman), President Ford, Victor Gilinsky, and Edward Mason.	3
Figure 3:	The accident at Three Mile Island in March 1979 marked a turning point in the regulation of operating reactors. It led to a greater focus by the NRC on severe accidents, human factors, and the use of new accident-assessment tools.	5
Figure 4:	After the accident at Three Mile Island, the NRC made its limited resident-inspector program a permanent program at all commercial facilities.	6
Figure 5:	Despite their size and their permanent appearance, most aging components in a nuclear power plant can be replaced. A new steam generator is to be installed at the Indian Point Energy Center in New York	9
Figure 6:	Critical to safety during a station blackout are the power plant’s emergency diesel generators, such as the one pictured here. In 1988, the NRC developed a new rule on station blackouts and guidance on diesel generator performance.	11
Figure 7:	The Browns Ferry fire damaged hundreds of safety-related electrical cables. It underscored the need for fire-safety training and greater safety research.	12
Figure 8:	In the decades after the Browns Ferry fire, the NRC sponsored numerous research initiatives on the causes, consequences, and coping strategies for nuclear-plant fires.	13
Figure 9:	Testing revealed that fine particulates from reactor piping insulation could break loose after a loss-of-coolant event, clog sump screens, and limit the sump systems’ performance. This long-standing generic issue was resolved for all nuclear power plants.	14
Figure 10:	Relatively small in size, the Mark I containment proved susceptible to damage from the ignition of combustible gasses during fuel-damaging accidents. Pictured are Mark Is under construction at the Browns Ferry Nuclear Power Plant.	16
Figure 11:	By the 1970s, reactor plant control rooms had become very complex and contributed to operator error, most notably during the Three Mile Island accident in 1979.	18
Figure 12:	Adding to the confusion reactor operators experienced during the accident at Three Mile Island was a noisy and crowded control room environment.	18
Figure 13:	The Davis-Besse nuclear power plant reactor vessel head experienced extensive erosion from a small leak. The event raised serious questions about the safety culture at the facility.	20

No Undue Risk: Regulating the Safety of Operating Nuclear Power Plants

Introduction

No Undue Risk is a history of some of the most important reactor safety improvements brought about by the U.S. Nuclear Regulatory Commission (NRC) at operating commercial nuclear power plants.¹ Many years have passed since most of these plants received their licenses. Some people worry that today's commercial reactors, like used cars, are aging technologies of questionable safety: "Most of us would not drive a 1967 car across the country," said one person. "No, we would want new, safer, and more reliable transportation." The comparison of reactors to old automobiles is misleading. Unlike an automobile whose design is largely fixed at the time it rolls off the assembly line, operating nuclear plants are continuously improved through numerous design upgrades, comprehensive maintenance programs, and better operations.

Why has the NRC required these improvements at plants already licensed as posing "no undue risk" to public safety?² Expanding knowledge and experience has led to identification of new safety issues, as well as a more comprehensive approach to reactor safety regulation. In the early 1960s, regulators at the NRC's predecessor, the Atomic Energy Commission (AEC), pursued safety largely through hardware design and quality assurance. Since then, the AEC and the NRC developed and implemented a regulatory approach that seeks to maximize safe operation by augmenting traditional qualitative approaches to safety pioneered by the AEC with quantitative insights about risks from human performance, plant management and operations, and reactor design. As a result, today's nuclear plants are not the same as when they were first designed and constructed. They are safer and more reliable.

Contents

The history of reactor plant safety improvements is intimately connected to the evolution of the NRC's regulatory system. As such, this report is divided into three parts:

¹ The NRC divides reactor plant safety regulation into three categories: (1) Reactor Safety—avoiding accidents and limiting their consequences, (2) Radiation Safety—reducing unnecessary radiation exposure to humans and the environment, and (3) Security—protecting the plant from sabotage and other security threats. No Undue Risk covers the history of reactor safety. Other NRC publications deal with radiation safety and safeguards. On radiation safety, see J. Samuel Walker, *Permissible Dose: A History of Radiation Protection in the Twentieth Century*, Berkeley: University of California Press, 2000. On security, see "Protecting Our Nation: A Report of the U.S. Nuclear Regulatory Commission," NUREG/BR-0314, Revision 3, June 2011.

² That a nuclear power plant must pose "no undue risk" or provide "adequate protection" to the health and safety of the public are among the requirements of the Atomic Energy Act of 1954, as amended.

Part I provides a brief history of the AEC's regulation of operating reactors until it was replaced by the NRC in 1975, and it covers the NRC's regulatory activity until the Three Mile Island accident in 1979. More focused on design and construction issues, the AEC and early NRC lacked a comprehensive regulatory framework for plant operations.

Part II outlines some of the significant regulatory changes and research programs launched by the NRC after the Three Mile Island accident. Over time, the NRC moved incrementally to incorporate a new understanding of reactor plant risks into its regulatory structure by adopting risk-informed technical requirements (risk-informed regulations). These changes led to numerous plant upgrades and management changes at operating facilities. In addition, the NRC moved incrementally to use a risk-informed decision-making process when adopting new safety regulations and making nuclear power plant licensing decisions.

Part III provides a detailed examination of several important safety issues that the NRC and nuclear industry sought to resolve through design changes and improvements to the human-machine interface with nuclear power plants.

PART I: REGULATING OPERATING REACTORS IN THE 1960s AND 1970s

Between the passage of the Atomic Energy Act of 1954 and NRC's creation in 1975, the AEC emphasized rapid development and licensing of new reactor designs. Regulators tried to ensure adequate safety at commercial plants by preventing and mitigating dangerous but unlikely accidents caused by hardware failures. The creation of the NRC, new analytical tools, and the Three Mile Island accident broadened the agency's approach to safety to include non-hardware related hazards.

Regulating Operating Reactors at the Atomic Energy Commission

Before the establishment of the NRC in 1975, the AEC's regulatory staff faced a heavy demand to approve the many construction permits and operating licenses that utilities sought every year. The AEC was responsible for promoting nuclear power and regulating its safety, a conflicted mission that simultaneously pulled the regulatory staff toward more and less regulation. The AEC wanted to avoid restrictive regulation that might stifle the young industry's creativity. To maximize industry latitude, AEC initially had few

hard-and-fast safety criteria, design guidelines, and rules for reviewing applications. The AEC did, however, take reactor safety seriously by requiring conservative safety margins (i.e., they had more than enough capacity to handle design-basis accident).³ Conservative safety margins and qualitative assessments of risk compensated for limited quantitative data, operating experience, and computer capability.

By the mid-1970s, much had changed. The major corporations offering nuclear power reactor designs—vendors such as General Electric, Westinghouse, Combustion Engineering, and Babcock and Wilcox—had largely settled on offering their own versions of light-water reactors using either pressurized water or boiling water.

At the same time, the AEC began to adopt technical regulations that reflected “lessons learned” from the AEC’s earlier licensing reviews and the construction and operation of the first licensed plants. A major milestone in the AEC’s process occurred in 1971 when the AEC issued its General Design Criteria—a set of safe-engineering principles required for all commercial designs. The AEC also issued regulatory guides that specified acceptable methods to address certain safety issues in a design. In 1975, the NRC published its Standard Review Plan to make more uniform staff reviews of construction applications.

Evolution toward standardized designs and the AEC’s approval process for new reactors was good for reactor safety, but it created complications. Between older and newer reactors there were at times significant differences in the design, documentation, and analysis of their safety features. Additionally, as safety research and plant operating experience grew, new safety questions surfaced that older plant designs did not address.

The AEC had a solution. Unlike a car whose design is complete when it arrives on the showroom floor, regulators could demand safety upgrades to operating plants, a process known as backfitting. The AEC’s Advisory Committee for Reactor Safeguards kept a “generic” list of the unresolved design safety issues. Generic issues were safety questions common to more than one plant that required additional investigation.⁴ The AEC permitted plants to operate while the staff investigated the generic issue as long as it did not seem to

³ A design-basis accident is a postulated accident that a nuclear facility must be designed and built to withstand without loss of safety systems necessary to ensure public health and safety. A beyond design-basis accident is an accident sequence that is possible but was not fully considered in a plant design because it was judged to be too unlikely.

⁴ Initially, the Generic Issues list included questions of large and small safety significance. To distinguish between short-term, easily resolvable questions and more complex problems, the NRC later adopted the term Unresolved Safety Issue to describe the latter. Unresolved Safety Issues were a subset of Generic Issues that were expected to take more than 6 months to resolve, were directly related to nuclear power plant safety, and raised questions about whether plants were providing reasonable assurance of adequate protection of public health and safety.

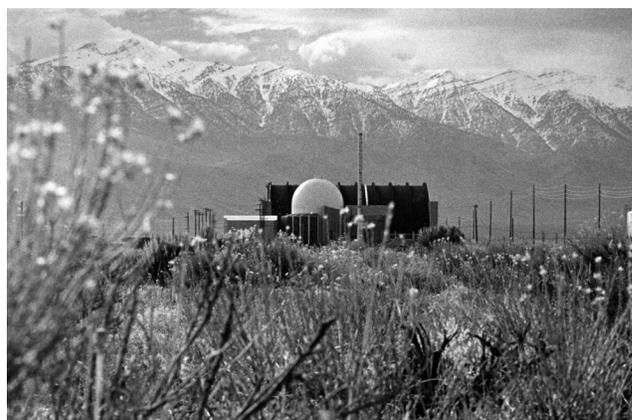


Figure 1: The design and construction of the Loss of Fluid Test (LOFT) reactor at Idaho’s National Reactor Testing Station (now called Idaho National Laboratory) raised questions about the adequacy of Emergency Core Cooling Systems to cope with a loss-of-coolant accident and led to controversial hearings

pose an undue risk to public safety. If staff investigations did not allay a safety concern, the AEC could require backfitting of the operating plants to address those safety concerns.

The AEC did not shy away from ordering backfits. The Humboldt Bay Unit 3 plant in Eureka, CA, began operations in 1962 and by 1976 the AEC had required it to make 22 safety upgrades related to generic issues and another 42 safety issues specific to its unique design. Licensees questioned the need for many backfits citing their expense and uncertain safety benefits.

Despite the AEC’s history of addressing safety problems by requiring backfitting, its record of solving generic and emergent safety questions was questioned in one of the most publicized safety controversies in the agency’s history: the 1973 rulemaking on the Emergency Core Cooling System (ECCS). ECCS is a critical cooling system that prevents reactor fuel from overheating and sustaining damage during unplanned plant events resulting from a serious leak in the primary coolant system, an event known as a loss-of-coolant accident (LOCA). There was significant variation in ECCS design between older and newer plants. Some tests and computer modeling at AEC laboratories indicated that ECCS as designed might not always work, though the research data was highly uncertain and disputed by experts. As critics of nuclear

power challenged the effectiveness of ECCS designs in hearings for new plant operating licenses, the AEC launched the rulemaking hearings to establish criteria that could be used to verify the effectiveness of ECCS designs.

The hearings sorted through conflicting information to establish minimum ECCS performance criteria, but only after a contentious debate. The AEC’s promotional mission, critics claimed, had interfered with regulation and research on ECCS. Press reports alleged that AEC had

harassed employees who had argued for stringent safety standards and claimed that the agency halted research that cast doubt on ECCS effectiveness. Whether the AEC had meddled with safety research or not, it was true that safety research had to compete for research dollars with the more popular development programs on the promotional side of the AEC. Lacking important research information, the staff struggled to draw up well-supported criteria.

