Risk-Informed Decision Making: A Survey of United States Experience

A report prepared by

The B. John Garrick Institute for the Risk Sciences, University of California, Los Angeles

and

The Nuclear Risk Research Center, Central Research Institute of the Electric Power Industry, Tokyo

2017

B. John Garrick Institute for the Risk Sciences
UCLA ENGINEERING

CRIEPI
Central Research Institute of Electric Power Industry
Nuclear Risk Research Center

Page intentionally left blank

Principal Investigators

Dr. George Apostolakis, Nuclear Risk Research Center (NRRC) of the Central Research Institute of the Electric Power Industry (CRIEPI), Tokyo

Professor Ali Mosleh, B. John Garrick Institute for Risk Sciences (GIRS), the University of California, Los Angeles (UCLA)

Project Managers

Professor Ali Mosleh

Toshiyuki Zama, NRRC

Contributors

Dr. George Apostolakis

Mark Cunningham, Consultant, United States Nuclear Regulatory Commission (NRC) - retired

Dr. B. John Garrick, GIRS, UCLA

C. Rick Grantom, Consultant, South Texas Nuclear Project Electric Generating Plant (STP) - retired

Additional Contributors

Dr. Samaneh Balali, GIRS, UCLA

Karl N. Fleming, KNF Consulting Services

Dr. David H. Johnson, ABS Consulting

Kenneth Kiper, Independent Consultant

Dr. Pamela Nelson, National University of Mexico

Editor

Dr. Chris Jackson, GIRS, UCLA

Contents

Acronyms

AC	Alternating Current
ACRS	Advisory Committee on Reactor Safeguards
AEA	Atomic Energy Authority (United Kingdom)
AEC	Atomic Energy Commission
AIPA	Accident Initiation and Progression Analysis
AOV	Air Operated Valve
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOP	Abnormal Operating Procedure
AOT	Allowed Outage Time
APS	American Physical Society
ASLB	Atomic Safety and Licensing Board
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transients without SCRAM
BOP	Balance of Plant
BNCS	Board on Nuclear Codes and Standards (ASME)
BWR	Boiling Water Reactor
CAL	Confirmatory Action Letter (issued by the NRC)
CCF	Common Cause Failure
CCDP	Conditional Core Damage Probability
CCTP	Cumulative Conditional Trip Probability
CDF	Core Damage Frequency
CDF_0	"no-maintenance" CDF
CDF_{avg}	"average" CDF
CDF_i	"specific configuration" or "maintenance state" CDF
CFR	Code of Federal Regulations

CNRM	Committee on Nuclear Risk Management (ASME)
CRAC	Calculation of Reactor Accident Consequences
CRIEPI	Central Research Institute of the Electric Power Industry (Japan)
CRM	Configuration Risk Management
CRMP	Configuration Risk Management Program
CVCS	Chemical Volume and Control System
DBA	Design Basis Accident
DG	Diesel Generator
DOE	Department of Energy
DRDT	Division of Reactor Development and Technology
EAB	Electrical Auxiliary Building
ECCS	Emergency Core Cooling Systems
EDG	Emergency Diesel Generator
EOP	Emergency Operating Procedure
EPA	Environmental Protection Agency
EPRI	Electric Power Research Institute
EPZ	Emergency Planning Zone
ERT	Event Review Team
EST	Engineering Support Team
FEG	Functional Equipment Group
GIRS	B. John Garrick Institute for the Risk Sciences
HCF	High Cycle Fatigue
HFIR	High Flux Isotope Reactor
HTGR	High Temperature Gas Reactor
HVAC	Heating, Venting and Air-conditioning
ICBM	Inter-Continental Ballistic Missile
ICDP	Incremental Core Damage Probability

ICTM	Incremental Conditional Trip Probability
IDP	Integrated Decision-Making Panel
IDCOR	Industry Degraded Core Rulemaking
INPO	Institute of Nuclear Power Operations
INSAG	International Nuclear Safety Advisory Group
IPE	Individual Plant Examination
IPEEE	Individual Plant Examination for External Events
IPEC	Indian Point Energy Center
INL	Idaho National Laboratory
ITP	Incremental Trip Probability
JCAE	Joint Committee on Atomic Energy (United States)
JCNRM	Joint Committee of Nuclear Risk Management (ASME and ANS)
LAR	License Amendment Requests (LARs)
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accidents
LOFT	Loss-of-Fluid-Test
LPZ	Low Population Zone
LRF	Large Release Frequency
LWR	Light Water Reactor
MCA	Maximum Credible Accident
MOV	Motor Operated Valve
MW	megawatts
NEI	Nuclear Energy Institute
NFPA	National Fire Protection Association
NOED	Notification of Enforcement Discretion
NRA	Nuclear Regulation Authority (Japan)
NRC	Nuclear Regulatory Commission (United States)

NRMCC	Nuclear Risk Management Coordinating Committee (ASME and ANS)
NRTS	National Reactor Testing Station (of the then-AEC, now known as the INL).
NRRC	Nuclear Risk Research Center (Japan)
NSSS	Nuclear Steam Supply System
NUMARC	Nuclear Management and Resources Council (now known as NEI)
NUSCo	Northeast Utilities Service Company
OEM	Original Equipment Manufacturer
PLG	Pickard, Lowe and Garrick Incorporated
PSA	Probabilistic Safety Assessment
PTS	Pressurized Thermal Shock
PWR	Pressurized Water Reactor
QA	Quality Assurance
QHO	Quantitative Health Objective
PI	Performance Indicator
PRA	Probabilistic Risk Assessment
RAI	Requests for Additional Information
RCS	Reactor Coolant System
RCP	Reactor Coolant Pump
RG	Regulatory Guide
RI-GQA	Risk-informed Graded Quality Assurance
RI-ISI	Risk-informed In-service Inspection
RI-IST	Risk-informed In-service Testing
RIDM	Risk-Informed Decision Making
RISC	Risk Informed Standards Committee (ANS)
RMTS	Risk-Managed Technical Specifications
ROP	Reactor Oversight Process
SBO	Station Blackout

SCP	System Certification Program
SCWE	Safety Conscious Work Environment
SER	Safety Evaluation Report
SFP	Spent Fuel Pool
SDO	Standards Development Organization
SNAP	Systems for Nuclear Auxiliary Power
SPRA	Standardized Plant Risk Assessment
SPAR	Standardized Plant Analysis Risk
SSC	Structures, System and Component
STP	South Texas Nuclear Project Electric Generating Plant
RSS	Reactor Safety Study
THERP	Technique for Human Error-Rate Prediction
TMI	Three Mile Island Generating Plant
TMI-2	Refers to the 1979 accident in reactor number 2 of TMI
TVA	Tennessee Valley Authority
UCLA	University of California Los Angeles
UCS	Union of Concerned Scientists

Chapter 1: Introduction and Summary

The fundamental principle behind Probabilistic Risk Assessment (PRA) and, more broadly, Risk-Informed Decision Making (RIDM) was articulated very elegantly by the philosopher René Descartes four centuries ago:

> *The actions of life often not allowing any delay, it is a truth very certain that, when it is not in our power to determine the most true opinions, we ought to follow the most probable.*

The Japanese nuclear industry is committed to the continuous improvement of the safety of its nuclear power plants. In 2014, it established the Nuclear Risk Research Center (NRRC) within its Central Research Institute of the Electric Power Industry (CRIEPI). The NRRC mission statement is the following:

> *To assist nuclear operators and the nuclear industry to continually improve the safety of nuclear facilities by developing and employing modern methods of Probabilistic Risk Assessment (PRA), risk-informed decision making and risk communication.*

The United States nuclear industry has pioneered the use of RIDM and PRA virtually since its emergence. Importantly, PRA has helped RIDM evolve to consider many things such as licensee business models and cost efficiency more broadly. PRA use has resolved several challenging licensing situations. There is much to be learned – in terms of both successes and failures – from the United States experience.

The NRRC is currently focused on aligning existing Japanese PRAs to international standards of quality. [1] Japanese use of PRA in actual RIDM is in its infancy. In many respects, RIDM requires a regulatory

[1] Complementing the NRRC mission is the role of the Japan Nuclear Safety Institute (JANSI). As NRRC works towards improving the technical acceptability of Japanese PRAs, JANSI works towards determining how the PRAs are used by utilities in utility-specific risk management programs.

agency that is willing to accept risk-informed arguments - which is not the current situation in Japan.

A very encouraging recent development is the decision by the Nuclear Regulation Authority (NRA) to pursue a Japanese version of the United States Nuclear Regulatory Commission's (NRC's) Reactor Oversight Process (ROP) that is discussed later in this document. The NRC's ROP has evolved over the years and is now heavily risk informed which has made the program more objective and effective. Should the NRA adopt a similar risk informed ROP it would be expected that this would accelerate efforts to establish RIDM processes for both NRA and Japanese utilities. An example of this acceleration is the recent establishment by the NRRC of a RIDM Promotion Team that includes senior industry managers.

The Japanese nuclear industry requested that the NRRC produce a paper discussing the United States' PRA and RIDM experience. The NRRC engaged the B. John Garrick Institute for the Risk Sciences (GIRS) of the University of California, Los Angeles (UCLA) to jointly produce this paper. The paper provides a history of United States RIDM development, along with several case studies. The actual regulations are publicly available and not described in detail herein. The intent is to outline the motivation for the various risk-informed initiatives and rules, the challenges faced in implementing them, and the benefits that have been produced.

Many industries, including aerospace, pioneered reliability and system analysis methods critical to the eventual development of PRA by the nuclear industry. The journey for the nuclear industry is described below and provides a chronology of events that have shaped the current risk management sciences topography from the perspective of the United States nuclear power industry. Milestones, events, and developments occurring over the last five decades are included herein.

Even with so many accomplishments in the pursuit of knowledge and application of the risk sciences, challenges in scope, applicability, and organizational acceptance of risk information in some industry and regulatory disciplines remain. Work and research continue to pursue consistency with nuclear industry core values relative to nuclear safety and continuous improvement.

Section 1.1: The United States Nuclear History and PRA – The Narrative

The first organization in this story is the United States Atomic Energy Commission (AEC). The AEC initially managed risk using a 'deterministic' approach. Nuclear plants were built in accordance with a 'design basis:' the set of events or conditions that the plant needs to be able to encounter, and successfully deal with.

Commercial entities, such as Atomics International, were starting to champion PRA approaches. They were realizing that the 'design basis' approach did nothing to help understand what risk consequences actually were – in terms of consequence or likelihood. Designers found it challenging to prioritize risks they needed to contend with.

This awakening emerged in parallel among international organizations. F. R. Farmer of the United Kingdom's Atomic Energy Authority (AEA) wrote a seminal paper arguing that, if the likelihood of various amounts of Iodine-131 released from a particular reactor could be estimated, so could the risk associated with its operation on any site.

Other commercial organizations then started to incorporate methods that later became associated with PRA. Holmes & Narver Incorporated and General Atomics undertook safety analyses that used probabilistic methods.

These people and organizations were laying the path for something important: that turned out to be the groundbreaking Reactor Safety Study (RSS) which initiated an industry-wide change in perspective.

Section 1.2: The Reactor Safety Study (RSS) of 1975

The AEC commissioned the RSS to answer the question:

What is the risk of nuclear power in general?

The RSS (also known as "WASH-1400") is the first comprehensive PRA ever conducted. The prevailing thought was that nuclear accidents were both rare (on the order of 1 every million reactor years) and catastrophic. The United States House and Senate's Joint Committee on Atomic Energy (JCAE) had previously asked the AEC to study nuclear accidents in greater detail. It was identified in 1967

that existing containment systems could fail in certain accident scenarios, heightening awareness on Emergency Core Cooling Systems (ECCS). This demanded a more comprehensive understanding of nuclear risk. Then-Senator Mike Gravel initially insisted that the RSS be undertaken, with support quickly followed by a 1971 letter from then-JCAE Chairman Senator John O. Pastore. One key motivation in this letter was the public's need to know its exposure to nuclear power risk.

This direction had to overcome some prominent skeptics who primarily thought that there were not enough data for a PRA to be successful. Others fundamentally believed that quantifying nuclear risk was impossible. But they were misinformed: quantifying risk does not mean knowing it precisely, but being able to explicitly define the relevant uncertainties.

The impetus for the study was irresistible. It focused on two nuclear plants extrapolated to 100. Amongst many of the profound methodologies developed therein, the RSS introduced human error and Common Cause Failure (CCF) models.

But perhaps the most profound RSS outcome was the identification of a new primary risk contributor: small Loss of Coolant Accidents (LOCAs) and not the large ones as previously thought.

The conduct of the RSS received criticism, including from anti-nuclear groups. A United States House Subcommittee asked then-Professor of the University of California, Santa Barbara, Harold W. Lewis, to chair a committee to undertake a review. The Committee concluded that the RSS methodology was sound, but was unable to confirm the uncertainties contained therein with an opinion that they were understated. The NRC did not endorse the RSS and withdrew its previous endorsement of its executive summary. But this was going to be abruptly reversed.

The accident at reactor number 2 of the Three Mile Island Generation Plant (TMI-2) in 1979 was a small LOCA – the primary risk contributor identified by the RSS and previously overlooked. There was now empirical evidence to support the study's role in better understanding nuclear risk.

For it to become the groundbreaking study that it turned out to be, the RSS needed significant human effort. It was the product of some 40 engineers and scientists working over a three year period. The

study's leader was Norman C. Rasmussen of the Massachusetts Institute of Technology and its project manager was Saul Levine of the NRC who, in no small part, contributed to the study's success.

Importantly, the RSS answered the questions "what can go wrong?"; "how likely is this?" and "what are the consequences?" This triplet [2] of questions was developed later as the definition of risk assessment.

Section 1.3: The Establishment of PRA

With the success of the RSS, PRA started to inform more regulatory decisions.

Two of the most important post-RSS milestones were the Zion Nuclear Power Station and Indian Point Energy Center (IPEC) PRAs of 1981 and 1982 respectively. These were the first plant-specific and industry-sponsored PRAs to rigorously deal with containment response, external events, uncertainty and directional dependence of radioactive atmospheric plumes. These studies aimed to answer the following question:

What is the risk of particular nuclear power plants?

The PRA outcomes went on to contribute to the legal basis for regulatory decisions. IPEC's proximity to New York City had led to a petition from the Union of Concerned Scientists (UCS) asking it to be shut down, effectively threatening its operating license. At the very least, IPEC was facing the installation of very expensive backfits to mitigate the perceived risk. [3]

The Zion plant saw itself in a similar situation due to its proximity to Chicago. Both plants commissioned PRAs to specifically deal with the risk they imposed on nearby population centers.

The NRC licensing process successfully incorporated the PRA results to inform the ongoing proceedings in a way that previous

[2] Kaplan, S. and B. John Garrick. "On the Quantitative Definition of Risk." *Risk Analysis* 1, no. 1 (1981): 11–27.

[3] These backfits included a filtered-vented containment, a refractory core ladle and hydrogen combiner.

methodologies could not – all after being legally tested in the NRC's Atomic Safety and Licensing Board.

Further, the PRAs identified that many of the expensive backfits each plant was originally facing would have negligible impacts on risk and identified low cost modifications that had more significant risk impact. The PRA essentially saved the licensees hundreds of millions of dollars and improved risk.

The Seabrook Station Nuclear Power Plant was faced with a similar existential problem in the early 1980s. Although located in the state of New Hampshire, its proximity to the state of Massachusetts required cooperation from its neighbor in the development of evacuation management plans. Massachusetts, for its own reasons, was not willing to become involved. Fortunately, the plant had an exceptionally strong primary containment. PRA showed that acceptable risk levels were met by having evacuation plans extending to a one mile radius around the plant – with Massachusetts two miles away, their involvement was no longer required. The impasse was resolved.

PRAs were also conducted on other nuclear power plants. The Oconee Nuclear Station was subject to a collaborative industry-led PRA to further develop plant-specific PRAs, incorporating new methods such as the flooding risk methodology still in use today. The Tennessee Valley Authority internally developed plant-specific PRAs for the Browns Ferry Nuclear Power Plant, Sequoyah Nuclear Generating Station, Watts Bar Nuclear Generating Station and Bellefonte Nuclear Generating Station. In the mid-1980s, the South Texas Nuclear Project Electric Generating Plant (STP) Generating Station developed a plant-specific PRA to better characterize the safety benefit of their unique design (which incorporated three independent safety divisions).

More broadly, the industry collectively responded to the TMI-2 accident by studying severe accidents in greater detail. This led to the establishment of the collaborative Industry Degraded Core Rulemaking (IDCOR) Program that introduced degraded core scenario tools and methods to complement similar work undertaken by the NRC.

The RSS and operating experience identified two accident sequences that led to the NRC establishment of two new rules: the

1981 "Anticipated Transients without Scram" (ATWS) and the 1986 "Station Blackout" (SBO). The SBO rule included quantitative reliability targets for diesel generators.

All this PRA activity quickly raised a new question: "if we can quantify risk, what is an 'acceptable' level of risk?" The NRC's 1986 Safety Goal Policy Statement answered the question "how safe is safe enough?" It included two qualitative goals:

> *Individual members of the public should be provided protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life or health,*
>
> *[AND]*
>
> *Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.*

It also included two quantitative goals or Quantitative Health Objectives (QHOs):

> *The "prompt fatality" risk to an average individual in the vicinity of a nuclear power plant that might result from reactor accidents should not exceed 0.1 percent of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed (approximately 5 x 10-7 probability per year)*
>
> *[AND]*
>
> *The "cancer fatality" risk to the nuclear power plant local population that might result from nuclear power plant operation should not exceed 0.1 percent of the sum of cancer fatality risks resulting from all other causes (approximately 2 x 10-6 probability per year)*

These QHOs were supported with two subsidiary goals: a Core Damage Frequency (CDF) of 10^{-4} per reactor year and a Large Early Release Frequency (LERF) of 10^{-5} per reactor year.

The success of the previous plant-specific PRAs led the NRC to develop regulatory programs to examine plants individually and to encourage utilities to use PRA methods. These were called Individual Plant Examinations (IPEs) and Individual Plant Examinations with External Events (IPEEEs). Although not comprehensive PRAs, they were important studies that could inform later more robust analyses. Their impact was immediate and important: licensees identified over 500 risk-mitigating actions.

The NRC then commissioned a study called "NUREG-1150: Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants." Intended as an update of the RSS, this study refined typical 1980s methodologies. It became revolutionary in the way it used expert judgment. Nuclear power involves accidents that occur at very low frequency. This often requires subjective assessment – we cannot test nuclear power plants to failure to elicit data.

Beyond important developments in the field of PRA, the NUREG-1150 study found that nuclear power risk was lower than that estimated in the RSS – itself lower than industry expectations at the time.

Information was continually changing both the state of the art and PRA results. The NRC realized that beyond changing our understanding of risk, emerging information was also necessitating change on the nuclear power plant configuration. This saw the implementation of the "Backfit Rule" which governs plant modification for safety. By incorporating probabilistic analysis into the rule, the NRC had a framework that identified those modifications that had significant impact on risk at the exclusion of high cost-low effectiveness alternatives.

There were many other activities and events that helped shape PRA in this period. General Atomics extended the RSS outcomes to inform the design of its High Temperature Gas Reactor (HTGR). More PRAs were conducted by Northeast Utilities and The Oconee Nuclear Station. Internationally, the Kuosheng Nuclear Power Plant in Taiwan used many of the PRA methodologies being developed in the United States to deal with the unique geography associated

with its site. This list is not exhaustive and is developed in greater detail in Section 2.3:.

However, this activity was undertaken without any overarching intent. Probability methods were essentially voluntarily employed and their scope varied between each application. That was about to change.

Section 1.4: The NRC PRA Policy Statement

The NRC enshrined PRA as a permanent part of its regulatory policy by releasing a statement in 1995 which read in part:

> *The use of PRA should be increased to the extent supported by the state of the art and data and in a manner that complements the defense-in-depth philosophy.*
>
> *PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatisms associated with current regulatory requirements, regulatory guides, license commitments, and staff practices.*
>
> *Deterministic approaches to regulation consider a limited set of challenges to safety and determine how those challenges should be mitigated. A probabilistic approach to regulation enhances and extends this traditional, deterministic approach, by:*
>
> *(1) Allowing consideration of a broader set of potential challenges to safety,*
>
> *(2) Providing a logical means for prioritizing these challenges based on risk significance, and*
>
> *(3) Allowing consideration of a broader set of resources to defend against these challenges.*

As with all other advances with PRA methods, there was a body of skeptics and critics. But the utility of PRA was undeniable, and this had to be understood. Awareness was increasing regarding how PRA could identify traditional requirements that did not contribute much to safety. In this vein, the "Standards for combustible gas control system in light-water-cooled power reactors" (10 CFR 50.44) was eliminated as it was ineffective for reactors with large dry containments.

The PRA policy statement coincided with other evolutionary efforts to incorporate risk information in plant operations. Nuclear plant maintenance of the early 1990s did not adequately incorporate root-cause analysis, performance trending or prioritization in planning. Traditional rules could not adequately resolve this, but PRA could help. The resultant 1996 "Maintenance Rule" (10CFR50.65) with the associated development of PRA methods was initially challenging for licensees. An updated rule was released in 1999 under an overarching intent for licensees to assess maintenance risks associated with direct or inadvertent equipment unavailability. The (a)(4) portion of the rule stated:

> *Before performing maintenance activities (including but not limited to surveillance, post-maintenance testing, and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities.*

The Maintenance Rule was the first risk-informed, performance-based regulation. The rule's intent was for licensees to appropriately use risk methods to suitably minimize maintenance time while also controlling plant configuration in support of key safety functions. In this way, the intent of this requirement to balance availability and reliability was anticipated to be satisfied.

One of the key results of the NRC policy statement was that PRA methods started to become standardized. PRA depth and scope had varied wildly from plant to plant. The Electric Power Research Institute (EPRI) issued a "Probabilistic Safety Assessment [(PSA)] Guide." The American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS) collaborated to produce PRA standards. All these standards were combined into the standard

"ASME/ANS RA-S–2008." Following its 2013 revision, this standard remains the benchmark for all nuclear power plant PRAs. It currently allows the NRC to reduce its regulatory oversight role: if a PRA complies with the standard, no exhaustive review is required to establish its technical adequacy.

But PRA achieved something else that previous methodologies could not. It provided a language to communicate to the public. Instead of plants being "safe" or not, "frequency" and "consequence" became terms that had meaning. The NRC and others believed that this level of transparency could only enhance the standing of nuclear power with the general public.

The NRC continued to identify several rules that could be modified to provide more risk-informed implementation alternatives. These included rules 10 CFR 50.46 (Emergency Core Cooling Acceptance Criteria); 10 CFR 50.48 (Fire Protection); and 10 CFR 50.61 (Fracture Toughness Requirements for Protection against Pressurized Thermal Shock Events).

The NRC reactor oversight process (ROP) improved consistency and objectivity of plant inspections. It importantly focused licensee and regulatory resources on risk-significant aspects of plant operation, along with guiding regulators in response to inspection outcomes.

Regulatory Guide 1.174 was issued in 1997 promoting the use of PRA to inform the licensing basis of nuclear power plants. This provided an approach to RIDM that balances risk and deterministic approaches, decision acceptance guidelines, PRA quality standards and assurance, along with post modification monitoring.

Key risk-informed initiatives such "Risk-Informed In-Service Inspection (RI-ISI)" were implemented as part of this guide. Previously unidentified degradation mechanisms became part of the inspection process, along with risk-important but non-safety related piping. "Risk-informed Technical Specifications" introduced the use of risk-informed approaches to surveillance test frequency, mode changes with unavailable equipment, and Allowed Outage Time (AOT). "Risk-Informed Graded Quality Assurance (RI-GQA)" categorized equipment based on risk-significance. Some components previously classified as "safety related" were no longer

required to receive special treatment. [4] Conversely, non-safety related equipment with high risk-significance was identified as requiring more attention. [5] "Risk-Informed In-service Testing (RI-IST)" used PRA to introduce more realistic testing requirements, replacing the overly conservative traditional guidance.

Industry undertook its own risk-informed initiatives, particularly regarding outage risk management. Outage risk models leveraged defense in depth tools based on shutdown PRAs to manage outage configurations. The result was the identification of a number of undesirable combinations that helped inform plant operations.

Section 1.5: Key Observations and Challenges

Although traditional "deterministic" regulatory processes relying on "defense in depth" and Design Basis Accidents (DBAs) have served the United States nuclear industry well, PRA has demonstrated their imperfections. PRAs saw safety considerations expand to include things like human error and quantified uncertainty. PRAs routinely identified vulnerabilities and risk contributors that traditional approaches had not.

The establishment of RIDM faced several challenges. A major one was cultural. Most engineers in the United States do not take classes in probability and statistics in college let alone PRA. Asking them to change some of the traditional "deterministic" approaches to regulations to probabilistic methods was a significant cultural change.

Both the industry and the NRC trained employees in short courses and conferences. A good example is the ROP. The decision to make changes to the NRC inspection program was particularly challenging because of the large size of that program, in terms of both the number of NRC staff (e.g., hundreds of affected staff) and the number of licensed facilities affected (i.e., all licensed power reactors). New training programs were established within NRC to provide information on PRA to inspectors and their management.

[4] These components included most test and drain valves in safety related systems, local instrument indicators, post-accident sampling systems, radiation monitoring and meteorological systems

[5] These components included instrument air compressors, and certain on-site power sources such as Balance-of-Plant and Technical Support Center Diesel Generators

These programs ranged from overviews to detailed training on specific technical subjects. In addition, the NRC created a new category of inspector, the "senior reactor analyst," with expertise in both inspection processes and risk assessment. Each NRC regional office is staffed with several of these experts, all of whom are supported by the PRA expertise available elsewhere in the agency.

Another challenge was the varying technical acceptability of industry PRAs, especially before the 2009 Regulatory Guide 1.200 "An Approach for Determining the Technical Adequacy of PRA Results for Risk-Informed Activities." This document defined "what" must be done, not "how". It endorsed the industry PRA Standard (ASME/ANS RA-S-2008) and complemented a peer review process developed by the nuclear industry. These initiatives combined to create a uniform method for establishing PRA technical adequacy for a spectrum of potential risk-informed plant licensing applications.

However, challenges remain in both utility and regulatory organizations. Risk information and analyses are seen as an important addition to the current body of safety analyses that satisfy regulatory requirements to better understand risk and develop strategies for long-term operations. Continued leadership, focus and advocacy will be essential to break through residual cultural barriers. It will be up to leaders and champions to continue to advocate improving knowledge and understanding of risk. It is important for the regulator to better understand risks associated with their licensees to ensure that regulatory actions truly improve risk - not divert resources to items of little safety significance.

In the United States, risk-informed initiatives are voluntary. It is,then, natural that the utilities weigh their costs and benefits before adopting them. A common problem is that regulatory approval costs are usually incurred before initiative implementation, while the benefits are only realized in the future. Developing a technically adequate plant-specific PRA to support risk-informed applications impacts the entire organization's processes. Some utilities quickly invested in PRA while others adopted a "wait-and-see" posture. Those utilities that made early and steady investments now have substantial core competencies in risk analysis and management – the remainder have not.

The safety benefits are unquestionable. An excellent example is the RI-ISI (described above briefly, and in more detail later in this paper). In addition to improving plant safety, plant staff radiation exposure was reduced significantly. RI-ISI also reduced the number of inspections and associated costs. PRAs have also identified safety improvements in areas of vulnerability that lead to backfits, risk management compensatory actions, or other process changes.

The issue of cost savings deserves more discussion. A utility is always interested in running its plants in a cost-effective way. However, there is an additional safety benefit when unnecessary regulatory burden is removed: more resources become available to manage risk-significant issues. The NRC's 1995 policy statement explicitly recommended this. Unnecessary conservatisms add to costs without contributing to safety.

PRA use outside of strict regulatory guidance has resulted in more focus on items of risk significance in prioritization processes, audit and inspection scopes, corrective action program treatments, and maintenance strategy development.

An additional benefit is encountered in the ROP. The NRC found that the previous inspection, assessment, and enforcement processes were not clearly focused on the most safety important issues, consisted of redundant actions and outputs, and were overly subjective. The ROP contributed to resolve this.

Some other risk-informed initiatives did not fare so well. While both the NRC and ASME have developed programs that could be used by licensees to implement RI-IST, they have not attracted much attention. The initial regulatory approval and implementation costs outweighed the perceived (not actual) long-term benefits.

RI-GQA has also met limited success for the same cost argument. Alternate treatment procedural processes were not well developed or understood, and licensee return on investment was difficult to quantify and spread out over many future years. Regulatory approval processes were considered uncertain and extensive as some NRC staff were reluctant to permit QA relaxations regarding special treatment. One outcome of this appeared to be a more demanding regulatory approval process. It is unclear at present whether future licensee applications for implementing RI-GQA will

meet with greater success, but a growing number of licensees are pursuing this.

All this being said, the United States nuclear industry has and continues to benefit from PRA and RIDM. History has demonstrated that, in spite of consistent skepticism and criticism, PRA leads to better decisions being made – often involving both large costs savings and the improvement of risk.

Chapter 2:The History of United States Nuclear Regulation

This history of United States nuclear industry regulation can be best summarized by examining it over three time periods. The first period extends from the 1960s to 1975, and includes the birth of the nuclear industry as we know it. The end of this period occurs when the RSS results are released, which are worthy of their own section in this document. The second period starts immediately after the RSS was completed in 1975 and extends to the 1990s. This period is largely defined by the regulatory changes emanating from the TMI-2 accident in 1979. The final period extends from the 1990s to the present. It is characterized by the advances in computational power that facilitated and increased accompanying PRA scope and level of detail.

Section 2.1: Before the Reactor Safety Study (RSS) - From the 1960s to 1975

A complete discussion on PRA incorporates the Renaissance of the 14th through 17th centuries. Contemporary thoughts about probability and risk were essentially formulated by luminaries such as Cardano, Galileo, Pascal, Fermat, de Mere, Huygens, von Leibniz, followed by Bernoulli, de Moivre, Bayes, Port Royal Paris monastery, and LaPlace. Later there was Cox, Shannon, Pólya, Jeffries, and Jaynes, just to name a few. Telling the complete story is beyond the scope of this document. Even doing justice to the nuclear period that started in the 1940s would require a far broader coverage than that presented herein.

This chapter instead focuses on the 1960s to 1975 where the "probability thought process" was developed to better answer the question:

What is the risk of nuclear power in general, and nuclear power plants in particular?

Select events, individuals, activities, and organizations that initiated PRA growth are discussed below. The scope of this chapter adequately covers the key elements of this period's timeline in the context of United States' nuclear safety.

2.1.1 Early Activities

The first relevant regulatory body was the AEC. An internal 1956 memo to the AEC Division Director stated that consideration should be given to operations research and probabilistic approaches to assessing nuclear safety. [6] Logic models (such as fault trees and activity networks) along with supporting theory and algorithms for carrying out NPP PRAs were proposed in the 1960s. [7] The methodology was used to perform the first owner-operated sponsored reactor PRA on the Oyster Creek Nuclear Power Plant (which is discussed in sub-section 2.3.1.1.)

[6] B. John Garrick, "Memo to the Director, Division of Civilian Application, on Considering the Use of Probabilistic Methods in Nuclear Reactor Safety Analysis," n.d.

[7] B. John Garrick, *Unified Systems Safety Analysis for Nuclear Power Plants*, 1968.

2.1.2 Challenging the Status Quo

Atomics International was a division of the North American Aviation Company, which was later acquired by the Rockwell International Company. It was involved in the early development of nuclear technology and commercial and government applications.

In 1965, Atomics International's C.A. Willis wrote an internal memo titled, "Statistical Safety Evaluation of Power Reactors." [8] Had this been published in a refereed journal or a government report, Willis would likely be considered more of a pioneer in PRA development than he currently is. He challenged the then Maximum Credible Accident (MCA) methodology by identifying its shortcomings as a safety measure, stating:

> *[The MCA] approach does not determine the hazard magnitude nor indicate where improvements should be made.*

Willis had identified that (among other things) the MCA concept had no logical way to differentiate between "credible" and "incredible" accidents. He proposed that the aggregate of the products of probability and consequence for each risk scenario as a risk measure. He also suggested using fault trees as a quantitative model of undesired events. Willis wrote:

> *Statistical safety evaluations utilize the fault tree analysis system, which has proven so effective in improving intercontinental ballistic missile (ICBM) reliability and can lead to similar improvements in nuclear reactor safety.*

Atomics International applied the methodology to the Systems for Nuclear Auxiliary Power (SNAP) Program, even including containment in the underlying model. [9] The results, even by today's standards noting they were generated ten years before the RSS, are reasonable.

[8] C. A. Willis, "Statistical Safety Evaluation of Power Reactors," Memo (Atomics International, 1965).

[9] R. S. Hart and W. T. Harper, "Final SNAPSHOT Safeguards Report," Atomics International, North American Aviation, March 20, 1965.

2.1.3 A New Way to Understand Risk

Although the United States nuclear regulatory system of the 1960s was "deterministic," there was a lot of activity involving probabilistic methods. In 1967, then-Safety Advisor to the United Kingdom's AEA F. R. Farmer argued that, if the likelihood of Iodine-131 release could be estimated by quantity for a particular reactor, the risk associated with its operation could also be calculated. [10] His position was based on International Commission on Radiological Protection findings.

Farmer proposed an "accident/frequency" graphical representation of nuclear power reactor accidents (Figure 2.1-1). He also proposed a "limit line" as a criterion for acceptable risk. This limit line was a forerunner to the safety goals that are still being developed today. In fact, Farmer and his staff originated the term "Probabilistic Risk Assessment."

Whereas Willis challenged the MCA methodology, Farmer provided an alternative as a design basis for reactors. The United Kingdom's nuclear siting criteria of the mid-1960s (and reaffirmed in the 1970s) were based on Farmer's work.

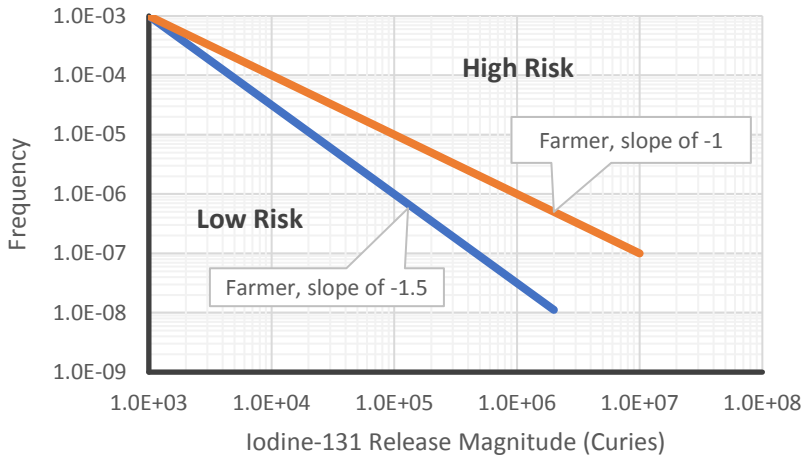


Figure 2.1-1: Farmer's "accident/frequency" graphical representation for Iodine-131 release, which was then used to represent the risk of many nuclear plant accident scenarios.

[10] F. R. Farmer, "Siting Criteria–a New Approach," in *Proceedings of the IAEA Symposium on Nuclear Siting*, 1967, 303–29, http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/44/070/44070762.pdf#page=317.

2.1.4 The First Applications of Probabilistic Methods

Holmes & Narver, a Los Angeles engineering, construction and technology firm, where Dr. Garrick was the Chief Nuclear Scientist, was repeatedly contracted from 1962 to 1967 by the AEC's Reactor Development Division to evaluate the United States safety experience in research, test, and power reactors. [11,12,13,14] At the time, only first generation power reactors were in operation or design.

These studies were undertaken to improve safety analyses. The power reactor phase of the work began in 1965, during other attempts to upgrade reactor safety analysis methodologies. Holmes & Narver's focus followed suit, changing to support the improvement of reliability and probabilistic safety analyses. The capstone power reactor study [15] developed a database for reliability and probabilistic safety studies and used logic models (including fault trees) for PRAs. The studies included a stylized fault tree model of a first generation United States nuclear power plant. Several probabilistic analysis examples of specific engineered safety systems were included. The methods were subsequently applied to the Carolinas Virginia Tube Reactor engineered safety systems. [16]

[11] B. J. Garrick, W. J. Costley, and Gekler, W. C., "A Study of Test Reactor Operating and Safety Experience," Prepared for Phillips Petroleum Company, Prime Contractor to the US Atomic Energy Commission (Homes & Narver, Inc., May 10, 1963).

[12] B. J. Garrick et al., "A Study of Research Reactor Operating and Safety Experience," Prepared for Phillips Petroleum Company, Prime Contractor to the US Atomic Energy Commission, June 12, 1964.

[13] B. J. Garrick, W.C. Gekler, and H. P. Pomrehn, "An Analysis of Nuclear Power Plant Operating and Safety Experience," Prepared for US Atomic Energy Commission (Homes & Narver, Inc., December 1966).

[14] B. J. Garrick et al., "Reliability Analysis of Nuclear Power Plant Protective Systems," Prepared for US Atomic Energy Commission (Homes & Narver, Inc., May 1967).

[15] Ibid.

[16] B. J. Garrick et al., "Reliability Analysis of Carolinas Virginia Tube Reactor Engineered Safety Systems," Prepared for Phillips Petroleum Company, Prime Contractor to the US Atomic Energy Commission (Holmes & Narver, Inc, August 1967).

2.1.5 Linking Risk to Society

Chauncey Starr [17,18] has contributed to and written as much or more about risk as anyone. His contribution is enormous primarily because it reaches far beyond the nuclear field. His seminal paper on "Social Benefits versus Technological Risk," has attracted many professionals across many disciplines to the risk field. Starr made major contributions to public understanding of the risks of nuclear power. But more than this, he articulated the benefits of the risk thought process to other fields such as social science, economics, and technology in general.

Starr's work included relating the assessment of risk to the subtleties of societal activities (both voluntary and involuntary) and how psychological factors influence risk as it relates to decision making. He provided a philosophical basis for risk analysis and has written extensively on risk management, assessment, and acceptability. In terms of the relevance of the risk sciences to all fields and to society, Starr was the most active and effective proponent.

A SEMINAL PAPER

Starr's work related the assessment of risk to the subtleties of societal activities such as those that are voluntary versus those that are involuntary. He also examined how psychological factors enter into the risk equation and decision making. Starr provided a philosophical basis for risk analysis and wrote extensively on risk management, assessment, and acceptability.

2.1.6 PRA and Accident Progression

The goals of the General Atomics' High Temperature Gas Reactor Accident Initiation and Progression Analysis (AIPA) were to:

1. establish an HTGR abnormal event ranking framework,
2. provide quantitative data for the identification of research and development requirements for HTGRs,
3. facilitate the consideration and comparison of alternative designs, and
4. provide guidance on the evolution of HTGR risk quantification methodologies.