The AEC eventually developed effective performance criteria for ECCS—criteria so stringent that some reactor designers made significant changes to fuel assemblies, and one utility closed an older plant rather than make extensive safety backfits. Nevertheless, the episode cast doubt on the agency’s reputation as an effective safety regulator. Critics claimed that the AEC didn’t take its safety responsibilities seriously and that it favored its mission to promote nuclear power. What was needed, they claimed, was an agency whose sole mission was safety regulation and research. In the wake of the hearings, the AEC substantially increased its research budget to confirm ECCS effectiveness. In the late 1970s and 1980s, Idaho National Laboratory conducted some of the most important research by testing ECCS performance under various pipe-break scenarios at its Loss of Fluid Test (LOFT) facility.

The Creation of the Nuclear Regulatory Commission

Concerns about the AEC’s oversight of operating reactors and safety research contributed to the passage of legislation to break up the AEC in January 1975 and create the independent U.S. Nuclear Regulatory Commission and the Energy Research and Development Administration, with the latter agency eventually becoming the Department of Energy. To bolster the NRC’s independence, Congress required that the five members of the Commission be appointed to staggered 5-year terms. No more than three commissioners could come from the same political party. Protecting the role of safety research within the agency, the Office of Nuclear Regulatory Research became a statutorily protected office that focused only on safety research.



Figure 2: In 1975, the first NRC Commission meets with President Gerald Ford. Pictured from left to right are Richard Kennedy, Marcus Rowden, William Anders (Chairman), President Ford, Victor Gilinsky, and Edward Mason.

During the NRC’s first year, public concern about operating plant safety grew more intense. In March 1975, the Browns Ferry Unit 1 fire (see page 12) raised a host of questions about fire safety design, safety training, and maintenance practices. Later that year, three engineers at General Electric and an NRC staffer resigned their positions to protest what they claimed was a lax attitude by industry and the NRC toward plant safety at operating reactors.

The NRC inherited three challenges from the AEC that were particularly important to operating plants: (1) Oversight, regulatory enforcement, and data collection needed more prominent organizational support; (2) The NRC needed to compare older plants to current safety standards and determine if there were any need to require backfits; (3) The NRC had to prioritize and solve outstanding generic safety issues.

1. Organizational Support: The NRC quickly doubled its personnel devoted to operations and created the Division of Operating Reactors in late 1975 to handle oversight, enforcement, and data collection on plant performance and unplanned events. The division was responsible for disseminating this information to other licensees and to support safety research.

2. Safety at Older Plants: In 1977, the NRC sought to deal with the perceived gap between the current NRC safety requirements applied to newly-licensed reactors and the safety requirements which were applied to older plants by launching the Systematic Evaluation Program (SEP). NRC staff reviewed the designs of 10 older operating reactors to reconfirm and document their safety. Staff compared their safety margins with existing design criteria to determine whether identified differences warranted backfitting. In 1980, the NRC began using new assessment tools to weigh the relative risk of the older designs and the benefits of making safety upgrades. The NRC found that many issues did not warrant action or could be resolved with changes in operating and emergency procedures. But numerous issues also required hardware changes to the plants to improve safety margins.

3. Generic Safety Issues: Based on the results of the Systematic Evaluation Program for the original 10 plants, the NRC identified 27 “Generic Safety Issues” from the SEP that needed analysis for the 41 plants that received operating licenses before the approval of the General Design Criteria. Of the original 27 Generic Safety Issues, the NRC identified 21 that needed further resolution and incorporated them into other ongoing regulatory programs. The SEP program was closed out in 1995. The NRC’s assessment of generic issues, however, became a permanent program with annual updates regarding the agency’s progress in resolving them.

These actions helped resolve many of the safety hardware issues the NRC took over from the AEC, but the process of improving operating reactors continued through the generic safety issues program. Additionally, new computer risk-assessment tools and the Three Mile Island accident took the NRC in new directions, leading to a broader assessment of reactor safety and backfits.

Risk Assessment—The Reactor Safety Study (WASH-1400)

When the AEC first began reviewing nuclear plant designs in licensing, and establishing generic safety requirements in regulations, quantitative methods to evaluate risk, computer-based analytical tools, and extensive data on nuclear power plant performance and operation were limited or unavailable. Today, the NRC defines risk through three questions known as the “risk triplet”:

1. What can go wrong?
2. How likely is it to go wrong?
3. What are the consequences?

In the 1960s, answering the second question was particularly difficult. The analytical models for sophisticated safety calculations did not yet exist, and programming the computers of that era, which were relatively slower and less powerful than those of today, was expensive and labor-intensive. A risk-assessment program that answered all three questions in a quantitative way needed operational data that did not exist in such a young industry. Accordingly, risk was considered without numerical analysis through qualitative or empirical methods, or the second question was ignored and instead the designer assumed that the “wrong” condition occurred.

This latter approach to safety was known as “determinism,” a method of analysis tailored to the technical limitations of that era. It achieved safety by answering questions one and three. Design engineers used their knowledge and experience to postulate the most dangerous accidents that seemed credible (“What can go wrong?”) and estimated the most pessimistic outcomes of the accident (“What are the consequences?”). If reactor designers could answer those questions adequately, their design was deemed acceptable.

The AEC staff judged the worst credible accident to be a sudden break of a large reactor coolant pipe, known as a large-break LOCA. The LOCA became the primary accident scenario that safety systems had to cope with. Engineers specified safety features needed to prevent and mitigate a loss-of-coolant accident’s consequences through requirements for layers of physical barriers and systems that limited the loss of cooling water and prevented the fuel rods from dangerously overheating and releasing radioactive materials. This layered approach was called “defense in depth.”

Working under worst-case scenarios, deterministically designed plants tended to have conservative safety margins. The advantage of deterministic design was its pessimism. It set a reliable outer boundary on accident consequences. Its success, however, depended on the judgment of engineers to anticipate the most dangerous, yet credible, accident scenarios.

Having the capability to answer question two by performing a risk assessment was greatly desired by AEC engineers. With it, they could explore many more scenarios than a large loss-of-coolant accident and select the ones most deserving of attention, research, and resources. For operating reactors, a risk assessment could identify the most effective design improvements.

By the mid-1970s, computer advances and a growing body of data from plant operations made it feasible to conduct quantitative risk assessment based on large sets of operating plant data. In 1975, the NRC published the Reactor Safety Study (WASH-1400), which had been started a few years earlier by the AEC. It had two key findings:

1. An accident releasing significant radiation was very unlikely and posed a much lower hazard than other forms of energy production.
2. The AEC’s and NRC’s deterministic focus on a large-break loss-of-coolant accident overlooked important hazards posed by other mishaps, particularly natural catastrophes, smaller LOCAs, and human error. They contributed more to the overall risk of a plant accident than a large-break LOCA.

Nuclear power critics strongly objected to the Reactor Safety Study’s first claim, that nuclear power was safer than other technologies. They argued that risk-assessment techniques used in the study could not estimate the true probability of a major accident because of the limited data and large uncertainties in the results. They pointed out that there were likely accident scenarios that the study had not considered.

These criticisms were credible enough that in 1979 the Commission withdrew its support from the report’s executive summary that compared nuclear safety to other societal risks. The Commission continued to endorse the main report, and experts praised the Reactor Safety Study’s methodology, but this distinction between the summary and the main report was often not understood in press reports. The perception that the full report was discredited made it uncertain whether the NRC would use risk assessment. The accident at Three Mile Island gave risk assessment new life.

The Three Mile Island Unit 2 Accident



Figure 3: The accident at Three Mile Island in March 1979 marked a turning point in the regulation of operating reactors. It led to a greater focus by the NRC on severe accidents, human factors, and the use of new accident-assessment tools.

The Three Mile Island accident in March 1979 posed three challenges to NRC regulation that led it to strengthen safety regulation, expand the meaning of defense-in-depth to address matters other than design and hardware, and increase the NRC's reliance on quantitative consideration of risk.

1. New Tools: The accident validated the use of new computer-based assessment tools such as risk assessment to supplement deterministic analysis for quality assurance, plant safety design, and reliable operation. In the furor over the Reactor Safety Study's claims of proving nuclear plant safety, its value for revealing plant hazards and improving safety received less attention. The accident made its value obvious. While the Reactor Safety Study did not predict Three Mile Island's exact sequence of malfunctions and misjudgments, it identified two of the main culprits behind the accident—operator error and small loss-of-coolant accidents.

Risk assessment and accident modeling programs could aid in evaluating severe accident probabilities, and the NRC sought to develop a standard methodology to conduct them. But before it could use risk assessment as a regulatory tool, it needed to reduce the uncertainties that had called into question the results of the Reactor Safety Study through data collection and analysis of operating experience. The agency created a new office to collect and analyze data on safety issues such as accident sequence precursors—relatively small events that could lead to a large accident when combined with other small mishaps.

2. Severe Accidents: Three Mile Island raised questions about the adequacy of current reactor designs and operations to deal with severe accidents. Viewed

narrowly, it was not obvious that the accident demanded regulatory change. The negligible safety consequences of Three Mile Island seemed to confirm the wisdom of the NRC's emphasis on deterministic design and defense-in-depth. More than half of the reactor core melted. Hydrogen and radioactive isotopes leaked into the containment building where the hydrogen ignited. Nevertheless, the containment building prevented the escape of all but a negligible amount of radiation to the environment. Radiation levels at the site were so low that the 1986 Chernobyl accident, which occurred some 5,000 miles away, brought radiation levels three times higher to the site than were measured there during the Unit 2 accident in 1979. Defense-in-depth worked.

From a broader perspective, however, Three Mile Island was a troubling indication that determinism did not address all of the credible threats to plant safety. The Reactor Safety Study and Three Mile Island demonstrated that a series of minor malfunctions and human errors could cascade into a serious accident. The NRC needed to expand its research program into the progression and consequences of a severe accident. The agency also needed to expand its regulatory reach beyond the large-break LOCA to find ways to limit the consequences of a range of severe accidents. (For more on severe accidents, see page 7)

3. Human Factors: Three Mile Island vividly revealed the critical role humans played in the operation of safety systems and expanded the NRC's concept of defense-in-depth. Before the accident, the AEC and NRC thought of defense-in-depth almost entirely in terms of safety hardware. In the 1960s, for example, AEC experts described a plant's layers of defense as three well-designed and constructed static physical barriers—the fuel rod cladding, primary coolant piping and vessel, and containment building. By the 1970s, the AEC and NRC emphasized active safety systems, such as Emergency Core Cooling Systems, as an added layer of defense. By 2003, defense-in-depth, as defined in a regulatory decision by the director of the Office of Nuclear Reactor Regulation, had evolved to include five elements combining machine and human aspects: (1) conservative safety margins in reactor design; (2) high-quality design, construction, and operation to reduce malfunctions and errors; (3) redundant safety systems; (4) containment structures and safety systems to minimize the release of radioactivity; and (5) comprehensive emergency planning. Similarly, a recent informal staff definition described it as “a strategy that employs successive levels of defense and safety measures in the design, construction, and operation of the nuclear power plant to ensure appropriate barriers, controls, and personnel are in place to prevent, contain, and mitigate exposure to radioactive material.”

PART II: REGULATORY CHANGES INFLUENCING REACTOR DESIGN

Many of the changes instituted by the NRC after the Three Mile Island accident addressed the three main challenges raised by the accident—the use of new analytical tools, the need to study and regulate severe accidents, and human factors considerations. New regulations, new programs, and new research led to important design changes and improved operations.

The NRC Moves Toward Risk-informed Regulation

The Reactor Safety Study and the Three Mile Island accident raised significant new safety questions. New analytical tools and changes to the regulatory process offered solutions. Deterministic design remained the foundation of NRC regulation, but the insights of risk assessments made possible a shift toward a “risk-informed” regulatory process.

Risk-informed regulation enhanced determinism with a broad consideration of hardware and human-related safety issues and with its ability to prioritize these issues by their safety significance.

A risk-informed approach could delve into the details of safety in ways determinism could not. Its calculations could show where a design was unnecessarily conservative and where additional requirements might be necessary. Risk-informed regulation could answer questions such as “How much safety will be gained during a station blackout by adding another diesel generator?” or “Does taking a pump out of service for maintenance significantly increase the risk that its safety systems won’t work if something goes wrong?” In the decades after Three Mile Island, the NRC took incremental steps toward risk-informed regulation.

Reactor Oversight

It took several decades to develop a satisfactory oversight process. In the AEC era, regulators directed their attention to identifying and analyzing safety-related design issues. The agency’s oversight of utility plant management was mostly reactive, and it lacked a comprehensive strategy that synthesized the findings of inspections, plant event data, and periodic reviews. Developing a performance-assessment process was essential because some of the more capable licensees had fewer safety-related events than other less-capable ones.

In 1976, the NRC launched an investigation of how to best evaluate licensee performance. The agency explored different evaluation approaches. Regulators examined statistical factors, particularly the number of plant events and instances in which licensees were out of compliance with regulations. They looked for trends that might identify repetitive operational problems or diverse issues

that had a common cause. The NRC also analyzed the effectiveness of NRC inspections.

None of the areas investigated provided a sure way of measuring performance. There wasn’t enough performance data to rely on quantitative measures alone. Another measure, NRC inspection results, lacked consistency. NRC inspectors could usually agree on large problems with plant operations, but there was significant variation from one inspector to the next on specifics. The performance of licensees often depended on hard-to-measure qualitative factors, such as the willingness of management to institute prompt remedial measures. Lacking sure-fire approaches, the NRC opted to experiment to find an optimal approach.

It expanded a successful resident-inspector pilot program begun by the AEC to improve inspection quality and communication with licensees. To assess licensee performance, the NRC also proposed a pilot oversight program to evaluate the pitfalls and potential of an integrated approach.



Figure 4: After the accident at Three Mile Island, the NRC made its limited resident-inspector program a permanent program at all commercial facilities.

After the Three Mile Island accident, the NRC and expert committees that evaluated the accident identified licensee performance as a significant concern. The Resident Inspector program became permanent for all operating plants. In 1980, the NRC launched the Systematic Assessment of Licensee Performance (SALP) Program, which incorporated many of the elements of the proposed pilot program. The NRC developed guidance documents, a system of staff evaluation and management reviews, and an escalating inspection program for licensees with performance weaknesses.

Reviews of the SALP indicated that it worked to improve licensee performance, but there were persistent complaints that it was subjective and produced arbitrary judgments. Industry critics said that the SALP lacked consistency from one region of the country to the next and that senior-level reviews were not transparent. The industry believed that the NRC paid too much attention to well-run plants

and not enough to poorly run ones, and that it did not distinguish between minor safety violations and more serious lapses. A review by the NRC's Inspector General and an external audit partly confirmed these views.

The SALP process suffered in part because it was organized around plant operational functions, such as maintenance and operations, rather than safety functions. Without reactor safety as the SALP's organizing principle, licensees lacked clear direction. A General Accounting Office (GAO) report concluded that the NRC did not precisely define safety and that this led to subjective judgments by utilities and the NRC. The lack of clear safety standards allowed "problem plants" to avoid the NRC's "watch list" of plants requiring greater oversight.

By 1999, the industry had several decades of operational experience, making possible a more risk-informed, plant-specific oversight program. The NRC launched the Reactor Oversight Process (ROP) to direct inspection resources to higher-risk areas. As the NRC's current oversight process, the ROP relies more on objective measures of plant performance and provides a more predictable, transparent agency response to violations. The ROP anchors performance monitoring and evaluation in "cornerstones of safety" that mirror the NRC's defense-in-depth safety philosophy. Three additional "cross-cutting" areas influence all cornerstones: human performance, a safety-conscious work environment known as a "safety culture," and a utility's program to find and fix problems.

A key difference between the SALP and the ROP is the latter's emphasis on risk. The ROP's Significance Determination Process calibrates the NRC's enforcement response to the safety significance of a performance issue. Except for issues found to be in the lowest category of safety significance, NRC specialists perform a risk assessment and categorize performance issues on a graduated scale-up to the most serious level. Higher-level findings require more NRC oversight resources, public involvement, and utility planning.

The ROP has largely achieved its goals to make oversight less arbitrary and more transparent. The Government Accountability Office (GAO) reviewed the program in 2006 and found that the NRC had improved the way it discharged its oversight responsibilities, particularly in focusing inspections on areas most important to safety. However, the GAO noted that there were weaknesses in the areas of human performance and safety culture that had a direct influence on keeping plant safety systems in optimal condition. The NRC instituted a number of changes to the ROP to consider safety-culture factors in licensee oversight (see "Safety Culture" on page 19).

Severe Accident Policy Statement

Since the 1950s, the AEC and NRC have performed studies that estimate the causes and consequences of severe accidents.⁵ However, the AEC had done few comprehensive severe-accident experiments to resolve questions about accident behavior, such as how a melting reactor core might interact with the steel and concrete of the reactor containment building. Until the late 1970s, such research was not considered a priority, because severe accidents involve the failure of multiple redundant safety systems. They seemed so unlikely that plants were not designed to prevent them in all cases.

After the Three Mile Island accident in 1979, the NRC launched several research programs on severe accidents. The NRC probed how a core meltdown might progress, the generation of flammable or explosive hydrogen gas during a meltdown, the potential for steam explosions when hot melting fuel contacted water, and chemical reactions between a melted core and the plant's concrete containment building.

The NRC's research helped inform development of a 1985 policy statement on severe accidents for both future designs and existing reactors. The policy statement declared that existing plants did not need further regulatory action unless significant new safety information emerged that might call into question whether a plant posed undue risk to public health and safety.

Nevertheless, the NRC sought more information to have reasonable assurance that it could close out the severe accident issue. It gathered data on containment performance (see page 16), conducted research on severe accidents, and reviewed licensee investigations of plant-specific vulnerability to severe accidents, known as Individual Plant Examinations (IPEs). IPEs identified plant vulnerabilities to internal events, such as LOCAs and station blackouts. A similar review was later initiated for external events, such as seismic and severe weather events (Individual Plant Examinations for External Events, or IPEEE).

Using risk assessment, utilities identified and opted to implement over 500 upgrades that would improve reactor safety. Changes to plant operation and design each constituted about half of the modifications. Operational changes included improved procedures and personnel training. Design changes included improvements to auxiliary feedwater systems; replacement of older, less reliable components with newer models; improvements to electrical power connections systems; installation of diesel generators; and the addition of auxiliary power supplies for key safety components.

5. A severe accident challenges safety systems at a level much higher than expected. They typically damage reactor fuel and can lead to a significant release of radiation to the environment.

While most licensees did not attempt to quantify the safety value of their improvements, those that did indicated that their upgrades reduced the risk of a core-damaging accident. The review of external events—an Individual Plant Examination of External Events—produced similar results. Over 90 percent of licensees proposed plant improvements. Seventy percent included seismic safety upgrades such as adding new supports or strengthening existing ones. Sixty percent proposed improvements to fire safety such as relocation of critical cables and improved fire barriers.

Maintaining Safety: The Maintenance Rule

The maintenance rule of 1991 demonstrated that improving safety involved more than hardware backfits. The agency concluded that “soft” factors, such as plant management and maintenance, played a critical role in avoiding accidents.

The AEC’s and NRC’s emphasis on design safety had overlooked the accident risk posed by maintenance activities. The Reactor Safety Study and some of the maintenance-related causes of the Three Mile Island accident led the agency and industry to take greater cognizance of the ways maintenance-related failures could force reactors to automatically shut down, safety systems to fail, and operators to make mistakes in a moment of high stress. Reducing unplanned events could reduce the chances of an accident.

Through much of the 1980s, the utility industry’s new Institute of Nuclear Power Operations sought to reduce unplanned shutdowns through improved maintenance programs. After several years of effort, the NRC sought greater progress. The agency found that about half of event reports were maintenance-related and that a substantial majority of safety system failures were caused by maintenance issues.

In crafting a new regulatory approach to maintenance, the NRC searched for lessons among international nuclear regulators and operators in Japan, France, and West Germany. These nations, particularly Japan, had established superior maintenance programs, and, as a result, experienced far fewer scrams than plants in the United States.

The very different cultures and regulatory systems of other nations made it impossible to implement their maintenance programs in the United States unmodified. For example, France had just one utility operator and a fleet of nearly identical power plants, far different from the unique plants and multiple vendors in the United States. Nevertheless, the NRC identified key practices common to all effective maintenance programs, such as a placing a high value on reliability, doing root-cause analysis, providing extensive technical training, and using systems of data collection and monitoring.

As a regulatory model, the NRC also reviewed the approaches used by other Federal agencies, such as the U.S. Federal Aviation Administration (FAA). The FAA operated in an environment similar to the NRC with multiple aircraft manufacturers and airlines. Given this diversity, it did not follow a prescriptive approach that spelled out one recipe for developing a maintenance program.⁶ It created a system that encouraged industry initiative to figure out how to meet performance goals.

In 1988, the NRC issued a proposed maintenance rule. Like the FAA’s approach, the proposed rule was very broad. It laid out two requirements: (1) licensees needed to establish and maintain an effective maintenance program, and (2) licensees needed to regularly assess the effectiveness of their program. The agency concluded that inspections, industry initiative, and trial periods for implementing the rule were necessary to determine whether the proposed rule was necessary.

The final rule was a hybrid of the FAA’s approach and the NRC’s traditional prescriptive approach. The NRC permitted a licensee the flexibility to modify its program on the basis of equipment performance. The rule only covered safety-related structures, systems, and components and some non-safety-related systems whose failure might prevent safety-related equipment from functioning, cause automatic shutdowns, or lead to the unnecessary operation of safety-related systems.

Licensees had five years to implement the rule and draw lessons from the rule’s early implementation at nine test plants. NRC inspections revealed that licensees did an adequate job of implementing the rule, but that there were a few weak areas. Use of general industry operating experience was limited, and plant structures received little maintenance consideration. Licensees did little risk assessment when they took a system out of service for maintenance, particularly when the plant was shut down or operating at low power. In 1999, NRC assessments concluded that industry had worked through most of these early problems and had implemented the rule adequately.