The study team showed considerable insight on the basic PRA structure. They adopted the idea of a structured set of representative initiating events before analyzing and classifying them according to their radionuclide release potential. Their goal was to determine which initiating events (or class of events)

[17] Chauncey Starr, "Radiation in Perspective," *Nucl. Safety* 5 (1964), http://www.osti.gov/scitech/biblio/4004706.

[18] Chauncey Starr, "Social Benefit versus Technological Risk," *Science,* Vol. 19, pp. 1232-1238, 1969.

represented the highest risk, and to provide a meaningful best design basis for safety.

The AIPA was a major contribution to PRA. The slowdown of the HTGR program and subsequent studies (discussed later in this document) effectively superseded the "direction" of the AIPA. Notwithstanding, it was studies like the AIPA that continued to build the momentum of PRA.

2.1.7 Other Contributions

There were many other scientists, engineers, and institutions searching for better ways to determine nuclear power plant risk. There were active programs in aerospace, academia, and industry from which subsequent risk analysts drew ideas, algorithms, logic models, data sets, and tools.

Reliability engineering also became a source of many PRA concepts. Reliability engineering developed quickly during and following World War II, initially in Germany and then the United Kingdom. Physicist Ed Jaynes' and mathematician Stan Kaplan's work of the 1950s and 1960s contributed greatly to Bayesian methods and uncertainty science which fed into the nuclear risk assessment field. Bell labs [19] and Boeing helped develop logic models such as fault trees. The decision sciences contributed the event tree for providing an inductive logic model representation of event sequences.

One of the most important nuclear PRA developments was a rational treatment of Common Cause Failures (CCFs.) A CCF emanates from a single, shared cause that impacts two or more components, systems, or structures within a specified time. E.P. Epler, working for the Oak Ridge National Laboratory, considered CCFs when assessing the reliability performance of complex systems - especially instrumentation and control systems. [20, 21] Canadian Ernest Siddall attempted to apply statistical analysis to evaluate the effectiveness of reactor safety standards in the late

[19] H. A. Watson, "Launch Control Safety Study," *Bell Labs*, 1961.

[20] E. P. Epler, "A PHILOSOPHY OF CONTROL-SYSTEM DESIGN" (Oak Ridge National Lab., Tenn., 1956), http://www.osti.gov/scitech/biblio/4351983.

[21] E. P. Epler and D. P. Roux, "Incipient Failure Diagnosis for Assuring Safety and Availability of Nuclear Power Plants," in *Proceedings of AEC-Sponsored Conference at Gatlinburg, Tenn, October 30-November 1, 1967. CONF-671011. January 1968*, 1967.

1950s. [22] The Planning Research Corporation's Robert J. Mulvihill proposed a probabilistic algorithm for the safety analysis of nuclear power plants. [23]

There were many more investigators contributing to the transition from deterministic nuclear safety analysis to PRA. Nuclear power risk assessment pioneers became encouraged to pursue a more complete representation of relevant contributors ultimately leading to the breakthrough RSS.

[22] E. Siddall, "Statistical Analysis of Reactor Safety Standards," *Journal of Occupational and Environmental Medicine* 1, no. 6 (1959): 352.

[23] R. J. Mulvihall, *A Probabilistic Methodology for the Safety Analysis of Nuclear Power Reactors* (Planning Research Corporation, 1966).

Section 2.2: WASH-1400: The Reactor Safety Study (RSS) – 1975

What is the risk of nuclear power in general?

A MISCONCEPTION

The decision to go forward with the RSS was not without its skeptics. They believed that much more data would be required to have any chance of quantifying the risk. The problem is "what is meant by quantification." In the risk sciences community what is meant is quantifying the uncertainties, which is possible regardless of the data limitations.

The first major study highlighting the need to account for the probability of nuclear power plant accidents was a study led by the Brookhaven National Laboratory - one of several laboratories operated by the US Department of Energy (DoE). This Reactor Safety Study (RSS) was commissioned by the NRC and published in 1975. The RSS (sometimes referred to as "WASH-1400") is justifiably credited as the world's first comprehensive PRA. [24] The title of the study was, "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants."

This chapter tells the story of how the RSS came about, the advancements it made, and the challenges it faced. It is interesting to explore Congressional activities that contributed to RSS funding through the Joint Committee on Atomic Energy (JCAE), a joint committee between the United States House of Representatives and the United States Senate. The role the RSS played in shaping contemporary attitudes to PRA in nuclear power safety is very clear.

2.2.1 WASH-740: The Brookhaven Study

The prevailing thinking of the 1950s and 1960s was that reactor accident probability was nearly impossible to quantify, but very low. It was also thought that the consequences of an accident would be catastrophic. This view was reinforced by a 1957 study by the Brookhaven National Laboratory overseen by Dr. Clifford Beck and Dr. Garrick of the AEC staff (WASH-740), also known as the "Brookhaven Study." [25]

[24] "Reactor Safety Study. An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants. Executive Summary: Main Report." Nuclear Regulatory Commission, Washington, D.C., October 1, 1975) http://www.osti.gov/scitech/biblio/7134131.

[25] Atomic Energy Commission, *Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants: A Study of Possible Consequences If Certain Assumed ... Were to Occur in Large Nuclear Power Plants.* University of California Libraries, 1957.

Speculative estimates were made in WASH-740 that a major reactor accident could occur with a probability of about one in a million during the life of a reactor. The report went on to observe that: [26]

> *… the complexity of the problem of establishing such a probability, in the absence of operating experience, made these estimates subjective and open to considerable error and criticism.*

WASH-740 challenged advocates of risk assessment who believed that nuclear power risk could not be quantified. Many studies were to follow, primarily including United States, British, and Canadian efforts to prove these skeptics wrong. What followed were probabilistic analyses of military reactors, several studies sponsored by the AEC and studies in industry and academia.

2.2.2 Congress and the Inadequacy of Containment Systems

In the late 1960s, nuclear accidents and their consequences attracted the attention of the JCAE. A 1967 AEC special task force investigated core melt consequences and found that containment systems, which were thought to be the ultimate defense against radioactive material release, could be penetrated by some accident scenarios.

There were two primary effects of this finding. Containment systems' limitations became perhaps the most influential factor on the Congressional nuclear plant safety agenda prior to the RSS. These limitations also changed the focus of nuclear plant safety from containment system design to Emergency Core Cooling Systems (ECCS).

The switch in safety emphasis involved determining whether ECCS could be tested in severe accident scenarios – specifically to prevent core damage and containment failure. The AEC had planned to build a Loss-of-Fluid-Tests (LOFT) experimental reactor at its then National Reactor Testing Station (NRTS) in Idaho, now known as the Idaho National Laboratory (INL). The LOFT experimental reactor had a troubled history due to the diversion of funds from the Light Water Reactor (LWR) program to the AEC's fast breeder program. While the LOFT project began in 1963, no meaningful tests were performed until 1978. By 1982, 43 tests were performed covering a

[26] Ibid.

spectrum of small to large breaks. These provided an important database of the processes and phenomena occurring during a LOCA.

The LOFT project was delayed in spite of strong support from Congress and the Advisory Committee on Reactor Safeguards (ACRS). In 1971, tests were made on an existing NRTS "Semi-Scale Facility" indicating that some particular ECCS designs were deficient: back pressure created in simulated accidents blocked the flow of water. A great deal of publicity with concern over nuclear power plant safety resulted.

The AEC divided up the task of better understanding nuclear power risk between its Division of Reactor Development and Technology (DRDT) and the Division of Regulation in early 1971. A DRDT study (WASH-1250) did not generate a quantitative approach to risk assessment, but supported the JCAE's desire to hold hearings. The study also generated a great deal of useful nuclear safety source material that supported later activities.

JCAE Chairman Senator John O. Pastore, wrote a letter on October 7, 1971 to the then-AEC Chairman, James R. Schlesinger, supporting a previous JCAE suggestion:

> *The members suggested that a comprehensive assessment of the safety aspects of nuclear reactors be made with the intent of setting down for the industry and public a clear-cut summary of what the facts are in this matter.*

It should be noted that this letter included the public's need to know nuclear reactor risks. The JCAE Chairman said in an appendix: [27]

> *One way of accomplishing this objective would be to prepare a report which, by addressing the probability of occurrence and consequences of the spectrum of accidents which could befall a nuclear power plant, would represent an*

[27] More information can be found at "NRC: History," http://www.nrc.gov/about-nrc/history.html.

assessment of the risks involved in the use of nuclear plants.

For instance, the report could discuss in quantitative terms the probability of occurrence of a loss of coolant accident, the probability of the emergency core cooling system fulfilling its intended function and the consequences of the loss of coolant accident with and without emergency core cooling functioning properly.

As another example, it could consider, under a number of appropriate conditions, the probability and related consequences of the failure of both normal and emergency electric power supplies.

The AEC held hearings on operational and developmental ECCS capability and reliability that lasted for 135 days from 1972. Transcripts of the hearings exceeded 22,000 pages. [28] The events before and during the hearings resulted in some actions by both the AEC and Congress. Senator Mike Gravel got the AEC to commit to a study on nuclear power plant risks around a year prior to the start of the RSS.

An often overlooked fact is that Congress, through the JCAE, provided excellent guidance to the AEC, including a direction that the performance capability of engineered safety systems become more transparent. Quoting the NRC when retrospectively summarizing the focus on ECCS of the late 1960s and early 1970s:

Often bitter debates over the reliability of emergency core cooling systems, pressure vessel integrity, quality assurance, the probability of a major accident, and other questions received a great deal of attention from the AEC and NRC, Congress, the nuclear industry, environmentalists, and the news media.

Congress had further legislative impetus to monitor nuclear plant safety. The Price-Anderson Act is a United States federal law first

[28] More information can be found at "Seventies," http://users.owt.com/smsrpm/nksafe/seventies.html.

passed in 1957. It capped non-military nuclear facility owner liability. The federal government became liable beyond that cap. The act is routinely renewed with the cap adjusted over time. Clearly, Congress had the mandate and responsibility to the public to oversee nuclear safety generally, and regulation specifically.

In spite of resistance and skepticism to quantitative methods, the number of large nuclear power plants announced or commissioned in the 1960s and 1970s increased the pressure to better measure nuclear power health and safety risk. WASH-740 was in the process of being updated, but it was clear that it was not going to answer the risk issue in any quantitative form. The update was never published. A different kind of study was requested focusing on nuclear power plant risk. The decision was made to proceed with the RSS.

The AEC chose Massachusetts Institute of Technology Professor Norman C. Rasmussen to lead the study with the AEC's Saul Levine managing the project.

2.2.3 Challenges and Skeptics

The RSS was not without its skeptics. The AEC's Task Force for the Study of the Reactor Licensing Process [29] believed that much more data would be required to quantify the risk than was available. The problem is "what is meant by quantification." Quantifying risk involves quantifying uncertainties, which is possible regardless of the data limitations. Embracing uncertainty allows the quantification of any parameter. Uncertainties become large if data (information) is limited, but they are not unquantifiable.

2.2.4 The Study Commences

A draft report was publicly issued in October 1974 attracting 2000 pages of comments many of them constructive. An American Physical Society (APS) committee identified serious errors in the draft consequence model, [30] leading to a new model being developed. [31] The Calculation of Reactor Accident Consequences

[29] L.V. Gossick, M. L. Ernst, et al., "Task Force Report for the Study of the Reactor Licensing Process," October 1973.

[30] Howard W. Lewis et al., "Report to the American Physical Society by the Study Group on Light-Water Reactor Safety," *Reviews of Modern Physics* 47, no. S1 (1975): S1.

[31] Nuclear Regulatory Commission and others, "Overview of the Reactor Safety Study Consequence Model," NUREG-034, June 1977.

(CRAC) Code was developed to calculate the accidental radioactive material release health and economic consequences. A number of other lesser flaws were corrected and the final RSS was published in October 1975 by the newly formed NRC (the entity resulting when the AEC split into separate regulatory and development organizations).

The RSS used two nuclear power plants (extrapolated to 100) to answer the question of how safe is nuclear power generally. These plants were the Surry-1 Pressurized Water Reactor (PWR) and the Peach Bottom-2 Boiling Water Reactor (BWR). Multiple data sources were mined, including industry failure rate data, the Holmes and Narver studies, United States Navy data and foreign sources. Human error rates were obtained from the United Kingdom, Denmark, and other sources for use in the Technique for Human Error-Rate Prediction (THERP) model. [32]

The RSS addressed fires and external events including earthquakes, albeit superficially. CCFs were considered using bounding estimates. Models were developed for core melting and fission product migration. This led to more realistic analysis-driven CCF parametric models based on operating experience in subsequent studies. [33] The RSS also developed probability distributions for failure rates thus utilizing the Bayesian approach to probability without stating it explicitly. This led to a more formal acceptance of this interpretation of probability later.[34]

The RSS findings were many and profound. It determined that small - not large - LOCAs were the major contributors to nuclear power plant risk. The previous regulatory focus was on hardware failures,

[32] A good overview of THERP can be found at "Technique for Human Error-Rate Prediction," *Wikipedia*, April 15, 2015, https://en.wikipedia.org/w/index.php?title=Technique_for_human_error-rate_prediction&oldid=656627365.

[33] The Beta Factor Method by Fleming was introduced in 1975 as part of an HTGR PRA.

[34]Apostolakis, George, "Probability and Risk Assessment: The Subjectivistic Viewpoint and Some Suggestions," *Nuclear Safety*, 19:305-315, 1978.

large pipe breaks and ensuing LOCAs. [35] Core melting was assumed to not occur and that there would be no public risk in such a circumstance. The RSS determined that small pipe breaks, as well as transient events such as the loss of electric power to primary system relief valves, were significant risk contributors. Human error was also identified as a major risk contributor. Support systems such as the Auxiliary Feedwater System (AFWS) were realized as being "safety related," and that core melting was necessary for significant offsite consequences.

2.2.5 More Challenges and Critics

The RSS continued to have its doubters and critics, even though it represented a major breakthrough in nuclear plant risk management. Doubt and criticism were both inside and outside the NRC. Anti-nuclear groups questioned the methodology, its results, and its use to renew the Price-Anderson Act. These groups ignored the low accident frequencies, arguing that the large consequences associated with core damage and early containment failure proved that nuclear power was unsafe.

The NRC was uncomfortable with RSS criticism with some internal groups strongly defending existing deterministic safety approaches. At the request of a United States House Subcommittee, the NRC organized a group of experts, chaired by Professor Harold W. Lewis of the University of California, Santa Barbara, to review the final RSS. [36] The "Lewis Committee" was asked to clarify the RSS achievements and limitations, assess peer review, study the existing state of the methodology, and recommend how and whether such methodology could be used in the regulatory and licensing process.

The Lewis Committee findings were both positive and critical. They concluded that the methodology was sound and should be used to make regulatory processes more rational and better align resources to risk. However, the Committee was unable to assess the accuracy of the absolute probabilities and expressed a belief that

[35] Originally, LOFT was only intended to address large pipe breaks. The one advantage of the delays in the LOFT schedule was that it was able to incorporate the RSS results, which led to considering a larger spectrum of pipe breaks, including small breaks.

[36] Harold W. Lewis et al., "Risk Assessment Review Group Report to the US Nuclear Regulatory Commission," *IEEE Transactions on Nuclear Science* 26, no. 5 (1979): 4686–4690.

uncertainties were understated. The RSS was described as being "inscrutable" and that the executive summary did not represent the report well.

The NRC withdrew endorsement of the executive summary and the numerical nuclear plant risk estimates. It considered the estimates to be unreliable, issuing a draft policy statement that PRA was to remain a research topic only, not a regulatory decision-making tool. It would take a major accident in 1979 to cause a rethinking of that position.

2.2.6 Three Mile Island and the NRC Turnaround

The TMI-2 accident in 1979 largely silenced RSS criticism and forced the NRC to review its caution regarding the RSS. [37] The sequence leading to the accident - a transient-induced small LOCA with core damage caused by human error – was identified as a major risk contributor in the RSS.

To be fair, the RSS found the TMI-2 sequence risk significance somewhat small as it was performed on a Westinghouse plant whose steam generators have a large secondary water inventory that buffers interactions between the secondary and primary coolant systems. The TMI-2 accident occurred in a Babcock and Wilcox PWR with once through steam generators that make transient primary relief valve induced opening more likely. But the utility of the underlying methodology was made evident and clear – had it been applied to the Babcock and Wilcox PWR it would most likely have shown the substantial risk significance of the 1979 accident sequence.

Examination of NRC database precursor events with accident potential without correction was also in the RSS, increasing confidence in the study. Meanwhile, improvements were continuously being made in the RSS methodology through some early applications by industry.

The NRC eventually released policy statements urging the increased use of PRAs in regulatory decision making, even though problems

[37] More information regarding TMI-2 can be found at "NRC: Backgrounder on the Three Mile Island Accident," http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html.

continued with risk being fully embraced by regulators. The policy statement included: [38]

> *The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data, and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.*

Industry had embraced PRA to the point that all United States nuclear plants had some level of a PRA. The value of PRA to nuclear safety could no longer be dismissed.

2.2.7 Ultimate Success and a Giant Step Forward in Nuclear Safety Assessment and Risk Management

The success of the RSS was due in large measure to study leader Norman C. Rasmussen and project manager Saul Levine. It involved some 40 engineers and scientists and took 3 years to complete. Their foresight to reach beyond the nuclear industry (as suggested in the Attachment to the Pastore letter above) for expertise in systems modeling and analysis proved crucial. The fault tree methodology emanated from the aerospace industry. [39] The event tree concept was taken from the decision analysis field. [40] Both were critical to the success of addressing the complexities of nuclear power plants that many believed were beyond comprehensive modeling.

Nuclear safety analysis paradigms were fundamentally changed by the RSS, even with all its challenges and setbacks. It became the foundation for the evolution of nuclear safety analysis into a rigorous and quantitative form. It provided the framework for answering the basic risk questions: "what can go wrong, how likely

[38] "NRC: Commission Policy Statements - Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities (60 FR 42622)," August 16, 1995, http://www.nrc.gov/reading-rm/doc-collections/commission/policy/.

[39] Watson, "Launch Control Safety Study."

[40] Among the comments received from the draft report was one from a member of the Farmer team, who pointed out that event trees had been used in the earlier Farmer work in PRAs carried out for some of the early Magnox reactors in England. It is not clear that the Rasmussen team was aware of that.

is it, and what are the consequences?" [41] It did this while making contributors and their importance to risk transparent. While many improvements of the methodology have and are being made, the RSS has remained as the fundamental building block from which the changes have evolved. Its implementation and acceptance have been gradual, but its results have changed the way we think about analyzing risk: not only for nuclear power plants but increasingly for any kind of natural or anthropogenic threat.

[41] Stanley Kaplan and B. John Garrick, "On the Quantitative Definition of Risk," *Risk Analysis* 1, no. 1 (1981): 11–27.

Section 2.3: From the Reactor Safety Study to the 1990s: The Establishment of PRA

PRA became increasingly prevalent across the United States nuclear industry, buoyed by the success of the RSS and its ensuing validation after the TMI-2 accident. The nuclear industry sponsored and conducted its own PRAs, simultaneously yielding safety and cost improvements.

This section outlines the first steps that both regulators and licensees took in implementing PRA across the United States nuclear industry. Importantly, PRA became accepted as a legal basis to resolve regulatory issues. The significance of this cannot be understated.

INITIAL INDUSTRY CONTRIBUTIONS

Industry initiatives in the 1970s and 1980s improved PRA methods and further supported the acceptance of PRA as a decision-making tool for improving nuclear power plant safety.

2.3.1 Initial Industry Contributions

Industry contributed substantially to PRA methods throughout the 1970s and 1980s in ways that are evident in contemporary practices, standards and regulations. Improving technical methods helped achieve regulatory and industry PRA acceptance. PRA technology improved incrementally across several early industry efforts to develop operational risk management programs. This section outlines several key industry initiatives in this regard.

2.3.1.1 Oyster Creek Nuclear Generating Station

The first utility-sponsored PRA was conducted on the Oyster Creek Nuclear Generating Station in the late 1970s. [42] The RSS was released during the Oyster Creek PRA, enabling its breakthrough methods to greatly extend the PRA's scope and relevance (which was published in 1979). [43]

The Oyster Creek PRA included several noteworthy advancements including the use of "scenario" representation of risk which incorporated a more natural "language" for describing what can go wrong. A scenario description starts with an initiating event followed by the sequential successes or failures of systems and operator actions leading to either a success or a failure state (such as core damage). While the "reduced" representations of plant

[42] B. John Garrick and et al., "OPSA—Oyster Creek Probabilistic Safety Analysis," Prepared for Jersey Central Power & Light Company (Pickard Lowe and Garrick Incorporated (PLG), August 1979.

[43] Ibid.

response developed in the RSS are an adequate analytic representation scheme, other useful information is lost in the Boolean reduction of the responses into a compact failure depiction. A scenario description allows a dialog or script to be developed that provides details into equipment failures and their cascading effects, as well as organizational and human response events.

The Oyster Creek PRA also developed the "seismic risk curve" which has been used in all nuclear power plant PRAs since. The accompanying dispersion analysis code accounted for directional dependence of the radioactive plumes (if supported by meteorological data) rather than maintaining a constant heading as the regulatory code continues to mandate.

2.3.1.2 General Atomics High Temperature Gas Reactor (HTGR):

Closely following the publication of the draft of RSS, General Atomics (GA) extended the RSS methodology in the design of their HTGR. [44] This included a framework for the ranking of abnormal event sequences, quantitative information to inform on-going development, a basis for the selection of alternate design solutions, and insights for the continued development of PRA tools.

The GA analyses also included the propagation of uncertainty in the containment performance analysis (Level 2 PRA) results to identify and prioritize future consequence assessments.

2.3.1.3 Northeast Utilities

Northeast Utilities Service Company, the engineering arm of the utility, performed a risk assessment of Unit 1 of the Millstone Nuclear Power Plant in the late 1970s. [45] It is noteworthy that this study was performed using only in-house utility personnel.

2.3.1.4 Oconee Nuclear Station

The Oconee PRA of the early 1980s was a collaborative industry effort to develop a plant-specific PRA and to further explore new

[44] T Pasternak, K. Fleming, and W.J. Houghton, "HTGR Accident Initiation and Progression Analysis Status Report - Volume III: Preliminary Results (Including Design Options)" (General Atomic Co., San Diego, Calif. (USA), November 1975), http://www.osti.gov/scitech/biblio/7283894.

[45] J.A. Chunis and P.J. Amico, "Millstone Unit 1 Probabilistic Risk Assessment of the Decay Heat Removal Systems." Northeast Utilities Services Company, January 1979.

methods. [46] The most significant outcome of this effort was the flooding risk methodology which forms the basis for methods used today.

2.3.2 The Zion and Indian Point PRAs – 1981 and 1982

What is the risk of particular nuclear power plants?

The Zion Nuclear Power Station and Indian Point Energy Center (IPEC) first generated power in the 1970s. The Zion Nuclear Power Station is approximately 40 miles north of Chicago and 42 miles south of Milwaukee on the west shore of Lake Michigan in northeast Illinois. IPEC is 36 miles north of Manhattan on the banks of the Hudson River in the town of Buchanan, New York.

IPEC was subject to an early 1980s petition from the UCS to shut it down due to the high perceived risk to nearby population centers. [47] The Zion Nuclear Power Station was similarly close to cities, meaning that the IPEC petition could have ramifications well beyond the state of New York. The licensees collaborated to undertake the first industry-sponsored PRAs to rigorously treat containment response to a severe accident, external events and uncertainty as an integral part of the basic risk model.

2.3.2.1 PRAs and the Atomic Safety and Licensing Board (ASLB)

The Zion (Units 1 and 2) and IPEC (Units 2 and 3) Nuclear Plant PRAs, completed in 1981 [48] and 1982 [49] respectively, were major milestones in PRA evolution. Directional dependence of radioactive atmospheric plumes on offsite consequences were included in underlying models. They were the first commercial nuclear power

THE IMPACT

The results of the hearings that followed the completion of the Zion and Indian Point PRAs were favorable to the owners of the plants, saving hundreds of millions of dollars in plant modifications. There were two important outcomes of the studies and the hearings. First, the PRA results were accepted as a basis to justify continued operation of the plants without the need for backfits because it was shown that the backfits would have a negligible impact on the overall risk. Second, the PRAs identified several low-cost changes in the plants having a favorable impact on risk. The precedent was set in these hearings that PRA results can provide a legal basis to resolve regulatory issues.

[46] Pickard Lowe and Garrick Incorporated, "Oconee PRA, A Probabilistic Risk Assessment of Oconee Unit 3," Cosponsored by the Electric Power Research Institute, Nuclear Safety Analysis Center, and Duke Power Company, June 1984.

[47] Union of Concerned Scientists (UCS), "Petition for Decommissioning of Indian Point Unit 1 and Suspension of Operation of Units 2 and 3," 1979.

[48] "Zion Probabilistic Safety Study," Prepared for the Commonwealth Edison Company, Chicago, Illinois: Pickard Lowe and Garrick Incorporated, 1981.

[49] "Indian Point Probabilistic Safety Study," Prepared for Consolidated Edison Company of New York and the New Your Power Authority, New York, Pickard Lowe and Garrick Incorporated,1981.

plant PRAs to be tested as evidence for decision making in an NRC Atomic Safety and Licensing Board (ASLB) hearing.

The two primary issues reviewed in the associated ASLB hearings were whether the plants should continue operation, and whether costly backfits should be installed to reduce the risk. The backfits under consideration were a filtered-vented containment, a refractory core ladle, and a hydrogen combiner.

Both PRAs were conducted from 1978 to 1982. No regulatory policies, rules, regulations or guidance on the use of PRA existed at that time. [50] The licensees were relying on new technology and PRA to demonstrate plant safety in response to the UCS petition. These PRAs followed the first nuclear power plant PRA of the Oyster Creek Generating Station in 1979 [51] and were conducted in the immediate aftermath of TMI-2.

This was a courageous move by an industry not known for taking risks - a move that provided a step change in PRA technology and methodology. The incentive to demonstrate plant safety was monumental to prevent other high-population sites from having to shut down their plants. Nonetheless, initiating a PRA was a substantial demonstration of confidence in the process. [52]

But the use of PRA was not just an 'exploratory' or 'novel' research activity. The years of successful operation, compliance and certification documentation (including safety analysis reports, the NRC's Safety Evaluation Report, and many other reports associated with licensing) were judged by the licensees to be insufficient evidence to rebut the petition.

2.3.2.2 Plant Characteristics

The two Zion reactors examined by the PRA (Units 1 and 2) were essentially identical 1,040 megawatt (MW) four loop Westinghouse PWRs with startup dates of June and December 1973 respectively.

---

[50] B. John Garrick, "PRA-Based Risk Management: History and Perspectives," *Nuclear News*, 2014, http://www.ans.org/pubs/magazines/download/a_940.

[51] B. John Garrick and et al., "OPSA—Oyster Creek Probabilistic Safety Analysis."

[52] At about the same time, Philadelphia Electric Company commissioned a PRA on the Limerick Generating Station with Nuclear Utilities Services Corporation having the lead. This is another example of industry taking the initiative.

The plant's cylindrical containment structure had a shallow dome roof and a flat foundation slab. The cylindrical portion was pre-stressed by a post tensioning system consisting of horizontal and vertical tendons. A leak-tight steel plate membrane internally lined the entire structure. The containment enclosed the entire primary coolant system, consisting of the reactor, steam generators, reactor coolant loops, and portions of the auxiliary and engineered safety features systems. [53]

The IPEC reactors examined by the PRA were similar to those from the Zion Plant. Both reactors (Units 2 and 3) were similar four loop Westinghouse PWRs with generating capacities of 1,032 and 1,051 MW and completion dates of 1974 and 1976, respectively. Both reactors had containment structures consisting of four to six feet thick steel-reinforced concrete with carbon steel liner. They enclosed the same systems that the Zion containment structure enclosed.

2.3.2.3 The conduct and outcomes of the PRAs

The PRA team included plant owner-operators, Westinghouse, and Fauske and Associates. The RSS offered the hope of something more rigorous than the existing safety cases. However, it became clear that the RSS methodology needed to be "tweaked." The RSS goal was an understanding of the entire nuclear industry risk: "what is the risk associated with the operation of 100 nuclear power plants in the United States?" This was not plant-specific risk, and consequently did not align with the goals for Zion and IPEC.

The Zion-IPEC PRAs built on RSS methodologies, adding to the discipline through initiatives such as including the "triplet definition

[53] The Zion Nuclear Power Station was retired on February 13, 1998.

of risk," [54] explicitly adopting Bayesian methods, [55,56,57] developing a scenario approach to risk assessment, and creating a matrix formalism for assembling the plant, containment, and site models (a process later labeled as a Level 3 PRA.) The matrix also allowed rigorous diagnostics to facilitate importance ranking of scenarios, model inputs and output states.

Methods were developed to integrate and propagate uncertainties and external events through the model. Atmospheric dispersion methods accounting for directional dependence and terrain-specific features were also developed, along with the introduction of numerous analytical aids. Terms such as "master logic diagram" and "plant damage states" were used for the first time, which included the most comprehensive assessment of containment capability to that point with the use of the first containment event tree.

The peer review of these PRAs was extensive, including an independent review group of PRA scientists and engineers, the Advisory Committee on Reactor Safeguards, the NRC staff, various national laboratories, the ASLB and its consultants, and intervener groups. [58]

The signature achievement of the Zion-IPEC PRAs was the rigor of the containment response analysis. While PLG provided the event tree framework for the containment response analysis, the collaboration of Westinghouse and Fauske and Associates provided a depth to set it apart from previous studies. This became the model of all subsequent PRAs.

---

[54] Kaplan, S. and Garrick, B.J., "On the Quantitative Definition of Risk" *Risk Analysis* 1, no. 1 (1981): 11–27.

[55] Apostolakis, G., "Probability and Risk Assessment: The Subjectivistic Viewpoint and Some Suggestions," *Nuclear Safety*, 19:305-315, 1978.

[56] Apostolakis, G., Kaplan, S., Garrick, B.J. and Duphily, J.R., "Data Specialization for Plant Specific Risk Studies," *Nuclear Engineering and Design*, 56:321-329, 1980.

[57] Apostolakis, G. and Kaplan, S., "Pitfalls in Risk Calculations," *Reliability Engineering*, 2:135-145, 1981.

[58] H. Specter, "Lessons from the Indian Point Hearing," *Nuclear Safety,* 27, no. 3 (1986), http://www.osti.gov/scitech/biblio/5407889.

The knowledge gained by these PRAs was immense. For example, it was determined that the IPEC containment structure could stand a pressure greater than twice the nominal design pressure. Similar results were obtained for the Zion plant.

The ASLB hearings used the PRAs to conclude that the risk to nearby population centers was acceptable, thereby saving hundreds of millions of dollars in backfits. The PRAs showed the proposed backfits would have had a negligible impact on the overall risk and (more importantly) identified several other low-cost options with more significant risk impacts. The ASLB hearings set a precedent by using these PRA results as a legal basis to resolve regulatory issues.

The PRAs also identified plant-specific vulnerabilities with respect to internal fires and earthquakes. Without regulatory prompting, licensees modified their respective plants to mitigate these hazards. When owners are aware of the risk quantitatively, they are more motivated to resolve them. The NRC responded to this proactivity by launching their own internal research thrusts that included the risk contributions of seismic events and internal fires.

So, where do these studies fit in the historical development of PRA? While the RSS was the single most important advancement in PRA, a strong case exists for these PRAs collectively being the second. The plant-specific, rigorous studies performed on the Zion and IPEC nuclear power plants broadened the scope and had immediate impact on nuclear plant operation. The ASLB referred to the Zion-Indian Point PRAs as "watershed PRAs" because of their "pioneering" contribution. [59]

2.3.3 The Seabrook PRA

In the 1980s, the state of Massachusetts effectively interfered with the licensing of the Seabrook Station Nuclear Power Plant located in nearby New Hampshire. The proximity to Massachusetts resulted in the State and the Clamshell Alliance attempting to block plant licensing by refusing to participate in the development of emergency plans. At issue was the ability to safely evacuate a nearby beach and Massachusetts' towns within the 10-mile Emergency

[59] F. J. Schon, O. H. Paris, and J. P. Gleason, "Opinion and Recommendations to the Commission on Societal Significance of Risk Estimates," Syllabus in the Matter of the Indian Point Special Proceedings, Dockets 50-247G and 50-286G, October 24, 1983, NRC Public Document Room.

Planning Zone (EPZ) created after the TMI-2 accident. This change was implemented during the plant's construction which was based on the previous requirement based on a much smaller Low Population Zone (LPZ).

The Seabrook Station is approximately 40 miles north of Boston and less than 2 miles from the Massachusetts border in Seabrook, New Hampshire. Westinghouse supplied a 1,296 MW reactor for the first unit, which began full power operation in 1990. A second unit was never completed due to delays, cost overruns, and finance difficulties. The original owner was Public Service of New Hampshire with the plant currently 88.2 per cent is currently owned by NextEra Energy Resources. The remaining share of the plant is owned by municipal utilities in Massachusetts.

The Seabrook PRA [60] followed the Zion-IPEC studies - but with some important extensions. These extensions included an assessment of a double containment system, development of accident management procedures (including emergency planning strategies) and the first (albeit limited scope) evaluation of the risks associated with multi-unit accidents. The Seabrook PRA also resolved the licensing impasse described above.

The plant containment system is a double-dome of concrete and steel construction. The inner dome is 4.5 feet thick, 140 feet high and provides primary containment against severe accident loads and external hazards. The outer dome is 15 inches thick, 180 feet high and provides an additional level of confinement for radiological releases. The "containment/confinement" design was required to meet the site boundary dose requirements to effectively eliminate the need for Massachusetts' involvement in licensing emergency planning development.

2.3.3.1 The conduct and outcome of the PRAs

The PRA was based on the RSS's scenario based approach, implementing the "risk triplet" framework [61] with extensions based on the Zion-IPEC PRAs.

THE SEABROOK LEGACY

The legacy of the Seabrook PRA is its depth and breadth of analysis and the vision it portrayed of things to come in the future. This vision included the need to extend PRA scope to enhance recovery, emergency planning and response, and accident management. The PRA scope also needs to consider the interaction of multiple units during natural disasters and accidents that not only impact the plants, but the site, its accessibility, and the rest of the supporting infrastructure. While there is much more to be done in all these areas, the Seabrook PRA has pointed the way for many of them.

[60] Pickard Lowe and Garrick Incorporated, "Seabrook Station Probabilisic Safety Assessment," Prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, December 1983.

[61] B. John Garrick and Robert F. Christie, *Quantifying and Conrolling Catastrophic Risks,* Academic Press, 2008.

An early application of the PRA was an emergency planning study that quantified the risk reduction benefits of emergency actions. These included limiting power operation during summer months when the beach population was high, and many variations of evacuation and sheltering to various distances from the site.

The PRA showed that the primary containment pressure capacity allowed acceptably low frequencies of large, early releases caused by a severe accident. The primary containment was designed to withstand a military aircraft crash, meaning the pressure capacity margins were higher than any other United States LWR.

Offsite risk consequences with no evacuation turned out to be significantly lower than those assessed by the NRC and the United States Environmental Protection Agency (EPA) when they set the EPZ requirement to 10 miles. [62] It was eventually demonstrated that either sheltering or evacuating out to 1 mile within the original evacuation zone was sufficient to meet requisite risk reduction benefits. [63]

The outer confinement was found to provide negligible benefits in limiting releases if the primary containment failed (noting the former was never designed to function when the latter failed.) When the primary containment is functional, the releases were found to be negligible regardless of the functionality of the outer confinement. The PRA also demonstrated that the primary containment radius grew at median pressure capacity [64] to an extent that the outer confinement would rupture. The only benefit of the outer confinement was the reduction of releases associated with intact primary containment with functional heat removal systems. Even in this scenario, primary containment releases would be very low.

[62] H. E. Collins, B. K. Grimes, and F. Galpin, "Planning Basis for the Development of State and Local Government Radiological Emergency Response Plans in Support of Light Water Nuclear Power Plants," *ResearchGate*, December 1, 1978, doi:10.2172/5765828.

[63] It should be noted that years later the Fukushima event provided invaluable experience for new strategies and thinking on evacuation.

[64] Pressure at which the probability of containment failure due to overpressure reaches 0.5.

2.3.3.2 The New Legacy

The Seabrook PRA was among the first to demonstrate how the RSS methodology and the lessons learned from the Zion-IPEC PRAs can be extended to develop accident management procedures. The event sequence diagrams (scenarios originally developed to support the PRA) were expanded to identify key accident management strategies for SBO sequences that progressed beyond the point assumed by the existing emergency operating procedures. The strategies derived during the Seabrook PRA were the starting point for the accident management procedures now employed in all the Westinghouse and Mitsubishi PWR plants.

An issue that remains important today is the development of risk models that account for multiple units on the same site. [65] In this regard, the Seabrook PRA was ahead of its time. A model of initiating events and accident sequences involving accidents on both units was developed. CCF models and supporting data analyses for the single unit PRA were refined for Emergency Diesel Generators (EDGs) and motor operated valves to distinguish between failures of components within and between the reactor units. The source terms for severe accidents involving a single unit were simply doubled to get a bounding estimate on multi-unit accident consequences.

An important insight was that the likelihood of a multi-unit accident approaches that of a single unit accident as initiating events (such as seismic events and loss of offsite power) challenge units concurrently. Critically important lessons were subsequently learned from the Fukushima accident, not only about the interaction of multiple units, but also about the interaction between the units and the site that reinforced what was discovered during the early 1980s.

The Seabrook PRA was the first to analyze CCF data for the electrical breakers in a PWR reactor protection system. This analysis yielded an estimated high frequency of a PWR ATWS event and in this way foretold the actual ATWS events that occurred at Salem some 6 months later in 1983. The CCF data analysis in the Seabrook PRA for

[65] Canadian Nuclear Safety Commission, "Summary Report of the International Workshop on Multi-Unit Probabilistic Safety Assessment," July 16, 2015, https://www.cnsc-ccsn.gc.ca/eng/resources/research/technical-papers-and-articles/2015/2015-multi-unit-safety-assessment.cfm.

all active redundant components in a nuclear power plant provided the basis for a major EPRI sponsored research project led by PLG which produced the first industry CCF database and the methods currently used in PRAs for CCF modeling and data analysis. The Seabrook PRA formed the basis of a major Electric Power Research Institute (EPRI) project that produced the CCF methods and data currently used in most international PRAs. [66]

The Seabrook PRA was the first to include a comprehensive treatment of accidents during low power and shutdown that included mechanistic source term development, Level 3 assessment of radiological consequences, and a full spectrum of internal and external hazards.