The long gestation for the maintenance rule paralleled a period during which the NRC and the industry made substantial gains in their understanding and use of quantitative risk assessments to improve reactor safety. While the 1988 proposed rule did not put much emphasis on the use of risk insights, those insights became a critical component in the rule’s implementation by the mid-1990s.

6. The difference between prescriptive and performance-based requirements is the difference between means and ends. The NRC’s prescriptive requirements, as traditionally used, tell a licensee what they shall do—the acceptable means to reach a safety goal, usually by specifying design features. A performance-based requirement focuses on the safety end. It relies upon a licensee demonstrating that a certain design produces satisfactory, measurable results. It provides more flexibility as to the means licensees use to achieve safety goals.

There were challenges to using risk assessment for maintenance. While a risk assessment might cover about 2,000 components and systems, the maintenance rule touched on ten times that number. Industry and NRC guidelines bridged the gap for components not considered in a risk assessment with expert panels that analyzed risk data and combined them with engineering judgment.

Risk assessment helped overcome a maintenance paradox first highlighted by the Reactor Safety Study: Maintenance improves the reliability of a safety system, but the chances of an accident go up during maintenance work because an out-of-service component cannot respond to an accident. Was doing maintenance worth the added short-term risk? Early NRC assessments of the maintenance rule's implementation indicated that licensees rarely managed the maintenance paradox using risk insights. The NRC revised the maintenance rule to require that licensees assess and manage maintenance risk during all modes of operation. Licensees developed computer programs to estimate maintenance risk and matrices that limited certain combinations of equipment from being removed from service at the same time.

Has the maintenance rule worked? The NRC has not performed a thorough assessment of the maintenance rule because of its complexity, cost, and many uncertainties. There is extensive evidence of improved performance in the area of maintenance-related component and system failures, and there are fewer initiating events; however, these positive trends began before the maintenance rule's implementation in 1996. Nevertheless, the rule was a manifestation of a long-standing commitment by the NRC to improve safety by improving maintenance activities.



Figure 5: Despite their size and their permanent appearance, most aging components in a nuclear power plant can be replaced. Pictured above is a new steam generator to be installed at the Indian Point Energy Center in New York.

License Renewal

The NRC issues 40-year licenses to commercial nuclear power plants. By the 1980s, the possibility of renewing licenses became an important issue. The selection of a 40-year term for licenses originally had nothing to do with technical considerations of plant aging. Forty years was a compromise between the Justice Department's desire for a short license period to keep utilities from monopolizing power sources and utility officials who favored a longer period to amortize the capital costs of a plant.

The 40-year license might not have had a technical basis but it had technical implications. Engineering analysis and component selection as part of the original design of a plant were often made on the assumption of 40-years of operation. The nuclear industry sought to address age-related questions about components by completing two studies on the feasibility of a life extension for nuclear plants. They indicated that refurbishing plants for a license renewal was technically and economically feasible.

In 1982, the NRC established a program for Nuclear Plant Aging Research. Its results indicated that aging phenomena were readily manageable and didn't pose obstacles to life extension. The obstacle that did exist was regulatory. The NRC didn't have a process in place to renew licenses or address plant-aging issues. In 1988 the NRC issued a proposal for rulemaking on license renewal. The key question was whether a license renewal should be based on a plant's current licensing basis—the safety requirements it currently operated under—or meet the safety requirements of a new plant. The staff concluded that the current licensing basis was acceptable as long as it was modified to take into account age-related safety issues. They determined that a 20-year renewal was appropriate.

The NRC issued a final rule in 1991 to a less-than-enthusiastic response from the nuclear industry. A pilot project sponsored by industry groups and the DOE indicated to utilities that the renewal process was overly burdensome and lacked predictability. Industry did not believe it received adequate credit for age-related programs already in place, particularly the new maintenance rule. The maintenance rule already covered the aging of "active" safety components—pumps, valves, and breakers—and utilities argued that these components did not need special review during license renewal.

The NRC agreed. In 1995, the agency revised the rule to focus on aging management of "passive" structures and components, such as piping, containment buildings, and pressure vessels. If a licensee couldn't demonstrate that the maintenance rule or other program covered these issues, they had to address them during the license renewal process.

PART III: HARDWARE CHANGES

The broadening of the NRC's regulatory system and defense-in-depth philosophy resulted in hardware changes and improvements in human performance. This section provides a history of some of the most important hardware- and human performance improvements. Many of these issues took years to resolve. Some, such as fire protection, continue to receive considerable regulatory attention. The thorny nature of some safety issues reveals the NRC's persistence in resolving technical questions. These topics are arranged by the Reactor Oversight Process's (ROP's) Cornerstones of Safe Operation that relate to reactor safety:

initiating events
mitigating systems
barrier integrity
cross-cutting areas

INITIATING EVENTS

Any potential occurrence that could disrupt plant operations and challenge safety functions is an initiating event. These events could include internal plant floods and fires, external events such as earthquakes and floods, equipment failures leading to a plant shutdown, shutdowns with unexpected complications, or large changes in the plant's power output.

Anticipated Transient Without Scram

Anticipated transients are plant events caused by human error or plant malfunctions that are expected to happen at least once during the life of the plant. An example of an anticipated transient is when the plant's turbine generator stops operating because of a component malfunction. Such a transient usually leads to a reactor shutdown in which control rods are automatically "scrammed" by inserting them rapidly into the reactor fuel region. Control rods are made of material that slows down a nuclear chain reaction. When plant operators partially withdraw the rods from the reactor fuel region, the nuclear chain reaction begins. Scramming the rods stops the reaction.

What if the rods don't automatically scram during an anticipated transient? The Atomic Energy Commission's Advisory Committee on Reactor Safeguards (ACRS) asked that question in 1969 after an event at a test reactor in Idaho indicated that such a scenario was possible. Reactor manufacturers believed that an Anticipated Transient Without Scram (ATWS) event was very unlikely given the redundant circuit breakers and signals within the reactor protection system which causes plant scrams. The ACRS and the AEC regulatory staff were less certain. Even with redundant systems, a common-cause failure, such as a manufacturing defect that disables identical electrical breakers, could foil an automatic scram.

Early investigations of ATWS events indicated that they could have serious consequences for plant safety. A pressurized-water

reactor (PWR) might experience pressure spikes sufficient to rupture the primary coolant system piping. A boiling-water reactor (BWR) could experience core damage and overpressurize or rupture the containment building.

The AEC and the NRC staff worked with reactor manufacturers to study the probability and consequences of ATWS events. Regulatory staff released studies of ATWS in 1973 and 1978 calling for design objectives that met defined safety goals. Citing other studies, the nuclear industry opposed the NRC approach. The NRC, however, continued to press for plant modifications. In 1980, the agency published a fourth volume of its 1978 report that included specific design changes to be required of licensees through rulemaking.

The NRC determination to address ATWS received further support in June 1980 after an event at the Brown's Ferry Unit 3 nuclear power plant in Alabama. The hydraulic system used to scram the control rods failed to insert 76 of 185 control rods when an operator attempted to do so during a routine shutdown. Only repeated scram attempts finally inserted the rods. A year and a half later, a reactor trip signal failed to open breakers to scram the Salem 1 nuclear power plant during a plant startup. In neither case did the events cause damage, but they confirmed the possibility of ATWS events.

In June 1984, the NRC adopted a final rule on the ATWS issue. The rule sought to limit the likelihood of an ATWS event by requiring that scram systems incorporate the principles of redundancy, reliability, independence, and diversity. All PWRs installed diverse means to trip the turbine offline and start auxiliary feedwater systems; both actions mitigate the effects of an ATWS. Plants designed by Combustion Engineering and Babcock & Wilcox Co. installed diverse scram systems. General Electric's BWRs mitigated the effects of an ATWS with diverse ways of stopping reactor recirculation pumps, a standby liquid control system, or with improved emergency operating procedures. BWRs also improved the reliability of automatic scrams with alternate rod insertion circuitry.

The NRC also advised plant operators to reduce the probability of an ATWS by cutting down on the numerous automatic scrams that occurred each year. Every time a plant scrambled, there was a small chance of an ATWS. Over time fewer scrams meant a lower likelihood of an ATWS event. Since the 1980s, scram rates have dropped dramatically through more effective maintenance and operations. Reducing scrams, it is estimated, has cut the probability of an ATWS by 10 times (that is, has made an ATWS 10 times less likely than it was previously).

In September 2003, the NRC assessed the effectiveness of the ATWS rule. It found that the design changes and procedural improvements mandated by the rule had increased safety for less expense than estimated. The NRC set risk-based criteria that an ATWS event should be no more likely than once in 10,000 reactor-years of operation. All four reactor vendors met that target.

Station Blackouts

Nuclear power plants rely on alternating current (ac) power to safely shut down the plant and remove decay heat. Before 1988, there was no explicit requirement that plants be capable of coping with a loss of all ac power, known as a station blackout. Nevertheless, the earliest commercial nuclear power plant designs typically included blackout-related safety features. For example, the Yankee Rowe nuclear plant had one small diesel generator that could supply just enough power for essential instruments, makeup water pumps for the reactor coolant, and pressure control. It had one steam-driven auxiliary feed pump with about a one-day supply of water to remove decay heat from the reactor. Because of the multiple component failures necessary to cause a station blackout, safety grade redundant systems were not required.

The Reactor Safety Study, operating experience, and agency critics raised concerns about station blackout hazards. The Reactor Safety Study indicated that a station blackout was an important contributor to the overall risk from plant operations. By the end of 1975, ACRS and staff had identified station blackouts as a generic issue. The Reactor Safety Study's calculations were borne out by operating experience when a few brief station blackouts occurred. Nuclear critics also gave greater attention to the issue. In 1976, an NRC employee, Robert Pollard, resigned his position at the agency and testified before Congress about the need to resolve generic safety issues, including station blackouts. In 1977, Congress added a new section to the Energy Reorganization Act directing the NRC to develop an ongoing plan for what it called Unresolved Safety Issues.

The ACRS took a special interest in station blackouts and pressed applicants for new plants to show how they would cope with a loss of all ac power, particularly by installing diverse power sources for systems such as auxiliary feedwater. In 1978, the NRC staff elevated station blackouts to an Unresolved Safety Issue.

While the Three Mile Island accident in March 1979 was not a result of a station blackout, it made the NRC think twice about any accident scenario that might lead to a loss of cooling capability. In 1980, as a result, the NRC developed a plan to resolve the station blackout issue. The following year, the NRC issued a letter to all licensees to review their ability to cope with station blackouts. They had to develop training and procedures to ensure an adequate response to a station blackout by plant personnel and restore ac power through offsite or onsite power sources.

NRC-sponsored research investigated the probability of a station blackout, the reliability of onsite backup power sources, and the potential for severe accidents once power was lost. These investigations indicated that offsite and onsite power systems were not as reliable as had been assumed. Stations lost offsite power about once every 10 years. In 90 percent of those cases, power was restored within 3 hours. Plants needed reliable diesel generators. Research found that

decay heat removal systems that did not depend on ac power were critical to avoiding reactor damage. It was important that plants be designed to cope with a station blackout for a period of time until offsite ac power is restored.