2.3.3.3 The Challenges

The licensing issue was eventually resolved by a combination of the Seabrook PRA results and a new NRC rule that enabled emergency planning without Massachusetts' participation. The PRA also exposed flaws in previous emergency and accident management procedures, such as the primary system emergency depressurization procedures in place at that time did not include SBO scenarios. This flaw was demonstrated 28 years later in the response to the Great East Japan Earthquake and tsunami of March 11, 2011 that severely damaged the Fukushima-Daiichi Nuclear Power Plant.

The Seabrook PRA was motivated not only by the desire to quantify the risk, but to demonstrate that emergency planning did not require evacuation - a major and unprecedented achievement. Its legacy is its depth and breadth of analysis and the vision it portrayed for the future generation of risk models. This vision included enhancing recovery, emergency planning and response, and accident management. It also demonstrated the need to consider the interaction of multiple units during natural disasters and accidents in a way that separately looks at the plants and the

[66] A. Mosleh et al., "Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Procedural Framework and Examples," *ResearchGate*, January 1, 1988, https://www.researchgate.net/publication/236371031_Procedures_for_treating_common_cause_failures_in_safety_and_reliability_studies_Procedural_framework_and_examples.

site infrastructure. While there is much more to be done in all these areas, the Seabrook PRA continues to point the way.

2.3.4 Early Rule Changes

The fundamental design and operational characteristics of United States nuclear power plants are governed by the NRC's Code of Federal Regulations (CFR), Title 10 Part 50 (CFR 50). [67] Each of these regulations is referred to as a "rule." Almost all of these rules were established before PRA methods were developed, meaning they were primarily deterministic and prescriptive. Modifying these rules was necessary to benefit from risk-informed approaches.

While the studies and events of the 1970s primarily illustrated the value of PRAs, they also pointed out the importance of operating experience reviews which had been demonstrably inadequate before the TMI-2 accident. Two events in the early 1980s reopened the issue of reactor protection system reliability and the likelihood of ATWS with subsequent core meltdown. A condition in the reactor protection system hydraulic controls of the Browns Ferry Nuclear Power Plant prevented the full insertion of about half of the control rods. A different condition in the electrical portion of the Salem Nuclear Power Plant reactor protection system prevented an automatic shutdown that should have occurred as a result of an instrumentation signal.

There were also emergency AC power system issues. A number of nuclear power plants experienced complete losses of offsite AC power, some of which were lengthy. Some plants experienced both offsite and onsite AC power loss, albeit for short durations. Further, diesel generators were demonstrating lower than expected reliabilities during tests.

These events spurred an impetus for change. Change faced significant challenges which included understanding the technical aspects of the events and their significance to other plants and designs, assessment of the adequacy of the then NRC regulatory general design criteria, consideration of the need for additional rules (which tend to be more generic) versus the imposition of plant-specific requirements, and understanding the risk associated

EARLY RULES

The two rules governing Anticipated Transients Without Scram (ATWS) and Station Blackout (SBO) were established in the 1980s. They reflected early knowledge of accident risks combined with the review of operating experience. They have been effective in improving nuclear power plant safety ever since.

[67] "NRC: 10 CFR Part 50—Domestic Licensing of Production and Utilization Facilities," accessed November 29, 2016, http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/.

with such operational events. Ultimately, two new rules were established.

2.3.4.1 Rule 10 CFR 50.62: Anticipated Transients without Scram (ATWS)

ATWS for BWRs was among the accident sequences the RSS identified as having a higher risk than previously thought. The NRC proposed a rule in late 1981 to: [68]

> *… reduce the likelihood of failure of the reactor protection system to shut down the reactor (SCRAM) following anticipated transients and to mitigate the consequences of Anticipated Transient without Scram (ATWS) events [and thereby] reduce the risk.*

The proposed rule (in an unusual approach) included three alternative regulatory solutions: two of which were developed by the NRC, and one developed by the nuclear industry. Comments were requested for each. The first NRC approach was basically deterministic while the second NRC approach advocated a "reliability assurance" program based on risk analysis concepts. The third approach set out by the nuclear industry included more specific, deterministic changes.

All approaches generated substantial positive and negative comment. The NRC's final rule was similar to industry's deterministic proposal, but included a statement encouraging (while not requiring) utilities to develop and use a reliability assurance program to minimize reactor protection system failure likelihoods. [69]

2.3.4.2 Rule 10 CFR 50.63: Station Blackout (SBO)

SBO for PWRs was similar to ATWS in that it was among accident sequences identified by the RSS with higher risk than previously thought. The NRC issued a proposed rule in 1986 to: [70]

---

[68] (NRC), "Nuclear Regulatory Commission," November 24, 1981, https://loc.heinonline.org.

[69] (NRC), "Nuclear Regulatory Commission," June 26, 1984, https://loc.heinonline.org.

[70] (NRC), "Nuclear Regulatory Commission," March 21, 1986, https://loc.heinonline.org.

> *… require that light-water-cooled nuclear power plants be capable of withstanding a total loss of alternating current (AC) power (called "station blackout") for a specified duration and maintaining reactor core cooling during that period.*

The proposed rule further noted that its objective was to:

> *… reduce the risk of severe accidents resulting from station blackouts by maintaining highly reliable AC electric power systems and, as additional defense-in-depth, assuring that plants can cope with a station blackout for some period of time.*

The supporting documentation, including a proposed regulatory guide, [71] discussed the proposed rule's basis which included risk information from the RSS and operating experience (discussed above). The approach included both deterministic and probabilistic aspects, with the latter including quantitative reliability targets for diesel generators and a plant-specific PRA of SBOs that would determine the implementation approach.

Following a public comment, the NRC issued the final rule, [72] essentially maintaining the approach set out in the proposed rule - including the risk approach.

The 1980's saw considerable growth in the number and quality of PRAs. This is reflected by the differences in these two rules. While the earlier ATWS rule discussed risk in a more general context, the later SBO rule incorporates risk and PRA results more directly.

2.3.4.3 Legacy

While there was little disagreement on the significance of the preceding operating events, there was significant disagreement on

[71] (NRC), "Nuclear Regulatory Commission," June 21, 1988, https://loc.heinonline.org.

[72] U.S. Nuclear Regulatory Commission, "Regulatory Guide 1.155 (Task SI 501-4) Station Blackout" (Washington DC: Nuclear Regulatory Commission, August 1988).

the need and form of the new rules. This disagreement was evident in the comments received by the NRC.

The establishment of these rules is reflected in all subsequent PRAs, including the Individual Plant Examinations (IPEs) (Section 2.3.6), and the NUREG-1150 Study (Section 2.3.7). Perspectives on the effectiveness of the rules are provided in the NRC staff review of IPEs, [73] and in a specific review of the effectiveness of the SBO rule. [74]

The accident scenarios of concern for these two rules are now monitored in the NRC's Reactor Oversight Process (ROP) (Section 2.4.6). The set of ROP Performance Indicators (PI) includes some related to the frequency of an ATWS accident (such as unplanned scrams per 7000 critical hours) and some related to the frequency of an SBO accident (such as emergency AC power reliability.) [75] This and other information are used to provide a statement on individual plant performance [76] and to provide industry-wide perspectives on issues such as reliability.

2.3.5 Quantitative Health Objectives (QHOs) - 1986

The President's Commission on the Accident at Three Mile Island recommended that safety goals be established. The ACRS recommended in 1979 that the NRC consider establishing nuclear power plant quantitative safety goals. The ACRS also recognized the difficulties and uncertainties in quantifying risk, acknowledging that engineering judgment would often be the primary decision basis. [77] Nevertheless, the ACRS believed that the existence of quantitative

[73] "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance." (Nuclear Regulatory Commission, Division of Systems Technology, December 1, 1997), http://www.osti.gov/scitech/biblio/569126.

[74] "NRC: Regulatory Effectiveness of the Station Blackout Rule (NUREG-1776)," accessed November 27, 2016, http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1776/.

[75] Chapter 0308 of "NRC: Inspection Manual Chapters," accessed November 27, 2016, http://www.nrc.gov/reading-rm/doc-collections/insp-manual/manual-chapter/.

[76] Nuclear Regulatory Commission, "Individual Plant Performance Summaries," 2016, https://www.nrc.gov/NRR/OVERSIGHT/ASSESS/.

[77] ACRS letter to NRC Chairman Hendrie on quantitative safety goals, May 1979.

safety goals and criteria could provide important yardsticks for such judgment.

The first set of trial goals was developed by the ACRS in 1980. [78] These safety goals were the basis for the NRC Safety Goal Policy in 1983. [79, 80] The policy established goals that broadly defined acceptable radiological risk levels. It answered the question of "how safe is safe enough." This statement is effectively the culmination of work started by Farmer on the "limit line" as a criterion for acceptable risk. (Section 2.1.3).

Numerous PRAs created the need to understand "acceptable" nuclear plant radiological risk, particularly with respect to the public. The NRC Safety Goal Policy Statement satisfied this need. [81]

In developing the policy statement, the NRC sponsored two public workshops in 1981, obtained public comments, held four public meetings in 1982, conducted a 2-year evaluation and received views from its ACRS during the period 1983-1985. The NRC determined that the qualitative safety goals remained unchanged from its March 1983 revised policy statement and adopted them as the safety goals for the operation of nuclear power plants. The policy statement was also informed by the recommendations of the President's Commission on the Accident at Three Mile Island.

2.3.5.1 Implementation

The NRC established two qualitative safety goals that are supported by two quantitative objectives. These goals were initially published in January 1983 and were finally published in the Federal Register

[78] U. S. Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, *An Approach to Quantitative Safety Goals for Nuclear Power Plants* (The Committee, 1980).

[79] Nuclear Regulatory Commission (NRC), "Safety Goals for Nuclear Power Plants: A Discussion Paper" (Nuclear Regulatory Commission, 1982), http://inis.iaea.org/Search/search.aspx?orig_q=RN:14724072.

[80] Nuclear Regulatory Commission (NRC), "Safety Goals for Nuclear Power Plant Operation" (Nuclear Regulatory Commission, 1983), http://inis.iaea.org/Search/search.aspx?orig_q=RN:14792318.

[81] United States Nuclear Regulatory Commission, "Policy Statement on Safety Goals for the Operation of Nuclear Power Plants" (Washintong DC: Nuclear Regulatory Commission, August 21, 1986).

in 1986, after a series of public meetings. The qualitative goals state that:

> *Individual members of the public should be provided protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life or health,*
>
> *[AND]*
>
> *Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.*

The quantitative goals or QHOs (which are sometimes referred to as "quantitative design objectives") of the NRC Safety Goal Policy are:

> *The "prompt fatality" risk to an average individual in the vicinity of a nuclear power plant that might result from reactor accidents should not exceed 0.1 percent of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed (approximately 5 x 10^{-7} probability per year)*
>
> *[AND]*
>
> *The "cancer fatality" risk to the nuclear power plant local population that might result from nuclear power plant operation should not exceed 0.1 percent of the sum of cancer fatality risks resulting from all other causes (approximately 2 x 10^{-6} probability per year)*

The NRC believed that establishing a level of safety considered to be "safe enough" would enhance public understanding of regulatory criteria and public confidence in nuclear power safety. It is important to note that the QHOs are aspirational guidance (the "Backfit Rule" discussed in subsection 2.3.8 uses them explicitly).

In August 1986, the NRC approved a performance guideline as a basis for determining whether a level of safety ascribed to a plant is consistent with the safety goal policy:

"Consistent with the traditional defense-in-depth approach and the accident mitigation philosophy requiring reliable performance of containment systems, the overall mean frequency of a large release of radioactive materials to the environment from a reactor accident should be less than 1 in 1,000,000 per year of reactor operation."

The NRC provided additional guidance in 1989. [82] In 1993, the NRC concluded that defining large release beyond a simple qualitative statement related to its 10^{-6} per reactor year release frequency was neither practical nor required for regulatory or design purposes. Further work on the development of a large release risk definition and magnitude was consequently terminated.

Because these high-level objectives were impractical for regulatory decision making, subsidiary goals for CDF and Large Early Release Frequency (LERF) were established. Using these metrics as the basis for determining plant safety was considered consistent with the safety goal policy statement. The subsidiary goals of 10^{-4} and 10^{-5} per reactor year for CDF and LERF respectively were consistent with the QHOs above and continue to be a target for risk-informed regulations and applications. [83,84]

2.3.5.2 Challenges

While the safety goals address the question of "how safe is safe enough", practical implementation of the NRC's guidance proved difficult. This was due to the large uncertainties in risk calculations. Utilities did not know how to implement or demonstrate compliance with the safety goals, primarily delegating this responsibility to reactor vendors. All this occurred before the establishment of national consensus PRA standards.

---

[82] Nuclear Regulatory Commission (NRC), "Implementation of the Safety Goals" (1989, n.d.).

[83] The significance of the goals and objectives, their bases and rationale, the plan to evaluate the goals and public comments are provided in Nuclear Regulatory Commission (NRC), "Safety Goals for Nuclear Power Plant Operation."

[84] United States Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions on Plant Specific Changes to The Licensing Basis," RG 1.174, May 2011.

As the scope of PRA grew to include hazards beyond internal events (such as fire, seismic events, and flooding), a reduction in the margin between plant specific baseline risks and safety goals has become more challenging. This is partially due to the conservatisms used to quantify those hazards.

2.3.5.3 Stakeholder Reactions

Generally, the various architect engineers, utilities and vendors endorsed the NRC policy statement. Some utilities began to develop preliminary PRAs to determine whether there were any significant severe accident contributors.

The IDCOR Program was formed under the sponsorship of the Atomic Industrial Forum and later the Nuclear Energy Institute (NEI) to evaluate severe accident risk for existing reactors. The IDCOR group developed new computer models for assessing the severe accident risk based on available data. Four of the six NRC's Severe Accident Research Program's "Source Term Reference Plants" were used as a basis for developing the models.

The NRC performed special PRA studies (such as NUREG-1150, which is discussed Section 2.3.7) to improve PRA methods. NRC initiated IPEs and IPEs for External Events (IPEEEs) to identify vulnerabilities and assess "outliers" using RSS methods (with limited scope.) The NRC now requires all new plants to have a PRA.

At the 2001 Atomic Energy Society of Japan and American Nuclear Society Topical Meeting on Safety Goals and Safety Culture, NRC Chairman Richard A. Meserve described how the NRC viewed safety goals, safety culture and their interaction. He stated his belief that a strong safety culture, augmented by an appreciation for the risk implications of actions of both licensee and regulatory organizations, assist the development and maintenance of excellence in nuclear plant operational safety. [85]

The IAEA published 75-INSAG-3 in 1988, stating that the general nuclear safety objective was:

> *… [to] protect individuals, society and the environment by establishing and maintaining in*

[85] Richard A. Meserve, Atomic Energy Society of Japan/American Nuclear Society Topical Meeting On Safety Goals And Safety Culture, 2001.

nuclear power plants an effective defence against radiological hazard.

The objective was deemed met when nuclear power plant risk did not exceed that associated with competing energy sources. By extension, it became necessary to use PRA models and quantitative targets or safety goals. [86]

2.3.5.4 Legacy

Over-regulation potentially robs licensees of a sense of "ownership" of plant safety performance, which generally degrades commitment and results. Under-regulation has its own obvious set of perils. A balance must exist. Part of this balance is an appreciation of the role of licensee safety culture and safety goals.

The 1984 PRA reference document "Probabilistic Risk Assessment (PRA): Status Report and Guidance for Regulatory Application" (NUREG-1050) was a product of the safety goal evaluation program. [87] This document contains an extensive discussion of past PRAs results, strengths, weaknesses, and uncertainties. The way PRA supports regulatory analysis and the implementation of severe accident requirements was tailored based on the results of this report.

Risk is only one factor that guides regulatory decisions. The relationship of risk to defense-in-depth, safety margin, and how they complement the decision making process, was part of later work in Regulatory Guide RG 1.174. [88]

An early example of explicit consideration of risk in regulation is the NRC's Backfit Rule (Section 2.3.8), originally issued in 1988. More comprehensive application of risk in regulation has occurred since. The aim is to use risk to reform the regulatory system so that the NRC focuses on risk-significant activities - enhancing safety and

[86] IAEA, "Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1," 1999, http://www-pub.iaea.org/books/IAEABooks/5811/Basic-Safety-Principles-for-Nuclear-Power-Plants-75-INSAG-3-Rev-1.

[87] U. S. Nuclear Regulatory Commission Division of Risk Analysis, *Probabilistic Risk Assessment (PRA): Status Report and Guidance for Regulatory Application, Draft Report for Comment* (Division of Risk Analysis, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1984).

[88] United States Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to The Licensing Basis." Regulatory Guide 1.174.

reducing needless regulatory burden. In implementing this approach, the NRC still adheres to many concepts discussed in the original Safety Goal Policy Statement, such as risk being one factor of many for regulatory decisions.

A STEP FORWARD

The IPE and IPEEE initiatives provided assurance that any major severe accident vulnerability would be identified and addressed. Through this effort, United States utilities were able to build baseline PRA models, acquiring the technical expertise to assume technical ownership and stewardship of nuclear power plant risk models.

2.3.6 Individual Plant Examinations (IPEs) and Individual Plant Examinations for External Events (IPEEEs)

In its 1985 policy statement, the NRC concluded that existing plants posed no undue risk to the public health and safety and that there was no basis for immediate action on any regulatory requirements for these plants. However, the NRC recognized (based on experience with plant-specific PRAs) that systematic examinations are beneficial in identifying plant-specific vulnerabilities that could be mitigated through modification.

The NRC developed regulatory programs and initiatives as part of the Integration Plan for Closure of Severe Accident Issues. This Integration Plan included IPEs, IPEEEs, Severe Accident Research and Accident Management Programs.

> *[The] NRC expected that a site-specific consideration of severe accident mitigation for license renewal will only identify procedural and programmatic improvements (and perhaps minor hardware changes) as being cost-beneficial in reducing severe accident risk or consequence.* [89]

These programs and initiatives were intended to provide assurance that any major plant specific severe accident vulnerability would be identified and addressed.

In 1988, the NRC issued Generic Letter 88-20 requesting that each licensee conduct an IPE. As a generic letter, all licensees are required to provide a formal response.

IPEs were probabilistic analyses that estimated CDF and containment performance for internally initiated accidents (including internal flooding, but not internal fires). IPEs allowed licensees to appreciate severe accident behavior, understand likely severe accident sequences, more quantitatively understand CDF

[89] "NRC: Generic Environmental Impact Statement for License Renewal of Nuclear Plants—Final Report (NUREG-1437, Revision 1)," accessed November 28, 2016, http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1437/r1/.

and fission product release frequency, and (if necessary) reduce these frequencies by modifying hardware and procedures.

It was reasoned that more utility participation would make effective follow-up actions more likely. Utilities also desired solutions to severe accident issues and viewed IPEs and IPEEEs as useful in this regard.

2.3.6.1 Implementation

Generic Letter 88-20 consisted of four supplements listed below. Licensees were instructed to perform analysis to identify vulnerabilities to severe accidents.

- Supplement 1: Initiation of The IPE For Severe Accident Vulnerabilities-10 CFR 50.54(F).
- Supplement 2: IPE.
- Supplement 3: Completion of Containment Performance Improvement Program and Forwarding of Insights for Use in the IPE for Severe Accident Vulnerabilities
- Supplement 4: IPEEE for Severe Accident Vulnerabilities. This supplement specifically requested licensees to perform an IPEEE with respect to seismic events, internal fires, high winds, floods, transportation accidents, nearby facility accidents, and plant-unique hazards.

Some utilities performed a Level 1 and 2 PRA to satisfy the requirements for IPEs and IPEEEs. Others implemented an IDCOR IPE methodology, which the NRC considered as acceptable.

It was recognized that IPEs and IPEEEs could identify the need for and be expanded to undertake a PRA. The NRC determined that it was premature to require all utilities to develop full scope PRAs due to the associated time and the lack of consensus standards. License amendment request procedures for incorporating PRAs (such as risk-informed applications) were yet to be developed.

2.3.6.2 Challenges

The IPEs and IPEEEs required substantial licensee effort. Different technical methods and approaches were used, making best-practice consensus difficult. It also resulted in variable results for similar reactor types.

The NRC delayed the issuance of the request for IPEEE until relevant external hazards had been identified, acceptable examination methods had been created, procedural guidance was developed, and industry and public input had been solicited through workshops.

Among the challenges was the lack of definition for "vulnerability," a key term used in Generic Letter 88-20. Licensees were asked to determine whether a vulnerability existed and whether corrective actions were needed. There was variability in technical approaches, making CDF comparisons between similar reactor designs difficult. Most utilities reported CDFs and containment failure probabilities in the form of point estimates, not mean values and without a characterization of uncertainty.

2.3.6.3 Stakeholder Reaction

The nuclear industry frequently met with the NRC to determine acceptable approaches to resolve the severe accident issue. It was recognized that IPEs and IPEEEs would require substantial industry and NRC effort over a number of years. In 1988, the Nuclear Management and Resources Council (NUMARC) [90] indicated to the ACRS that the industry was ready to proceed with IPEs and IPEEEs. Over the next several years, this process enabled utilities to build plant-specific baseline PRA models and acquire (through technology transfer efforts) the technical expertise to maintain and develop plant-specific PRAs.

2.3.6.4 Legacy

The NRC received 75 IPEs for 104 nuclear power plants. Key conclusions were: [91]

- Licensees identified severe-accident "vulnerabilities" and considered more than 500 mitigating plant improvements.
- Some licensees performed PRAs to determine risk reduction, as well as the cost and benefit of improvements.

The NRC received 70 IPEEEs covering all operating nuclear reactors. The NRC then instituted a program to identify and document

[90] NUMARC is now known as the Nuclear Energy Institute (NEI).

[91] "Individual Plant Examination Program."

general perspectives and significant safety insights resulting from the IPEEE program. Key observations included: [92]

- earthquakes and fires were important contributors to CDF,
- offsite power and electrical system failure were the most common contributors to seismic initiated CDF, and
- control-room fires, switchgear rooms, cable-spreading rooms, and turbine-generator building fires were the most common contributors to CDF.

The IPE and IPEEE program integrated the intent outlined in Supplement 3 of Generic Letter 88-20 regarding containment performance improvements. This introduced a focus on resolving hardware and procedural issues related to generic containment challenges. Generally, results from the Supplement 3 effort were related to severe accident management actions and not related to structural issues.

Licensees were not requested to calculate offsite health effects: most of the IPE results cannot be directly used to demonstrate compliance with QHOs. All licensees estimated two related risk measures: containment failure frequencies and radionuclide release frequencies. These results were compared with other studies of similar scope – such as NUREG-1150. [93] In this (indirect) way, risk management insights from the IPEs and IPEEEs and the plant-specific risks were evaluated and compared to the NRC's safety goals.

2.3.7 The NUREG-1150 Study - 1987

The NUREG-1150 "Severe Accident Risks: An Assessment for Five United States Nuclear Power Plants" study was a major NRC effort to view system behavior and phenomenological aspects of severe accidents from a risk perspective. [94] Importantly, it examined risk differences between different plants and designs. The goal was to

A MAJOR STUDY

The NUREG-1150 study was a significant turning point in the use of risk concepts in regulatory processes. It enabled the NRC to greatly improve its methods for assessing containment performance after core damage and accident progression. The methods and results from this study provided a valuable foundation in quantitative risk techniques.

[92] "NRC: Perspectives Gained From the Individual Plant Examination of External Events (IPEEE) Program - Final Report (NUREG-1742, Volume 1)," accessed November 28, 2016, http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1742/vol1/.

[93] "NRC: Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (NUREG-1150)," accessed November 21, 2016, http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1150/.

[94] Ibid.

describe acceptable technical PRA methods for addressing internal and external events. NUREG-1150 extended the RSS approach to include external events, uncertainty and expert judgment elicitation processes. The industry's Zion-IPEC methods were a valuable input to the study. The use of expert judgment was particularly challenging. The technical and academic community needed to be convinced that subjective opinion was a legitimate source of information for risk assessment.

NUREG-1150 ultimately showed that severe accident risk estimates were lower than those of the RSS through the use of improved data and sophisticated models. It was a significant turning point in the conceptual use of PRA for regulatory processes, enabling the NRC to greatly improve methods for assessing containment performance throughout accident sequences.

2.3.7.1 Implementation

A severe accident PRA (level 1, 2, and 3 internal and external events) was performed on five United States nuclear power plants: Peach Bottom Nuclear Generating Station, Surry Nuclear Power Plant, Sequoyah Nuclear Generating Station, Grand Gulf Nuclear Generating Station, and Zion Nuclear Power Station. The first two (Peach Bottom and Surry plants) were examined in the RSS. The risk contributors were measured in a number of ways, including:

- CDF initiated from both internal and external events for two plants,
- performance of containment structures under severe accident loadings,
- magnitude of potential radionuclide releases and offsite consequences, and
- overall risk.

In many respects, the five PRAs were performed using methods typical of the mid-1980s. More advanced techniques were developed in certain areas including:

- CDF uncertainty estimation emanating from system responses, severe accident progression, containment building structural response, and in-plant radioactive material transport;
- expert elicitation process and documentation;

- plant damage state definition (improving the efficiency of the accident frequency and progression analyses interface);
- integration of experimental and analytical results in radioactive material release assessment;
- more efficient methods for estimating CDF due to external events (such as seismic events); and
- new risk analysis and risk information integration computer models.

Expert panels were assembled to examine accident frequency analysis, reactor pump seal performance, in-vessel accident progression, containment loadings, molten core-containment interactions, containment structural performance, and source term.

A large number of reports and analyses from the technical community supported the study. The ensuing methods were subsequently used as a basis for the NRC's Generic Letter 88-20 (discussed in Section 2.3.6).

2.3.7.2 Challenges

Quantitatively characterizing risk remained the main challenge – an enduring feature of any PRA. The underlying technical challenges were associated with uncertainties in system or plant response, accident progression, containment performance, and radiological release. However, the largest challenge in terms of significance was convincing the technical community that the utilization of expert judgment was a legitimate source of information for PRA.

2.3.7.3 Stakeholder Reactions

The first study report received over 800 pages of comments. There were both a general appreciation of effort and concerns that the findings were already obsolete. Licensees were unconvinced about the study's value, concerned that it: [95]

- failed to consider significant industry sponsored research and analysis;

[95] Tennessee Valley Authority, "Comments on Draft NUREG-1150 (Reactor Risk Reference Document)," September 28, 1987, http://www.nrc.gov/docs/ML1111/ML111151348.pdf.

- involved lower bound probability estimates that exceeded comparable IDCOR values;
- overstated the risk due to early containment failure;
- overstated the magnitude of fission product releases;
- did not adequately represent the ability of operators to terminate or mitigate accidents;
- relied heavily on expert opinions of a limited and select group of individuals (which included no utility or vendor organization) with inadequate documentation;
- used inadequate Sequoyah Nuclear Power Plant models based on inappropriate assumptions; and
- demonstrated significant conservatism.

The draft of the following year substantially resolved these concerns. The NRC considered that the study advanced the state of the art in PRA, particularly in terms of uncertainty analysis. It also considered that the study's models, results, and risk perspectives could be used in a variety of regulatory applications including:

- a PRA Policy Statement,
- regulatory analysis guidelines validation,
- subsidiary numerical objectives validation,
- risk-informed rulemaking,
- prioritization of generic safety issues and nuclear safety research programs, and
- IPEs and IPEEEs.

2.3.7.4 Legacy

NUREG-1150 results were used in several areas of reactor regulation, including the development of alternative radiological source terms for design basis accident evaluation. NUREG-1465 was published in 1995 and defined an alternative accident source term for regulatory applications whose release fractions were based on NUREG-1150. [96]

[96] "NRC: Accident Source Terms for Light-Water Nuclear Power Plants (NUREG-1465)," accessed November 28, 2016, http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1465/.

The improved data and more sophisticated models used in the five PRAs produced severe accident risk estimates lower than those of the RSS. SBO and ATWS accidents (discussed in Section 2.3.4) were found to be major contributors to BWR CDF. Electrical power disturbances, small LOCAs, interfacing LOCAs and steam generator tube ruptures were found to be major contributors for PWRs.

A wide spectrum of phenomenological data was provided from both experimental and analytical models, such as information on hydrogen generation. The methods used in the study added depth to the accident management strategies at the time, especially in the explicit treatment of uncertainties.

2.3.8 Rule 10 CFR 50.109: The Backfit Rule

New information that questions existing approaches to nuclear power plant safety always arises over time. This new information can emanate from operating experience and research findings to name two. The NRC's ability to review new information that informs new requirements depends on its legislative mandate and internal processes to implement that mandate.

Modifications mandated by the NRC are known as "backfits." The NRC Backfit Rule was established in its current form in the mid-1980s. It provided stability to reactor regulatory processes in the context of new information. This risk-informed rule defines how nuclear power plant modifications should be evaluated in a way that does not impose overly burdensome regulation.

NRC experience indicates that PRA effectively measures potential plant modification benefit. This includes how the cost of a potential backfit (especially in relation to the amount of risk it retires) can be used to decide whether that modification will proceed. The rule outlines circumstances where backfits are not subject to cost analysis: [97]

> *… [t]wo types of exceptions, compliance exceptions and adequate protection exceptions, do not require findings of substantial safety improvements and costs are not considered.*

REGULATORY STABILITY

The NRC Backfit Rule is key to the stability of reactor regulatory processes. This risk-informed rule defines how nuclear power plant modifications should be evaluated, thus providing a stable process that helps ensure that licensees are not subject to overly burdensome regulation.

The backfit process is an effective approach for publicly considering and resolving reactor safety issues.

[97] "NRC: Backfitting Guidelines (NUREG-1409)," accessed November 28, 2016, http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1409/.

More specifically, the rule states:

> *… that economic costs cannot be considered (1) when a modification is necessary to bring a facility into compliance with Commission rules or written licensee commitments, (2) when regulatory action is necessary to ensure adequate protection of public health and safety, or (3) when the regulatory action involves defining or redefining the adequate protection standard.*

The NRC decides when these exceptions are invoked. The NRC published guidance in 2004 on decision criteria and the conduct of potential modifications using PRA. [98]

2.3.8.1 Challenges

The first challenge addressed by the rule was defining "backfit." Backfits are nominally those modifications proposed by the NRC, not modifications implemented solely by the licensee. For example, a licensee implementing an alternative solution for achieving the intent of a particular rule is not considered a backfit.

The next challenge was outlining when costs need to be considered. A regulatory authority's legislative mandate should define the authority's power to require a modification and how cost should be considered. The NRC's mandate has been tested in court, with an outcome that permits consideration of costs in certain circumstances and not others.

This created the third challenge: who is responsible (i.e., burden of proof) for defining the cost effectiveness of a backfit. If cost considerations are permitted, a decision is required as to where the burden of proof resides. The backfit process in the United States requires the NRC to characterize the associated costs and benefits.

The last challenge was measuring benefit and decision criteria. Characterization of a plant modification's potential benefit can be qualitative or quantitative. The NRC adopted an approach in the 1980s that included qualitative and quantitative considerations, using risk analysis methods to estimate the risk-reduction value of

[98] "NRC: Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission (NUREG/BR-0058, Rev. 4)," accessed November 28, 2016, http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0058/.

a proposed plant modification. Specific risk metrics used in this approach include CDF, conditional containment failure probability, and averted population dose risk.

2.3.8.2 Implementation

Several aspects of the backfit process have facilitated its implementation:

- **Structure established in a regulation.** The regulatory inclusion of the backfit process solidifies its importance and practice.
- **Public availability.** The NRC's backfit rule guidebook is publicly available, with modifications subject to public consultation.
- **Public review of the process.** Information used by the NRC to initiate a backfit is subject to public review and comment.

It is noteworthy that the rule uses risk information directly in the decision-making process when costs are considered. Risk information is used initially to disregard backfits that don't have "substantial" safety benefit. Risk information is subsequently used to quantify safety benefit (or risk reduction value).

2.3.8.3 Stakeholder reactions

Although the rule was established in the 1970s, the TMI-2 accident spurred important changes to the backfit rule in the 1980s. The NRC required licensees to implement a large number of backfits, some of which either didn't directly relate to the TMI-2 accident or had little safety benefit.

In response to stakeholder concerns, the NRC proposed a revision to the rule in 1983 that introduced new language. Specifically, the rule stated that backfits had to provide a "substantial increase" in safety. PRA methods and a regulatory process were then developed to define "substantial."

2.3.8.4 Legacy

The rule was released in 1985. The UCS legally challenged the NRC regarding when costs were considered in regulatory decisions. The NRC made its final modification to the rule in 1988 to clarify when costs could be considered, including costs related to PRA analyses. The rule is now considered mature, stable and effective.

2.3.9 Additional Industry Contributions

By the mid-1980s, the value of plant-specific PRAs had been made clear. A review of the PRA results available in 1984 confirmed the value of plant-specific analyses and offered several observations including: [99]

> *Experience indicates PRAs to be even more plant specific than was realized following the first few studies performed. The extent to which risk is plant specific was demonstrated by the differences in risk levels and contributors between Indian Point Units 2 and 3, which are sister plants.*

The report goes on to say:

> *Contributors to risk vary depending on the damage index adopted. Not only is there a difference in contributors to core melt frequency and health risk, but there are even differences in different types of health risk.*

2.3.9.1 Kuosheng Nuclear Power Plant (Taiwan)

The Kuosheng PRA was a Level 3 PRA like many others of that era. [100] The Kuosheng plant is near the ocean and surrounded by tall hills. The dispersion analysis code was modified to include a "particle transport" model to reflect the plume trajectories impacted by its unique topology. This was a key step in the evolution of dispersion modeling capabilities through accounting for multiple releases separated by release type, release location, elevation and timing. The treatment of close-in dispersion effects and multiple release points became a key element of multi-unit risk PRA.

2.3.9.2 Tennessee Valley Authority (TVA)

The TVA was also an early user of PRA, developing both in-house and collaborative PRA models (the latter involved specialized consultants) for the Browns Ferry Nuclear Power Plant, Sequoyah Nuclear Generating Station, Watts Bar Nuclear Generating Station

[99] B. John Garrick, "Recent Case Studies and Advancements in Probabilistic Risk Assessment," *Risk Analysis* 4, no. 4 (1984): 267–279.

[100] Pickard Lowe and Garrick Incorporated, "EPZ Determination for the Republic of China - Phase I: Preliminary EPZ for Kuosheng (Volumes 1 and 2)," Prepared for the Atomic Energy Council of the Republic of China, June 1990.

and Bellefonte Nuclear Generating Station. The TVA made three key contributions to the field of PRA.

Firstly, the TVA noted that the three Browns Ferry Nuclear Power Plant units shared systems. These included the electric power system, normal and emergency service water, firewater, and plant control air. "Loop selection logic" and "common accident signal logic" potentially impacted the availability of one division of ECCS on either Units 1 or 2. [101,102,103] Supporting the sequential return to service of the three units required unit-specific PRAs that accommodated the risk emanating from companion units returning to service. [104]

The second key contribution was the observation that the design of the Bellefonte Nuclear Generating Station included a significant dependence on solid-state control systems: both for ECCS and Balance of Plant (BOP) responses. The "limited scope" Phase 1 Level 3 Bellefonte PRA identified a lack of understanding of the solid state equipment thermal failure modes and thermal fragilities. [105]

The third key contribution was TVA's development of a success oriented PRA using the "GO" methodology developed for the Sequoyah Nuclear Generating Station. [106] The GO methodology was then used at other plants to assess the plant system operational

[101] If accident signals are present on both units (meaning high drywell pressure and sustained low vessel water level) one division of ECCS will be lost on each Unit 1 and Unit 2.

[102] Pickard Lowe and Garrick Incorporated, "Browns Ferry Nuclear Plant Unit 2 Probabilistic Safety Assessment with Unit 3 Operating," Prepared for the Tennessee Valley Authority (Decatur, Alabama, May 1996).

[103] Pickard Lowe and Garrick Incorporated, "Browns Ferry Multi-Unit Probabilistic Risk Assessment," Prepared for the Tennessee Valley Authority (Decatur, Alabama, January 1995).

[104] Pickard Lowe and Garrick Incorporated, "Browns Ferry Nuclear Plant Unit 3 Probabilistic Safety Assessment with Unit 2 Operating," Prepared for the Tennessee Valley Authority (Decatur, Alabama, May 1996).

[105] Pickard Lowe and Garrick Incorporated, "Bellefonte Unit 1 Phase I Probabilistic Risk Assessment," Prepared for the Tennessee Valley Authority (Knoxville, Tennessee, October 1985).

[106] Pickard Lowe and Garrick Incorporated, "Application and Comparison of the GO Methodology and Fault Tree Analysis," Prepared for The Electric Power Research Institute, December 1981.

status to assist plant operations and maintenance supervisors to comply with the "limited conditions for operation."

2.3.9.3 Three Mile Island Accident at Unit 2 (TMI-2) Response

The nuclear industry collaborated in response to the TMI-2 accident. The result was improved severe accident understanding, which was reflected in improved scenario definition of level 1 and 2 PRAs. [107] The IDCOR Program was developed in 1984 and produced methods to understand degraded core scenarios, complementing NRC work.

A key industry contribution was the adoption of symptom-based abnormal and emergency procedures, removing the "diagnosis" burden that earlier procedures placed on the operations staff.

2.3.9.4 Midland Nuclear Power Plant

PRA was used to improve the design of the Midland plant. The Midland PRA was used in an iterative manner to investigate plant changes until an acceptable balance of risk contributors was found. The STP was used as a basis to suggest changes in plant hardware and logic to improve safety. [108]

2.3.9.5 Beznau Nuclear Power Plant

The Beznau Nuclear Power Plant is the oldest continually operating commercial power plant in the world with two, two-loop PWR units. The authorities and licensee identified a number of costly modifications, but the PRA showed that many of these were expensive while only improving safety modestly. The PRA identified substantial risk reduction measures that were more cost effective. [109]

2.3.9.6 Oak Ridge High Flux Isotope Reactor (HFIR)

Use of PRA in design has extended beyond commercial nuclear power plants. HFIR uses uranium dioxide fuel dispersed in an aluminum matrix in the form of fuel plates. These plates are

---

[107] A **Level 1 PRA** estimates the frequency of accidents that cause damage to the nuclear reactor core. This is commonly called core damage frequency (CDF). A **Level 2 PRA**, which starts with the Level 1 core damage accidents, estimates the frequency of accidents that release radioactivity from the nuclear power plant.

[108] Pickard Lowe and Garrick Incorporated, "Survey of System Improvements for Application of Probabilistic Safety Assessments," Prepared for IEA of Japan, Ltd, August 1997.

[109] M. Richner and S. Zimmermann, "Applications of Simplified and of Detailed PSA Models," in *Probabilistic Safety Assessment and Management*, 1998.

approximately 50 mils thick with 50 mil coolant channels. The primary system is operated in a "water solid" condition with an original 1 MW per liter design power density. The high power density and the aluminum matrix make the fuel integrity sensitive to the rate of change in pressure.