Figure 6: Critical to avoiding a station blackout are the power plant's emergency diesel generators, such as the one pictured here. In 1988, the NRC developed a new rule on station blackouts and guidance on diesel generator performance.

Responding to these insights, the NRC developed in 1988 a new rule and a regulatory guide on station blackouts. Utilities had to develop a "specified period" for the length of a station blackout at their facility, and then perform a coping analysis to demonstrate that the facility was able to safely withstand and recover from the station blackout. The regulatory guide established a diesel generator reliability goal of having no more than one "failure to start" in 20 demands, provided guidance on acceptable training and recovery procedures, and how to establish a minimum blackout time during which a plant had to be able to avoid fuel damage.

Hardware changes typically included the addition of an alternate source of ac power, increased battery and water storage tank capacity, and improved instrument air systems. An NRC analysis published in 2003 indicated that the station blackout rule had exceeded initial expectations in reducing in the risk of a core-damaging station blackout. The plants that made the greatest improvements usually were those that had been most vulnerable to a blackout.

The Fukushima Dai-ichi Nuclear Power Plant accident in March 2011 demonstrated the risks associated with extreme natural events and the challenges they pose to the United States' nuclear safety approach. The earthquake and subsequent tsunamis led to an extended station blackout and extensive reactor and building damage for four of the six plants at the site. Exceeding the design basis of the plant, the tsunami overwhelmed the defense-in-depth layers of the facility.

In response to the accident, the NRC established a Task Force to make recommendations on safety improvements for existing plants, including specific proposals for

long-term station-blackout mitigation. The task force called for changes to the existing station blackout rule to establish a minimum coping time of 8 hours during a blackout, as well as develop procedures, training, and equipment to cope with an extended loss of all ac power lasting 72 hours affecting the reactor and spent fuel pools.

The task force recommended that utilities develop plans to bring in offsite resources within 72 hours for extended coping. The task force drew on existing coping capabilities at reactor plant sites. After the September 11, 2001, attacks on the World Trade Center and Pentagon, the NRC had ordered licensees to develop procedures and equipment to mitigate the consequences of external security threats. This same equipment could be used during station blackouts, and the task force recommended that licensees (1) ensure that this equipment be protected from the effects of extreme natural phenomena and (2) add equipment as necessary for a multiunit blackout.

In March 2012, the NRC published an advance notice for proposed rulemaking to modify the existing station blackout rule. The Commission approved an order to modify existing plant licenses to implement mitigating strategies for beyond-design-basis external events. Like the recommendation by the task force, the order required licensees to develop a three-phased approach that relies first on installed equipment to restore core and spent fuel pool cooling. In the second phase, plant operators turn to onsite equipment to maintain cooling until offsite equipment arrives in the third phase to provide indefinite cooling capability.

In August 2012, the nuclear industry responded to the issues raised by the Fukushima accident by developing a comprehensive plan, “Diverse and Flexible Coping Strategies (FLEX) Implementation Guide,” to meet the requirements of the March 2012 NRC order. The NRC staff endorsed this industry guidance document.

MITIGATING SYSTEMS

These are safety systems that alleviate the effects of initiating events. Mitigating systems can prevent an accident or reduce its consequences.

Fire Safety

In the 1960s and early 1970s, the AEC regulatory staff lacked expertise on fire safety and an overarching regulatory approach. It deferred to professional engineering and fire insurance organizations to develop safety standards, but was dissatisfied with the results. Worried that water would short-circuit backup safety systems, the AEC promoted CO₂ fire suppression systems rather than water in new construction around electrical safety-related cables, electronics, and computer systems. By contrast, experts for fire insurance corporations had advocated supplementing CO₂ systems with sprinklers or readily available fire hoses. However, the AEC did not pursue research to support its position on water suppression of fires.

A number of cable fires demonstrated the unique hazards that fires presented to nuclear plants. In 1968, undersized cables overheated and burned at Unit 1 of the San Onofre Nuclear Generating Station, disabling numerous safety systems. Over 500 cables were destroyed, including many connected to safety-related components and their backup equipment.

The San Onofre fire and a similar one at the Indian Point Energy Center in 1971 demonstrated that redundant safety-system cables needed greater physical separation with more effective barriers. The AEC staff worked with professional engineering organizations to draft new standards, but was not satisfied with the minimal separation requirements they contained. In the early 1970s, the staff developed its own criteria in regulatory guides for new construction.

The NRC learned, however, that there was more to fire protection than separation criteria. Coming just months after Congress created the agency in 1975, the Browns Ferry fire provided an alarming example of the vulnerabilities of safety equipment to fire and the inadequacies of current fire suppression equipment, fire protection management, and personnel training.



Figure 7: The Browns Ferry fire damaged hundreds of safety-related electrical cables. It underscored the need for fire-safety training and greater safety research.

The fire broke out on March 22, 1975, at Browns Ferry Unit 1 in a penetration for electric cables running into the reactor containment building. Normally the openings around the cables were sealed with polyurethane and a flame-retardant coating. Workers opened holes in the seal to install additional cables. After resealing one opening with an incorrect and more flammable kind of polyurethane, a technician checked for leaks using a candle—a common practice for the time. The rush of air through even small openings, technicians learned, could disturb the flame and rising smoke from a lit candle. This time the air sucked the flame into the flammable polyurethane, igniting it.

The fire burned for about 7½ hours, largely because plant personnel used less effective CO₂ and chemical extinguishers than water for fear of causing short-circuits in safety equipment.

As the fire spread along cable trays into the reactor building, the control room received numerous real and false signals that plant components were starting or stopping on their own. The damage was so extensive that all of Unit 1 and part of Unit 2's emergency core cooling system became inoperable. Only creative actions by control room operators averted damage to the reactor core. When water was finally turned on the fire, it was put out in minutes. By then, over 1,600 electrical cables were destroyed, including 628 that powered or controlled safety-related equipment.

An NRC special review group examining the fire called for a broad defense-in-depth approach with programs on prevention, detection, and fire suppression. It called for management reform, including a designated supervisor at each facility to coordinate and command training, planning, prevention, and firefighting. The guidance called for design changes that included appropriate combinations of greater physical separation of redundant safety systems, fire barriers that could last several hours, improved fire detection systems, and selected use of water-based fire hose stations, sprinklers, and CO₂ systems on a plant-specific basis.



Figure 8: In the decades after the Browns Ferry fire, the NRC sponsored numerous research initiatives on the causes, consequences, and coping strategies for nuclear-plant fires.

The drive to reform fire safety culminated in 1980 with new rulemaking. It expanded the use of water extinguishing systems and established separation distances or barriers between redundant safety systems. While utilities could propose other ways of satisfying the rule, it generally required that safety components have automatic fire detection and suppression equipment, and that cables to redundant safety equipment had to be spaced 20 feet apart with no combustible material between them. The new rule required a remote shutdown station away from the main control room and fire response team training. New plants had to have cable material with a low propensity to spread fire.

The NRC initiated a substantial fire safety research program. Studies conducted by Sandia National Laboratory sought to verify whether the 20-foot rule was effective. The tests indicated that the 20-foot separation requirement needed to be augmented by other mitigating features to be effective. Investigations confirmed the effectiveness of water as an extinguisher and that fire retardants did not work as well as barriers and shields. The NRC and industry performed research and data collection to identify likely sources of fire, turbine building fire hazards, and ways in which external events, such as flooding and hurricanes, might cause fires. Finally, the agency initiated research about fire barrier materials and how equipment and computers responded to the environment created as a fire burned.

The NRC's research and data collection initiatives paralleled efforts to improve risk assessment methodology for fires. Information from national and international sources created greater understanding of the risks of electrical shorts, flammability of materials, and major fires, as well as of the risks and benefits involved with fire detection and suppression. In June 2004, the NRC endorsed a new risk-informed fire regulation, "National Fire Protection Association Standard NFPA 805." The new regulation served as a risk-informed alternative to existing regulations. This allowed licensees to focus on correcting fire safety issues that had significant risk. Forty six nuclear power plants have submitted letters of intent to move to the new regulation.

Containment Building Sump Performance

The work done after the 1972–1973 hearings to upgrade Emergency Core Cooling Systems led to a broader inquiry by regulators into systems used to cope with loss-of-coolant accidents (LOCAs). A particular concern related to pressurized-water reactor (PWR) containment building sumps. Sump systems collect water that escapes the reactor piping system during a LOCA through drains at the bottom of the containment building. Pumps then feed this water back into the containment building as a spray to condense the building's steam-filled environment or directly into the reactor vessel to cool the core.

The pumps in the system needed enough water from the drains to operate properly. There were concerns that air might be sucked into the drains. Debris might break loose, wash

into the drains and be pumped into the reactor. There were also concerns that screens installed to block the debris might clog and cause the pumps to lose suction. Without adequate suction, the pumps might cavitate, shake violently, and damage themselves. In the 1970s, the AEC and NRC issued several regulatory guides to prevent these problems, and they required tests to demonstrate that the sump drains operated properly.

Testing performed by utilities in the 1970s generally confirmed that air and clogging were not major safety issues, but the tests raised enough questions that regulators were not assured that sumps would receive water free of air and debris. The NRC identified sump issues as an Unresolved Safety Issue in 1979. DOE provided funding to construct a full-scale sump test facility at Alden Research Laboratory at Worcester Polytechnic Institute in Massachusetts. The NRC surveyed existing plant insulation materials and performed calculations and experiments supplemental to those performed at Alden to determine how insulation might wash into the drains and clog the debris screens covering the sumps.

Results from the Alden tests and NRC investigations led to several conclusions: (1) air ingestion was less severe than hypothesized, (2) debris ingestion was unlikely to disable sump pumps, but some designs were more vulnerable than others, and (3) the effect of insulation blockage depended on the type of insulation used in each plant. As a result, the NRC concluded in 1985 that sump issues did not require a generic backfit for all plants and should be dealt with on a plant-by-plant basis. The NRC issued a revised regulatory guide for the modification or replacement of vulnerable piping insulation.

After 1985, several blockage events in the United States and abroad led the NRC to look more closely at boiling-water reactors (BWRs). The most notable event occurred in 1992 at the new Barseback Unit 2 plant in Sweden where a safety valve accidentally opened and the resulting flow caused some insulation to break free. This insulation clogged the BWR's suppression pool strainers badly enough to cause pump cavitation.



Figure 9: Testing revealed that fine particulates from reactor piping insulation could break loose after a loss-of-coolant event, clog sump screens, and limit the sump systems' performance. This long-standing generic issue was resolved for all nuclear power plants.

In conjunction with international regulators, the NRC launched a round of experiments and investigations of BWR strainer performance. Computer models indicated a high likelihood of strainer blockage during a LOCA. In 1996, the NRC issued a bulletin to BWR plant owners to devise their own approved solution or to use one of three NRC-approved alternatives. The options included the installation of large-capacity passive strainers, self-cleaning strainers, or a backflush system to remove debris. The industry chose the first option, large-capacity strainers.

BWR sump issues led the NRC to look again at PWR sumps. Models and investigations indicated that clogging could be worse than expected, particularly from chemical reactions among the debris washing into the sump or if the insulation produced very fine debris. In 2003, an NRC bulletin requested that licensees determine whether in light of recent information their plants were assured of long-term cooling. Working with industry to develop guidance, the NRC permitted two methods of evaluation: a deterministic, conservative approach and a risk-informed alternative.

Licensee assessments led PWR owners to redesign their sump strainers to make them much bigger. Some also replaced vulnerable insulation. Further industry testing produced unexpected results that made closing the sump issue very difficult. For example, testing indicated that a small amount of debris could hinder sump performance and that clogging was very sensitive to the order in which different types of debris flowed down to the sump.

In 2010, staff concluded that industry efforts to reduce conservatism in evaluation and test methods were not working. Industry officials objected to making extensive modifications that might expose workers to significant levels of radiation with no correspondingly significant benefit. The NRC permitted utilities to select from several different combinations of deterministic and risk-informed options. By 2011, two-thirds of PWRs had closed out the sump strainer issue. In July 2012, the Commission approved three options to close out the debris accumulation issue for the remaining PWRs.

The protracted effort to close out the sump issue revealed the challenges of a difficult technical problem. An issue can drag on for years unless there is excellent communication between regulators and licensees regarding expectations and questions. There are often large uncertainties and conflicting data to resolve from vendor and licensee testing. The sump issue also reaffirmed the value of risk assessments: Even when they were time-consuming, risk assessments helped settle differences between and among regulators and licensees.

Auxiliary Feedwater Systems

In PWRs, the auxiliary feedwater system supplies water to the steam generators when a reactor plant scrams and power is lost to the main feedwater system. Auxiliary feedwater removes the reactor's decay heat, which is produced by the reactor fuel even after the reactor is shut down. If it is not cooled, reactor fuel can produce enough decay heat to cause the fuel rods to disintegrate and the fuel to melt. Auxiliary feedwater is a backup system to ensure that the reactor can be cooled even if the plant suffers a station blackout.

The 1975 Reactor Safety Study showed that auxiliary feedwater was more important to safety than previously recognized. The possibility of the failure of auxiliary feedwater systems was a significant contributor to a nuclear plant's overall risk of experiencing a core-damaging accident. Previously, the AEC and NRC were mostly concerned about large-pipe-break LOCAs, and the auxiliary feedwater system did not seem as important to safety because it did not help in such situations. The Reactor Safety Study demonstrated, however, that smaller pipe breaks contributed more to accident risk than large ones. For these small breaks, as well as for loss-of-power events such as a station blackout, the auxiliary feedwater system was critical to keeping the reactor cool. In response to the Reactor Safety Study, the ACRS requested that the staff evaluate the adequacy of auxiliary feedwater systems.

Developing a common resolution to auxiliary feedwater issues was not easy. System designs varied greatly from one plant to the next. Some plants had only one pump and interconnections between multiple reactor units on the same site. Some plants included electric and steam-powered pumps for diversity, others did not. The water supply for systems in older plants often did not meet the highest earthquake standards. There was, then, no simple generic solution for upgrading auxiliary feedwater systems.

The NRC initially sought to upgrade auxiliary feedwater designs for plants in the construction pipeline. Regulatory guidance developed in 1978 stipulated that auxiliary feedwater systems for new plants should meet the standards of safety-grade equipment, including earthquake standards. The NRC initiated an investigation into station blackouts, which included a review of whether older plants had auxiliary pumps that could be depended on to operate during a blackout.

After the Three Mile Island accident in March 1979, the NRC lessons-learned task force made numerous recommendations to upgrade auxiliary feedwater system design, maintenance, and operational procedures. Equipment upgrades included the installation of safety-grade power sources, circuits, controls, signals, and indicators. Some plants added alternate water supplies. Procedural changes simplified the rapid initiation of auxiliary feedwater operation and system reconfiguration. Other procedural changes ensured that the systems were properly aligned during normal operation and after the performance of

maintenance. Plants that relied on manual control of auxiliary feedwater installed automatic initiation systems.

While the upgrades to auxiliary feedwater systems were substantial, the seismic qualification of auxiliary feedwater systems at about 10 older PWRs was not resolved immediately. The NRC conducted site visits and a review of plant design information. In 1981, the staff issued a resolution plan to increase auxiliary feedwater seismic resistance so that the systems could withstand forces up to those of the plants' design Safe-Shutdown Earthquake.⁷ Utilities completed seismic upgrades to older plants in the late 1980s.

The upgrades after Three Mile Island improved auxiliary feedwater capability, but operational experience raised new issues of human performance and plant design. In the early 1980s, licensees reported numerous instances in which hot water from the main feedwater system leaked past check valves in the auxiliary feedwater system. In some cases the leakage was severe enough that the water flashed to steam, causing "steam binding" that prevented the pumps from working. The NRC issued requirements for temperature monitoring of auxiliary feedwater piping and procedures to lower piping temperature when leakage was discovered. The NRC remained concerned about the excessive leakage of check valves at some plants, and recommended that operators be aware of check valve issues as plants aged.

On several occasions, auxiliary feedwater systems shut down, or tripped, after their pumps reached excessive speeds, a condition called "overspeed." After an overspeed trip, operators typically had to go down to the pumps to reset them to resume operations. In 1985, the most serious loss-of-auxiliary-feedwater event occurred at the Davis-Besse Nuclear Power Plant in Ohio. A loss of the main feedwater system and a subsequent operator error touched off a transient that exceeded the design basis of the plant. The auxiliary feedwater system started up as designed, but both steam-powered pumps experienced an overspeed trip. It was later determined that a long run of cold piping to the pumps caused excessive amounts of steam to condense to water. The flow of steam mixed with water slugs led to oscillations in pump speed and an overspeed trip. As a result, the steam generators were without feedwater for 12 minutes before operators restored auxiliary feedwater flow.

An NRC review team concluded that a combination of poor maintenance practices and training, as well as poor system design, contributed to the event. The failure of both pumps was an example of a common-cause failure that underscored the value of diversifying the power source to the feed pumps, as was done on most auxiliary feedwater systems. Davis-Besse's operator instituted procedural and maintenance upgrades

7. A Safe-Shutdown Earthquake is the maximum earthquake potential which certain "important to safety" structures, systems, and components are designed to sustain and remain functional.

and diversified its auxiliary feedwater system by installing a motor-driven feed pump before the plant restarted in 1986.

The NRC assessment of the Davis-Besse event mirrored trends elsewhere in the industry. Auxiliary feedwater systems failed at a higher-than-expected rate. Human error and poor maintenance practices were significant contributors to auxiliary feedwater events, as was a lack of diversity in pump power sources. The staff proposed that all operating plants demonstrate through a probabilistic risk assessment that their auxiliary feedwater systems had a failure rate of less than one failed operation in 10,000 demands. These assessments had to account for common-cause failures, maintenance practices, and operator errors.

The assessments led to system upgrades by many plant operators. The NRC determined that a few plants were not sufficiently reliable to meet the failure-rate criteria and required upgrades. For two of these plants, the staff called for the installation of a motor-driven feed pump similar to the one added at Davis-Besse to improve auxiliary feedwater reliability.

BARRIER INTEGRITY

There are three important barriers between the highly radioactive fuel inside the reactor and the environment outside the plant: (1) the sealed metal rods containing the fuel pellets, (2) the heavy steel reactor vessel and associated piping, and (3) containment structure surrounding the reactor. (See also the Davis-Besse incident covered on page 20 under Cross-Cutting Areas.)

Combustible Gases in the Containment Building

In the 1960s, reactor plant designers and regulators developed systems to cope with a loss-of-coolant accident. One consequence of a loss of coolant was the production of hydrogen gas from overheating fuel rods. The hydrogen might escape through the pipe break and into the reactor containment building. Once free in the building, it could burn or explode, damaging plant components or even breaching the containment building.

AEC regulators required measures to limit the buildup of hydrogen, typically with hydrogen recombiners that act on principles similar to those used in automobile catalytic converters to turn hydrogen and oxygen into water. But recombiners could cope with only a small amount of fuel damage and escaping hydrogen. This is a particular concern for the relatively small General Electric (GE) Mark I–III series containments and Westinghouse’s ice condenser containment.⁸ In the late 1970s, the NRC began developing regulations to require owners of these models to develop other ways to control hydrogen buildup.

8. An ice condenser containment has a smaller containment building than a dry containment and compensates for its size by using over 2 million pounds of ice to condense steam escaping during a loss-of-coolant accident.

The Three Mile Island Unit 2 accident led the NRC to revisit its regulatory scheme for hydrogen control. About 10 hours into the accident, a pressure spike was detected in the containment building as a result of the ignition of a half-ton of hydrogen created from Unit 2’s damaged fuel. The pressure pulse damaged plastic, paint, bent doors, and crushed barrels.

The pressure pulse did not damage Three Mile Island’s vital reactor components or containment building, but the event exceeded the capacity of installed hydrogen control systems. NRC staff sought to resolve hydrogen control issues for the smaller more vulnerable containment buildings. Large dry containment buildings, like the one at Three Mile Island Unit 2, were not included in the investigation because their volume was about 56,634 cubic meters (2 million cubic feet) larger than the smaller Mark I–III and ice condenser containments. Even a large explosion would not damage them.

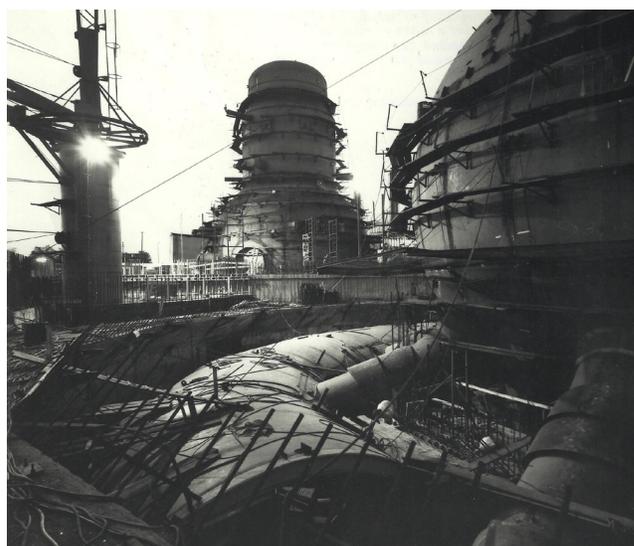


Figure 10: Relatively small in size, the Mark I containment proved susceptible to damage from the ignition of combustible gasses during fuel-damaging accidents. Pictured are Mark Is under construction at the Browns Ferry Nuclear Power Plant.

In the early 1980s, the NRC expanded its research on hydrogen combustion and implemented rulemaking on hydrogen control. Mark I and II containment buildings had to be “inerted.” With inerting, plant operators replace the containment-building air atmosphere with a non-combustible gas like nitrogen to prevent the hydrogen from igniting. The slightly larger Mark III and ice-condenser containments had to install equipment to prevent hydrogen from reaching dangerous levels. The industry chose to do this by installing systems to ignite hydrogen and burn it off before concentrations became explosive.