Concerns surfaced in the late 1980s about vessel embrittlement. The design was changed to protect it from over-pressurization. Two small air operated valves were installed that would fail open on loss of air. The PRA quickly identified that "fail open" was only a "safe" failure mode from an over-pressurization perspective. Inadvertent opening of the valves (which would occur on loss of control air) initiated a plant response that was challenging to survive. The PRA then identified that the likelihood of vessel failure without the valves was low, leaving the valves in the "fail closed" position on loss of air. [110]

Another interesting element of the HFIR PRA concerns the integration of two portable AC power generators into the risk model. The loss of normal and emergency AC power was a prominent scenario for initiators such as earthquake and high wind. One of the portable generators required transport to the site via a road that (given a seismic or high wind scenario) might involve felled trees. This would impact delivery time. A probabilistic model was developed representing the transport, connection and operation of these generators under diverse site damage conditions. This analysis foreshadowed the evaluation of FLEX equipment now remotely stored to support United States' nuclear plants in response to severe conditions.

2.3.9.7 Legacy

While much of PRA's foundational contributions have come from United States industry, significant contributions originated internationally. Dr. Tadakuni Hakata was a senior manager in the safety department at Mitsubishi Heavy Industries when he

[110] Pickard Lowe and Garrick Incorporated, "The High Flux Isotope Reactor Probabilistic Risk Assessment: Analysis of the Risk from Internal and External Events," Prepared for Martin Marietta Energy Systems, Inc., August 1991.

commissioned the first comprehensive seismic PRA in 1989. [111] This exposure to PRA perhaps inspired Dr. Hakata (as an independent consultant) to develop a methodology and software to address multi-unit seismic risk based on simulation and correlation. [112] Following the 2011 Great Eastern Japan Earthquake, his method was expanded to include seismic and tsunami events. [113]

It was also identified after the RSS that human reliability analysis needed improvement. While much energy has been expended by both industry and regulators in this area, this subject requires ongoing effort.

The enduring legacy of industry contributions is substantial. An expanded database now exists which includes plant and site-specific data, along with improved methods for quantifying uncertainties due to lack of data. More accurate risk models for earthquakes, fires, floods, and winds have been developed. Improved analysis methods for damaged core phenomena and the role of engineered safety systems during an accident has also been studied. The RSS was analyzed to identify the extent of conservatism in its radioactive material release conclusions. And methods for full-scope, site-specific PRAs (such as the containment event tree and advanced dispersion models) were also developed by industry.

[111] Pickard Lowe and Garrick Incorporated, "Seismic and Fire Risk Analysis, Typical Japanese 4-Loop PWR Plant," Prepared for Mitsubishi Atomic Power Industries, Inc. (Tokyo, Japan, July 1988).

[112] Tadakuni Hakata, "Seismic PSA Method for Multiple Nuclear Power Plants in a Site," *Reliability Engineering & System Safety* 92, no. 7 (2007): 883–894.

[113] Tadakuni Hakata, D.H. Johnson, and W. Epstein, "Improvement of External Event (Tsunami Seismic) PSA Approach for Severe Accidents of Nuclear Power Plants" (American Nuclear Society, 2013).

Section 2.4: From the 1990s: The Growth of PRA

PRA continued to grow in terms of scale and sophistication. It transitioned from fighting to become an accepted methodology to becoming an embedded methodology. This required a number of actions such as standardization and guidance. In particular, methods for quantifying risk prompted questions about how safe nuclear power plants should be in terms of particular metrics.

Computational power also advanced in ways that allowed more sophisticated methodologies. Ultimately, PRA became more useful and accepted.

This section outlines the continued growth of PRA from a potential approach to risk to a valid way of ensuring safety.

2.4.1 Rule 10 CFR 50.65: The Maintenance Rule - 1991, 1999

In the early 1990's, NRC inspectors and managers identified licensee practices that were judged to potentially unacceptably reduce safety. This included a number of concerns with respect to maintenance programs that included inadequate root cause analyses, a lack of equipment performance trending, and a lack of RIDM in maintenance planning. NRC rules at that time were considered insufficient to address these concerns.

The NRC issued a rule to ensure proper maintenance practices at nuclear power plants in 1991 [114] – at a time when licensees had limited PRA capability. The rule was established using the "Backfit Rule" (as discussed in Section 2.3.8). It was judged that the rule would substantially increase public safety with justifiable costs.

The final rule was issued in 1999, which included more quantitative methods. [115] The NRC indicated that:

> *… during plant visits in mid-1994, several NRC senior managers expressed concerns that licensees were increasing both the amount and frequency of maintenance performed during power operation without adequately evaluating*

[114] Nuclear Regulatory Commission (NRC), "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," July 10, 1991.

[115] Nuclear Regulatory Commission (NRC), "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," July 19, 1999.

safety when planning and scheduling these maintenance activities.

The most important addition to the rule was a new paragraph a(4) that states:

Before performing maintenance activities (including but not limited to surveillance, post-maintenance testing, and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities.

The requirement's intent was for licensees to assess proposed maintenance activity risk. This included considering direct and inadvertent equipment unavailability, allowing licensees to minimize maintenance time in an informed way and additionally to establish reliability performance measures that were consistent with those contained in the plant specific PRA. It also supported plant configuration control that enabled key plant safety functions.

Maintenance programs in nuclear power plants are necessarily complex. Developing and managing a program that balances safety and maintenance burden is a substantial challenge – which makes PRA methods attractive.

POLICY STATEMENT

The importance of a high-level regulatory statement on the value of PRA methods cannot be overstated. Implementation of this policy has led to important changes in the NRC's regulatory processes. Even this, however, is insufficient without continued reinforcement by senior management.

Each rule revision was circulated for comment, with the industry indicating that they believed additional rule revisions were unnecessary. They wrote that improvements in existing industry programs would be sufficient to achieve the intent of the rule. The NRC did not agree, believing that a regulatory requirement was necessary. Comments from other stakeholder organizations were generally supportive of the rule change.

2.4.1.1 PRA Policy Statement (1995)

By the 1990s, PRA credibility was such that the NRC issued its 1995 PRA policy statement. [116] Beyond the utility of the guidance it

[116] The 1993 Technical Specification Policy Statement acknowledged the importance of risk information in identifying equipment that should be added to the scope of the technical specifications, but specifically did not support using risk information to remove equipment. This more limited perspective changed by the time of the rule change two years later.

contained, it also meant that PRA was a permanent element of the regulatory process. The statement read in part:

> *The use of PRA should be increased to the extent supported by the state of the art and data and in a manner that complements the defense-in-depth philosophy.*
>
> *PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatisms associated with current regulatory requirements, regulatory guides, license commitments, and staff practices.*
>
> *Where appropriate, PRA should be used to support the proposal of additional regulatory requirements in accordance with 10 CFR 50.109 (Backfit Rule).*
>
> *Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is understood that the intent of the PRA policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.*
>
> *Deterministic approaches to regulation consider a limited set of challenges to safety and determine how those challenges should be mitigated. A probabilistic approach to regulation enhances and extends this traditional, deterministic approach, by:*
>
> *(1) Allowing consideration of a broader set of potential challenges to safety,*
>
> *(2) Providing a logical means for prioritizing these challenges based on risk significance, and*

(3) Allowing consideration of a broader set of resources to defend against these challenges.

This implied that licensees could use PRA for license amendment purposes. At that time, industry PRAs varied widely in approach, detail, realism, and plant specificity. License amendments using PRA would need to be submitted with a determination that the PRA was "technically adequate" for the application. This policy guidance resulted in joint efforts by the industry and NRC to create plant-specific PRA standards.

This policy statement was one result of a number of NRC programs focused on improving regulatory performance. These programs were established (in part) based on feedback from the ACRS and nuclear industry. [117] Licensees asserted that some NRC regulations had little safety benefit, required excessive testing, and mandated quality assurance on non-safety critical equipment – all of which imposed significant costs. [118] Further, concerns had been raised about the consistency of PRA use and NRC resistance to its increased application.

2.4.1.2 Challenges

By 1995, essentially all United States nuclear plants had been designed using 10 to 20 year old concepts. Substantial infrastructure had been created to implement or comply with contemporary practices. Plant-specific IPEs and IPEEEs had identified and helped address severe accident vulnerabilities (Section 2.3.6). New PRA applications were challenged with difficult goals of either finding new vulnerabilities or identifying unnecessary conservatisms. This work has met with mixed success.

The PRA focus before 1995 was to provide a general measure of reactor safety and identifying plant-specific concerns, using CDF and LERF as metrics. The NRC decision to expand its use to "all regulatory matters" required new methods along with associated

[117] The associated ACRS letter can be found at the end of Chapter 1 of NUREG-1489.

[118] These and similar concerns have been collectively termed "unnecessary regulatory burden," meaning that the safety benefit was not commensurate with the implementation costs. In the NRC's PRA Policy Statement, this is referred to as "unnecessary conservatism."

training and education. Many subsequent public discussions helped communicate the NRC's intentions and its priorities.

2.4.1.3 Implementation

NRC policy statements provide perspective on the regulatory intentions, but are not legally binding. A draft policy statement was circulated for public comment in 1994. The comments received were generally supportive of the proposal to increase PRA use.

The NRC developed a "PRA Implementation Plan" describing extant PRA-related activities. It became the mechanism by which new activities were managed, outlining specific implementation activities.

2.4.1.4 Legacy

High-level regulatory policy statements on the value of PRA methods remain crucially important. The policy statement has led to important changes in NRC's regulatory processes and spurred risk-related action across the nuclear industry. Some activities and associated improvements in nuclear power plant regulation are discussed in various parts of this document. However, experience has shown that the intent of the policy statement can only be implemented with continuing reinforcement and managerial commitment from both the regulator and regulated.

2.4.2 PRA Scope and Quality

By 1995, most licensees had completed IPEs. Licensees expected changes to plant operation, maintenance or design to involve PRAs. They also expected PRAs to be involved with prioritization of resources expenditure.

With these applications in mind, EPRI issued a "Probabilistic Safety Assessment (PSA) Applications Guide" to assist the preparation, application, interpretation, and maintenance of plant-specific PRAs. [119] The NRC released its PRA procedures guide in 1983, outlining its underlying technical methodology. [120]

PRA STANDARDS

The ASME PRA Standard took more than three years to develop with a consensus committee including utilities, NRC, contractors, consultants, and academia. The Standard defines "What" must be done, not "How". It is based on three "Capability Categories". The Capability Categories are graded from simplest to more comprehensive and apply to all the technical requirements contained in the standard based on scope and level of detail, plant specificity, and realism.

[119] D. True et al., "PSA Applications Guide. Final Report" (Electric Power Research Inst., Erin Engineering and Research, 1995), http://inis.iaea.org/Search/search.aspx?orig_q=RN:27015409.

[120] "NRC: PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants: (NUREG/CR-2300)," accessed November 28, 2016, http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr2300/vol2/.

Since the RSS, the levels of PRA detail, realism and conservatism have been debated. Important initiatives to improve PRA quality (or technical adequacy) followed the NUREG-1150 Study (discussed in Section 2.3.7). This led to discussions with Standards Development Organizations (SDOs) on consensus committee establishment.

After completing IPEs, many licensees continued to update and improve their PRAs. During 1999 and 2000, the NRC met with the NEI, Nuclear Steam Supply System (NSSS) owner groups, licensees, and the public. These meetings explored ways to facilitate regular and voluntary exchange of risk-related information that addressed plant-specific, owner-group specific, and generic nuclear risk issues. Various stakeholders considered an ongoing cooperation with respect to the following initiatives:

- annual reporting of progressive PRA insights and plant improvements that reduce risk,
- ensuring NRC risk-informed assessment tools and processes use current information,
- providing a forum to address technical issues that arise from the ROP or other NRC reviews, and
- identifying generic risk insights that can help resolve issues associated with severe-accident-mitigation alternatives.

The NRC previously encouraged and participated in the development of standards by ASME, the American Nuclear Society (ANS), and other groups. The NRC's goal for standardization started to be implemented. For example, in SECY-99-256 (Option 2 in risk-informed Part 50 efforts) the proposed Advance Notice of Proposed Rulemaking indicated that PRAs used to support the SSC categorization process should conform to the consensus ASME/ANS PRA Standard documents, as endorsed by the NRC. This negated the requirement of PRA review and approval before NRC approval.

ASME formed a Committee on Nuclear Risk Management (CNRM) in 1998 to write a Level 1 PRA standard. The ANS concurrently formed its Risk Informed Standards Committee (RISC) and began writing standards on external events, Level 2 and Level 3 PRAs. BWR and PWR owner groups implemented their own RISCs. EPRI also established a risk management technical steering committee.

The ASME PRA Standard took more than three years to develop with a consensus committee including licensees, the NRC, contractors, consultants, and academia. The standard defined "what" must be done: - not "how". It is based on three "Capability Categories" graded from simple to comprehensive. These categories were applied to all the technical requirements based on scope, detail, plant specificity, and realism.

The ASME Board on Nuclear Codes and Standards (BNCS) and ANS Standards Board mutually agreed in 2004 to form a Nuclear Risk Management Coordinating Committee (NRMCC) to coordinate and harmonize nuclear PRA standards. ASME and ANS formed a Joint Committee on Nuclear Risk Management (JCNRM) to develop and maintain PRA standards – an initiative proposed by the NRMCC. The JCNRM operates under procedures accredited by the American National Standards Institute (ANSI).

ASME issued an initial Level 1 and LERF PRA standard in 2002 for internal LWR events at-power. In 2003 and 2007, ANS issued two PRA standards for external hazards and internal fires at-power for LWRs. In 2008, the three standards were combined to form "ASME/ANS RA-S–2008." Revised in 2013, it is currently maintained by the JCNRM. [121]

All PRAs need to align with the as-built, as-operated configuration. The standards outline requirements for updating the models, changes in plant procedures and how configuration controls are used to update PRAs.

To reduce or eliminate the need for regulatory PRA technical review, industry developed a peer review process that provided a consistent and uniform method for establishing PRA technical adequacy. [122] The industry's peer review process has evolved over time to include

[121] "ASME - STANDARDS - Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," accessed November 28, 2016, https://www.asme.org/products/codes-standards/ras-2008-standard-level-1-large-early-release.

[122] Nuclear Energy Institute, NEI 00-02, "Probabilistic Risk Assessment Peer Review Process Guidance," March 20, 2000.

peer reviews structured for specific hazard groups such as external hazards and internal events. [123,124]

Currently, standards have been developed that cover Levels 1 through 3, low power, shutdown and non-LWR PRAs. Standards are currently being extended to include advanced reactors.

Regulatory Guide (RG) 1.200 "An Approach for Determining the Technical Adequacy of PRA Results for Risk-Informed Activities" is the NRC's mechanism for endorsement of the Level 1 and LERF PRAs. [125] It is envisioned that this, or a similar guide, will govern the process for other PRA standards.

2.4.2.1 Challenges

Getting stakeholders to collaboratively standardize PRAs without being overly prescriptive was at times difficult. Standards' authors were primarily chartered with writing "what to do" but sometimes included "how to do it." Subsequent removal of "how to" methodology from standards required considerable effort. Unnecessary incorporation of conservatisms into standards has also been challenging – particularly for fire-based PRAs using guidance from NUREG/CR-6850 "Fire PRA Methodology for Nuclear Power Facilities." A seismic standard currently being reviewed has encountered similar difficulties regarding conservatisms and explicit methodologies.

In certain cases, RG 1.200 has negated the need for standards. Areas of confusion must be specifically addressed with formalized regulatory guidance, which can be a resource intensive process.

Some concerns have also been raised regarding "checklist reviews" versus thorough audits. This criticism applies to the assessment of "continuous improvement", which at times is not readily acknowledged in the current peer review process. This has resulted in the opinion of some that the peer review process has become a series of subjective audits of conformance in lieu of their original intent.

---

[123] NEI 12-13, External Hazards PRA Peer Review Process Guidelines.

[124] NEI 05-04, Rev 3 Process for Performing Internal Events PRA Peer Reviews Using the ASME/ANS PRA Standard

[125] Nuclear Regulatory Commission (NRC), "An Approach for Determining the Technical Adequacy of PRA Results for Risk-Informed Activities," 2009.

Timeframe is an ongoing issue with many risk-informed regulatory applications using PRA as a technical basis supporting license amendments. License Amendment Requests (LARs) trigger Requests for Additional Information (RAIs) from the NRC for risk-informed applications. There have been many cases where the RAI and subsequent regulatory review takes many years. Licensees (as with businesses in general) need responsive review processes. Regulators want thorough technical reviews. An ongoing balance between business reality and regulatory due diligence needs to be continually struck.

2.4.2.2 Stakeholder Reactions

The industry is generally committed to RIDM and determining PRA technical adequacy through its peer review process. Every United States nuclear power plant maintains a quantitative internal events PRA model, with around three quarters maintaining a fire PRA model. This has facilitated high-level insights and subsequent safety improvements even though many of the methods and models remain developmental.

That said, in spite of some notable exceptions such as Southern Company's adoption of Rule CFR 50.69 "Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors" and Risk Informed Technical Specification (RITS) Initiative 4B, the overall level of industry support for risk-informed initiatives is relatively low. [126] However, recent events have renewed interest in these applications.

2.4.2.3 Legacy

PRA technical adequacy has improved significantly over time. Many early RIDM applications have yielded immediate benefit by reducing outage durations and increasing plant reliability. Specific initiatives (such as Rule 10 CFR 50.69, Risk-Managed Technical Specification and Risk-Informed In-Service Inspections) have shown benefits in improving nuclear and worker safety.

Challenges clearly still exist within some NRC engineering disciplines. Notwithstanding, the NRC has endorsed the PRA methods and other risk tools as a way to enhance the traditional deterministic regulatory frameworks. NRC policy recognizes that both deterministic and probabilistic approaches have strengths and

[126] Nuclear Energy Institute, "Letter to the NRC," December 19, 2013.

weaknesses, and can best contribute to nuclear safety if used in an integrated way.

EVOLUTION

The goal of modifying the NRC rules to better reflect risk information is laudable and essential for safety rules to truly reflect the associated risk. In practice, proposing rule changes for already-operating plants have not been fully successful because of the complexity (and inter-connected nature) of these rules and implementation costs.

2.4.3 New NRC Rules

Following its 1995 PRA policy statement, the NRC identified a set of possible risk-informed applications. While 1980s rules were reactively based on reactor protection system reliability concerns (where PRA based rules were seen as useful), 1990s rules involved proactive searches for areas of improvement. This included the modification of some of the basic regulatory rules with a process that was approved by the Commission and initiated in 1998 [127] and continues today.

Rule changes are not easy. NRC regulatory changes follow prescriptive, resource-intensive, and time-consuming processes. [128] Implementation timeframes are expressed in terms of years. Considerable effort is already expended by licensees to comply with existing rules - effort that can be "wasted" should that rule subsequently change. Change management, of itself, is also resource intensive. Both licensees and the NRC have sometimes been reluctant to expend these resources to modify rules.

Some rules are "intertwined" in often obscure ways. The (conceptually simple) evaluation of a proposed rule modification is often exacerbated by researching and mitigating follow on effects in other rules.

2.4.3.1 Implementation

The NRC initially developed a voluntary, alternative rule regarding "special treatment" requirements. It then started to examine the regulations in greater detail, identifying the need for additional or modified rules along with scope for the elimination of rules. Potential rules were presented as voluntary alternatives for licensees.

[127] Annette Vietti-Cook, "SECY-98-300: Options for Risk-Informed Revisions to 10 CFR Part 50 - Domestic Licensing of Production and Utilization Facilties.," June 8, 1998, http://www.nrc.gov/docs/ML0037/ML003751348.pdf.

[128] The NRC's processes include provisions for shortening the rulemaking process under certain circumstances, but these provisions are rarely used.

The NRC identified several other rules that could be modified for more risk-informed implementation alternatives. These rules are discussed below.

2.4.3.2 Rule 10 CFR 50.46: Emergency Core Cooling Acceptance Criteria

The NRC internally proposed in 2002 that rule 10 CFR 50.46 be modified to be more risk-informed. [129] In many ways, 10 CFR 50.46 requirements are central to the design and safety case for current nuclear power plants. This added significance to the goal of increasing PRA use. It was also anticipated that implementation costs and savings would be significant. The proposed modification was approved in 2003. [130]

The NRC has since developed several possible rule modifications, held public meetings, and discussed the issue with the ACRS. Around the same time, industry invested significant resources on this subject. No modified rule has yet been endorsed.

2.4.3.3 Rule 10 CFR 50.48: Fire Protection

Again, the NRC internally proposed in 2000 that Rule 10 CFR 50.48 be modified to be more risk-informed. [131] This alternative was based on a fire protection standard "Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants" (Number 805) issued by the NFPA. Following approval [132] and the promulgation of a draft rule for comment, the final rule was

---

[129] William D. Travers, "SECY-02-0057 - Update To SECY-01-0133, 'Fourth Status Report On Study Of Risk-Informed Changes To The Technical Requirements Of 10 CFR Part 50 (Option 3) And Recommendations On Risk-Informed Changes To 10 CFR 50.46 (ECCS Acceptance Criteria),'" March 29, 2002, http://pbadupws.nrc.gov/docs/ML0206/ML020660607.pdf.

[130] Annette Vietti-Cook, "Staff Requirements - SECY-02-0057 - Update To SECY-01-0133, 'Fourth Status Report On Study Of Risk-Informed Changes To The Technical Requirements Of 10 CFR Part 50 (Option 3) And Recommendations On Risk-Informed Changes To 10 CFR 50.46 (ECCS Acceptance Criteria),'" March 31, 2003, http://www.nrc.gov/docs/ML0309/ML030910476.pdf.

[131] William D. Travers, "SECY-00-0009 - Rulemaking Plan, Reactor Fire Protection Risk-Informed, Performance-Based Rulemaking (WITS Item 199900032)," January 13, 2000, 00-0009, http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2000/secy2000-0009/2000-0009scy.pdf.

[132] William D. Travers, "Staff Requirements - SECY-00-0009 - Rulemaking Plan, Reactor Fire Protection Risk-Informed, Performance-Based Rulemaking (WITS Item 199900032)," February 24, 2000, http://www.nrc.gov/reading-rm/doc-collections/commission/srm/2000/2000-0009srm.pdf.

released. [133] About half of the United States nuclear power plant licensees have indicated an intent to implement the alternative rule.

While many U.S. licensees are implementing the new rule, the process has been contentious and costly. Concerns have been raised by industry, and are being addressed. These concerns were raised formally: [134]

> *Fire PRAs performed to NUREG CR-6850 and the NRC responses to "frequently asked questions" for NFPA 805 produce results that are inconsistent with operating experience and do not depict actual plant fire risk. As an example, these methods predict that over 100 severe fires should have been observed to propagate from low voltage electrical cabinets, when in reality few such events have been observed in 3000 reactor years of U.S. plant operation. These and other such assumptions combine to produce exaggerated fire core damage frequencies.*

2.4.3.4 Rule 10 CFR 50.61: Fracture Toughness Requirements for Protection against Pressurized Thermal Shock (PTS) Events

Pressurized Thermal Shock (PTS) requirements contained in Rule 10 CFR 50.61 were recommended for modification in 2006. [135] The original 1985 rule included the use of risk analysis methods that were very conservative in some areas, potentially limiting reactor vessel lives. The NRC and industry researched the issue and proposed rule revisions.

---

[133] "Voluntary Fire Protection Requirements for Light Water Reactors; Adoption of NFPA 805 as a Risk-Informed, Performance-Based Alternative," *Federal Register*, November 1, 2002, https://www.federalregister.gov/documents/2002/11/01/02-27701/voluntary-fire-protection-requirements-for-light-water-reactors-adoption-of-nfpa-805-as-a.

[134] Nuclear Energy Institute, "Letter to the NRC."

[135] Luis A. Reyes, "SECY-06-0124 - Rulemaking Plan to Amend Fracture Toughness Requirements for Protection against Pressurized Thermal Shock Events (10 CFR 50.61)," May 26, 2006, http://www.nrc.gov/docs/ML0605/ML060530624.pdf.

Following the publication of a draft rule for public comment period, the NRC issued the final version of the rule in 2010. [136] Additional regulatory guidance (in the form of a regulatory guide and a supporting technical document) has since been developed. It is not clear at this time how many licensees will choose to implement the rule.

2.4.3.5 Legacy

Stakeholder reaction on the proposed rule changes reflected concerns about reducing safety (from public interest groups) and implementation costs (from licensees and others in the nuclear industry). Some rules were changed to reduce the burden on some licensees. Other proposed rule changes generally did not interest licensees due to concerns regarding implementation costs and the uncertainty in the anticipated benefit.

Notwithstanding, the modification of rules to better reflect risk information is laudable conceptually and essential for safety rules to truly reflect the associated risk. Rule changes for operating plants have not been fully successful in practice due to rule complexity, rule interconnectivity and implementation costs.

2.4.4 PRA in Technical Specifications

Technical specifications, plant operating conditions and limits regulated by the NRC can have significant impacts on the availability of important plant equipment. By extension, this can affect the ability to reliably generate electricity.

There was a trend to include more equipment (on a plant-by-plant basis) within the scope of the technical specification rule up until the mid-1980s. [137] This saw a very large set of variable technical specifications. From 1987 to 1995, the nuclear industry and the NRC worked to rationalize equipment within the scope of technical specifications. This resulted in sets of "standard" technical

[136] Nuclear Regulatory Commission (NRC), "10 CFR 50.61a Alternate Fracture Toughness Requirements for Protection against Pressurized Thermal Shock Events," January 4, 2010, federalregister.gov.

[137] Nuclear Regulatory Commission (NRC), "Rule 10 CFR50.36: Technical Specifications," 2016.

specifications, a 1993 policy statement [138] and 1995 rule change. [139,140]

With the implementation of the Maintenance Rule, the potential of risk analysis became evident. The nuclear industry has proposed new methods, generally called "Risk-Managed Technical Specifications" (RMTS).

2.4.5 Regulatory Guide 1.174 - 1997

Following its 1995 PRA Policy Statement, the NRC focused on the process for making changes to the licensing basis using PRA. [141,142] This focus resulted in Regulatory Guide (RG) 1.174 that defines basic principles and an associated series of regulatory guides. [143] RG 1.174 guidance has since been used for integrating deterministic and probabilistic analysis methods well beyond the original intended scope.

2.4.5.1 Challenges

Converting general policy into practical licensing guidance was a primary challenge due to primarily deterministic licensing processes. The NRC understood that introducing risk information shouldn't make the process more burdensome.

The risk-informed approach permitted small risk increases, which was a significant cultural change. Essentially, small, specific risk

---

[138] Nuclear Regulatory Commission (NRC), "Technical Specification Policy Statement," 1993.

[139] Nuclear Regulatory Commission (NRC), "Final Rule - Technical Specifications," July 19, 1995.

[140] The 1993 Technical Specification Policy Statement acknowledged the importance of risk information in identifying equipment that should be added to the scope of the technical specifications, but specifically did not support using risk information to remove equipment. This more limited perspective changed by the time of the rule change two years later.

[141] L. Joseph Callan, " SECY-97-077: Draft Regulatory Guides, Standard Review Plans and NUREG Document in Support of Risk Informed Regulation for Power Reactors," April 8, 1997, http://www.nrc.gov/reading-rm/doc-collections/commission/secys/1997/secy1997-077/1997-077scy.pdf.

[142] John C. Hoyle, "Staff Requirements - SECY-97-077 - Draft Regulatory Guides, Standard Review Plans And NUREG Document In Support Of Risk Informed Regulation For Power Reactors," June 5, 1997, http://www.nrc.gov/docs/ML0037/ML003752391.pdf.

[143] United States Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions on Plant Specific Changes to The Licensing Basis," Regulatory Guide 1.174, 1997.

increases could be acceptable in the context of expected overall safety.

PRA Quality Assurance (QA) requirements and standards had yet to be established. RG 1.174 addressed QA, while standard development was undertaken separately (discussed in Section 2.4.2).

2.4.5.2 Implementation

The RG 1.174 concepts were tested using a set of volunteer plants. Application of the RG 1.174 in more specific regulatory areas was accomplished with the publication of four additional regulatory guides. These guides addressed the use of risk information in in-service testing of mechanical equipment, quality assurance, technical specifications, and in-service inspection of piping. These guides are discussed below.

It is worth noting that individual licensees also used RG 1.174 to request one-time specific exemptions from the regulations, such as the STP (examined in the case study in Section 3.2).

2.4.5.3 Risk-informed In-Service Inspection (RI-ISI) of reactor coolant piping

Degradation mechanisms not addressed by previous ASME guidance were incorporated into the inspection program. Risk-important, non-safety related piping was added to the scope of the inspections (as discussed in Section 3.16).

2.4.5.4 Risk-informed Technical Specifications

A set of risk-informed technical specification initiatives were identified, including risk-informed approaches to missed surveillance tests, plant mode changes with certain unavailable equipment, owner controlled surveillance test frequency programs, and risk informed completion time programs (Section 3.17).

2.4.5.5 Risk-informed Graded Quality Assurance (RI-GQA)

RI-GQA allows the categorization of equipment according to risk significance (discussed in Section 3.19). PRAs showed that many components previously identified as safety related were not particularly important to plant safety and risk. This initiative later became Rule 10 CFR 50.69 "Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors."

2.4.5.6 Risk-informed In-Service Testing (RI-IST)

RI-IST uses PRA to reassess the originally conservative approaches to testing requirements and provides a more realistic and safety-focused testing program (discussed in Section 3.20).

2.4.5.7 Legacy

The use of RG 1.174 is voluntary for the licensees. Many licensees continue to use traditional, deterministic approaches due to their familiarity and perceived predictability. This has resulted in mixed success in terms of actual implementation on specific topics. Notwithstanding, the general guidance in RG 1.174 has been a model for integrating deterministic and PRA methods that has extended far beyond its initial scope.

2.4.6 Inspection Changes and the Reactor Oversight Process (ROP) - 1999

The ROP was subject to intense review in the second half of the 1990s. [144] Reflecting an intent to increase PRA use, the new ROP involved more risk-informed elements (discussed in Section 3.18). The new ROP used more objective and quantitative measures of plant performance. It focused NRC and licensee resources on aspects of performance that had the greatest impact on safe plant operation. It also provided explicit guidance on the regulatory response to inspection findings. The use of risk information has enabled the NRC's ROP to achieve its fundamental purpose to identify issues of safety significance and provide for their correction. This has resulted in both regulator and licensees becoming more aware of the equipment and plant functions that contribute most to nuclear safety thus providing a catalyst for focusing resources on these items that are of most importance.

The risk-informed ROP is working very well, as discussed more fully in Section 3.18.

2.4.7 PRA in the United States

The main motivation for PRA is to provide an integrated and realistic model of plant behavior under numerous abnormal conditions (which are deviations from normal operation). The traditional safety approach was based on the "defense in depth" principle and

[144] William D. Travers, "SECY-99-007: Recommendations for Reactor Oversight Process Improvements," January 8, 1999, http://www.nrc.gov/reading-rm/doc-collections/commission/secys/1999/secy1999-007/1999-007scy_attach.pdf.

employed a highly stylized and small number of postulated DBAs. Although this approach is useful in assuring safety, it fails to provide an integrated model and metrics for plant risk.

The QHOs, CDF and LERF have proven to be important metrics for communicating risk levels and their acceptability to both the nuclear community (industry and regulators) as well as the public. Saying that the plants are safe because they meet complex regulatory requirements is an unsatisfactory and confusing statement.

Analysis transparency, uncertainty quantification and broad communication of risk are major benefits of PRA and RIDM – all of which enhance objectivity. The integrated nature of PRA allows the prioritization of systems, structures, and components in terms of their contributions to risk.

The establishment of PRA and RIDM faced several challenges – the major one being cultural. Most United States engineers do not study probability and statistics in college, let alone PRA. Asking them to adopt probabilistic methods in lieu of traditional "deterministic" approaches to regulations was and remains a significant cultural challenge.

2.4.7.1 Outcomes

The risk-informed initiatives outlined above are voluntary (for the most part). Naturally, licensees weigh their costs and benefits before adopting them. A common problem is that costs are usually incurred entirely before an initiative is implemented while the benefits are realized sometime in the future – often with imprecise timeframes and quantities.

The safety benefits are unquestionable, with the best example being the RI-ISI. Plants became safer because degradation mechanisms that were not addressed previously by the ASME guidance were now part of the inspection program. Other examples include PRAs that have identified safety improvements in areas of vulnerability leading to modifications, compensatory actions or other process changes that improved safety.

Importantly, PRA has reduced costs while improving safety. There is a safety benefit when unnecessary (and costly) regulatory burdens are removed: more resources are available to manage risk significant issues.

The NRC's 1995 Policy Statement stated that:

> *PRA should be used to reduce unnecessary conservatisms associated with current regulatory requirements.*

Unnecessary conservatisms add to costs without contributing to safety. When developing the ROP, the NRC found that the previous inspection, assessment, and enforcement processes were not always focused on the most important safety issues, consisted of redundant actions and outputs, and were overly subjective leading to inscrutable and unpredictable actions being prescribed.

Some other risk-informed initiatives did not fare well. The NRC and ASME have developed programs that could be used by licensees to implement RI-IST but have not attracted much attention. It appears that one of the challenges outlined above regarding the initial costs of acquiring regulatory approval and implementing them outweigh perceived long-term benefits, especially in consideration of the more limited reductions in equipment testing.

There is reason to believe that industry will continue to advance PRA methodologies and applications. Licensees and designers of new reactor technologies have a broad set of risk metrics to consider. Where the regulator "only" has metrics (or surrogate metrics) that attempt to assess "adequate protection of the public," the industry must consider economic and performance measures. Some are now exploring "generation risk assessment" using PRA to increase plant availability. [145] PRAs are also being used to avoid costly scenarios that do not involve core damage. This would include the successful operation of bleed and feed in a PWR or chemical injection of sodium pentaborate or firewater in a BWR. In such scenarios, extensive down time potentially decreases remaining plant life.

[145] Pickard Lowe and Garrick Incorporated, "Quantitative Risk Assessment for Non-catastrophic Accidents at a Japanese Nuclear Power Plant," Prepared for Mitsubishi Atomic Power Industries, Inc., May 1994.

Chapter 3: Case Studies

Section 3.1: South Texas Nuclear Project Electric Generating Plant Electric Generating Station (STP) - Diagnostic Evaluation

EARLY APPLICATIONS

STP successfully used the PRA in the early 1990s to scope the systems that would require re-certification following the enforced NRC shutdown and subsequent Diagnostic Evaluation. This turned a projected 5-year shutdown into an actual 13-month shutdown.

The STP is a two-unit site. Each unit is a 4-Loop Westinghouse PWR with 1250 MW capacity and a large, dry containment. Each unit uniquely has three independent, redundant safety divisions. The units commenced operation in 1986 and 1987.

The rationale for including the third safety train was essentially to have a spare system beyond that required to meet safety requirements. STP was not a "true" three-train plant from a regulatory perspective due to design basis assumptions. These assumptions were associated with single failure criteria, the assumption of an installed spare, and assumed LOCA location. These assumptions (when combined with STP's Safety Injection and Reactor Coolant System) resulted in the plant being considered a modified "N+1" design: not a three-train "N+2" design. [146]

The STP safety injection system injection piping was Reactor Coolant System (RCS)-loop specific. In other words, it was not possible for an individual train's safety injection system to inject into any RCS loop. Under design basis assumptions, a safety train was considered to be unavailable as an installed spare (single failure criterion) as a second train would inject into the broken loop (the loop with the design basis LOCA), leaving the third train to inject into the RCS.

These design basis assumptions obviated the perceived benefit of the third safety train and left the "spare concept" unrealized. STP's Technical Specifications became effectively identical as a plant with two safety trains, but it now had more SSCs to maintain. This was in spite of general acknowledgment that the three train system had an actual safety benefit (for accidents beyond the design basis LOCAs.)

[146] The terms "N+1" and "N+2" refer to the number of ECCS safety trains, with "N" being a train that fails (single failure criterion) and "1" being the number of trains that perform safety injection function or other ECCS functions.

STP became motivated to determine the safety benefit of the third train, and to assess ways in which the investment in the third train could be realized. PRA became the avenue to achieve this.

3.1.1 Initial Implementation of PRA

A PRA program commenced in 1984 while both units were under construction. STP initially intended to identify vulnerabilities or other "curiosities" associated with the three-train design. STP wanted to internalize methods for a new PRA group who would be responsible for understanding, maintaining and applying the ensuing insights. A technology transfer objective ensured personnel would be capable of "owning" the plant-specific PRA model and its use.

STP formed a small PRA group consisting of three engineers and a supervisor. Their main responsibilities were to:

1. jointly develop STP's PRA with the primary consultant organization, and
2. acquire sufficient technology transfer to update, revise, and maintain the PRA.

Once this technology transfer was completed, the group acquired more responsibilities regarding special analyses and supporting licensing issues.

A Preliminary Scoping Study was presented to the NRC in 1985. This study was "Phase 1" of the plan to produce a plant-specific PRA. Since both units were under construction, study results were needed quickly to correct designs prior to hot functional testing and initial startup. The study results indicated that the highest uncertainty involved Electrical Auxiliary Building (EAB) Heating, Venting and Air-conditioning (HVAC) and Reactor Coolant Pump (RCP) Seal LOCAs.

The HVAC risk significance was a substantial safety insight that had not been identified. Remediation actions included operator training on how loss of room cooling could affect electrical and digital equipment operation. STP proactively developed and approved an "off-normal procedure" for degradation or loss of EAB HVAC. This included opening doors and performing a fan driven, once-through cooling mode referred to as "smoke purge". The off-normal

procedure was incorporated into the PRA resulting in a CDF decrease, and subsequently included in other utility PRAs.

A more comprehensive Phase 2 PRA Study was performed from 1986 to 1989 before NRC review. The NRC issued a Safety Evaluation Report (SER) and indicated that STP's PRA was considered suitable for regulatory purposes (including license amendments using PRA information and insights).

Design changes associated with the containment purge isolation valves and the Chemical Volume and Control System (CVCS) letdown valves were identified during the plant walkdown phases of the PRA. These valves were installed as Motor Operated Valves (MOV), meaning that under SBO or other loss of electric power conditions the valves would fail. If this occurred during normal containment purge operations or CVCS letdown operations, the containment isolation function would also fail. The isolation valves for both these areas were changed to fail-closed Air Operated Valves (AOVs).

The PRAs also identified a "risk-positive" insight. Within the CVCS, a Positive Displacement Pump (PDP) facilitated RCS hydrostatic testing after refueling operations. The piping arrangement of the CVCS enabled the PDP to also provide RCP seal injection. Normal RCP seal cooling function provided by the Component Cooling Water (CCW) system is lost during an SBO accident. Alternate RCP seal injection cooling methods were important to prevent seal degradation (a common PWR core damage scenario.) The PDP could be used for alternate RCP seal injection as it is powered by the Technical Support Center (TSC) Diesel Generator – not the EDGs. This was ultimately confirmed as a unique safety feature of the plant design.