The NRC and industry expanded research into the behavior of severe accidents with significant core damage, including investigations into the production of combustible

gasses. Utilities with common containment designs pooled their resources to conduct research specific to their plants. The NRC sponsored peer review of its hydrogen research by the National Research Council. The research council's report in 1987 concluded that the existing regulatory requirements made it very unlikely that hydrogen detonation would cause containment failure. Inerting containments and installing igniters, the report said, were reasonable ways of limiting the possibility of hydrogen detonation. The council's researchers agreed that large dry containments did not need additional safety features.

About 10 years later, the NRC sought to apply risk insights to combustible-gas control regulations. In 2000, the staff concluded that combustible gases were not a significant hazard to containment integrity in large dry containments and inerted Mark I and II containments during the first 24 hours of an accident. The same was true for igniter-protected Mark III and ice-condenser containments, except during a station blackout when the power source for the igniters would be lost.

In light of these insights, the NRC eliminated requirements for hydrogen recombiners in dry containments, and it performed a cost/benefit analysis for a backup power supply for igniters in Mark III and ice condenser containments. Using both qualitative and quantitative considerations, the NRC's research staff recommended adding a backup power supply for the igniters. Licensees agreed to voluntarily make the design changes.

After the March 2011 Fukushima accident, the staff developed a process to implement lessons learned from the accident. For Mark III and ice condenser containments, the NRC specified that licensees develop and maintain strategies to give the hydrogen igniters an alternative power source independent of the onsite power sources. (See also "The Fukushima Dai-ichi Accident" on page 21)

Containment Pressure Relief Performance

The 1975 Reactor Safety Study used two plants as reference designs for its calculations. One of those was the Westinghouse PWR with a large dry containment building and the other was a GE BWR with a Mark I containment building. The differences in containment design raised some significant safety questions. The Westinghouse dry containment was a large building with a steel liner designed to handle a pressure surge from a pipe break. The GE Mark I was designed to handle the same pressure surge but in an innovative way. The building volume was much smaller than that of the dry containment, but the Mark I design compensated by forcing the escaping steam into a large pool of water where it condensed and where the gases were scrubbed to significantly reduce radioactive particles.

The small containment space created problems during severe accidents. The Reactor Safety Study found that the

chance of a core-melt accident at a BWR was very low, but that the Mark I containment would be severely challenged if a core-melt accident occurred, much more than a large dry containment would be. It was not until 1987 that the NRC addressed Mark I issues when it performed an ambitious risk assessment of five plants and confirmed the findings of the Reactor Safety Study regarding Mark I vulnerability. The study found that GE BWR plants had a similar overall risk when compared to other reactors, but that this was mostly because of its superior ability to prevent accidents from starting. It was less successful in mitigating those accidents once core damage became serious. The NRC's emphasis on defense-in-depth demanded that there be a balance in capability between each layer of defense. Risk insights revealed an imbalance between prevention and mitigation in the Mark I's design.

NRC staff analysis concluded that reducing rising pressure in the containment building during an accident by venting substantially reduced the Mark I's risk. Most Mark I's, however, had low-pressure ductwork for venting. Venting through the ductwork when containment pressure was very high could rupture it. In 1989, the staff recommended to the industry that the ducting be replaced with hard piping. By the mid-1990s, all 24 Mark I plants had voluntarily made the hardened-vent modification.

The NRC also studied the overpressure issue for other smaller containments in the U.S. fleet, the Mark II, Mark III, and PWR ice condenser containments. Investigations indicated that the overpressure issue was not as severe for these slightly larger containments and that a generic fix was not necessary for these containment types. For individual plants, the NRC included safety improvements to be considered by licensees during their Individual Plant Examinations. After the 2011 Fukushima Dai-ichi accident, the NRC revisited the issue of the accessibility and operability of Mark I hardened vent systems and of Mark II venting. (See "The Fukushima Dai-ichi Accident" on page 21)

CROSS-CUTTING AREAS

Cross-cutting areas dealing with human factors in plant operation are so named because they influence all other Cornerstones of Safety Operation in the Reactor Oversight Process. After Three Mile Island, research and regulation of human factors became a primary component of the NRC's defense-in-depth safety philosophy. Discussed here are human performance issues relating to reactor design and to creating a safety-conscious work environment, also known as a "safety culture."

Human Performance

The AEC and NRC had been concerned with the role of human error in reactor mishaps, particularly the human-machine interface in the most critical area of the plant, the reactor control room. The agency did not involve itself in this issue in a significant way until the late 1970s



Figure 11: By the 1970s, reactor plant control rooms had become very complex and contributed to operator error, most notably during the Three Mile Island accident in 1979.

when the increasing complexity of reactor plants and design deviations from human engineering best practices compelled the agency to take action.

Early control room designs combined traits of fossil-fuel and U.S. Navy nuclear plants. They used large, widely spaced analogue meters, indicating lights and switches which usually displayed a single parameter or controlled an action on a single device (as opposed to implementing a sequence of events). Layouts located often-used devices within easy reach of the operators. Emergency controls were further away from the operators with redundant component controls sometimes installed at different panels. The need to move from one panel to another during an event was an awkward arrangement and was exacerbated by the increasing complexity of plants. The total number of devices in control rooms jumped from an average of 3,000 in early reactors to about 7,000 in the 1970s. Greater plant complexity and the resulting increase in the number of displays and controls increased the chance of human error, especially during accident situations.

Regulatory research indicated that greater attention to human engineering was necessary. A 1973 AEC study identified and recommended numerous improvements to control-room design, operator training, and procedures. In 1975, the Reactor Safety Study identified human error as a significant contributor to the overall risk of a plant accident, an assessment that was also supported by a review of the study by the American Physical Society. Additionally, three former engineers at General Electric alleged that the nuclear industry and the NRC neglected the role of human error in reactor plant accidents. Responding to this information, the Advisory Committee on Reactor Safeguards called on the NRC staff to investigate the need for improvements in human performance.

The NRC contracted for a report on human engineering in nuclear power plant control rooms. The February 1977 report found that existing control-room designs provided adequate safety, but it called on the NRC to issue regulatory guidance to incorporate human engineering principles into new designs. The study pointed to the essential role that simulators played in operator training and bemoaned that fact that many operators did not train on simulators that matched their own plant's design. The report's authors noted the paucity of useful data available on human error and called for greater data collection.

By early 1979, the NRC had launched a number of preparatory initiatives on human engineering. It joined international efforts to explore the human/machine interface at an experimental reactor in Norway. It sought training for its inspectors in recognizing human-error contributors. It began data evaluation from licensee event reports to provide a basis for future licensing criteria and regulatory guides. But after over six years of study, few changes were made to control-room design and layout. Believing that existing plants had sufficient safety margins, the NRC focused on new plants.

The cause of the Three Mile Island accident is often attributed to human error, but the NRC and nuclear industry recognized that a broader problem was the human/machine interface. The operators were confused by inadequate training and were misled by poor control-room arrangement and flawed plant indicators. While the NRC had done some work on control-room hardware and layout, assuring effective interaction between operators and the plant required much more. The agency sought improvement in three broad areas: (1) training and procedures, (2) control room design, and (3) management of accident support staff.



Figure 12: Adding to the confusion reactor operators experienced during the accident at Three Mile Island was a noisy and crowded control room environment.

There needed to be a better match between control-room design, operator training, and the plant procedures. Control rooms were collections of symptoms—pressures, temperatures, and component statuses—that were often not arranged in ways that made it easy for operators to diagnose the root cause of unexpected events. Operators had two complex tasks: diagnose root causes and respond rapidly to symptoms. Diagnosis was critical because emergency operating procedures were “event-based” and, to be useful, operators needed to know what event they were dealing with. Three Mile Island demonstrated that unexpected malfunctions might conceal the root cause of an accident, and operators might make an incorrect diagnosis. In late 1979, the NRC sought to lessen the burden of diagnosis on operators. It directed utilities to develop training programs and emergency operating procedures that responded to a limited number of critical symptoms—symptom-based emergency procedures—that could indicate when the reactor core was in danger of overheating.

The symptom-based approach to emergencies compelled control-room design changes. TMI’s operators had been hampered by scattered plant indicators that, if placed next to each other, might have alerted them to the danger the reactor faced. The NRC called for centralized emergency panels and new readings for the most critical symptoms.

The NRC sought to reduce distractions for operators during an event. This could be done in part by prioritizing the many alarms that are initiated during an event and reducing the number of people allowed in the control room during an accident. Dozens of support staff milled about the control room during the Three Mile Island crisis, distracting the operators. The NRC required licensees to establish technical and operational centers on site with robust plant monitoring and communications ability. This allowed the utilities to provide expert support while not

distracting operators from their key task of responding to immediate symptoms of reactor distress.

The NRC established long-term goals for “human-factors” research and regulation. It issued regulations on operator staffing, training, fitness-for-duty programs, operator licensing, and simulators. In crafting a human factors research program, the NRC consulted the Human Factors Society and the National Research Council. The NRC has pursued research on the human/machine interface; personnel issues such as training, licensing, and work schedules; prediction of human error, and management and organizational issues.

The nuclear industry has also pursued human-factors research. The Nuclear Energy Institute has taken the lead in human-performance programs aimed at refining the NRC’s regulatory programs. The Institute for Nuclear Power Operations seeks to improve training through an accreditation process. The Electric Power Research Institute performs research to improve plant personnel efficiency, particularly through control-room design, aids for maintenance personnel, and proficiency training.

Safety Culture

The NRC’s move in the late 1970s toward a comprehensive system of oversight came in part from its recognition that licensee management practices and culture influenced reactor safety. Previously, the AEC had avoided any direct assessment of plant management. The NRC’s Systematic Assessment of Licensee Performance continued this tradition by inferring poor management practices from plant events and accidents. Deferring to licensees on plant management seemed logical. Licensees, not the NRC, had to respond to an event. It was important to instill in plant operators a feeling of ownership and responsibility for plant safety. There were also practical difficulties. Even if the NRC had wanted to assume aggressive oversight, there was no clear set of criteria for what constituted effective safety management.

In the wake of the Three Mile Island accident, the NRC received heavy criticism from investigative committees that it had “virtually ignored the critical areas of operator training, human factors, engineering, utility management, and technical qualifications.” The NRC addressed a number of these areas, but the nuclear industry took the initiative to improve management practices. Licensees created the Institute of Nuclear Power Operations (INPO) to foster a culture of excellence at all nuclear plants. INPO created a system that relied on peer pressure to induce licensees to improve their performance and adhere to a set of safety principles that embodied the organization’s view of excellence.

The Chernobyl accident in 1986 challenged public confidence in the management of nuclear plants

worldwide. A panel for the International Atomic Energy Agency (IAEA) reported that much of the failure at Chernobyl was that its operators and managers lacked a “safety culture” where clear lines of authority existed and where there would be a “permanent awareness by all personnel of the potential safety implications of any deviation from the procedures.” In a later publication, the IAEA panel treated safety culture as an essential supporting element in the hardware used for defense-in-depth. Safety culture, the IAEA report noted, “strengthens each of the successive obstacles to the release of radioactive materials.”

The IAEA’s conception of a safety culture matched many of the elements that INPO had articulated in its concept of excellence and indicated that there was much agreement among experts on the basic concept of a safety culture. Regulating safety culture was a different matter. That safety culture was essential to defense-in-depth was as intuitively appealing as it was difficult to measure. As another IAEA publication put it, doing a safety-culture review at a nuclear plant was a search for “tangible evidence of an essentially intangible concept.” Turning safety culture into a meaningful factor in regulatory oversight took many years.

For the NRC, the IAEA documents on safety culture did not provide enough substance to integrate safety-culture assessments into the oversight process. The NRC funded a number of studies of how organizational structure and culture influenced safety performance at nuclear power plants. A 10-year effort by Pacific Northwest Laboratory sought to find statistically valid relationships between safe plant operation and elements of organizational structure such as staff size, resources, and organizational governance. Other studies examined organizational processes, such as communications, organizational culture, and decisionmaking.

The NRC also examined studies of non-nuclear industrial safety culture. The Challenger Space Shuttle explosion and the disaster at the Bhopal chemical plant in India spurred studies of safety culture in many industries. The advantage of safety-culture studies in non-nuclear industries was that they often had extensive accident data and sound correlations between safety culture and accident rates. However, some questioned whether their lessons could be transferred to nuclear power where there were few accidents. Nuclear power plants needed a model that linked culture to the precursors of accidents rather than accidents themselves.

By the end of the 1990s, experts had completed much research on the linkage between safety culture and safe operations. International studies, in particular, indicated that regulators had an important role to play. Applying these insights to the U.S. context was a challenge. INPO

had done a great deal of work to improve safety culture at U.S. plants, much of it exceeding regulatory requirements. The result was a dramatic order-of-magnitude reduction of significant events at nuclear power plants between 1990 and 2000. Why should the NRC get involved?

The answer to that question became clearer following a 2002 incident at the Davis-Besse Nuclear Power Station. A small leak caused corrosion the size of a pineapple on the thick steel reactor vessel head, a critical component in the reactor pressure boundary. The plant had come dangerously close to a loss-of-coolant accident.

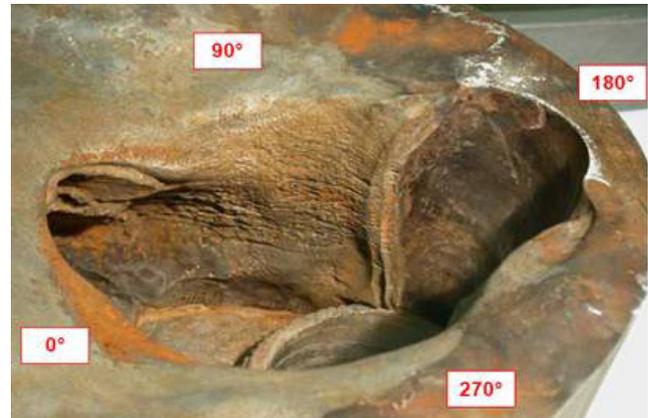


Figure 13: The Davis-Besse nuclear power plant reactor vessel head experienced extensive erosion from a small leak. The event raised serious questions about the safety culture at the facility.

As part of the plan to restart Davis-Besse, the NRC required the licensee to contract with a third party to conduct a safety-culture assessment. Using a methodology developed for the NRC by Brookhaven National Laboratory, the assessment examined organizational behavior and attitudes. It found that while the licensee had made several steps toward fostering a safety culture at Davis-Besse, it was inconsistently accepted across the organization. Weak areas included personnel taking ownership for plant safety, having cohesive safety leadership, effective communication of safety goals to all plant personnel, and making safety culture learning-driven. As NRC Chairman Richard Meserve noted, at Davis-Besse, operators stretched their resources not in the name of safety but to keep the plant in operation. The industry had improved its average performance, but there was still an important role for the NRC in addressing safety culture issues at plants that were encountering serious difficulties.

The close call at Davis-Besse illustrated how “soft” aspects of plant management had negative hardware consequences. A GAO report recommended that the agency improve its oversight of safety-culture issues among plant operators to gain an early indication of degrading plant performance. In 2006, the NRC incorporated over a dozen aspects of safety culture into some of its inspection procedures and guidance documents as part of the Reactor Oversight Process. It also included triggers graded to ROP

assessment results that compelled a licensee to perform a safety-culture assessment. For less serious findings of degrading performance, the licensee had to perform its own safety-culture assessment. For more serious ones, it had to contract for a third-party assessment.

The NRC's commitment to safety culture culminated in the issuance in 2011 of a policy statement addressing safety culture. The product of extensive consultation with stakeholders and workshops, the final statement defined safety culture as "the core values and behaviors resulting from a collective commitment by leaders and individuals to emphasize safety over competing goals to ensure protection of people and the environment." The statement included nine traits of a positive safety culture and noted that all individuals and organizations involved in NRC-regulated activities were expected to apply safety-culture traits to their organizational environments.

THE FUKUSHIMA DAI-ICHI ACCIDENT

On March 11, 2011, the Great East Japan Earthquake occurred off the coast of Japan's main island, Honshu. An earthquake rated at magnitude 9.0 led to the automatic shutdown of 11 nuclear power plants on the northeast coast of Japan. About 40 minutes later, the first of a series of tsunami waves swept through one of the sites, the Fukushima Dai-ichi Nuclear Power Plant. The earthquake and waves killed about 20,000 people throughout Japan and 1,000 residents of the Fukushima Prefecture. Two workers at Fukushima Dai-ichi drowned.

Reaching a maximum height of about 45 feet, the waves easily exceeded the site's design resistance to tsunamis and did extensive damage to the site's six power plants. A station blackout of all ac power ensued at all but the Unit 6 plant. A Unit 6 diesel generator was able to supply power to Units 5 and 6 to keep them shut down and stable. Unit 4 had been shut down for maintenance and its fuel relocated to a spent fuel pool. In the days after the earthquake, there was considerable concern about the condition of Unit 4's spent fuel pool, but its fuel rods remained cool and covered by water even though the reactor building around it sustained extensive damage.

The other three units—each a General Electric BWR with a Mark I containment—were not as fortunate. Operating at full power when the earthquake struck, they suffered an extended station blackout. Over the next few days, failure of the emergency core cooling systems led to core damage in Units 1–3. Combustible gases produced during the accident caused explosions that damaged portions of the reactor buildings.

Two weeks after the accident, the NRC created a senior-level task force ("the Task Force") to make recommendations in light of the accident as to how the agency should improve regulation of operating reactors.

The Task Force issued its report in July 2011. In justifying its recommendations, the Task Force argued that the NRC's mandate to ensure "adequate protection has been, and should continue to be, an evolving safety standard supported by new scientific information, technologies, methods, and operating experience." It noted that its recommendations fit within the NRC's long history of implementing knowledge-based regulatory change. After comparing data on the Fukushima accident to existing regulations, the Task Force concluded that "the time has come for such change."

To bolster existing layers of defense-in-depth most challenged by the Fukushima accident, the Task Force made 10 specific recommendations in three areas: (1) the ability of U.S. plants to protect against fuel-damaging external events, (2) mitigation of the consequences of a core-damaging accident, and (3) emergency preparedness to minimize public exposure to radiological releases.

1. Accident Protection:

- A. Evaluate and upgrade the design basis for seismic and flooding events.
- B. Initiate a long-term review to find potential enhancements to prevent seismically induced fires and internal floods.

2. Mitigation:

- A. Strengthen station-blackout mitigation capability.
- B. Install hardened containment vents at all facilities with Mark I and Mark II containments.
- C. Initiate a long-term review of hydrogen control and mitigation inside containment and adjacent buildings.
- D. Enhance spent-fuel-pool makeup capacity and instrumentation.
- E. Strengthen Emergency Operating Procedures and Severe Accident Management Guidelines.

3. Emergency Preparedness:

- A. Ensure that facility emergency procedures address prolonged station blackouts and events involving multiple units.
- B. Initiate a long-term review of emergency preparedness for multiple-unit events and prolonged station blackouts.
- C. Initiate a long-term review of emergency preparedness related to decisionmaking, radiation monitoring, and public education.

The Commission directed the NRC staff to prioritize the Task Force recommendations and consider recommendations from other sources. The staff agreed with the Task Force that none dealt with an imminent hazard to public health and safety. Nonetheless, many of the recommendations represented significant safety enhancements. The staff prioritized the recommendations into three tiers based on their potential to improve safety in the near term, the need for additional information, and an assessment of needed resources. Tier 1 activities were those whose safety benefits were substantial enough that they should begin without unnecessary delay. Tier 2 activities needed further technical assessment or were awaiting sufficient technical information or resources to begin. Tier 3 activities required long-term staff study.

In March 2012, the staff issued a series of orders, requests for information from licensees, and announced plans for rulemaking for Tier 1 activities.

- 1. Prevention:** The staff requested that licensees reevaluate the potential for seismic and flooding events to determine the necessity of safety upgrades. Licensees were also asked to perform seismic and flooding walkdowns to identify and correct degraded conditions. The staff issued an order that spent fuel pools be outfitted with instrumentation to ensure that water levels could be monitored during a beyond-design-basis event.
- 2. Mitigation:** The staff issued an order that licensees implement strategies to cope with a station blackout for an indefinite period of time. The strategies had to protect containment integrity and keep the reactor core and spent fuel pool both cool. A Station Blackout Mitigation Strategies rulemaking would make these orders permanent regulations. The NRC strengthened previous efforts to upgrade containment venting with an order that required a hardened venting system for BWRs with Mark I and Mark II containments. In June 2012, the NRC modified the order to ensure that the vents would remain functional even after extensive core damage and high pressures in the containment building. A proposed rulemaking will also consider additional strategies to confine or filter radioactive material following a core-damage accident.

- 3. Emergency Preparedness:** The NRC requested that licensees assess their staffing needs and communications capabilities to handle a multiple-plant accident. It also announced a proposed rulemaking to strengthen and integrate emergency procedures and plant capabilities.

Today, the NRC is working to address safety recommendations raised by the task force and others related to the Fukushima accident. Recently, Chairman Allison M. Macfarlane told an audience that the NRC's post-Fukushima activities aimed at ensuring "that the lessons we have learned are fully integrated into our regulatory work. We believe that by weaving the lessons learned from Fukushima into nearly all of our regulatory activities, we are ensuring their long-term sustainability."

Conclusion

Since the 1950s, nuclear power plant regulators have used insights from operating experience and research to broaden the AEC's initial safety approach of deterministic design, qualitative assessment methods, and defense-in-depth. That commitment to improving regulation continues. The Commission explicitly acknowledged this commitment in 1990 when it spelled out five Principles of Good Regulation that are now part of the agency's statement of values. It described the principle of "reliability" as regulation "based on the best available knowledge from research and operational experience. Systems interactions, technological uncertainties, and the diversity of licensees and regulatory activities must all be taken into account so that risks are maintained at an acceptably low level."

The NRC's post-Fukushima regulatory activity is part of this historic mission to use knowledge and operating experience to provide reasonable assurance of adequate protection of public health and safety. The Fukushima task force recognized the common connection its work shared with previous regulatory initiatives. It pointed out that its recommendations built on the regulatory changes of the 1970s and 1980s and would be the "fulfillment of past intentions" of the agency to realize "a more balanced and effective application of defense in depth." The NRC's safety mission for operating reactors has not changed, but the tools and knowledge used to achieve no undue risk will continue to evolve.



NUREG/BR-0518
June 2014

STAY CONNECTED