STP became more motivated to investigate PRA benefits. Of key interest were the Technical Specifications. Since STP's PRAs had been evaluated by the NRC, discussions regarding the evaluation of Technical Specifications were held. Changes based on PRA analyses and insights were proposed. Significant PRA modeling improvements resulted from this initiative to reflect the as-built, as-operated station. These modeling improvements were in the areas of configuration risk management and in the plant processes used to plan and perform station work activities.

3.1.2 Lead up to Operating Problems

STP's PRA program had already reached a level of maturity by the early 1990s. The licensee response to the NRC's Generic Letter 88-20 "Individual Plant Examination for Severe Accident Vulnerabilities – 10 CFR 50.54(f)" would involve existing PRAs rather than the conduct of a new analysis.

STP had not been operating for long. It would emerge that organizationally, the plant had not successfully transitioned from "construction" to "operational" mentalities – an issue that would soon become very apparent.

Safety related equipment work activities started to become seriously behind schedule. Equipment was failing surveillance inspection due to lack of preventive maintenance resulting in regulatory concern from the NRC.

The NRC initiated an augmented inspection which identified a negative management style, a cultural issue that is taken very seriously. A full regulatory Diagnostic Evaluation was ordered.

The NRC issued a Confirmatory Action Letter (CAL) in 1993 effectively halting STP operations and identifying items to be resolved before the reactors could be re-started. The 16 items that required resolution as outlined in the CAL were:

1. Correct the oversight trip condition that afflicts the turbine-driven auxiliary feedwater pumps.
2. Improve the process for reporting and correcting problems affecting equipment operability.
3. Reduce the backlog of open-service requests and the number of operator workarounds.
4. Improve the post-maintenance test program to provide confidence that equipment removed from service for maintenance is properly restored to operability.
5. Reduce the backlog of outstanding design modifications and temporary modifications.
6. Provide adequate staffing in the operations department.
7. Institute adequate training of the fire brigade leader.

8. Upgrade the reliability of the fire protection computers.
9. Improve management effectiveness in identifying and correcting plant problems.
10. Improve the effectiveness of "Speakout" (the employee nuclear safety concerns program at that time).
11. Improve diesel generator reliability.
12. Improve essential chiller reliability.
13. Institute the System Certification Program.
14. Improve the reliability of the feedwater isolation bypass valves.
15. Institute periodic testing of tornado dampers for safety-related ventilation systems.
16. Improve performance on emergency preparedness accountability drills.

STP estimated the corresponding reactor shutdown would last five years. As all safety-related and most non-safety related systems would need to undergo a recertification process, the System Certification Program (SCP) would need considerable resources. Certification was needed to ensure design basis requirements were met, the resolution of outstanding maintenance, as well as items contained in the CAL. Finally, STP would need NRC approval for the systems recertification.

The SCP was motivated to ensure that systems were returned to conditions that ensured design basis and performance requirements were met, thereby addressing outstanding regulatory issues. The SCP consisted of engineering reviews, engineering evaluations, system walkdowns, maintenance backlog reviews, reviews of long standing equipment issues, modification evaluations (permanent and temporary), and performance history reviews. Activities that required resolution in order to respond to the CAL would be identified in this process.

The SCP required substantial support from STP's engineering, operations and maintenance elements. Hundreds of items from many different systems would be assigned to responsible organizations, who would then monitor those items until closure. The NRC maintained regulatory oversight of the SCP throughout

the process. Each system within the SCP scope was evaluated for performance deficiencies (such as reduction in maintenance backlog), any unresolved regulatory issues (such as commitments) and modification status.

Risk insights from the PRA were used to prioritize items, which were then recorded in an SCP tracking system that included a unique item identifier, item description, responsible organization, schedule date for completion, and actual completion date.

A special engineering report was developed and submitted to the NRC using the PRA's SSC scope to define the systems that would be included in the SCP - both safety and non-safety related. It further identified important components that would need focused efforts (such as diesel generators and essential chillers). The NRC responded positively to the use of PRA and approved the systems identified in the report, thereby enabling a detailed project schedule.

3.1.3 Challenges

STP's organization and owners were significantly challenged by this regulatory shutdown. After the CAL, both STP units were placed on the NRC's "Watch List." It was not known at the time when restart could occur.

The NRC was surprised at the degraded performance of STP and faced criticism of its own, given that it had not acted sooner. Meetings between the NRC and STP's Board of Directors resulted in the majority of senior management being replaced. It was noted that the prevailing management style resulted in a "chilling environment" where employees did not feel comfortable identifying problems. It was also apparent that there was a lack of prioritization, with efforts focused on areas with less significance. The organization had not transitioned to an "operating mentality" from its "construction and startup mentality." Required changes in vision and philosophy had not materialized, resulting in collective ineffectiveness.

3.1.4 Legacy

The NRC authorized the restart of STP Unit 1 in 1994. The same authorization was given for STP Unit 2 in 1995, with both units removed from the "Watch List". A projected five year shutdown was ultimately reduced to an actual 13 month shutdown, primarily due

to the reduced SCP scope from the use of the PRA. Organizational changes helped to ensure previous issues did not recur.

STP's executive and senior management teams saw PRA as a significant tool for making safety decisions and for improving operational efficiencies. The end of the Diagnostic Evaluation marked the beginning of STP's risk-informed applications efforts. This was the moment where key risk-informed applications such as Risk Significance Categorization (Exemption from Special Treatment Requirements, later to become Rule 10 CFR 50.69), RMTS, and Generation Risk Assessments (non-regulatory) were proposed to and approved by management.

STP then became a pilot plant for these efforts. It was used to develop and test PRA for risk-informed applications. Several STP efforts formed the basis for initial proofs-of-concept to demonstrate how PRA methods could be used to support risk-informed regulation efforts being pursued by the NRC.

Section 3.2: STP - Emergency Diesel Generator (EDG) Failure

After the STP's 13-month shutdown (discussed in Section 3.1), operating costs and generation expectations were being challenged by long refueling outages (in the order of 45 to 55 days). PRA methods had advanced such that the risk impact of unavailable equipment could be appropriately calculated. This led to establishing a Configuration Risk Management Program (CRMP) supporting on-line maintenance program development.

Work activities continued to evaluate configuration risk and then determine acceptable methods to propose changes to Technical Specifications. The scope of the Technical Specifications was not seen as the problem: AOTs and surveillance testing requirements were. These two areas formed a focal point for investigations on how best to reflect the change in risk (ΔCDF) due to a change in AOT or surveillance testing intervals.

PRA insights led to developing different maintenance strategies – but they were limited by these restrictive AOTs. STP used its PRA in a risk informed license amendment request to extend the AOT for EDGs and ECCS components (such as safety injection and containment spray) from three to 14 days and three to seven days respectively.

Regulatory approval was granted which helped improve safety and equipment reliability. STP was able to reduce outage scope, increase generation, and still ensure that important equipment continued to be available and highly reliable. Work activities that were typically reserved for outages could now be performed when the unit was at-power. Refueling outages were reduced to around 20 to 30 days. The success led to the realization that PRA insights and Risk Management methods could be used to optimize station resources and improve effectiveness – not just safety.

3.2.1 An Outage Risk Management

During a normal mandatory monthly surveillance test in December 2003, STP Unit 2's EDG had a catastrophic failure that resulted in significant damage. This left the unit with two out of the required three EDGs.

EARLY SUCCESS

On December 9, 2003, STP's Unit 2, Diesel Generator (DG) #22 had a catastrophic failure that resulted in significant damage. Repair time was initially estimated to be 120 days.

On December 30, STP was granted a one-time extension of the Allowed Outage Time (AOT) to 113 days in order to make repairs. As part of the approval, STP would develop a planned risk profile showing the changes in risk levels (both CDF and LERF) over the extended AOT.

The risk management approaches taken were successful: STP units continued to provide power, and the regulator gained new insights on the DG failure. Importantly, the use of PRA provided robust means to manage allowed outage times.

Figure 3.2-1: Image of the damaged Emergency Diesel Generator

STP assembled an Event Review Team (ERT) to investigate the failure and assess operator response. Due to the extent of the damage, an Engineering Support Team (EST) augmented the ERT. The teams combined to coordinate the root cause investigation that included extensive metallurgical testing on the damaged parts, determining the scope of repairs and identification of replacement parts.

Repair time was initially estimated to be 120 days. STP Technical Specifications for EDGs had already been extended from three to 14 days, but the repair time in this instance fell well outside that range. STP was faced with a situation where Unit 2 would have to be shutdown at the end of the 14 day AOT for around 106 days, which coincidentally encompassed the short winter peak season.

The licensee evaluated the failure event significance using its plant-specific PRA model. Several calculations were performed to determine the CDF and LERF increase due to the EDG unavailability over the estimated repair time. The CDF and LERF calculations

confirmed that industry standard risk thresholds would not be exceeded. [147]

As part of the Maintenance Rule requirements, [148] the EDG unavailability would be factored into the total cumulative yearly risk estimate for component maintenance unavailability. This established a permanent impact of the EDG unavailability to determine if the risk significance criteria contained in RG 1.174 would also not be exceeded.

STP requested a Notification of Enforcement Discretion (NOED) from the NRC that would permit Unit 2 to continue power generation until the EDG was repaired. The NOED process is often used to repair inoperable equipment whose repair time will exceed AOT. The process is burdensome to both utilities and the NRC, leading to efforts to reduce the number of NOED requests.

Using risk information from plant-specific PRAs provided a technical basis to extend AOTs as long as the rules associated with NOEDs were also followed. NRC staff had not used risk profiles as a technical basis to approve past NOEDs, but this represented a way to determine the viability of risk profiles to manage safety and risk. The NRC ultimately approved the NOED, requiring STP to develop a planned risk profile showing the changes in risk levels over the extended AOT.

This was the first time risk profiles were used to manage risk levels at a nuclear power plant with unavailable equipment. Not only was this consistent with NRC risk-informed approaches, but it also provided an observable way to establish risk significant thresholds.

STP was granted a one-time extension of the AOT for 113 days. The planned risk profile was used as a basis to control planned and unplanned work activities that would remove Unit 2 equipment from service. Additionally, STP maintained an "actual" (real time) risk profile with exact times and occurrences of equipment failures within the scope that would demonstrate that actual risk was

[147] Nuclear Energy Institute, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants (Revision 4A)," February 22, 2000.

[148] Nuclear Regulatory Commission (NRC), "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," July 19, 1999.

consistent with planned risk. The actual risk overlay is shown in Figure 3.2-2.

The overlay of "planned" versus "actual" risk profiles provided important safety insights. It demonstrated that risk management actions combined with probabilistic methods could enable risk and

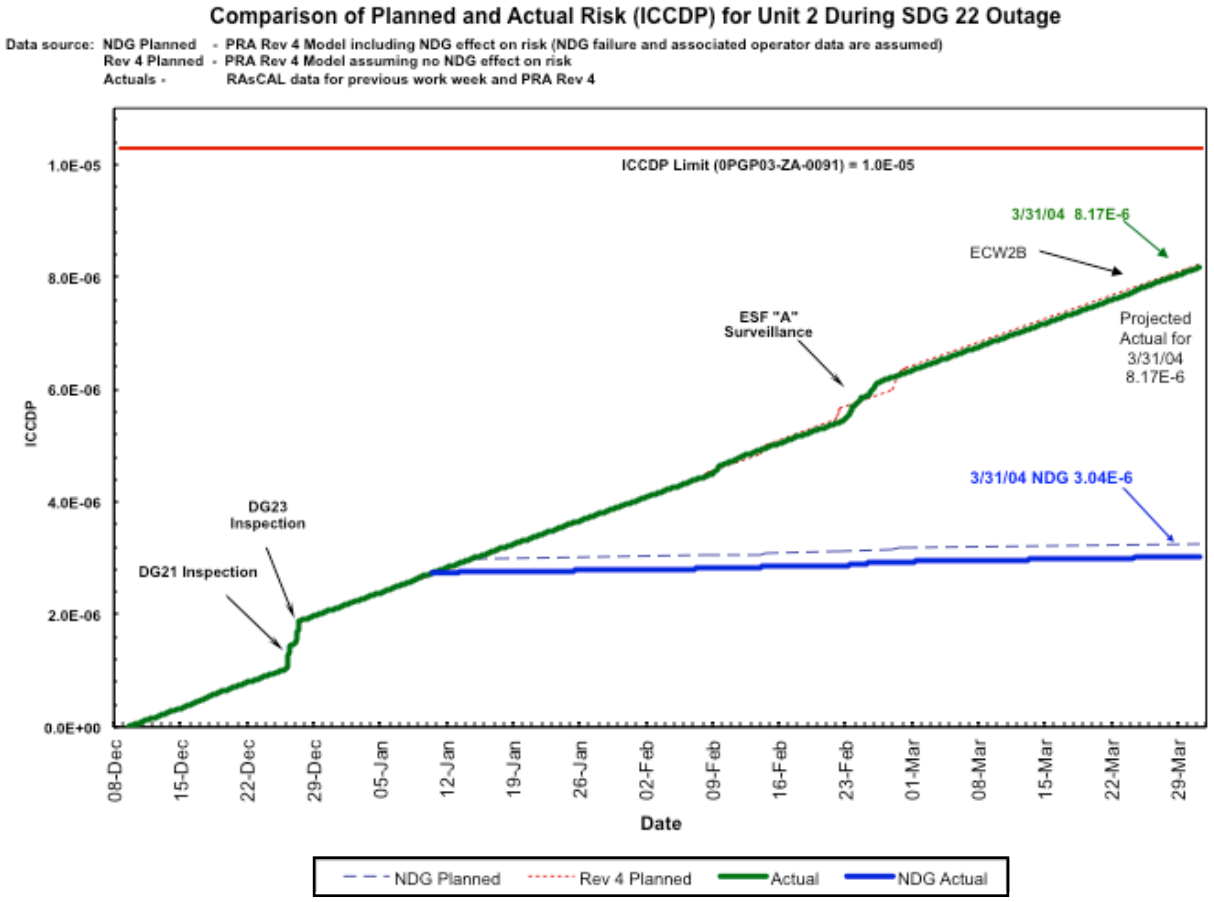


Figure 3.2-2: South Texas Nuclear Project Electric Generating Plant (STP) Plant Risk Profile – Diesel Generator (DG) #22 Outage of 1993

safety insights to be used by licensees. These insights could inform the prioritization of maintenance activities, mitigation of risk increases, and focus compensatory actions.

The risk profiles included other Unit 2 activities that would impact risk levels during the EDG outage. The risk reduction of the non-safety related DGs was also included. Solid lines indicated risk levels based on the project schedule, and dotted lines represented the actual risk levels. The risk threshold is shown in red. Only CDF profiles were generated, as they were considered an acceptable

surrogate for LERF. No equipment important to LERF was out of service during the repair time.

3.2.2 Challenges

The EDG design was over 20 years old at the time of the incident. Many of the original design drawings were no longer available from the Original Equipment Manufacturer (OEM), Cooper-Bessemer. This meant some parts had to be fabricated based on inspection of other Cooper-Bessemer DGs.

The main NRC challenge was related to public health and safety with the PRA critical in informing its regulatory response. The NRC had several discussions with STP during the NOED approval process where agenda items included DG failure cause. It was clear to the NRC that STP did not know the exact cause of the failure due to the extensive damage incurred.

A non-safety related temporary DG was made available to Unit 2 to maintain defense in depth – even though it met RG 1.174 risk significance criteria without it. STP's Risk Management Group also decided to suspend preventive maintenance activities on any equipment within the scope of the Configuration Risk Management Program (CRMP) to limit risk increases during the EDG repair.

3.2.3 Legacy

The root cause of the failure was determined to be micro-cracks on a master connecting rod created during manufacturing. Metallurgical testing identified that a High Cycle Fatigue (HCF) crack had originated near the top of the inside diameter of the crankshaft bearing bore of the master connecting rod. The HCF crack propagated across the ligament upward until it broached the other side at the articulated rod pin bore. The crack then spread outward (axially to the crankshaft) until failure.

The repairs were ultimately completed within the 113-day one-time AOT extension while Unit 2 operated at 100% power. The risk management approaches were clearly very successful. New insights were gained by the NRC and the industry more broadly in relation to EDG failure. However, the key legacy is the use of the plant-specific PRA and risk profiling to manage AOT, leading to subsequent rules and regulations.

3.2.4 Epilogue

PRA information was gradually used to provide risk insights and information to various site organizations. This included licensing, operations, work planning and scheduling, outage management, emergency response organization, engineering, and maintenance.

STP's PRA group also participated in plant initiative processes for improvements with funding for new initiatives being actively sought. These were typically related to maintaining and improving the PRA and for new risk informed initiatives that included the following:

- RI-ISI which improved inspection strategy, reduced total number of inspections, reduced personnel radiological exposures
- Exemption from Special Treatment Requirements or "Graded Quality Assurance" which removed low-risk significant components from the scope of regulatory programs, improved safety culture
- Risk-Informed Asset Management Evaluations using Enterprise risk methods and Generation Risk Assessment Model which led to:
- energize-to-actuate [149] modification for which STP received the NEI Top Industry Practice Award,
- reactor vessel head replacement, and
- major maintenance decisions which included RCP and circulating water motor rewinds.

Other risk-informed initiatives developed include:

- RMTS implementation in 2007 where STP won the 2008 Best-of-the-Best NEI Top Industry Practice Award, and
- Risk-informed closure of GSI-191 regarding emergency containment sump performance.

STP's PRA group is considered "high-performance." It expanded to 11 personnel during the peak of the risk-informed applications development and deployment phase. The PRA group consisted of

[149] Energize-to-actuate describes the actuation design of the valves within the scope of the modification.

three sections at the time: PRA Configuration Control and Analysis, Applications Development, and Implementation. The PRA group has since been reduced to around 7 to 8 engineers (after the Implementation section was eliminated). Most of the major risk-informed applications have been approved, deployed, and assimilated in organizational processes.

Section 3.3: The Emergence of Outage Risk Management

Several events in the late 1980s occurred during shutdown conditions that drew attention to "outage risk." These included the 1987 Diablo Canyon [150] and 1990 Vogtle shutdown events. [151] A lack of understanding of the risk in different outage configurations or plant operating states demonstrated a need for improved outage configuration control. Both the industry and the NRC undertook studies to better understand outage risk. Licensees were motivated to improve shutdown safety with an increased recognition that additional safety measures were needed beyond those already mandated.

New procedures were developed to support shutdown risk management programs. Outage risk management used defense-in-depth tools based on shutdown risk models. The shutdown risk models identified undesirable combinations of plant configuration and unavailable equipment by evaluating detailed outage plans. All United States licensees have detailed shutdown risk processes that require reviews of planned outage schedules. The actual schedules are reviewed daily to assure there are no new high-risk configurations. Risk levels are typically reported daily based on defense-in-depth risk charts along with look ahead reports for upcoming high risk conditions.

An increased focus on thermo-hydraulic analyses for shutdown configurations resulted in standardized "time-to-boiling" plot analyses for the reactor coolant system and spent fuel pool. This helped define protected equipment lists during different plant operating states, increased oversight during high risk evolutions (such as heavy load moves) and high-risk plant operating states (such as PWR midloop operations).

OUTAGE RISK MANAGEMENT

Active outage risk management has resulted in the reduction of outage risk. United States outage events have been steadily declining since the 1980s. Improved focus on industry shutdown risk experience and insights have occurred through INPO event reporting.

[150] "Loss of Residual Heat Removal System, Diablo Canyon, Unit 2, April 10, 1987 (Augmented Inspection Team Report April 15-21, 29 and 1 May 87). | National Technical Reports Library - NTIS," accessed November 30, 2016, https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/NUREG1269.xhtml.

[151] Nuclear Regulatory Commission (NRC), *Loss of Vital AC Power and the Residual Heat Removal System during Mid-Loop Operations at Vogtle Unit 1 on March 20, 1990* (Washington, D.C: U.S. Nuclear Regulatory Commission, 1990).

3.3.1 Challenges

Implementing outage risk monitors is primarily challenged by the need for comprehensive control of outage configurations. Outage risk management requires careful planning, tracking, controlling, and coordination of the many work activities during plant outages. Configuration control needs to adapt to changes in schedules required by emergent equipment issues and variations in the completion of specific outage tasks.

3.3.2 Legacy

The NRC considered the implementation of outage risk management throughout the United States nuclear industry to be sufficient to preclude the need for a "shutdown rule" that would have specified requirements for outage configurations. [152] Licensees have continued to improve shutdown risk assessment programs, which are now part of standard operational procedures in nuclear power plants.

Improvements in outage safety features (including instrumentation, procedures, and training), detailed outage planning, and active outage risk management have resulted in improved outage safety. The number of outage risk events in United States plants has significantly reduced from 1990 as illustrated in Figure 3.3-1.

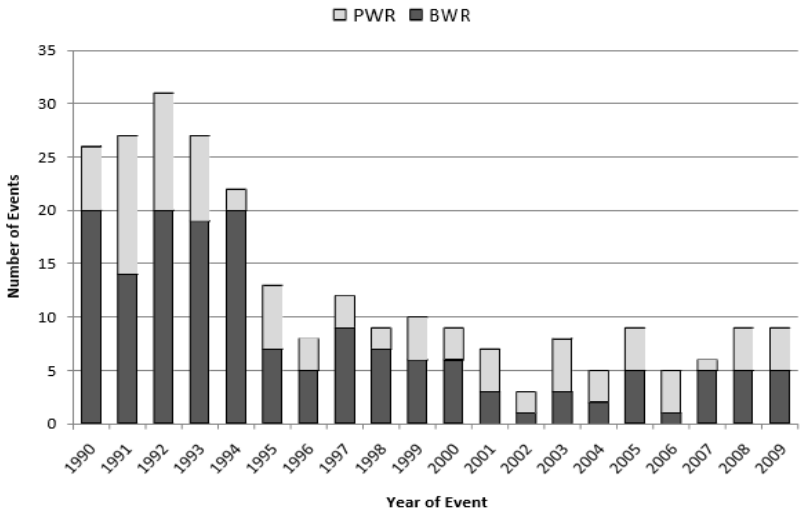


Figure 3.3-1: Trend of Loss of Decay Heat Removal Events during Shutdown, from 1990 to 2009

[152] L. Joseph Callan, "(For The Commissioners) SECY-97-168: Issuance for Public Comment of Proposed Rulemaking," July 30, 1997.

Section 3.4: Outage Duration and Risk Management

The average United States nuclear power plant capacity factor was around 60 per cent throughout the 1970s and 1980s. Protracted refueling outages significantly contributed to plant downtime. Recognition that the outage length was largely due to poor planning started to grow. It was also recognized that certain work activities performed during outages (such as EDG maintenance) could also be performed during at-power modes.

As described in Section 3.3:, several events occurred during shutdown configurations in the 1980s that helped focus attention on outage risk with respect to critical shutdown safety functions. They also demonstrated that a lack of detailed outage planning contributed to high outage risk.

Implementing outage risk models required the careful tracking and controlling of outage configurations, notwithstanding that they are somewhat simpler than full-power PRA models. Outage schedules were evaluated for shutdown risk by evaluating safety-function status across all plant operating states during an outage. Many outage scheduling changes were initially identified, but the increasing use of shutdown risk assessments ultimately caused outage schedules to inherently preserve improved levels of safety.

This same attention to detail in outage planning also led to shorter duration outages as work activities were better planned. Hand-offs from one activity to another were better controlled. The critical path and near-critical path activities could be carefully managed as the schedule evolved during the outage. Contingency plans were developed to assure that activities stayed on track.

While outage risk models put restrictions on equipment outages during some plant configurations, the focus on detail in outage planning served to help reduce the overall outage length. On-line maintenance activities were also expanded to further simplify outages and enable further reductions in outage duration thus increasing overall capacity factors.

3.4.1 Challenges

Detailed outage planning required tracking of work packages at a much finer level. This required some refinement in work processes and scheduling, which in turn led to schedule improvements that

OUTAGE RISK MANAGEMENT

Safety and economics are sometimes thought of as mutually exclusive goals - improved safety usually costs money. Implementing outage planning and controls has proven to realize both goals. Improvements in plant safety, refueling durations and generation performance have been realized concurrently.

were constrained by specific outage evolutions (such as vessel head removal). New procedural processes for shutdown risk assessment were implemented at stations with multi-disciplinary teams comprising of operations, outage scheduling, PRA, engineering, and maintenance personnel. These teams would then perform post-outage critiques for improvements or lessons learned.

3.4.2 Legacy

Safety and economics are sometimes thought of as mutually exclusive goals - improved safety usually costs money. Implementing outage planning and controls has proven to realize both goals. Improvements in plant safety, refueling durations and generation performance have been realized concurrently. The improvements in outage risk (discussed in Section 3.3:) occurred at the same time as plant capacity factors improved significantly. By 2000, the average plant capacity factor had risen to about 90 per cent. The average refueling outage decreased from about 60 to 30 days.

Section 3.5: Component Risk Significance and Notification

Traditional component significance for nuclear power plants is based on the regulatory definition of safety-related components. A "basic component" is an SSC (or part thereof) that assures reactor coolant pressure boundary integrity, reactor safe shutdown capability, or accident consequence prevention and mitigation. [153]

Basic components are designed and manufactured in accordance with a QA program. This program is combined with regulatory requirements ("Special Treatment Requirements") that are intended to ensure that safety-related SSCs are capable of performing their intended functions under design basis conditions. These Special Treatment Requirements include such items as Equipment Qualification, Pump and Valve Testing per ASME Section XI, and others.

Nuclear power plant components incur substantial additional costs due to this regulatory burden. Industry experience has identified significant cost savings and reliability improvement when the number of suppliers increases. Components can become obsolete from a lack of ongoing manufacturer support. In these situations, the use of a commercial dedication process was and still is used to "qualify" a non-safety-related component for a safety-related purpose.

The industry proactively started to use risk information to further define the significance of safety-related and non-safety-related SSCs relative to nuclear safety through blending PRA and deterministic insights. Risk Significance Categorization not only has regulatory relevance through Rule 10 CFR 50.69 (Section 3.19), but practical applicability in identifying risk-significant equipment. There are a number of non-regulatory applications that can be used to improve safety and equipment reliability generally. The NRC depicted the concept of risk significance categorization as shown in Fig. 3.5-1.

PRIORITIZING COMPONENTS

Prioritizing and targeting component maintenance both saves money and improves safety. A component risk significance categorization process is the method employed by the U. S. nuclear industry to do this. By correctly assigning priorities to components, maintenance (in terms of its effect on safety) is more efficient. It also yields substantial cost savings by being able to target components that are critical for the generation of electricity.

[153] "NRC: 10 CFR Part 21—Reporting of Defects and Noncompliance," accessed November 30, 2016, http://www.nrc.gov/reading-rm/doc-collections/cfr/part021/.

Figure 3.5-1: NRC Risk Significance Categorization

STP piloted an exemption from Special Treatment Requirements through the development a risk significance categorization process.

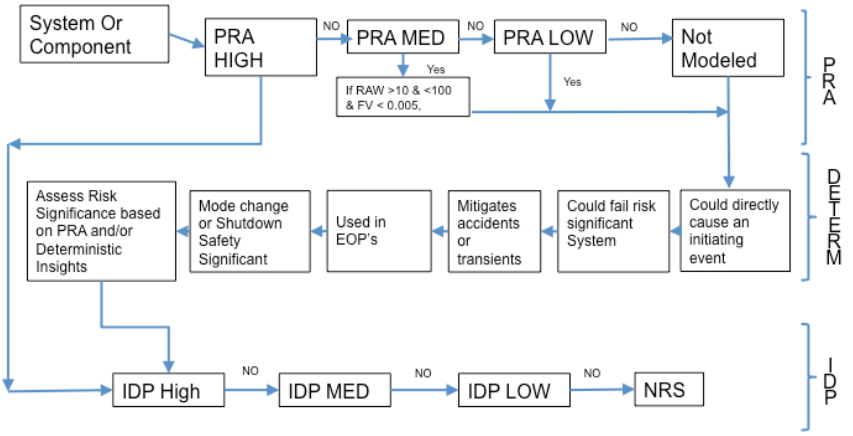


Figure 3.5-2: STP Risk Significance Categorization Process

The process used PRA information, engineering information, and operating experience. The risk significance is determined by an Integrated Decision-making Panel (IDP). Further efforts resulted in the development of industry risk significance categorization guidance NEI 00-04, [154] illustrated in Figure 3.5-3.

[154] Nuclear Energy Institute, "10 CFR 50.69: SSC Categorization Guideline," NEI 00-04, July 2005.

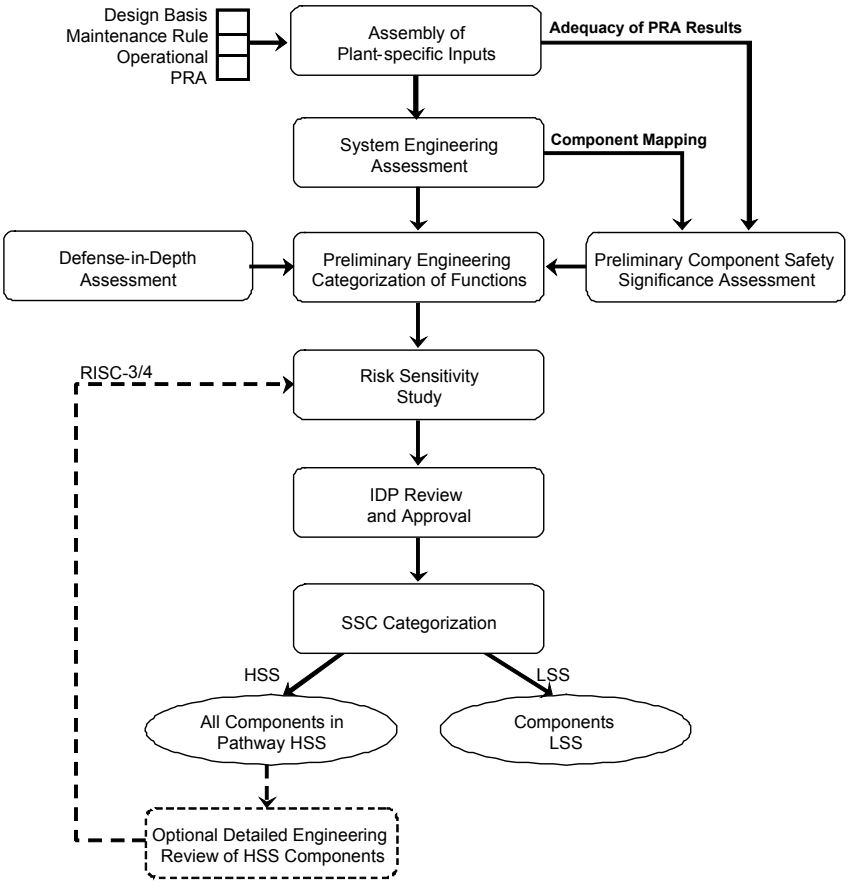


Figure 3.5-3: NEI 00-04 Risk-Informed Categorization Process

IDPs are used to assemble and approve equipment categorizations, and periodic performance assessments are performed.

3.5.1 Challenges

Licensees have only slowly embraced risk significance categorization due to the substantial initial investment. Categorization in and of itself does not provide benefits. The benefits are realized when a procedure or program is changed to recognize the categorization. Establishing a time schedule for plant system categorization is also a significant challenge.

3.5.2 Legacy

The risk significance categorization process results in the development of substantial understanding of key equipment, associated failure modes and sources of unavailability. Equipment prioritization processes can use the component risk significance categorizations to establish priorities across a large number of programs, establish audit scope, identify risk management actions

and others. The STP categorization process was extended to include plant generation risk, thus creating two categorization processes. These insights were significant in supporting safety culture as station databases could be structured to identify those times when plant processes (such as work control and planning) would impact a risk significant component.

Once a system or group of systems is categorized, programs and processes as defined through approved procedures can be changed based on component risk significance. This applies to both regulatory and non-regulatory applications. Non-regulatory applications of component risk significance include prioritization schemes for a wide range of issues. These include component risk significance training, reliability programs, operational focus areas, non-intrusive observation and examinations (such as predictive maintenance programs).

Utilities with risk significance categorization maintain this information in station equipment databases available to a wide range of user organizations. Generally, licensees want additional categorizations performed for different plant systems, and in some cases, apply the categorization concepts for different purposes. Non-regulatory categorization information may be used for risk communication to identify process changes for risk-significant component work activities, or to provide general information about SSCs and their importance.

It should be noted that in the US, industry initiatives are now taking place to update industry guidance documents and submit LARs to implement 10CFR50.69. These efforts are part of the larger industry initiative to make nuclear power plants safer and more efficient referred to as "Delivering the Nuclear Promise."

Section 3.6: Operator Training Insights based on Best-Estimate Accident Analysis

Before the general acceptance of PRA, operators' technical resources were limited to the results and insights from conservative, design-basis safety analysis to understand how the plant would respond to unusual challenges. Traditional nuclear power plant safety analysis is generally focused on demonstrating adequate design margin, introducing a number of conservatisms and bounding assumptions.

Conservatisms are useful for design when (for example) a heat exchanger has excess capacity and can tolerate degradation. They are not useful in helping operators understand how the plant responds and behaves. Conservatisms do not provide realistic accident sequence timing, which is necessary to establish acceptable operator action times. Safety analysis also uses design basis rules to limit the types of sequences that need to be evaluated. Again, operators need to broadly understand how the plant will operate given a wide array of accident scenarios.

PRA insights have informed operator training through procedure changes and simulator drills. The larger impact was the notion of "best-estimate plant response." PRA not only develops accident sequences with all credible combination of equipment failures, it also requires best-estimate accident sequence analyses to support realistic risk estimates.

United States PRA groups routinely use severe accident codes such as the Modular Accident Analysis Program (MAAP) to determine the plant response to different severe accident sequences, including key operator actions timing. Given (for example) a "design-basis" large LOCA (double-ended guillotine break of the largest RCS pipe), the time to switchover for recirculation can be as short as 30 minutes. Given a more realistic (though still low-frequency) small LOCA of 2-inch diameter break in the hot leg, switchover time to sump recirculation can be 10 hours or longer if the containment spray actuation set-point is not reached. For the same small LOCA without emergency feedwater, the switchover time to sump recirculation is about 2.5 hours. Thus, LOCAs can have drastically different accident sequence profiles based on the specifics of the scenario.

Value of Best-Estimate Analysis

PRA requires best-estimate accident analyses and other engineering analyses. The use of best-estimate technical analyses provides better insights into plant response to operational accidents than conservative design-basis analyses. For applications such as procedure writing and operator training, it is critical to understand the true performance of systems.

3.6.1 Challenges

The biggest challenge to best-estimate PRA acceptance is the perception that traditional safety analyses are always conservative and, therefore, intrinsically better. For system design purposes, this is generally true. But it is not true for operator actions: a conservative model may lead licensees to focus on the wrong set of accidents, fail to identify appropriate prevention or mitigation actions, or expect plant performance to be significantly different from the actual plant response.

3.6.2 Legacy

The understanding of actual plant accident scenarios and the development of better analysis codes to model best-estimate plant response has led to better operator training. United States PRA groups typically provide their operations training department the important operator actions identified in plant-specific PRAs. The operator training programs include an understanding of the risk basis for operator action and simulator exercises based on best-estimate analyses.

Section 3.7: Utilizing Insights from Operating Experience

Learning from failure is too slow to be (of itself) effective in improving long-term operations. Industry operating experience can help understand how equipment fails, how operators make errors, and how plants respond to abnormal conditions. Operating experience from other plants may appear to be irrelevant to plants of different types – yet licensees have recognized the importance of learning from all experiences. This includes minor events that may be precursors to more significant events. Ideally, the mistakes of the past are not repeated.

Licensees provide extensive reporting of operating experience to the Institute of Nuclear Power Operations (INPO). This information is organized to allow utilities to access high-level operating data (such as time trending of failures), functional level operating data (such as EDG failure events) or detailed operating data (such as a specific equipment model).

A PRA can provide insights from operating experience that can be applied at a functional or technical element level. A specific event involving components being incorrectly positioned may be unimportant due to the system it impacts. The same kind of error that involves more important systems may be much more risk significant. PRA methods for treating such a "latent error" include identifying administrative and hardware controls. Component being incorrectly positioned, even at another plant, allows evaluation of the barriers to see whether they are adequate or can be strengthened. This could include improving organizational awareness, increasing the emphasis on human performance tools and other administrative controls.

Operating experience reviews are typically required before major maintenance evolutions, plant modifications, or other higher risk evolutions. The intent is to look for experience that may be relevant to the specific component type, work activity, or plant configuration.

PRA provides additional information in the form of risk significance of events and equipment (such as key failure modes) that is not provided in typical industry operating experience data sources. Such precursor analyses assess the conditional risk given the actual events occurred.

Learning from Experience

The use of PRA insights has helped focus operating experience reviews by highlighting risk significant equipment, activities, and plant evolutions that increase safety against consequential events. This is a useful application of PRA to plant operations that does not involve the regulators.

Motivating good licensee behavior without the need for regulation is obviously a good thing, and learning from operating experience is one way in which this can be achieved.

3.7.1 Challenges

The main challenge revolves primarily around translating operating experience between nuclear power plants of different vintages or designs. Risk models helps to translate events into comparable information at a functional level.

Risk evaluation (such as an operating experience review) is a special task performed for specific high-risk evolutions. PRA analyses are not typically standard for utility operating experience reviews. Providing risk tools and automation for personnel within operating experience groups is an area that could be further improved through focused management efforts.

3.7.2 Legacy

United States licensees have embraced the concept of industry-wide operating experience learning. They have systems to collect operating experience at each plant and report to INPO on a regular and consistent basis. Significant events from other plants are now routinely assessed for their applicability to a specific plant. The use of PRAs allows this learning to be applied at functional, system and component levels in each plant.

While the value of an individual plant operating experience report may be small, the cumulative effect across the industry has been substantial. The use of PRA and its insights has helped focus operating experience reviews by highlighting risk significant equipment, activities, and plant evolutions that increase safety against consequential events. This is a useful application of PRA to plant operations that does not involve the regulators.

Section 3.8: Risk Information and Insights in Operational Decision Making

Managers are often faced with resource limitations that require prioritizing action. These limitations can be in terms of personnel, budget, time or money. PRA insights and operating experience information can help inform key operational decisions that require prioritization.

Operational challenges can come in many forms. Risk information (both quantitative and qualitative) generally supports other sources of decision information that can include engineering analyses, performance data and operating experience.

The following two examples illustrate the use of risk information and insights to address hypothetical but common "software" procedure errors and "hardware" equipment failures.

3.8.1 Emergency Operating Procedure (EOP) Example

An error is discovered in one of the EOPs: a sub-step was inadvertently left off when the procedure was revised. This sub-step was a continuation of the procedure step on the previous page - a classic error situation. Once discovered, it is not difficult to fix, but it raises the issue of the extent of condition. It raises the question of how many errors might exist in EOPs, Abnormal Operating Procedures (AOPs), and other operational and maintenance procedures. It also raises the question of what are appropriate measures to discover similar errors in other procedures. Table 3.8-1 shows a simple qualitative assessment of risk and possible risk management actions.

The risk assessment is a qualitative assessment of the frequency (or likelihood) of such a procedure error and the consequences to accident mitigation given an error is present. Risk management actions are proposed proportional to the assessed risk.

The example frequency assessment is based on a review of the plant-specific operating events which showed no other procedural errors. The frequency assessment was "very low" for AOPs and "Operations & Maintenance Procedures." The assessment was "low" for EOPs due to the original error. Because of the general importance of EOPs, the consequences of such an error is judged to be relatively high.

DECIDING FROM EXPERIENCE

The understanding of plant risk can provide insights into a number of operational challenges that face the managers of a nuclear power plant on a daily basis.

Risk measures and insights from a plant-specific PRA can be an important input into decision making regarding plant operational challenges. Utility use depends upon the level of awareness and training, meaning that its use needs to be continually reinforced even if those who are being convinced are likely to receive the most benefit.

Table 3.8-1: Risk Assessment and Management Actions to Address a Procedure Error

Procedure Type	Risk Assessment		Risk Management Actions
	Frequency	Consequences	
Emergency Operating Procedures (EOPs)	Low	High	Review all EOPs
Abnormal Operating Procedures (AOPs)	Very Low	Medium	Review a sample of AOPs
Operations & Maintenance Procedures	Very Low	Low	No review required

Since the EOPs have the highest risk, the risk management actions are focused on them. The actual risk may be low for all procedures, but the relative significance of the error is greatest for EOPs. The risk management actions are not an "all or nothing." A sample review of AOPs was determined to be appropriate because of their higher risk significance.

3.8.1.1 4 kV Breaker Example

A fault is discovered in a 4 kV breaker that would not open on demand. This breaker is one of dozens of safety and non-safety related breakers of this size and type in service. None of the other breakers show this fault, but the manufacturer has developed an improved maintenance refurbishment product that should fix this problem. The first question revolves around "operability:" is there reasonable confidence that the other breakers are still fully functional? Based on the fact that there are no historical issues with these breakers, that question would be answered positively. That is, the breakers are still operable. However, there is the question of long-term functionality of these breakers and how the refurbishment should be prioritized.

The performance-based insights from the plant experience indicated that this was not a common fault, but a search of the operating experience from other plants with similar breakers would provide more information relating to age or use. Once the

engineering analysis has identified the likelihood of failure, the licensee must decide on priority and schedule.

The PRA can provide quantitative support to prioritization. The breakers that are modeled directly in the PRA (or are associated with equipment that is modeled in the PRA) can be ranked by risk importance using a standard risk measure such as the Fussell-Vesely importance measure. Other breakers may have a related component in the PRA whose failure would have similar impact on plant risk (such as a surrogate component). Yet, other breakers could be categorized qualitatively based on risk potential.

In this example, the exact priority is not particularly critical: breakers can be grouped into three or four sets. Scheduling requires assessing the trade-off of performing the breaker maintenance with the plant at-power versus shutdown. There may be practical considerations for performing this work online (such as limited parts availability requiring work to be staggered over a number of months). In either case, the impact of component unavailability would be assessed as part of configuration risk management.

3.8.2 Challenges

The available risk information may not be perfectly relevant for the issue at hand. It may be necessary to identify surrogates to represent the actual components or component failure modes. However, the purpose is to make better decisions: the use of risk insights always improves decision-making. Even the use of uncertain risk insights is preferable to these insights not being used at all.

3.8.3 Legacy

Decision making is never a simple process, but the availability of risk measures and insights often provide valuable input into this process. Utility awareness and training in the use of PRA is the main factor in determining whether or not a utility will employ it. Operational decision-making processes cover many issues and conditions that may occur during the operating life of a nuclear power plant. The spectrum of issues covers the range of complex to the more simple and the use of PRA insights varies depending upon how closely associated the issue is with SSCs and processes within the scope of the PRA. Thus, some issues will require a heavy dependence on PRA information and risk insights while others will require less or

possibly none. However, even in those situations that are completely outside the scope of the PRA (e.g., environmental, worker safety), the risk concepts may be useful. Involvement of PRA groups in the operational decision-making process is key to establishing a risk-informed decision-making process.

Section 3.9: Transfer of Emergency Diesel Generator (EDG) Maintenance from Shutdown to On-Line

EDGs are among the most risk-significant components of nuclear power plants. The contribution of loss of offsite power and SBO to CDF and LERF is largely mitigated by EDGs. Licensees need to determine whether EDG maintenance is conducted "at-power' or during shutdown. This requires careful consideration of a number of competing factors, such as those positive (+) and negative (-) factors listed in Table 3.9-1.

Table 3.9-1: Comparison of EDG Maintenance Performed At-Power versus Shutdown

EDG maintenance performed with the plant shutdown	EDG maintenance performed with the plant at-power
(+) EDG is available with plant at-power, when risk in general is higher, compared to plant shutdown.	(-) EDG is unavailable with plant at-power, when risk is higher (although the risk can be adequately managed).
(-) EDG may be unavailable during certain plant outage configurations when the plant risk may be comparable to at-power risk (e.g., PWR midloop.)	(+) EDG maintenance can be scheduled to minimize any other major maintenance activities. Flexible scheduling helps to minimize weather-related challenges and other challenges to the grid.
(-) EDG is not available during some portion of outage. The frequency of loss of offsite power typically increases during plant outage due to test and maintenance activities that can only be performed with the plant shutdown.	(+) EDG is available with the plant shutdown when the frequency of loss of offsite power may be higher due to switchyard maintenance and other major electrical maintenance activities.
(-) EDG maintenance is performed during the most intense maintenance period throughout the plant, so EDG work may be performed by outside contract organizations.	(+) EDG maintenance is performed as the major activity during its maintenance week so focus is strictly on EDG work.
(-) Experienced utility maintenance personnel may be	(+) EDG maintenance is performed by the lead plant

On-Line Maintenance

Optimizing emergency diesel generator maintenance and other safety-critical systems requires risk to be considered during all plant modes. This optimization assessment has led to the decision for many utilities to perform maintenance with the plant at-power.

To perform maintenance at-power, U. S. utilities have to apply to the NRC for an extended allowed outage time. With pro-active regulatory support, operators can yield substantial commercial and safety benefits when looking at better ways to schedule maintenance.

EDG maintenance performed with the plant shutdown	EDG maintenance performed with the plant at-power
assigned to oversee other maintenance activities during outage work, and thus, not EDG maintenance.	maintenance individuals who have a long-term knowledge of the EDG.

When these factors are evaluated together, it is clear that at-power EDG maintenance offers a number of advantages both from a safety and a cost perspective, including better utility focus and management of risk. This has become the general practice for a number of United States nuclear power plants and has expanded to include other equipment in some situations. Those plants that had more restrictive EDG AOTs petitioned the NRC for longer AOTs to accommodate on-line maintenance. The NRC concurred that shutdown risk safety was improved while at-power maintenance risk levels were maintained to acceptable levels.

3.9.1 Challenges

Most utility and regulatory managers and engineers traditionally maintained a mind-set that "plant shutdown is safe." The notion of tradeoff between at-power and outage risk would have been illogical. However, a number of events that occurred during refueling outages demonstrated that this traditional mindset was flawed.

It was recognized that for some plant operating states (such as PWR midloop operations) risk levels could be substantially elevated for short periods of time. This warrants increased shutdown safety focus to include restrictions as identified by shutdown risk assessments. Detailed risk assessments of shutdown modes were capable of identifying configurations where the risk could be comparable to at-power risk. Subsequently, the development of shutdown PRA models to the same level of detail as at-power PRAs allowed them to be meaningfully compared.

3.9.2 Legacy

Once outage risk was better understood, utility managers and engineers could consider a broader range of issues that impact plant risk and EDG reliability. This improved awareness of other organizational issues such as safety culture and safety conscious

work environment. Licensees are evaluating conducting other equipment maintenance while "at-power." Some licensees have developed shutdown PRAs, supported by a Low Power / Shutdown PRA Standard, issued in 2015. [155]

[155] "ANS/ASME-58.22-2014, Requirements for Low Power and Shutdown Probabilistic Risk Assessment -- ANS / Store / Standards," accessed December 1, 2016, http://www.ans.org/store/item-240304-E/.

Section 3.10: Insights from a Spent Fuel Pool (SFP) PRA

FUEL AND RISK

With the obvious focus on operation and shutdown, it took some time before PRA was conducted on spent fuel. When it was, some alarming risks were identified.

The result of spent fuel PRAs was the identification of some simple remedies and mitigations that reduced this risk remarkably, making the industry safer. Recent events have reinforced the importance of dealing with spent fuel in a considered and judicious manner.

The insights from shutdown PRAs suggested that similar insights could be made from Spent Fuel Pool (SFP) PRAs, an issue whose significance (and lack of understanding) was reinforced by the Fukushima Disaster. SFP safety functions typically don't have the same level of redundancy as others such as safety injection and emergency feedwater systems. Monitoring key parameters that are important inputs into shutdown risk functions was identified as an area that could be improved as many stations did not remotely monitor SFP water levels.

A United States PWR SFP PRA showed that the large SFP water volume, along with the number of simple ways of providing water makeup, minimized associated risk. [156] However, the PRA's detailed analysis identified two new configurations with the highest conditional risk.

The first configuration occurs during a typical refueling outage, when all the spent fuel is offloaded to the SFP. This represents the largest SFP heat load. During this time, major safety trains are typically out of service for maintenance, including one of the essential AC high-voltage buses, which is one of the highest SFP risk configurations. The operating SFP cooling train and its support systems need to be protected. This protection can be provided through risk management compensatory actions to limit or prohibit work activities.

The second configuration occurs when a portion of the SFP is drained for fuel handling equipment maintenance. The pool level is protected by the fuel transfer gate and its air-supply seal. Failure of this gate would drain most of the water above the spent fuel assemblies, causing SFP cooling loss and high radiation levels. While the configuration duration is short, it represents a significant incremental risk increase (risk peak) to the otherwise low risk profile for the SFP.

[156] As with other risks, SFP risk may differ from plant to plant. This example is provided to illustrate the insights that can be gained by a detailed risk assessment. Specific insights may not be applicable to all SFPs.

3.10.1 Challenges

The most significant challenge for SFP PRAs is overcoming the belief that risk is controlled by design and equipment configuration as it would be during at-power operation. Risk is controlled by the infrequent but risk-significant configurations of the SFP - not the availability of SFP cooling systems.

3.10.2 Legacy

Once the risk and the simple mitigation measures were understood, utilities were supportive of the need to improve risk management programs associated with the SFP risk.

Section 3.11: Reactor Trip Rates

REACTOR TRIPS

Reducing reactor trip rates reduces risk (that is, improves safety) and enhances plant economics. Plant-specific PRAs are useful in identifying important equipment that prevent trips or mitigate risk significant events.

United States nuclear power plants were routinely experiencing multiple unplanned plant trips each operating cycle throughout the 1980s and 1990s. This incurred costs from both lost generation and plant transients that caused cyclic wear on systems. INPO also reported increases in safety-related operating events.

The average reactor trip rate has since decreased from more than three to less than one per unit-year, as illustrated in Table 3.11-1.

Table 3.11-1: U. S. Nuclear Power Plant Trip Rates

Year	PWR Reactor Trip Frequency (per plant-year)	BWR Reactor Trip Frequency (per plant-year)
1988	3.4	3.1
1992	2.2	2.0
2002	0.6	0.8
2012	0.4	0.6

This reduction was driven in part by the application of site-specific PRAs and the recognition that initiating events represent one element of accident sequences. Plant-specific PRAs not only identified initiating events and important accident sequences, but also important components that were associated with plant trips and accident mitigations. By identifying components within the scope of the PRA, utilities began to work to improve these components' reliability.

Root-cause investigations led to modifications that decreased recurrence levels. Reliability of equipment within the PRA scope was significantly improved.

Reducing the rate of initiating events is an effective means of improving nuclear safety. It also has a direct impact on plant economics – both from the improved plant capacity factor and from reduced cyclic wear of primary and secondary equipment from the heat and pressure transients.

3.11.1 Challenges

Reducing plant trips required their multiple causes to be understood, which informed changes in plant operation and

equipment. This trip-reduction effort required focused attention over a number of years. Plant-trip causes included both secondary-side and primary-side issues, hardware and instrumentation failures, human errors, and starting up or shutting down for an outage. While these causes all "lacked attention to detail," the actual improvements were varied based on a detailed understanding of the error.

3.11.2 Legacy

Both plant economics and safety were improved. The trip-reduction effort was strongly embraced by the licensees and encouraged by the NRC. It also resulted in additional investment into plant-specific PRAs to identify important equipment, especially support systems that tend to have less focus in traditional analyses and procedures. Licensees began to recognize PRA as a tool for identifying the importance of certain equipment for improving plant performance, reducing equipment failures in key components, and improving regulatory margins.

Section 3.12: Generation Risk Assessment

GENERATION RISK ASSESSMENT

PRA methods can be used to answer important operational issues. A Generation Risk Assessment (GRA) is structured to answer the question of how likely a plant trip or down-power event is based on equipment performance and balance-of-plant configuration.

This helps plant managers make decisions about how (essentially) to make money.

Nuclear power plant elements are divided into safety and non-safety related SSCs. Safety-related SSCs have regulatory requirements that result in organizational behaviors to ensure those components are functioning properly. Operational specifications, Technical Specifications, and other regulatory requirements (called "regulatory treatments") establish SSC design requirements, functional requirements, minimal permissible configurations, AOTs, and testing requirements.

Non-safety related SSCs are not subject to regulatory requirements. Utilities establish SSC significance based on operational priorities. This means there is no guidance on how long non-safety related SSCs can be unavailable. A Generation Risk Assessment (GRA) provides a technically-based prioritization method which could also be used to establish balance-of-plant (BOP) equipment AOTs using methods similar to those used for risk-informed Technical Specifications.

One nuclear power station has developed a GRA using PRA methods to establish the probability of a plant trip or down- power event based on equipment performance and configuration. Corrective and preventive maintenance is modeled and factored into the GRA.

The significance of BOP equipment failures depends upon the importance that SSC has for maintaining full or reduced power conditions. The GRA model is used to support operational decisions relative to equipment events or to answer "what if?" questions. For example, if a main feedwater pump were to trip or fail, the GRA would calculate the conditional probabilities that the plant will trip, not trip or reduce power.

GRA information was incorporated into the plant's risk monitoring program and associated procedures. Thus, configuration risk was monitored and measured in the Control Rooms for both CDF and BOP risk. CDF and BOP risk profiles are illustrated in Figure 3.12-1. The BOP profile has two parts: one is Incremental Conditional Trip Probability (ICTP) and the other is the weekly Cumulative Conditional Trip Probability (CCTP). The ICTP is expressed in terms the nominal (or average) trip frequency. The actual risk increases are

measured against the baseline zero-maintenance risk, which assumes all SSCs are available.

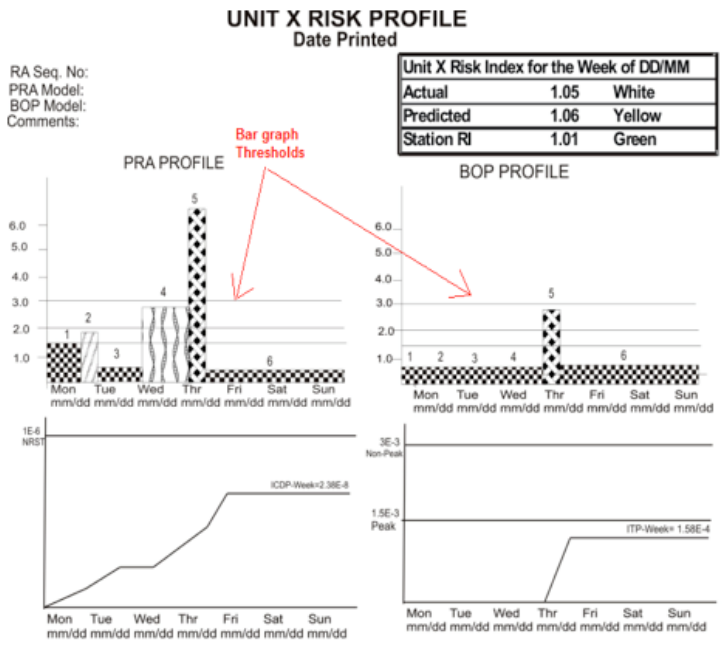


Figure 3.12-1: Core Damage Frequency (CDF – Safety) and Balance of Plant (BOP – Generation) Risk Profiles

Areas with risk increases are time periods where risk- significant equipment (in terms of generation) is out of service. The CCTP represents the weekly probability and accounts for the components out of service as well as the duration of BOP "maintenance states." The CCTP is compared against the management-defined risk thresholds for acceptability in Figure 3.12-2. If planned work were to exceed a threshold, then management notification would be required along with the development and implementation of risk management actions to mitigate undesired consequential events.

ITP Thresholds:

DEMAND PERIOD	NON-RISK SIGNIFICANT THRESHOLD	POTENTIALLY RISK SIGNIFICANT THRESHOLD
Peak	1.50E-03	3.00E-03
Off-peak	3.00E-03	4.50E-03

Figure 3.12-2: Incremental Trip Probability (ITP) Thresholds

This GRA included all the major BOP systems and was incorporated into the station's CRMP. The CRMP established GRA-based risk

thresholds in a similar fashion to that of the nuclear safety thresholds. Management and organizational actions were identified based on configuration risk as determined by the GRA. The GRA risk thresholds were established based on the Incremental Trip Probability (ITP) for BOP configurations resulting from either planned or unplanned maintenance.

BOP risk thresholds need to reflect peak versus off-peak risk sensitivity. Nuclear plants are base loaded electric generating facilities. As the electric power sector is an open market, competition between generating companies is encouraged in those states where the electric power is unregulated. This makes continued operation through the peak season extremely important. The ITP thresholds for peak season are reduced in order to increase managerial control and oversight during those time periods.

The GRA results were provided at the plant level in terms of unit trip frequency, unplanned MW-hour loss, and capacity factor. System level results are in terms of SSC contribution to unplanned production loss and event frequencies. Results at the equipment level are in terms of importance measures.

Operations and Work Control use BOP trip risk profiles to prioritize work activities, schedule work, and to determine out of service times for equipment. These capabilities provided the same administrative controls and strategies for equipment that were imposed by NSSS regulation. These programs allowed for contingencies and compensatory actions for unexpected events or issues and established a risk management structure for operational effectiveness.

3.12.1 Challenges

The incorporation of the GRA model into the risk monitoring software was an important challenge. Operations desired one tool for assessing risk and did not want multiple software programs. Additionally, the software verification and validation phase were handled in-house with a significant level of effort. Operations acceptance of the additional responsibility to record the actual out-of-service times for equipment within the scope of the CRMP required cultural change.

3.12.2 Legacy

Since the Work Control and Operations already had considerable experience generating and interpreting CDF risk profiles, the acceptance of the BOP risk profiles was easy. Operations and maintenance organizations use the GRA model to help assess configuration risk of BOP equipment and associated SSC alignments. Planned BOP trip risk is compared weekly to the actual BOP trip risk with insights and lessons learned identified for continuous improvement.

Section 3.13: Building a Safety Culture

AN IMPORTANT ISSUE

Safety culture is not an easily measured entity. It is identified through observation. Regulatory and industry safety culture training should include not only aspects of the current licensing basis but also risk information for events beyond the design basis. Risk management is an essential element of safety culture.

A number of events showed that nuclear "safety culture" needed to be improved, particularly after the TMI-2 accident. Although there were no public health consequences, the event bankrupted the utility and a billion-dollar unit was lost. Many fundamental problems involving hardware, procedures, training, and attitudes toward safety and regulation contributed to the event. Many of the same weaknesses resulted in the 1986 Chernobyl accident. It also highlighted the importance of maintaining design configuration, plant status control, line authority for reactor safety, and cultural attributes related to safety. INPO identified five events where lack of safety consciousness resulted in more than minor consequences. This industry experience led to a focus on programmatic improvements to safety culture and safety conscious work environment.

The NRC's "Policy Statement on the Conduct of Nuclear Power Plant Operations" refers to safety culture as

> *… the necessary full attention to safety matters [and the] personal dedication and accountability of all individuals engaged in any activity which has a bearing on the safety of nuclear power plants. A strong safety culture is one that has a strong safety-first focus.* [157]

The NRC referenced the International Nuclear Safety Advisory Group's (INSAG) definition of safety culture as follows:

> *Safety Culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.*

The Commission's policy statement "Freedom of Employees in the Nuclear Industry to Raise Safety Concerns without Fear of

[157] Nuclear Regulatory Commission (NRC), "10 CFR Parts 50 and 55: Policy Statement on the Conduct of Nuclear Power Plant Operations," n.d.

Retaliation," May 14, 1996, describes the Safety Conscious Work Environment (SCWE) as:

> *a work environment where employees are encouraged to raise safety concerns and where concerns are promptly reviewed, given the proper priority based on their potential safety significance, and appropriately resolved with timely feedback to the originator of the concerns and to other employees.*

SCWE is described as an attribute of safety culture in SECY-04-0111, "Recommended Staff Actions Regarding Agency Guidance in the Areas of Safety Conscious Work Environment and Safety Culture," August 30, 2004.

Both industry and the NRC responded to the TMI-2 and Chernobyl events by improving standards, hardware, emergency procedures, processes, training (including simulators), emergency preparedness, design and configuration control, testing, human performance, and attitude toward safety. INPO and NRC performed focused inspections on safety culture to further support improvements in this area. They recognized that the special characteristics of nuclear technology need to be considered in all decisions and actions. PRA insights need to be considered in daily plant activities and plant change processes.

3.13.1 Challenges

The principal problem is that safety culture is an organizational concept or characteristic - not a measureable commodity. One can observe it but cannot measure how it is created or how it is applied. The lack of a deep safety culture may indicate that there is no broad-based organizational knowledge relative to nuclear safety, or that there are no perceived benefits or incentives for performing additional safety improvements beyond what is required. Operations and technical groups will have heightened awareness of issues and situations affecting nuclear safety through training. This may not translate into a similar level of awareness to corporate or other plant staff.

This situation is also true of regulatory authorities. Of particular concern is the possibility that a false sense of security occurs when design basis is met, as well as when technical specifications and

A Misconception

A false sense of security occurs when design basis is met, as well as when technical specifications and other items are complied with. This results in complacency, with the responsibility for nuclear safety perceived to reside totally within the regulatory body.

In other words, the licensee only has a compliance responsibility but the regulator must decide what must be done.

This represents a significant threat to safety.

other items are complied with. If this mindset develops across regulatory or industry organizations, complacency can occur.

This type of thinking can result in deep-seated beliefs that the responsibility for nuclear safety resides totally and completely within the regulatory body. A mindset where compliance with the operating license equals safety effectively transfers the responsibility for identifying what is required for nuclear safety from the licensee to the regulator. In other words, the licensee only has a compliance responsibility but the regulator must decide what must be done. Without a good organizational understanding of risk as it relates to design basis and beyond design basis events, then it is much more likely that important safety provisions will be overlooked or made highly inefficiently without the use of risk insights and related performance measures. This type situation is not supportive of a growing and maturing safety culture.

All core-damaging events to date (except Chernobyl) were the result of beyond design-basis events: the plants were "compliant." The responsibility for nuclear safety needs to be shared between the regulator and the regulated.

The regulatory basis for granting operating licenses resides in meeting operational and technical requirements. This accounts for design-basis events - not all events that could reasonably be expected to occur over the life of the plant. Indeed, SBO and ATWS have since been added to United States nuclear power plant requirements. There were still licensing basis considerations in those rules that were not reflective of a real event. The SBO rule allows utilities to take credit for some on-site power sources. This would not be the case for an SBO modeled in a PRA. Thus, the current licensing basis must be augmented by incorporating risk management to account for items outside the design basis that may be more likely to occur than most all design-basis events.

Utility-initiated measures such as defense-in-depth, redundant and complex safety features, and 'managed' risk are all important. Regulatory initiatives that allow or promote the use of risk information to improve safety are equally so. Without these efforts, safety culture is confined to just design- basis events and can result in a sense of complacency. Again, the perception will be that "we meet design basis and comply with Technical Specifications … therefore we are safe".

Another factor to consider is the impact of organizational performance on safety, which can be represented by human errors. Human errors can be considered a manifestation of the underlying safety culture. Organizational factors in terms of cause and effect have not been fully understood by research organizations or by evaluation organizations such as INPO. They have also not been explicitly incorporated in PRAs. They cannot be directly incorporated into PRAs although their effects manifest themselves through consequential events. The lack of explicit representation of organizational factors results in an underestimation of risk, which produces a lack of understanding of the relationship between organizational responses, the PRA model, the human performance failure data, and cultural factors. Use of PRA insights is essential for identifying organizational performance deficiencies most important to safety.

Identifying and using risk insights to improve safety depends on the ability of PRAs to identify and focus attention on areas of safety significance. This occurs through traditional oversight methods such as audits and inspections but also by creating a platform where communication to utility staff creates safety awareness. This general or growing awareness should first be focused on the areas closest to personnel's specific areas of responsibility and extended over time through training, experience, and continuous improvement to create an inherent sense of "risk significance". This sense of risk significance can be applied at the individual contributor level for specific responsibilities on up to the site and corporate levels for responsibilities required from the perspective of enterprise risk. At the enterprise level, risk is managed, monitored, and measured across different types of risk hazards. This not only includes nuclear safety, but also generation risk, personnel safety risk, environmental risks, economic risks, regulatory compliance risk, and major project risk. Organizational performance can be more objective and focused so that deficiencies can be better identified and understood. This results in an improved organizational capability to identify more effective corrective measures such as training improvements, procedure improvements, and periodic feedback supporting continuous improvement.

3.13.2 Legacy

United States utilities have incorporated programs to evaluate safety culture. Surveys are performed yearly to assess safety culture

and the willingness of staff to identify problems. NRC and INPO inspections on safety culture and SCWE are also performed. Risk information is also used to emphasize certain aspects of the plant that have high safety significance. However, the use of risk insights to better inform safety culture surveys and other organizational data gathering efforts needs improvement to increase emphasis on the importance of risk information and insights in achieving improving levels of safety.

Section 3.14: Risk Monitoring to Integrate Risk Thinking into Daily Plant Status

One of the earliest PRA applications in the United States was applied to Configuration Risk Management (CRM): assessing the change in risk as components are taken in and out of service. This began to integrate PRA into daily work processes such as planning, scheduling, and execution. A means to communicate the changes in risk to plant personnel beyond the PRA group then became an absolute requirement.

Licensees developed several versions of risk monitoring programs based on CRM. This CRM included components within the PRA scope – both safety- and non-safety related components. Initially, risk monitors showed the change in calculated CDF based on the specific plant configuration each day. As risk-monitoring methods improved, the time increments for which CDF was calculated reduced to hours, then minutes.

To make sense of these numbers to plant personnel, a "no-maintenance" CDF (CDF_0) was introduced. This was the CDF assuming no test or maintenance activities are occurring, or all equipment within the scope of the CRM is available. The "average" CDF (CDF_{avg}) is the average annual CDF. In relation to CRM, the risk is associated with the likelihood that test or maintenance is occurring, where the likelihood is reflected in the maintenance or testing frequency and duration as reflected in the CDF_{avg} estimate.

For ease in understanding incremental risk profiles, the plant-specific CDF_{avg} is normalized graphically. A "specific configuration" or "maintenance state" CDF (CDF_i) would always be greater than the CDF_0. However, it may be less than or greater than the CDF_{avg} with roughly equal likelihood. When CDF_i exceeds CDF_{avg}, the risk associated with that configuration is "high," and "low" otherwise.

When the CDF_i is integrated over time, the ensuing cumulative probability over the work week can be measured against risk thresholds as determined by the risk values produced for each specific configuration change in the plant. Other important insights from risk profiles can be seen in the Incremental Core Damage Probability (ICDP) which is the probability of core damage given a specific configuration, and the Conditional Core Damage Probability (CCDP) which is the probability of core damage for a

AN IMPORTANT ISSUE

Robust risk monitors allow communication of complex risk assessment results in a way that plant personnel can understand and enable utilities to acquire the capability to manage risk levels. In short, this supports everything from establishing a good risk culture through to doing things to mitigate risk.

specific configuration. An on-line CDF risk profile is illustrated in Figure 3.14-1.

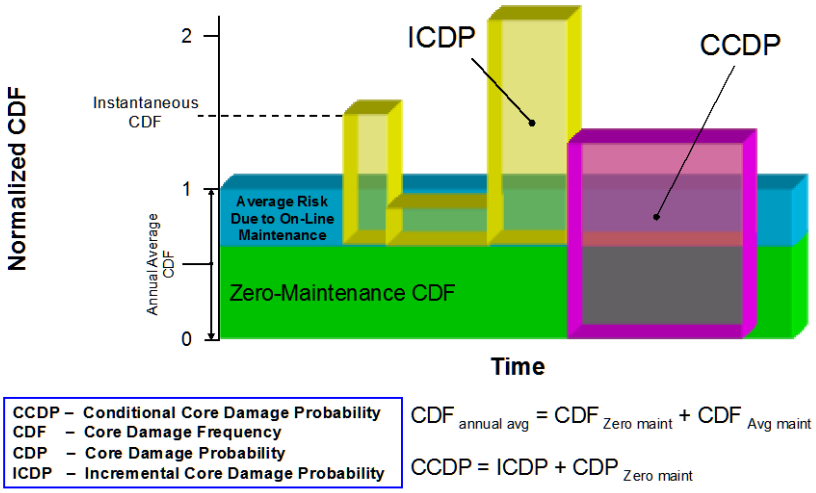


Figure 3.14-1: Example CDF On-line Risk Profile

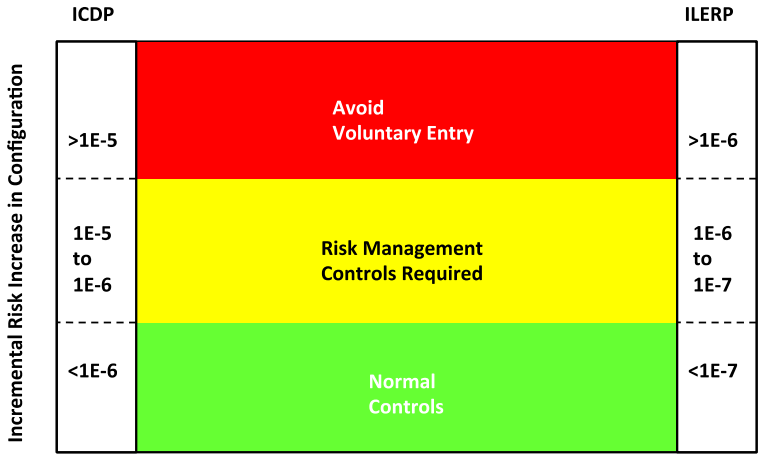


Figure 3.14-2: Risk Significance Thresholds [158]

At some point in the development of risk monitors, it was recognized that CDF numbers were not a good means of communicating levels of risk. The risk monitor evolved to a color-coded risk chart that showed different colors for higher risk levels as illustrated in Figure 3.14-2. Each color had general risk management actions associated with it. The lowest and highest risk

[158] Nuclear Energy Institute, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants (Revision 4A)."

levels are green and red respectively, with color gradations between. When cumulative risk levels are in the green region, normal work processes continue. Risk management actions may be required when risk is in the yellow region. There are to be no "voluntary entries" of risk into the red region. The risk significance thresholds for maintenance were used for CRMP. [159]

These risk profiling programs required the development of CRM and associated implementing procedures at United States nuclear power plants. Procedural documentation of required processes as well as identification of changing management roles and responsibilities based on risk thresholds resulted in these new CRM with commensurate formal training.

3.14.1 Challenges

The actual configuration risk can change a number of times throughout the day as maintenance activities are initiated and completed. Utilities recognized they needed a risk monitor of the planned activities so that work schedules could be adjusted if the risk from combinations of maintenance or test was too high.

Some utility PRA groups developed weekly risk profiles. One utility's method was based on a "bounding" approach by assuming all the work scheduled for a given week would occur concurrently. If the ensuing risk was still in the green region, there were no restrictions on scheduling or rescheduling for that workweek. If the risk was in the yellow or red regions, then consideration for rescheduling was needed.

At some plants, it was recognized that operations personnel were responsible for the actual risk since they had direct control of equipment. Their acceptance of the risk monitoring responsibility was an important organizational adjustment. This meant that Work Control and Planning were responsible for developing planned risk profiles, and Operations was responsible for the actual risk profile. Since Work Control and Planning schedule work by the hour the risk profiles were generated based on the number of hours in a week. The actual risk profiles; however, were based on when equipment was returned to service, which occurs based on time increments of minutes. Therefore, the actual risk profiles were generated based on risk level changes per minute as recorded by the on-shift Control

[159] Ibid.

Room crews. The Control Room crews were responsible for monitoring the actual risk as compared to the planned risk. The actual risk profile became the risk profile of record and has been used for satisfying Maintenance Rule requirements.

Beyond safety, risk profiling had a profound impact on the actual planning and maintenance philosophies. Plant-specific Functional Equipment Groups (FEGs) were revised so that the same amount of work could be accomplished but at a reduced risk, thereby improving nuclear safety. For example, risk profiling demonstrated the importance of conducting work activities for dependent systems (such as water cooled EDGs) concurrently, eliminating a "double hit" on the risk profile. Example risk profiles are illustrated in Figure 3.14-3, Figure 3.14-4, and Figure 3.14-5.

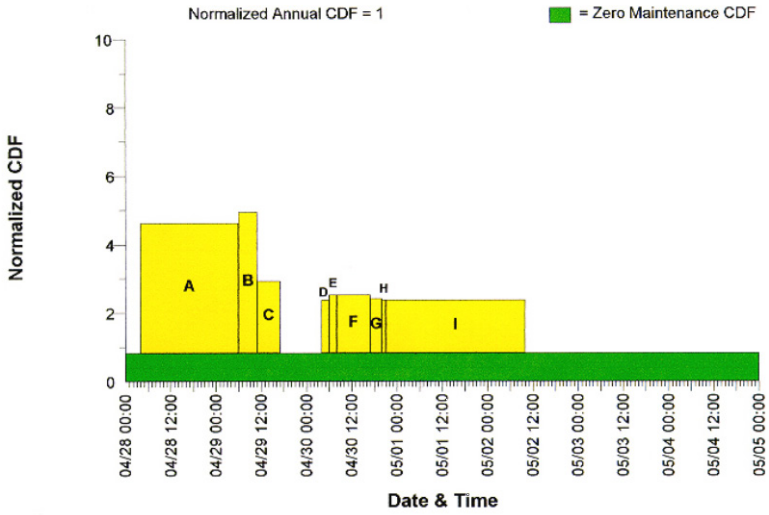


Figure 3.14-3: Example Planned Risk Profile for one week

3.14.2 Legacy

As risk monitors evolved from number-focused to colored CDF risk thresholds, plant personnel embraced them as a means of scheduling test and maintenance. This resulted in developing capabilities to "manage risk" at acceptable levels. This can be seen when actual risk profiles are displayed in graphs of rolling 52-week averages as illustrated in Figure 3.14-6 This "Risk Index" shows the change in normalized yearly CDF from a configuration risk perspective. These risk tools became the technical basis for scheduling and planning work activities. These tools also made it possible to identify specific risk management actions and adjustments for both planned and emergent work items.

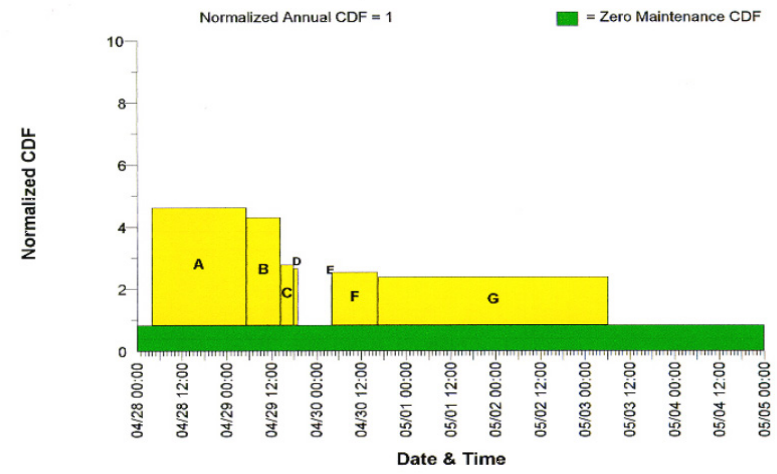


Figure 3.14-4: Example Actual Risk Profile for one week

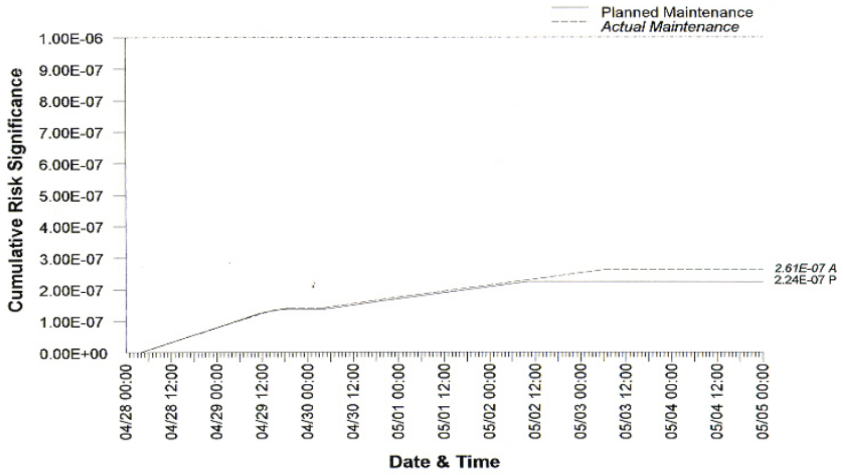


Figure 3.14-5: Planned vs Actual Cumulative Work Week Risk Profile

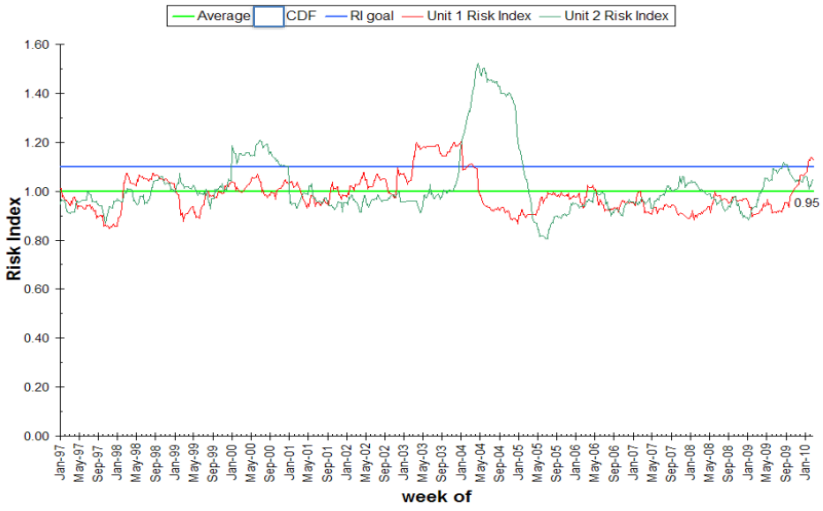


Figure 3.14-6: Example Rolling 52 week averages of Risk Profiles

Section 3.15: Communicating Risk Insights

COMMUNICATING RISK INSIGHTS

Risk communication is challenging but essential for utility and regulatory management. Safety awareness and a sense of ownership are not possible without it.

Expectations about training and continuous improvement should include risk management and the use of PRA as important new areas for corporate and site support in order to foster improved safety and operational performance.

Communicating plant-specific PRA information and insights helps safe and efficient plant operations across the industry. Knowledge transfer must be developed and deployed in a manner that allows information to be easily absorbed. United State licensees have recognized the value of the plant-specific PRA data and information in terms of the way they improve safety and cost. Transferring this information to personnel and identifying the programs, processes, and procedures that can provide these benefits improve safety culture and consciousness.

Licensees use several methods to communicate risk insights. Graphical representations of initiating event contributions, risk-significant equipment, important operator actions, program-specific insights (such as fire protection) and key sources of equipment unreliability are some of the more common media transmitted by PRA groups. Company newsletters are commonly used to heighten staff risk awareness.

Risk models provide different safety and operational perspectives from design or licensing bases. Most licensees have a good understanding of design and licensing basis approaches, as well as the regulatory framework in which they are administered. PRA brings a very different scope where internal events (such as plant trips, LOCAs, and steam generator tube ruptures), external events (such as earthquake, tsunami and wind), as well as events outside the design basis are considered. Structuring PRA information for communication can be challenging. Different organizations have different responsibilities, meaning they have different interests when it comes to data and information.

Data and information can be structured for communication to a broad audience (such as station employees) or a targeted group (such as fire protection engineers). PRAs can provide detailed information about event significance, equipment significance, key equipment failure modes, human error significance, and accident sequencing.

Figure 3.15-1 is an example of a chart that illustrates initiating event contributions. This information is useful for developing prevention and mitigation strategies as well as providing focus for organizational responses relative to recovery actions and

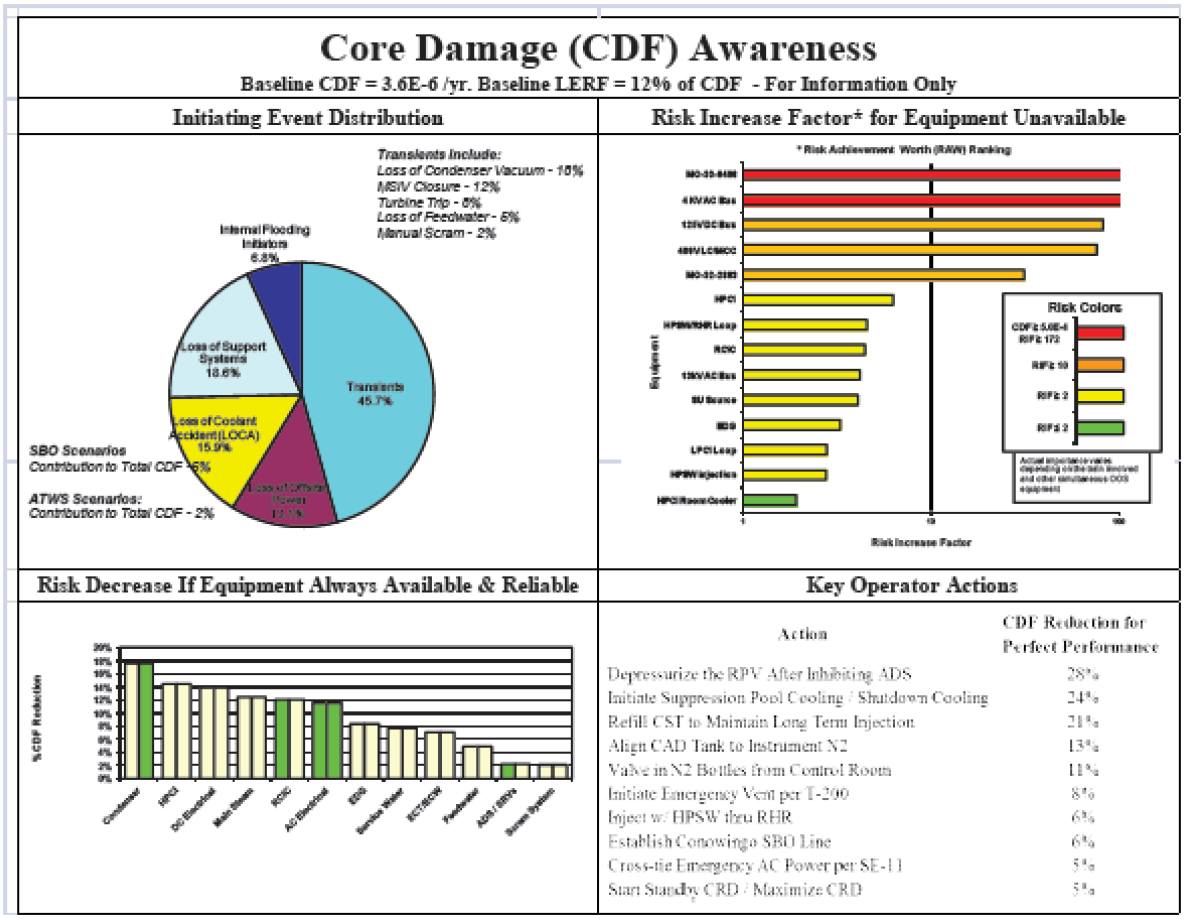


Figure 3.15-1: Core Damage Frequency (CDF) Awareness Chart

emergency response. It supports awareness of the types of events and associated plant response (such as equipment and human response) that fosters a safety awareness and culture such that there are organizational sensitivities to the importance of this equipment and how it is treated.

Charts like the one in Figure 3.15-1 are incorporated into company training programs, wall posters, pamphlets, and information booklets. Other forms of written communication can be developed to support charts like these. For example, important failure modes for risk-significant equipment as identified in a plant specific PRA can be used by equipment reliability groups to provide additional programmatic focus for preventive and predictive maintenance programs. Spatial insights from PRAs can be used to identify risk-significant fire zones or internal flooding areas. The following examples represent different types of PRA insights for different risk hazards and illustrate how communication and training tools can be

developed to improve risk awareness and safety culture of a nuclear power plant organization.

The external event comparison illustrated in Figure 3.15-2 communicates the relative significance of different external event hazards. Some of the external hazard group uncertainties are large, but this does not mean their relative contributions to CDF are not useful.

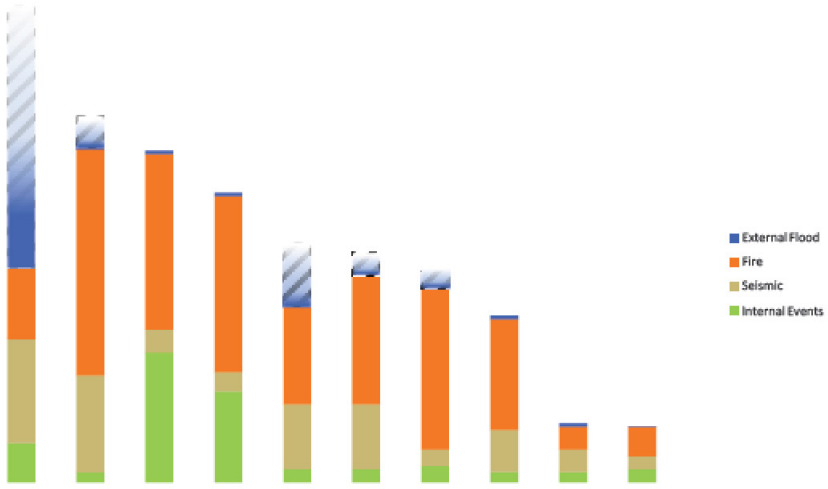
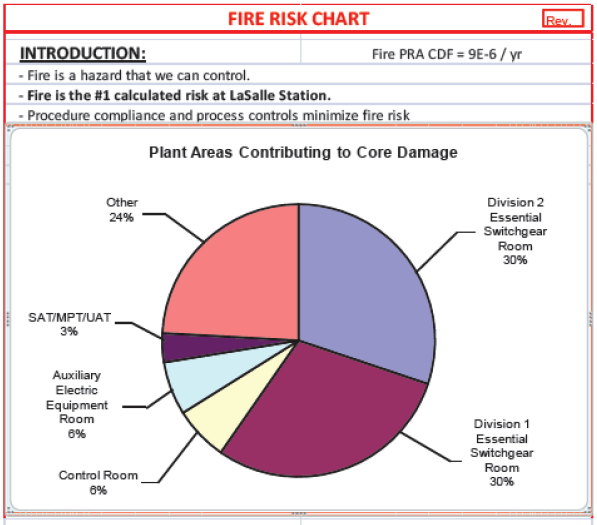


Figure 3.15-2: External Hazards Comparison – Combined CDF per Site/Unit

The fire risk chart in Figure 3.15-3 contains important spatial information relative to the risk contributions of different plant fire zones. Significant fire zones shown along with important prevention



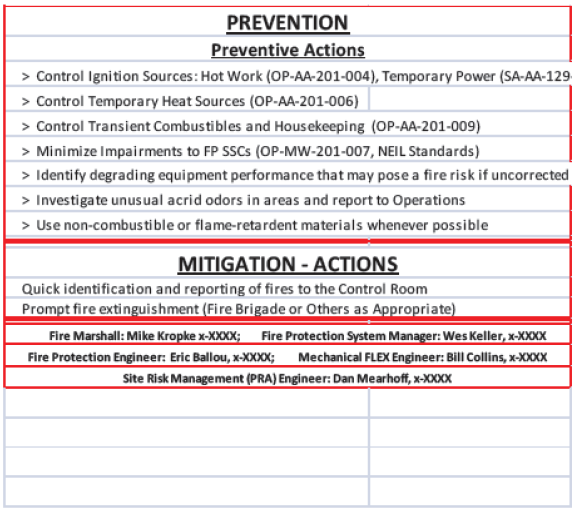


Figure 3.15-3: Fire Risk Chart

and mitigation information. This information can be used to strengthen risk management strategies for internal fire hazards.

An example of newsletter is shown in Fig. 3.15-4. This is an effective way to distribute new or updated PRA information and other important information related to hazards such as fire. The role that these hazards have with respect to regulatory compliance is also highlighted.

Licensees can use these means for communicating information over a wide range of PRA topics such as high risk activity sequences such as heavy load movements and PWR midloop operations along with timelines for successful event recovery actions.

The example in Figure 3.15-4 simply and easily provides a significant amount of information. Risk hazards and their associated major contributors are correlated to specific mitigating and preventive actions. This graphic also highlights the transition from preventive to mitigating strategies. More specific information could then be developed for each risk hazard and correlated to specific procedural steps, training, or other programmatic controls that address individual risk hazards and their associated contributors.

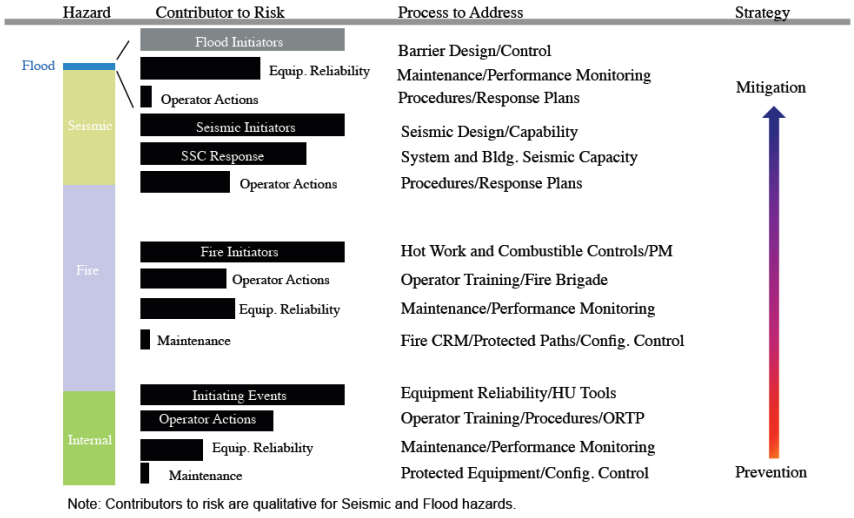


Figure 3.15-4: Example Nuclear Power Plant Risk Contributor Chart

Figure 3.15-6 provides more specific details with respect to a specific risk hazard and correlates it with organizational actions that can be performed to further address the organization's treatment and response. Again, this provides specific direction to plant organizations for enhancing employee awareness, strengthening

High Risk Fire Areas

Limerick has 6 (six) areas that contribute to ~55% of total plant risk due to fires. These high risk areas are as follows:

1. **Auxiliary Equipment Room** (Rm #542) – Control Enclosure, El 289'
2. **Division I, 4kV Switchgear Rooms** (Rm #435 & 429) – Control Enclosure, El 239'
3. **Safeguard System Valve Rooms** (Rm #309 & 376) – Reactor Enclosure, El 217' (Posted HI-Rad Area)
4. **Remote Shutdown Panel Room** (Rm #540) – Control Enclosure, El 289'
5. **13 kV Switchgear Room** (Rm #336) – Control Enclosure, El 217'
6. **Main Control Room & Auxiliaries** (Rm #529, 530, 531, 532, 533, 534 & 534) – Control Enclosure, El 269'

Plant personnel should be aware of these areas when performing work or traversing through the plant. It is the responsibility of each person to uphold housekeeping standards in the plant, and especially in these high risk areas. Poor housekeeping can lead to increased likelihood of fires due to improper storage of transient combustible materials and pooling of combustible fluids.

LGS Fire Risk Chart

A new LGS Fire Risk Chart has been developed. This chart combines risk insights from Limerick's approved Fire PRA model with deterministic Fire Protection information. The chart emphasizes the plant areas that are high contributors to fire risk at LGS. Additionally, important actions to help prevent and mitigate fires are identified, along with the applicable site and fleet procedures. Finally, essential equipment that falls within the scope of the site Fire Protection System (sys 022) is listed on the chart. The LGS Fire Risk Chart will be displayed in multiple locations throughout the site.

Fire Risk in Maintenance Rule (a)(4)

10CFR50.65, paragraph (a)(4) states that nuclear power plant licensees must assess and manage the risk prior to performing maintenance activities. This has historically been risk associated with the internal events PRA and defense-in-depth models. As of December 01, 2013, licensees will also have to evaluate the increase in fire risk prior to performing maintenance. LaSalle and Oyster Creek are NEI pilot plants for implementing this new "Fire in (a)(4)" process. Also, a Fire in (a)(4) workshop was hosted by NEI in Charleston, South Carolina on 01/23/13 and 01/24/13. Limerick is currently in the initial phases of implementing this process. Additional information will be communicated as implementation progresses.

Fire Protection Triennial FASA

A Fire Protection Program Triennial Focused Area Self-Assessment (FASA) will commence in February 2013. The FASA Plan was approved by the Self-Assessment Review Board (SARB) on 01/25/13. This FASA will review a sampling of Fire Protection program attributes related to the 4 (four) fire areas selected. Fire PRA risk insights were considered when determining the areas in the scope of the FASA, as 3 (three) of the areas selected are high contributors to fire risk. The Fire Protection FASA also contains 3 (three) objectives to review a sampling of Multiple Spurious Operations (MSO) scenario resolutions.

Transient Free Zones

Commercial US nuclear power generation facilities were required to resolve all MSO concerns by November 02, 2012. The MSO Project at Limerick was able to meet this milestone on time. The resolution of several MSO scenarios required the addition of new Transient Combustible Free Zones (TCFZ) in the plant. A TCFZ is an area in the plant in which transient combustible material is strictly controlled. TCFZs are used in lieu of a physical fire barrier to provide separation for fire safe shutdown methods, to justify the lack of automatic detection or suppression, or to satisfy other station specific commitments. Follow the requirements of OP-AA-201-009, Rev 11 for the control of transient combustible material in the plant. Transient combustibles can **not** be staged/stored in transient combustible free zones unless authorized by a Transient Combustible Permit (TCP), along with any other required evaluations. The Limerick Fire PRA does credit TCFZs in the plant. Contact the LGS Site Fire Marshall with any questions about approved Transient Combustible Free Zones in the plant.

Figure 3.15-5: Example Licensee Newsletter

training, and enhancing organizational programs and processes that improve nuclear safety.

Through these examples, it can be seen that risk communication can be structured to provide important insights horizontally and vertically within organizations. It is important for these types of communications to be developed as part of overall efforts to improve safety culture.

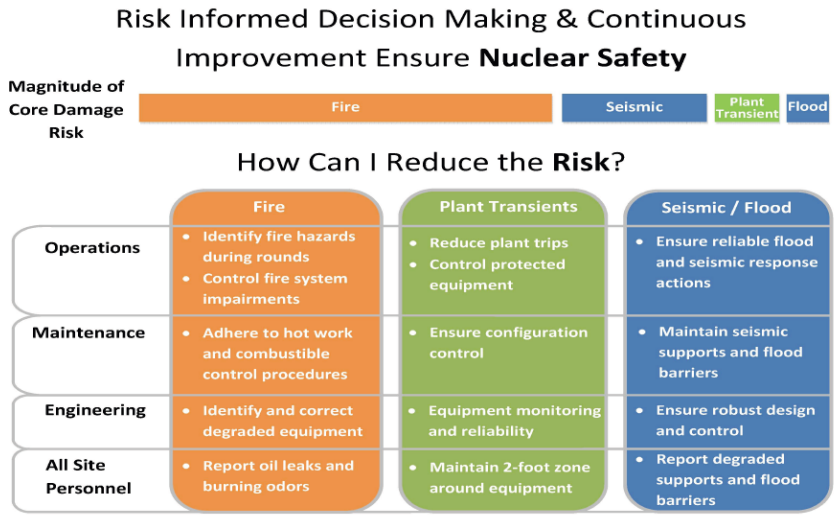


Figure 3.15-6: Risk Reduction Measures

3.15.1 Challenges

Effective risk communication is difficult and can easily result in misinterpretation. Differences between PRA and deterministic methods create perceptions that they conflict, with people tending to default to traditional deterministic mindsets. It is not the deterministic design-basis methods that are the problem: it is understanding DBA limits.

An understanding of PRA applications in relation to deterministic requirements is necessary: how can a safety-related component not be risk significant? Designating a component as safety-related requires specific criteria related to nuclear safety requirements, but its risk significance is related to the likelihood and role that component plays across of spectrum of events (some design basis some beyond design basis.)

Familiarity with design-basis requirements often results in individuals defaulting to them. Herein lies the challenge when it comes to communicating risk insights. The rules associated with

developing PRAs are not well understood - the restrictions applied to deterministic approaches are not applied in PRA. Key PRA tasks such as determination of likelihood directly conflict with the absolute assurance afforded by design-basis thinking (such as "a design basis LOCA concurrent with a seismic event.").

Leadership is an important prerequisite for effective incorporation of risk insights into safety culture. Leaders must have sufficient risk management training. PRA approaches for risk management programs need to be fully described and explained. It is essential that training includes comparisons between PRA and deterministic approaches. Trainees include company officers, executive management, corporate and site management, supervisory personnel and technical staffs along with contractors. Specific organizations include plant Operations, Maintenance, and Safety Engineering.

Development of an organization-wide risk management and PRA training plan is essential. Curricula for specific audiences ranging from basic to specific PRA training are needed. Training has always been an essential part of nuclear power culture, and through the development and delivery of this training, staff PRA understanding and acceptance can be promoted. Personnel can realize that deterministic and probabilistic approaches are compatible, synergistic, and necessary to ensure safety and effective operations over the plant life.

A significant challenge is assigning organizational responsibility for risk management and PRA. Core capabilities within licensee organizations and the NRC must exist to perform risk assessments and implement both qualitative and quantitative risk management programs. Without supportive leadership and organizational structures, fundamental PRA methodologies that include risk identification, assessment, prevention and mitigation cannot work.

3.15.2 Legacy

Once an organization has embraced and fully supported PRA as an important safety tool, organizational trepidations and conflicts between design basis and risk analysis methodologies are reduced. Concurrently, communicating risk with other methodologies and processes (e.g., design related codes and analyses, emergency preparedness requirements, testing and maintenance programs, etc.) further facilitates increased effectiveness and acceptance. If risk

data and information are incorporated into station databases, an opportunity is presented to proactively incorporate risk insights into daily work processes. These processes can include work planning and scheduling, equipment reliability programs and testing programs. Risk communication methods using station databases allows risk to be directly incorporated and reinforces risk awareness.

As with any skill-set, refresher training increases information transfer so that safety awareness continually improves. United States nuclear power plants that embrace PRA have achieved exemplary performance records in terms of nuclear safety, generation and cost reduction.

Section 3.16: Successful application of risk-informed in-service inspection of reactor coolant system piping

Reactor coolant system piping is a key element of the defense-in-depth design of LWRs. Inspection for degradation and leaks using ASME guidance has always been a part of plant operations and maintenance. [160] In the mid-1990s, several factors motivated the consideration of risk information for in-service inspection of reactor coolant system piping.

Piping inspections could only be performed while the plant was shut down, increasing both outage durations and licensee costs. Inspections were also increasing personnel radiation exposures, and the overarching ASME guidance was not fully effective.

The NRC directed an increase of PRA methods used to improve safety and reduce unnecessary burdens. Consequently, PRA information and operating experience indicated that risk-significant piping was not necessarily being subject to ASME identified inspections.

The ASME maintained an active program to ensure that its guidance reflected actual operating experience. As operating experience increased, it became clear that the extant guidance was insufficient as it did not identify many degradation mechanisms. Piping not included in the ASME guidance was also found to be degrading.

This inspection process was one part of a larger program to ensure the effectiveness of piping and other elements. Issues raised during the RI-ISI or other inspections continued to be reviewed, appropriate information disseminated and actions taken where necessary.

Piping degradation was the subject of research programs at the NRC and EPRI. This research included examination of the metallurgical basis for identified degradation mechanisms and development of more predictive, physics-of-failure methodologies.

A Great Success

Industry-wide success in RI-ISI of piping occurred because both the industry and regulator had incentives to improve an existing program using risk analysis. The PRA information needed was not onerous.

RI-ISI was beneficial in reducing the number of inspections (and associated costs) and the amount of radiological exposure of personnel. The plants became safer because degradation mechanisms that were not addressed by previous guidance were now part of the inspection program. Risk-important, non-safety related piping was added to the scope of the inspections.

[160] "Nuclear Inservice Inspection," accessed November 30, 2016, https://www.asme.org/shop/standards/new-releases/boiler-pressure-vessel-code/nuclear-inservice-inspection.

The 1995 NRC PRA Policy Statement stated (in part) that: [161]

> *… the use of risk information should be increased to the extent supported by the state-of-the-art in PRA methods and data.*

Since the PRA scope is not limited to "safety-related" (or similar regulatory designated) components, the RI-ISI program included a provision that some piping not previously inspected under ASME guidance would have to be included in the new program, if risk information demonstrated a level of significance.

The NRC requirements for RI-ISI were written in a way that facilitated staff implementation. NRC Rule 10 CFR 50.55a allows for alternatives to be used, if approved by the Director of the Office of Nuclear Reactor Regulation, and that the licensee: [162]

> *… shall demonstrate that: (i) The proposed alternatives would provide an acceptable level of quality and safety; or (ii) Compliance with the specified requirements of this section would result in hardship or unusual difficulty without a compensating increase in the level of quality and safety.*

This is in contrast to other regulations which are very prescriptive, such as the NRC's fire regulations established in the early 1980's.

Regulatory Guide (RG) 1.174 was one of the ways the NRC supported its policy statement (Section 2.4.5.) RG 1.178 provided supplemental guidance with respect to in-service inspection of

[161] "NRC: Commission Policy Statements - Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities (60 FR 42622)."

[162] "NRC: 10 CFR 50.55a Codes and Standards.," accessed November 30, 2016, http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0055a.html.

piping. [163] A companion staff standard review plan provided additional information on the review process. [164]

The NRC guidance facilitated RI-ISI change in a number of ways. Firstly, programmatic change became voluntary for a licensee. Licensees could continue with their current program should they desire to. Secondly, the extent of affected plant equipment was limited to the reactor coolant system and connected piping. This affected both the size and cost of the program, as well as the associated PRA information. The risk evaluation primarily focused on the internal-events portion of the PRA, although some consideration of external hazards was necessary. Since many licensee PRAs during that time period had robust models that include internal events as a result of completing IPE and IPEEEs, more plants could apply RI-ISI.

The Westinghouse Owners Group [165] and EPRI [166] developed more detailed guidance for industry that standardized and streamlined the RI-ISI process.

3.16.1 Legacy

Draft regulatory guidance on RI-ISI of piping was issued for public comment in late 1997. Comments mirrored those associated with the PRA Policy Statement about the use of risk assessment, focusing on the limitations of the methods. After considering the public comments, the NRC issued RG 1.178 in 1998. Almost all United States licensees have since adopted RI-ISI. [167] RG 1.178 and

[163] Nuclear Regulatory Commission (NRC), "Regulatory Guide (RG) 1.178: An Approach for Plant Specific Risk-Informed Decisionmaking for Inservice Inspection of Piping," April 2003, http://www.nrc.gov/docs/ML0317/ML031780764.pdf.

[164] Nuclear Regulatory Commission (NRC), "NUREG-0800: Standard Review Plan For the Review of Risk-Informed Inservice Inspection of Piping - Chapter 3.9.8," September 2003, http://www.nrc.gov/docs/ML0325/ML032510135.pdf.

[165] Westinghouse Energy Systems, "Westinghouse Owners Group Application of Risk Informed Methods to Piping Inservice Inspection Topical Report," 1999.

[166] Electric Power Research Institute, "Revised Risk-Informed Inservice Inspection Evaluation Procedure," February 10, 2000.

[167] IAEA, "Risk Informed In-Service Inspection of Piping Systems of Nuclear Power Plants: Process, Status, Issues and Development," 2010, http://www-pub.iaea.org/books/IAEABooks/8375/Risk-Informed-In-service-Inspection-of-Piping-Systems-of-Nuclear-Power-Plants-Process-Status-Issues-and-Development.

implementation guidance from the Westinghouse Owners Group and EPRI provide a stable environment for piping RI-ISI.

Comparisons made at one nuclear power plant indicate that the number of inspections made in a particular year was reduced by over 80 per cent and the staff dose (man-rem) was reduced by about 90 per cent. [168] These savings are illustrated in Figure 3.16-1 and Figure 3.16-2.

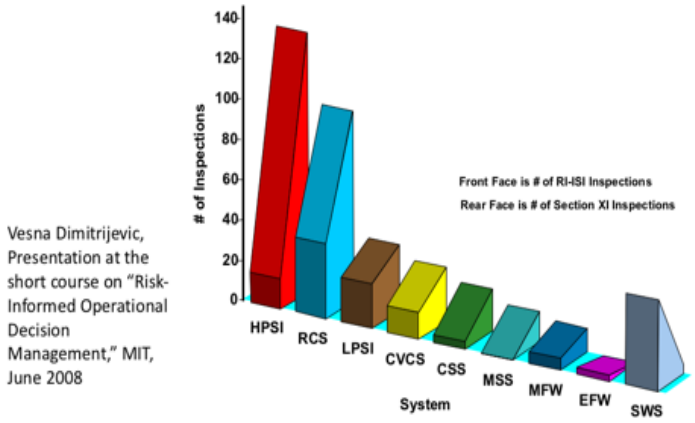


Figure 3.16-1: Number of Inspections before and after the implementation of RI-ISI

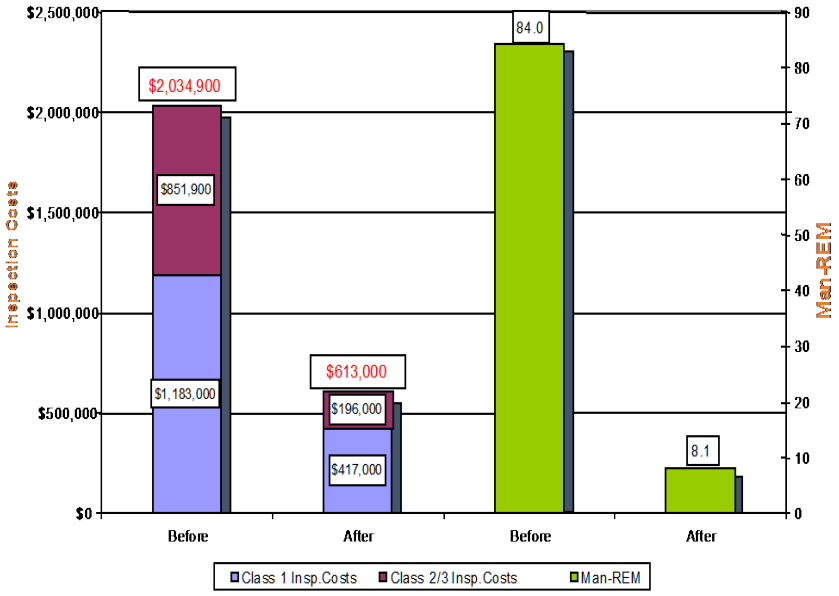


Figure 3.16-2: RI-ISI Cost and Man-REM Savings (per year)

[168] V. Dimitrijevic, "Short Course: Risk-Informed Operational Risk Management" (Massachusetts Institute of Technoloy (MIT), 2008.

RI-ISI implementation occurred because both the industry and the NRC had incentives to improve an existing program. The RI-ISI program reduced the number of inspections, costs and personnel radiation exposure. Plants became safer as degradation mechanisms that were not addressed previously by the ASME guidance were now being identified.

Section 3.17: Risk-Managed Technical Specifications (RMTS)

The NRC requires technical specifications to help ensure that equipment testing and maintenance do not result in unsafe conditions. [169] The first limits and conditions established were based on deliberately conservative engineering judgments, potentially incurring unnecessary costs.

As the number of plants increased, so too did operating experience. More PRAs were performed, and it became clear that the original technical specifications were sometimes severely conservative, and sometimes not conservative enough. Both licensees and the NRC were motivated to improve technical specifications so that plant availability, operating costs (regulatory and industry costs) and safety would always improve.

The industry and the NRC met over several years to identify a set of risk-informed technical specification initiatives. These included risk-informed approaches to missed surveillance tests, plant mode changes with unavailable equipment, owner-controlled surveillance test frequency programs, and risk-informed completion time programs.

RMTS is implemented via a complex set of interactions between NRC general guidance, standards development organizations (SDOs), owner groups, industry groups, and the approach developed by licensees.

Regulatory Guide (RG) 1.177 [170] and Standard Review Plan Section 16.1 [171] provide key information on acceptable licensee programs for RMTS. Using the general regulatory model described in

TECHNICAL SPECIFICATIONS

Technical specifications, plant operating conditions and limits required by the NRC regulations, can have a significant impact on the availability of important plant equipment. By extension, these elements affect the ability of the plant to reliably generate electricity.

Risk-managed technical specifications provide an effective means for better managing plant operations and improving safety.

[169] Nuclear Regulatory Commission (NRC), "Rule 10 CFR50.36: Technical Specifications," 36.

[170] Nuclear Regulatory Commission (NRC), "Regulatory Guide (RG) 1.177: An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications," May 2011, http://www.nrc.gov/docs/ML1009/ML100910008.pdf.

[171] Nuclear Regulatory Commission (NRC), "NUREG-0800: Risk-Informed Decision Making: Technical Specifications - Chapter 16.1," March 2007, http://www.nrc.gov/docs/ML0325/ML032510135.pdf.

Regulatory Guide 1.174, [172] these documents describe a three-tiered process:

1. Assessment of individual technical specification changes using the plant-specific PRA to ensure small or no changes in annual-average CDF and incremental conditional core damage probability; [173]
2. Review and management of potentially high-risk configurations; and
3. Establishment of an overall program to ensure that other risk-important configurations are managed (this tier aligns with the requirements of the Maintenance Rule.)

SDOs, owner and other industry groups such as the NEI have proposed approaches for the NRC to consider. Upon approval, these approaches can be implemented by individual licensees. Most United States nuclear licensees have implemented the missed surveillance and mode change with inoperable equipment risk initiatives for their plant-specific technical specifications

For the past several years, the industry efforts have focused on two areas. The first area is surveillance test frequencies. This approach (termed "technical specification initiative 5b") is intended to provide licensees more flexibility in technical specification implementation by moving certain test frequency information from the technical specifications to a licensee-controlled document. A guidance document was submitted [174] and approved by the NRC in 2007. [175]

[172] United States Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions on Plant Specific Changes to The Licensing Basis."

[173] This is a measure of the risk while a particular test or maintenance activity is taking place, which may place the plant in a high risk condition for a limited amount of time.

[174] Nuclear Energy Institute, "Risk-Informed Technical Specifications Initiative 5b: Risk-Informed Method for Control of Surveillance Frequencies," April 2007, http://pbadupws.nrc.gov/docs/ML0713/ML071360456.pdf.

[175] Ho Nieh, "Final Safety Evaluation for Nuclear Energy Institute (NEI) Industry Guidance Document NEI 04-10, Revision 0, 'Risk-Informed Technical Specifications Initiative 5b, Risk-Informed Method for Control of Surveillance Frequencies' (TAC NOS. MB2531 and MD3077)" (Washington, D.C: Nuclear Regulatory Commission, September 28, 2006).

Since that time a number of licensees have chosen to implement this approach. [176]

The second area of industry effort has been RMTS. This approach (termed "technical specification initiative 4b") provides licensees with greater flexibility in calculating completion times for certain technical specification requirements based on the plant-specific PRA. The PRA is used extensively to evaluate appropriate completion times based on the risk significance of unavailable equipment, and the potential payoff is substantially greater than the "5b" approach described above. A guidance document was submitted [177] and approved by the NRC in 2007. [178] A smaller number of licensees are now implementing this approach relative to the "5b" approach described above, reflecting its greater complexity. [179]

3.17.1 Challenges

Modern plants are complex and comprise thousands of SSCs. Each has its own design pedigree, operating history, test specifications, and maintenance requirements. Systematically assessing plant risk and the changes in plant risk that could occur if one or more pieces SSCs are unavailable requires considerable effort.

PRAs used for RMTS need to be of sufficient technical acceptability. PRAs meeting the ASME/ANS Standard RA-S-2009 (discussed in Section 2.4.2) Capability Category II, are generally deemed technically adequate. The assessment requires consideration of both annual average CDFs (the typical result of PRAs) and "incremental" frequencies that reflect the impact of individual equipment outages. Consideration of the value of non-safety equipment (which can play an important role if safety systems are

[176] Nuclear Regulatory Commission (NRC), "Overview of Risk-Informed Regulatory Activities Associated with Technical Specifications," February 2015.

[177] Nuclear Energy Institute, "Risk-Informed Technical Specification Initiative 4b: Risk-Managed Technical Specifications (RMTS) Guidelines," November 2006, http://pbadupws.nrc.gov/docs/ML0713/ML071360456.pdf.

[178] "Final Safety Evaluation for Nuclear Energy Institute (NEI) Industry Guidance Document NEI 06-09, Revision 0, "Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specificaitons" (Washington, D.C: Nuclear Regulatory Commission, May 2007).

[179] Nuclear Regulatory Commission (NRC), "Overview of Risk-Informed Regulatory Activities Associated with Technical Specifications."

out of service) and a broad spectrum of initiating events (including fire initiators) also demand high quality PRAs.

Reactor designers, operators and the NRC have historically worked to standardize plant technical specifications. Variability among plants can make this goal difficult to achieve.

The Maintenance Rule (discussed in Section 2.4.1) introduces additional requirements with respect to plant safety while using plant-specific PRA results, and introduces key risk concepts into the regulation (such as balancing availability and reliability). Synchronizing technical specification and Maintenance Rule programs is in itself a complex operation.

3.17.2 Legacy

The NRC and licensees both recognize the value in improving technical specifications. Both continue to dedicate significant resources in this area, including supporting the work of SDO and owner groups.

The discussions of both the policies and implementation of risk-managed technical specifications are available to the public. Draft policies and rule changes are specifically published for public comment.

Technical specifications, plant operating conditions and limits required by NRC regulations can have a significant impact on the availability of important plant equipment. By extension, this affects the ability of the plant to reliably generate electricity. There has been a continuing interest in improving the objectivity of the specifications. PRA has proven to be valuable means for accomplishing this improved objectivity. With the implementation of the Maintenance Rule, particularly as revised in 1999, the potential value of risk analysis has become even more evident.

Section 3.18: Reactor Oversight Process (ROP)

A fundamental aspect of the NRC's mandate to ensure public health and safety involves the inspection of licensed facilities. Inspections verify that licensees are operating their facilities in compliance with all relevant regulations.

In the late 1990s, the NRC reevaluated its inspection program. In 1999, the NRC internally concluded that: [180]

> *… the current inspection, assessment, and enforcement processes (1) are at times not clearly focused on the most safety important issues, (2) consist of redundant actions and outputs, and (3) are overly subjective with NRC action taken in a manner that is at times neither scrutable nor predictable.*

These concerns were echoed by external stakeholders such as Congress, the industry, and the public.

The NRC identified the opportunity to improve the regulatory oversight of licensees, directing the staff to work towards this goal. The overall objective of developing improvements to these processes was to:

- improve the objectivity of the oversight processes so that subjective decisions and judgment would not be central process features;
- improve the scrutability of these processes so that NRC actions would have a clear tie to licensee performance; and
- risk-inform the processes so that NRC and licensee resources would be focused on those aspects of performance having the greatest impact on safe plant operation.

The resultant inspection program now implemented for all United States reactors uses risk information to determine what is inspected, monitor individual plant performance over time, and judge the event significance.

SUCCESSFUL OVERSIGHT

Risk information has been used successfully in the ROP

Improvements in the consistency and objectivity relative to the previous process were realized through the use of more objective and quantitative measures of plant performance.

Explicit guidance on the regulatory response to inspection findings was made possible.

Considerable investment was required to develop and test the new program. Full implementation also required considerable resources.

The benefits of the program justified the costs incurred.

[180] W. Travers, "SECY-99-007: Recommendations for Reactor Oversight Process Improvements."

The NRC developed a plan for the further development and implementation of the programmatic changes. The implementation was trialed on pilot plants prior to full implementation.

The resulting program consists of a set of high-level performance goals such as "maintain a low frequency of events that could lead to a nuclear reactor accident." It involves more detailed "cornerstones" that connect high-level goals with designing NPPs that could be inspected and operational characteristics such as the performance of mitigating systems. It also includes a set of PIs, with one or more PI for each cornerstone (such as emergency AC power reliability).

The program has a "baseline" inspection program that monitors licensee performance in areas not covered by the performance indicators noted above. NRC resident inspectors, supported by other inspectors as needed, provide on-going monitoring. The areas of plant design and operations most closely watched are based on the plant-specific PRA, as described in the following from the NRC inspection manual: [181]

> *Risk has been factored into the baseline inspection program in four ways: (1) inspectable areas are based on their risk importance in measuring a cornerstone objective, (2) the inspection frequency, how many activities to inspect, and how much time to spend inspecting activities in each inspectable area is based on risk information, (3) the selection of activities to inspect in each inspectable area is based on plant-specific risk information, and (4) inspectors are trained in the use of risk information.*

Information from the PIs, the baseline inspection program, and other inspections are periodically compiled and reviewed. The resulting measure of plant performance is indicated by an "action matrix" that defines the future level of NRC oversight. The matrix has five levels, from "licensee response" (meaning the licensee will not be subject to additional NRC inspection) to "unacceptable" performance. All of this information is summarized for public review

[181] Chapter 0308, Attachment 2 of "NRC: Inspection Manual Chapters."

on the NRC's website and discussed in annual public meetings between the NRC and each licensee.

The results of individual inspection findings are assessed with respect to their risk significance. The resulting conclusion on risk significance is used to determine the extent of follow-up inspection, which can range from no additional inspection to an extensive multi-week inspection by one or more inspectors. The results are color-coded in a four-level system (green, white, yellow, and red), and included in the action matrix evaluations discussed above.

As implemented, PRA information is used to help determine what aspects of plant design and operations should be inspected on a routine basis and during other inspections. PRA information helps define the content of and action thresholds for a set of industry-wide and plant-specific performance indicators, and to help judge the significance of conditions found or events that occurred.

The NRC undertook a series of projects to improve the risk capabilities of its staff. New training programs provided PRA information to inspectors and their managers. These programs ranged in subject from overviews to detailed training on specific technical subjects. A new "senior reactor analyst" inspector category was developed. These inspectors had expertise in both inspection processes and risk assessment. Each NRC regional office is staffed with several of these experts.

3.18.1 Challenges

The NRC inspection program was very large in terms of staff and the number of affected facilities. It included the assessment of licensee performance using the analysis of plant performance data and inspection findings – all requiring considerable effort.

All of the affected licensed reactors had conducted PRAs of varying quality and regulatory compliance in response to earlier regulatory initiatives. [182] Methods and tools (such as fault tree analysis) varied across the studies, reflecting the lack of PRA standards at that

[182] Nuclear Regulatory Commission (NRC), "Generic Letter (GL) 88-20: Individual Plant Examination for Severe Accident Vulnerabilities 10 CFR 50.54(f)," November 23, 1988.

time. [183] Some PRA elements (such as fire risk analysis) were relatively simplistic and conservative.

This variability was a significant challenge to the NRC when it attempted to develop realistic and objective assessment tools. The NRC developed and maintained a set of Standardized Plant Analysis Risk (SPAR) models. Some perspectives on this development are provided in a separate paper, attached to the end of this section.

The development of performance indicators using plant data (such as equipment test results translated into quantitative estimates of system reliability) required the development of methods to collect and analyze the data, techniques for displaying the results, and action "thresholds" that would trigger remediation.

The new "baseline" inspection program was a significant change, with focus on the most risk-significant plant equipment. Some licensee activities were not covered by the new performance indicators. The new program included benchmarking the utility's plant-specific PRA with the NRC SPAR model for that station. [184] This benchmarking was intended to ensure consistency in risk significance between the more simplistic SPAR models and the plant-specific PRA. Additional baseline inspection efforts were performed for plant performance metrics, current regulatory issues and associated status.

Both the NRC and affected licensees had limited personnel with PRA expertise. PRA expansion into the ROP required more expertise than what was available, particularly among the parts of the NRC directly involved in inspection activities. Extensive training programs were established.

[183] The SPAR models, like many licensee risk models, reflect the limitations in realistically modeling certain hazards such as fire or certain plant operating states. The SDP process includes provisions (alternative approaches) for considering the risks from such hazards. In some cases, the results of using these alternative approaches can become the focus of considerable discussion between the NRC and licensees.

[184] Brian W. Sheron, "SECY-15-0124: Status of the Accident Sequence Precursor Program and the Standardized Plant Analysis Risk Models," October 5, 2015, http://www.nrc.gov/docs/ML1518/ML15188A101.pdf.

3.18.2 Legacy

Deciding to revise the ROP involved extensive interactions with stakeholders, the public and the NRC. This extensive interaction and pilot plant trials were key to successful program implementation.

Licensee response since has been varied, reflecting (at least in part) the variability of licensee commitments to PRA plant-specific risk models. Some licensees with more sophisticated PRA models use the PRA to provide additional insights for interacting with the NRC. For example, a plant event or condition can use the PRA to reflect its level of significance. [185] Other licensees spend considerable resources to address specific issues contained in the NRC assessment if this reduces the significance of the finding (such as from "yellow" to "white").

The ROP has succeeded because it provides more objective information on plant performance, focuses agency inspection resources on the most risk-important equipment and activities, and continually assesses plant performance publicly.

The NRC requires extensive internal infrastructure, staff expertise, training, and plant models. The associated costs can be avoidable in other circumstances - PRAs that align with common standards and use common software could obviate the need for regulatory models and software. Externally provided regulatory PRA training may now be available that could reduce developmental and implementation costs. However, the benefits of the program, including the objectivity and public availability, justified the costs incurred.

3.18.3 Addendum: Evolution of NRC's SPAR Models

In the mid-1990s, the NRC began developing a set of risk models that were intended to serve internal needs. These models, called "simplified" risk analysis models (now "standardized" risk analysis models) or SPAR models, have seen increasing use since that time.

One issue facing the NRC after the publication of its 1995 PRA Policy was how to deal with "generic safety issues" that affected the entire

[185] The SDP process includes a step for licensees to review and comment on the USNRC risk evaluation. The USNRC staff considers the comments, adjusts the evaluation as it considers appropriate, and finalizes its evaluation.

industry. [186] The set of then available risk models consisted of a few detailed plant-specific PRAs (see Section 2.3.2), the NUREG-1150 study (see Section 2.3.7), IPEs and IPEEEs (see Section 2.3.6). These models were also subject to wide variation from licensee to licensee.

The NRC examined a number of options for developing a library of PRA models that could support regulatory decisions. This library would include (in one option) all licensee models and related software, and training staff in their use. The NRC ultimately pursued another option and developed a set of simplified risk models using common modeling approaches and software, adapted as necessary to reflect important plant-specific information. These became the "SPAR" models.

In subsequent years, the NRC significantly expanded the uses of the SPAR models. Importantly, the NRC began using the models to aid assessment of inspection findings and judging the significance of these findings. With these additional uses, more complete and accurate models were judged to be needed. As one result, SPAR model scope has expanded to include external hazards, accidents initiated during shutdown conditions, and PRA Level 2 information. SPAR models have been compared with plant-specific PRAs and adjustments made, as necessary. [187]

Concurrently, the United States nuclear industry invested in the development of PRA standards and a related peer review process (see Section 2.4.2). In the late 2000's, the NRC decided that the SPAR models should also meet the standards, and conducted a peer review in 2009. [188] SPAR model improvements were undertaken, and completed several years later.

---

[186] Generic safety issues are those that could affect multiple NRC licensees. The agency maintains a database of such issues, reporting on their identification, the analysis of their implications to safety, and their regulatory disposition. More information is contained in "NUREG-0933, Main Report with Supplements," 0933, accessed December 1, 2016, http://nureg.nrc.gov/sr0933/.

[187] SPAR evolution is discussed in greater detail in Richard R. Sherry, Peter L. Appignani, and Robert F. Buell, "The NRC's SPAR Models: Current Status, Future Development, and Modeling Issues," 2008, https://inldigitallibrary.inl.gov/sti/4074965.pdf.

[188] The results of this peer review are discussed in James Knudsen et al., "Peer Review of NRC Standardized Risk Analysis Models" (ANS PSA 2011 International

Given the state of PRA information at the time, it was not an unreasonable decision to develop the SPAR models. They have since been very useful, but had the decision been made today in light of PRA standards that were not available in the 1990s, it is likely that SPAR models (or something similar) would not have been developed.

More specifically, a modern-day decision to develop and use SPAR-like models should take into consideration several factors:

- **Intended use.** If the NRC had not expanded the uses of the SPAR models, then subsequent investment in model improvements (including the peer review and comparisons with standards) may not have been cost-effective. Once the decision was made to use the models in regulatory activities such as the ROP, this investment became reasonable.
- **State of development of licensee PRA models.** If all licensees are developing PRAs according to modern standards and using common software (such as SAPHIRE) then they can be adopted by the regulatory authority more efficiently. This was not the case when the NRC started its SPAR model development.
- **Availability of licensee PRA models to regulatory authority.** If licensees are willing or required to provide their PRA models (and updates) to the regulatory authority, then the authority's adoption and subsequent use could be more efficient. This also was not the case when the NRC made its initial SPAR decisions.

Topical Meeting on Probabilistic Safety Assessment and Analysis, Wilmington, NC: American Nuclear Society, 2011).

Section 3.19: Limited Success of Risk-Informed Graded Quality Assurance (RI-GQA) or Rule 10 CFR 50.69

A LIMITED SUCCESS

RI-GQA has met with limited success for practical reasons, such as the shear complexity of the plants and the associated record keeping. Further, this concept has challenged existing philosophies leading to reluctance of some regulatory staff to permit changes. It is unclear at present whether future licensee applications will meet with greater success.

When United States reactors were originally licensed, QA and other special treatment requirements were implemented on many plant components. [189] The intent of these requirements was to provide additional confidence that the equipment would be reliable and dependable (see Section 3.5).

PRA emerged after these plants commenced operation, allowing more objective and integrated risk measurement. This showed that many components previously identified as needing special treatment were not particularly important to plant safety and risk.

The NRC's 1995 PRA Policy Statement led to suggestions that less important components could be identified with PRA. The costs incurred by licensees in the initial implementation would by offset, at least conceptually, by reduced future operating costs. The resultant Rule 10 CFR 50.69 "Risk-Informed Graded Quality Assurance (RI-GQA)" was the formalization of this idea.

3.19.1 Challenges

The RI-GQA process could be applied to the many thousands of pieces of equipment in a plant. [190] All of the associated special treatment requirements for each component would be identified, including the basis for their requirement. This required extensive resources.

A PRA that is used to identify and evaluate components is required to meet industry PRA standards and Regulatory Guide (RG) 1.200. PRA results were supplemented with a qualitative risk assessment

[189] In the NRC paper proposing the publication of the draft Rule 10 CFR 50.69 for comment, the staff indicated that special treatment requirements are "current requirements imposed on SSCs that go beyond industry-established requirements for equipment classified as commercial grade that provide additional confidence that equipment is capable of meeting its functional requirements under design basis conditions. These additional special treatment requirements include additional design considerations, qualification, change control, documentation, reporting, maintenance, testing, surveillance, and quality assurance requirements."

[190] The NRC guidance permitted limited applications within a plant to, for example, a subset of plant systems; however, each system selected had to be fully evaluated.

that incorporated other factors such as mode change, shutdown safety, use in emergency operating procedures, initiating events, failure of a separate risk-significant component, or use to mitigate accidents/ transients.

The risk-significance categorization process was performed in accordance with industry guidance and plant implementation requirements. Many safety-related systems contain thousands of components, all of which had to be categorized and evaluated by an IDP. The IDP is a representative, multi-disciplinary committee of experienced experts with special training in risk-informed applications and the use of PRA. The risk significance categorization approved by the IDP would then be implemented into databases to implement alternate treatment requirements.

NRC personnel raised concerns about relaxing special treatment requirements. These concerns were in part technical, relating to potential decreases in equipment performance. They were also part philosophical, as the resources saved by the licensee may not necessarily be re-invested in safety. This reluctance may have contributed to a more restrictive review process. There was certainly utility reluctance, lack of understanding, and resistance to change due to trepidation that additional regulatory scrutiny or inspections would occur in areas where the controls, permitted to be relaxed, were reduced. These challenges are now being revisited as a part of the new industry effort on "Delivering the Nuclear Promise."

Estimates of the potential cost savings were rather uncertain reflecting both uncertainty in potential relaxations in burden and the ability to forecast such reductions to allow reassignment of resources and associated savings. Significant benefits in certain areas showed that categorization and scope reductions did result in an emphasis on risk significant equipment (safety and otherwise) - which improved reliability.

Implementation of RI-GQA required an extensive licensee program. This included procurement programs that had to deal with differences in form, fit, or function. There was also a lack of criteria for "additional confidence" which resulted in several procurement applications failing. A lack of an engineering alternate treatment development procedure and associated processes resulted in long delays for achieving benefits. A lack of management focus and priority on achieving the benefits exacerbated this issue. And there

was also licensee uncertainty in the level of regulatory exposure from additional NRC inspections if non-safety related parts were being used for safety related applications.

In terms of safety-related repair and replacement, there is currently a lack of appropriate codes, standards, or code cases that would allow the practical use of alternative non-safety related power piping codes.

These challenges are now being addressed through new industry efforts to have more utilities submit license amendment requests to implement Rule 10 CFR 50.69.

3.19.2 Implementation

From the mid-1990s, STP initiated a RI-GQA program leveraging the unusual redundancy of its design and the sophistication of its PRA model. The NRC later issued guidance (in the form of a regulatory guide) that described one acceptable approach for implementing RI-GQA. The STP application was approved in 2002, allowing it to adjust the scope of the special treatment requirement programs such as Appendix J (Type B & C Containment Leakage Testing) as well as other engineering testing programs (such as MOV, Generic Letter 89-10).

Scope reductions that reduced the level of effort to comply with special treatment requirements allowed increased organizational focus on backlog work items and other activities. In contrast, procurement of industrial components for safety-related applications for minimal risk significant equipment was marginally successful. There were instances where identical non-safety related parts could be obtained, and in some cases, a limited commercial dedication process was able to be performed.

Minor design or material differences between current and candidate replacement parts effectively stopped this initiative in some instances. The ability to employ alternative ASME non-safety related codes and standards for repair and replacement of piping and other passive components could not be achieved. Various code cases were developed by ASME to support the categorization of SSCs relative to the repair/replacement of passive components such as piping and supports. The restrictions required by the NRC (such as repairs having to span from anchor point to anchor point, greatly

exceeding the scope of the repair) obviated the use of alternative treatment.

At this time, STP has expanded the risk significance categorization to include all safety and many non-safety related systems for a total of 96 systems. The categorization effort produced significant understanding of the importance and relationship of SSCs to their associated activities and treatments. This allowed easy and technically based prioritization of many plant activities, and also focused treatments of components across many plant programs. The risk significance categorization process has evolved into a specialized qualitative risk significance categorization process that has even been used to categorize station doors and access ways.

This early work was followed by the development of a new NRC voluntary regulation, Rule 10 CFR 50.69, which was tested at the Vogtle Electric Generating Plant. This rule provided an alternative means of treating safety-related, low-risk significant equipment. Following NRC review, a Vogtle license amendment was approved in 2014. The licensee intends to perform a full implementation of RI-GQA, but will still develop alternate treatment programs for various engineering divisions and establish procurement processes. These items will require a multi-year integrated strategic plan to provide for both the risk significance categorization efforts, as well as the alternate treatment program development.

3.19.3 Legacy

In general, licensees have been reluctant to pursue RI-GQA. The additional analysis of equipment and related record keeping appeared substantial with uncertain cost savings. The obvious exception was STP, with its unusually redundant design and well established plant-specific PRA increasing the utility of this process. This effectively reduced implementation costs as it could leverage previous work. It is unclear at present whether future licensee applications for implementing 10CFR 50.69 will meet with greater success, but some licensees are pursuing this.

Section 3.20: Risk-Informed In-Service Testing

No Success

Although both the NRC and ASME have implemented programs that could be used by licensees to implement RI-IST, neither has attracted much attention.

It appears that the initial costs of regulatory approval and implementation outweigh the perceived long-term benefits, especially in consideration of the more limited reductions in equipment testing.

Little information regarding the testing of safety-related equipment such as pumps and valves existed when United States nuclear power plants were originally designed. Consensus standards committees that included ASME developed standards to define testing requirements, frequencies, and scope. Conservative approaches were initially adopted, which permeated future testing acceptance criteria.

PRA provided a more realistic assessment of the safety importance of plant equipment, important equipment failure modes, and the safety implications of operational decisions such as testing frequency and system testing configurations. By extension, PRA provided a method for reassessing the originally conservative testing approaches. [191] The NRC PRA Policy Statement helped spur the development of RI-IST.

3.20.1 Challenges

Several challenges faced the RI-IST program. Licensees had to develop new testing procedures with alternate testing approaches based on component risk significance levels. They also had to develop extensive information collection systems to catalog equipment potentially involved in the RI-IST program.

Regulatory approval of new test programs was required to replace those in use. This approval sometimes took an extensive period to resolve regulatory reviewer concerns. Further, the associated PRA scope and quality needed to be "sufficient," with little guidance on what this meant.

3.20.2 Implementation

The RI-IST program could be implemented in two ways. One way involved Regulatory Guide (RG) 1.175 and an application for license amendment to NRC. The other involved the development of "code cases" by SDOs. These code cases involved developing new methods with ongoing refinement. The NRC would approve the updated code case for inclusion in a regulatory guide. Licensees

[191] PRA studies also indicated that some equipment were much more important to safety than previously expected.

could then implement the new method without further NRC interaction.

Six licensees submitted requests in the late 1990's. Four were withdrawn, and two were approved (San Onofre and Comanche Peak). [192]

The NRC endorsed a number of code cases in 2003 in Regulatory Guide (RG) 1.192. [193] It is unclear at this time how many licensees have used the code cases that support the implementation of RI-IST. [194]

3.20.3 Legacy

Regulatory Guide 1.175 was issued for public comment in 1997. Public feedback followed historical trends with the support from the nuclear industry and objection from public groups. The final versions were published in 1998.

At about the same time, concerns emerged both within and outside of the NRC regarding RI-IST. Some individuals involved with the existing IST programs raised concerns that the RI-IST programs could lead to safety-related equipment degradation and potentially unacceptable performance in emergency situations, even though the risk-informed approach indicated more optimal approaches could be available.

It appears that, in practice, the allowable changes are not sufficient to outweigh implementation costs related to NRC approval.

[192] Comanche Peak participated in a pilot program to test RI-IST methods, information from which supported the development of Regulatory Guide 1.175.

[193] Nuclear Regulatory Commission (NRC), "Regulatory Guide (RG) 1.192: Operation and Maintenance Code Case Acceptability," August 2014, http://www.nrc.gov/docs/ML1334/ML13340A034.pdf.

[194] At the time of its withdrawal, at least one licensee previously using the RG 1.175 approach indicated their intent to use the code cases.

Bibliography

Analysis, U. S. Nuclear Regulatory Commission Division of Risk. *Probabilistic Risk Assessment (PRA): Status Report and Guidance for Regulatory Application, Draft Report for Comment*. Division of Risk Analysis, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1984.

"ANS/ASME-58.22-2014, Requirements for Low Power and Shutdown Probabilistic Risk Assessment -- ANS / Store / Standards." Accessed December 1, 2016. http://www.ans.org/store/item-240304-E/.

"ASME - STANDARDS - Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications." Accessed November 28, 2016. https://www.asme.org/products/codes-standards/ras-2008-standard-level-1-large-early-release.

Atomic Energy Commission. *Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants: A Study of Possible Consequences If Certain Assumed ... Were to Occur in Large Nuclear Power Plants*. University of California Libraries, 1957.

Callan, L. Joseph. "(For the Commissioners) SECY-97-077: Draft Regulatory Guides, Standard Review Plans and NUREG Document in Support of Risk Informed Regulation for Power Reactors," April 8, 1997. http://www.nrc.gov/reading-rm/doc-collections/commission/secys/1997/secy1997-077/1997-077scy.pdf.

———. "(For The Commissioners) SECY-97-168: Issuance for Public Comment of Proposed Rulemaking," July 30, 1997.

Chunis, J.A., and P.J. Amico. "Millstone Unit 1 Probabilistic Risk Assessment of theDecay Heat Removal Systems." Connecticut: Northeast Utilities Services Company, January 1979.

Collins, H. E., B. K. Grimes, and F. Galpin. "Planning Basis for the Development of State and Local Government Radiological Emergency Response Plans in Support of Light Water Nuclear Power Plants." *ResearchGate*, December 1, 1978. doi:10.2172/5765828.

Dimitrijevic, V. "Short Course: Risk-Informed Operational Risk Management." Massachusetts Institute of Technoloy (MIT), 2008.

Electric Power Research Institute. "Revised Risk-Informed Inservice Inspection Evaluation Procedure," February 10, 2000.

Epler, E. P. "A PHILOSOPHY OF CONTROL-SYSTEM DESIGN." Oak Ridge National Lab., Tenn., 1956. http://www.osti.gov/scitech/biblio/4351983.

Epler, E. P., and D. P. Roux. "Incipient Failure Diagnosis for Assuring Safety and Availability of Nuclear Power Plants." In *Proceedings of AEC-Sponsored Conference*

at Gatlinburg, Tenn, October 30-November 1, 1967. CONF-671011. January 1968, 1967.

Farmer, F. R. "Siting Criteria–a New Approach." In *Proceedings of the IAEA Symposium on Nuclear Siting*, 303–29, 1967. http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/44/070/44070762.pdf#page=317.

"Final Safety Evaluation for Nuclear Energy Institute (NEI) Industry Guidance Document NEI 06-09, Revision 0, "Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specificaitons." Washington, D.C: Nuclear Regulatory Commission, May 2007.

Garrick, B. J., W. J. Costley, and Gekler, W. C. "A Study of Test Reactor Operating and Safety Experience." Prepared for Phillips Petroleum Company, Prime Contracto to the US Atomic Energy Commission. Homes & Narver, Inc., May 10, 1963.

Garrick, B. J., W.C. Gekler, J. M. Duncan, R. H. Karcher, and B. Shimizu. "A Study of Research Reactor Operating and Safety Experience." Prepared for Phillips Petroleum Company, Prime Contractor to the US Atomic Energy Commission, June 12, 1964.

Garrick, B. J., W.C. Gekler, L Goldfisher, R. H. Karcher, B. Shimzu, and J. H. Wilson. "Reliability Analysis of Nuclear Power Plant Protective Systems." Prepared for US Atomic Energy Commission. Homes & Narver, Inc., May 1967.

Garrick, B. J., W.C. Gekler, and H. P. Pomrehn. "An Analysis of Nuclear Power Plant Operating and Safety Experience." Prepared for US Atomic Energy Commission. Homes & Narver, Inc., December 1966.

Garrick, B. J., B. Shimzu, E Behrens, W.C. Gekler, L Goldfisher, and J. H. Wilson. "Reliability Analysis of Carolinas Virginia Tube Reactor Engineered Safety Systems." Prepared for Phillips Petroleum Company, Prime Contracto to the US Atomic Energy Commission. Holmes & Narver, Inc, August 1967.

Garrick, B. John. "Memo to the Director, Division of Civilian Application, on Considering the Use of Probabilistic Methods in Nuclear Reactor Safety Analysis," n.d.

———. "PRA-Based Risk Management: History and Perspectives." *Nuclear News*, 2014. http://www.ans.org/pubs/magazines/download/a_940.

———. "Recent Case Studies and Advancements in Probabilistic Risk Assessment." *Risk Analysis* 4, no. 4 (1984): 267–279.

———. *Unified Systems Safety Analysis for Nuclear Power Plants*, 1968.

Garrick, B. John, and Robert F. Christie. *Quantifying and Controlling Catastrophic Risks*. Academic Press, 2008.

Garrick, B. John, and et al. "OPSA—Oyster Creek Probabilistic Safety Analysis." Prepared for Jersey Central Power & Light Company. Pickard Lowe and Garrick Incorporated (PLG), August 1979.

Gossick, L.V., M. L. Ernst, and et al. "Task Force Report for the Study of the Reactor Licensing Process," October 1973.

Hakata, Tadakuni. "Seismic PSA Method for Multiple Nuclear Power Plants in a Site." *Reliability Engineering & System Safety* 92, no. 7 (2007): 883–894.

Hakata, Tadakuni, D.H. Johnson, and W. Epstein. "Improvement of External Event (Tsunami Seismic) PSA Approach for Severe Accidents of Nuclear Power Plants." American Nuclear Society, 2013.

Hart, R. S., and W. T. Harper. "Final SNAPSHOT Safeguards Report." Atomics International, North American Aviation, March 20, 1965.

Hoyle, John C. "Staff Requirements - SECY-97-077 - Draft Regulatory Guides, Standard Review Plans And NUREG Document In Support Of Risk Informed Regulation For Power Reactors," June 5, 1997. http://www.nrc.gov/docs/ML0037/ML003752391.pdf.

IAEA. "Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1," 1999. http://www-pub.iaea.org/books/IAEABooks/5811/Basic-Safety-Principles-for-Nuclear-Power-Plants-75-INSAG-3-Rev-1.

———. "Risk Informed In-Service Inspection of Piping Systems of Nuclear Power Plants: Process, Status, Issues and Development," 2010. http://www-pub.iaea.org/books/IAEABooks/8375/Risk-Informed-In-service-Inspection-of-Piping-Systems-of-Nuclear-Power-Plants-Process-Status-Issues-and-Development.

"Indian Point Probabilistic Safety Study." Prepared for Consolidated Edison Company of New York and the New Your Power Authority. New York, n.d.

"Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance." Nuclear Regulatory Commission, Division of Systems Technology, December 1, 1997. http://www.osti.gov/scitech/biblio/569126.

Kaplan, Stanley, and B. John Garrick. "On the Quantitative Definition of Risk." *Risk Analysis* 1, no. 1 (1981): 11–27.

Knudsen, James, Robert F. Buell, John Schroeder, Anthony Koonce, and Peter L. Appignani. "Peer Review of NRC Standardized Risk Analysis Models." Wilmington, NC: American Nuclear Society, 2011.

Lewis, Harold Walter, Robert J. Budnitz, W. D. Rowe, H. J. C. Kouts, F. Von Hippel, W. B. Loewenstein, and F. Zachariasen. "Risk Assessment Review Group Report to the US Nuclear Regulatory Commission." *IEEE Transactions on Nuclear Science* 26, no. 5 (1979): 4686–4690.

Lewis, Howard W., R. J. Budnitz, A. W. Castleman, D. E. Dorfan, F. C. Finlayson, R. L. Garwin, L. C. Hebel, et al. "Report to the American Physical Society by the Study Group on Light-Water Reactor Safety." *Reviews of Modern Physics* 47, no. S1 (1975): S1.

"Loss of Residual Heat Removal System, Diablo Canyon, Unit 2, April 10, 1987 (Augmented Inspection Team Report April 15-21, 29 and 1 May 87). | National Technical Reports Library - NTIS." Accessed November 30, 2016. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/NUREG1269.xhtml.

Meserve, Richard A. Atomic Energy Society Of Japan/American Nuclear Society Topical Meeting On Safety Goals And Safety Culture (2001).

Mosleh, A., K. N. Fleming, G. W. Parry, H. M. Paula, D. H. Worledge, and D. M. Rasmuson. "Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Procedural Framework and Examples." *ResearchGate*, January 1, 1988. https://www.researchgate.net/publication/236371031_Procedures_for_treating_common_cause_failures_in_safety_and_reliability_studies_Procedural_framework_and_examples.

Mulvihall, R. J. *A Probabilistic Methodology for the Safety Analysis of Nuclear Power Reactors*. Planning Research Corporation, 1966.

Nieh, Ho. "Final Safety Evaluation for Nuclear Energy Institute (NEI) Industry Guidance Document NEI 04-10, Revision 0, 'Risk-Informed Technical Specifications Initiative 5b, Risk-Informed Method for Control of Surveillance Frequencies' (TAC NOS. MB2531 and MD3077)." Washington, D.C: Nuclear Regulatory Commission, September 28, 2006.

(NRC). "Nuclear Regulatory Commission," November 24, 1981. https://loc.heinonline.org.

———. "Nuclear Regulatory Commission," June 26, 1984. https://loc.heinonline.org.

———. "Nuclear Regulatory Commission," March 21, 1986. https://loc.heinonline.org.

———. "Nuclear Regulatory Commission," June 21, 1988. https://loc.heinonline.org.

"NRC: 10 CFR 50.55a Codes and Standards." Accessed November 30, 2016. http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0055a.html.

"NRC: 10 CFR Part 21—Reporting of Defects and Noncompliance." Accessed November 30, 2016. http://www.nrc.gov/reading-rm/doc-collections/cfr/part021/.

"NRC: 10 CFR Part 50—Domestic Licensing of Production and Utilization Facilities." Accessed November 29, 2016. http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/.

"NRC: Accident Source Terms for Light-Water Nuclear Power Plants (NUREG-1465)." Accessed November 28, 2016. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1465/.

"NRC: Backfitting Guidelines (NUREG-1409)." Accessed November 28, 2016. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1409/.

"NRC: Backgrounder on the Three Mile Island Accident." Accessed November 24, 2016. http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html.

"NRC: Commission Policy Statements - Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities (60 FR 42622)," August 16, 1995. http://www.nrc.gov/reading-rm/doc-collections/commission/policy/.

"NRC: Generic Environmental Impact Statement for License Renewal of Nuclear Plants—Final Report (NUREG-1437, Revision 1)." Accessed November 28, 2016. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1437/r1/.
"NRC: History." Accessed November 24, 2016. http://www.nrc.gov/about-nrc/history.html.
"NRC: Inspection Manual Chapters." Accessed November 27, 2016. http://www.nrc.gov/reading-rm/doc-collections/insp-manual/manual-chapter/.
"NRC: Perspectives Gained From the Individual Plant Examination of External Events (IPEEE) Program - Final Report (NUREG-1742, Volume 1)." Accessed November 28, 2016. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1742/vol1/.
"NRC: PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants: (NUREG/CR-2300)." Accessed November 28, 2016. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr2300/vol2/.
"NRC: Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission (NUREG/BR-0058, Rev. 4)." Accessed November 28, 2016. http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0058/.
"NRC: Regulatory Effectiveness of the Station Blackout Rule (NUREG-1776)." Accessed November 27, 2016. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1776/.
"NRC: Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (NUREG-1150)." Accessed November 21, 2016. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1150/.
Nuclear Energy Institute. "10 CFR 50.60: SSC Categorization Gudeline," July 2005.
———. "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants (Revision 4A)," February 22, 2000.
———. "Letter to the NRC," December 19, 2013.
———. "Probabilistic Risk Assessment Peer Review Process Guidance," March 20, 2000.
———. "Risk-Informed Technical Specification Initiative 4b: Risk-Managed Technical Specifications (RMTS) Guidelines," November 2006. http://pbadupws.nrc.gov/docs/ML0713/ML071360456.pdf.
———. "Risk-Informed Technical Specifications Initiative 5b: Risk-Informed Method for Control of Surveillance Frequencies," April 2007. http://pbadupws.nrc.gov/docs/ML0713/ML071360456.pdf.
"Nuclear Inservice Inspection." Accessed November 30, 2016. https://www.asme.org/shop/standards/new-releases/boiler-pressure-vessel-code/nuclear-inservice-inspection.
Nuclear Regulatory Commission. "Individual Plant Performance Summaries," 2016. https://www.nrc.gov/NRR/OVERSIGHT/ASSESS/.

Nuclear Regulatory Commission (NRC). "10 CFR 50.61a Alternate Fracture Toughness Requirements for Protection against Pressurized Thermal Shock Events," January 4, 2010. federalregister.gov.
———. "10 CFR Parts 50 and 55: Policy Statement on the Conduct of Nuclear Power Plant Operations," n.d.
———. "An Approach for Determining the Technical Adequacy of PRA Results for Risk-Informed Activities," 2009.
———. "Final Rule - Technical Specifications," July 19, 1995.
———. "Generic Letter (GL) 88-20: Individual Plant Examination for Severe Accident Vulnerabilities 10 CFR 50.54(f)," November 23, 1988.
———. "Implementation of The Safety Goals." 1989, n.d.
———. *Loss of Vital AC Power and the Residual Heat Removal System during Mid-Loop Operations at Vogtle Unit 1 on March 20, 1990*. Washington, D.C: U.S. Nuclear Regulatory Commission, 1990.
———. "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," July 10, 1991.
———. "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," July 19, 1999.
———. "NUREG-0800: Risk-Informed Decision Making: Technical Specifications - Chapter 16.1," March 2007. http://www.nrc.gov/docs/ML0325/ML032510135.pdf.
———. "NUREG-0800: Standard Review Plan For the Review of Risk-Informed Inservice Inspection of Piping - Chapter 3.9.8," September 2003. http://www.nrc.gov/docs/ML0325/ML032510135.pdf.
———. "Overview of Risk-Informed Regulatory Activities Associated with Technical Specifications," February 2015.
———. "Regulatory Guide (RG) 1.177: An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications," May 2011. http://www.nrc.gov/docs/ML1009/ML100910008.pdf.
———. "Regulatory Guide (RG) 1.178: An Approach for Plant Specific Risk-Informed Decisionmaking for Inservice Inspection of Piping," April 2003. http://www.nrc.gov/docs/ML0317/ML031780764.pdf.
———. "Regulatory Guide (RG) 1.192: Operation and Maintenance Code Case Aceptability," August 2014. http://www.nrc.gov/docs/ML1334/ML13340A034.pdf.
———. "Rule 10 CFR50.36: Technical Specifications," 2016.
———. "Safety Goals for Nuclear Power Plant Operation." Nuclear Regulatory Commission, 1983. http://inis.iaea.org/Search/search.aspx?orig_q=RN:14792318.
———. "Safety Goals for Nuclear Power Plants: A Discussion Paper." Nuclear Regulatory Commission, 1982. http://inis.iaea.org/Search/search.aspx?orig_q=RN:14724072.
———. "Technical Specification Policy Statement," 1993.

Nuclear Regulatory Commission, and others. "Overview of the Reactor Safety Study Consequence Model." *NUREG-0340)(June 1977)*, 1977.

"NUREG-0933, Main Report with Supplements." Accessed December 1, 2016. http://nureg.nrc.gov/sr0933/.

Pasternak, T, K. Fleming, and W.J. Houghton. "HTGR Accident Initiation and Progression Analysis Status Report - Volume III: Preliminary Results (Including Design Options)." General Atomic Co., San Diego, Calif. (USA), November 1975. http://www.osti.gov/scitech/biblio/7283894.

Pickard Lowe and Garrick Incorporated. "Application and Comparison of the GO Methodology and Fault Tree Analysis." Prepared for The Electric Power Research Institute, December 1981.

———. "Bellafonte Unit 1 Phase I Probabilistic Risk Assessment." Prepared for the Tennessee Valley Authority. Knoxville, Tennessee, October 1985.

———. "Browns Ferry Multi-Unit Probabilistic Risk Assessment." Prepared for the Tennessee Valley Authority. Decatur, Alabama, January 1995.

———. "Browns Ferry Nuclear Plant Unit 2 Probabilistic Safety Assessment with Unit 3 Operating." Prepared for the Tennessee Valley Authority. Decatur, Alabama, May 1996.

———. "Browns Ferry Nuclear Plant Unit 3 Probabilistic Safety Assessment with Unit 2 Operating." Prepared for the Tennessee Valley Authority. Decatur, Alabama, May 1996.

———. "EPZ Determination for the Republic of China - Phase I: Preliminary EPZ for Kuosheng (Volumes 1 and 2)." Prepared for the Atomic Energy Council of the Republic of China, June 1990.

———. "Oconee PRA, A Probabilistic Risk Assessment of Oconee Unit 3." Cosponsored by the Electric Power Research Institute, Nuclear Safety Analysis Center, and Duke Power Company, June 1984.

———. "Quantitative Risk Assessment for Noncatastrophic Accidents at a Japanese Nuclear Power Plant." Prepared for Mitsubishi Atomic Power Industries, Inc., May 1994.

———. "Seabrook Station Probabilisic Safety Assessment." Prepared for Public Service Company of New Hampshire Nd Yankee Atomic Electric Company, December 1983.

———. "Seismic and Fire Risk Analysis, Typical Japanese 4-Loop PWR Plant." Prepared for Mitsubishi Atomic Power Industries, Inc. Tokyo, Japan, July 1988.

———. "Survey of System Improvements for Application of Probabilistic Safety Assessments." Prepared for IEA of Japan, Ltd, August 1997.

———. "The High Flux Isotope Reactor Probabilistic Risk Assessment: Analysis of the Risk from Internal and External Events." Prepared for Martin Marietta Energy Systems, Inc., August 1991.

"Reactor Safety Study. an Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants. Executive Summary: Main Report. [Pwr and Bwr]." Nuclear Regulatory Commission, Washington, D.C. (USA), October 1, 1975. http://www.osti.gov/scitech/biblio/7134131.

Reyes, Luis A. "SECY-06-0124 - Rulemaking Plan to Amend Fracture Toughness Requirements for Protection against Pressurized Thermal Shock Events (10 CFR 50.61)," May 26, 2006. http://www.nrc.gov/docs/ML0605/ML060530624.pdf.

Richner, M., and S. Zimmermann. "Applications of Simplified and of Detailed PSA Models." In *Probabilistic Safety Assessment and Management*, 1998.

Safeguards, U. S. Nuclear Regulatory Commission Advisory Committee on Reactor. *An Approach to Quantitative Safety Goals for Nuclear Power Plants*. The Committee, 1980.

Safety Commission, Canadian Nuclear. "Summary Report of the International Workshop on Multi-Unit Probabilistic Safety Assessment," July 16, 2015. https://www.cnsc-ccsn.gc.ca/eng/resources/research/technical-papers-and-articles/2015/2015-multi-unit-safety-assessment.cfm.

Schon, F. J., O. H. Paris, and J. P. Gleason. "Opinion and Recommendations to the Commission on Societal Significance of Risk Estimates." Syllabus in the Matter of the Indian Point Special Proceedings, Dockets 50-247G and 50-286G, October 24, 1983. NRC Public Document Room.

"Seventies." Accessed November 24, 2016. http://users.owt.com/smsrpm/nksafe/seventies.html.

Sheron, Brian W. "SECY-15-0124: Status of the Accident Sequence Precursor Program and the Standardized Plant Analysis Risk Models," October 5, 2015. http://www.nrc.gov/docs/ML1518/ML15188A101.pdf.

Sherry, Richard R., Peter L. Appignani, and Robert F. Buell. "The NRC's SPAR Models: Current Status, Future Development, and Modeling Issues," 2008. https://inldigitallibrary.inl.gov/sti/4074965.pdf.

Siddall, E. "Statistical Analysis of Reactor Safety Standards." *Journal of Occupational and Environmental Medicine* 1, no. 6 (1959): 352.

Specter, H. "Lessons from the Indian Point Hearing." *Nucl. Saf.;(United States)* 27, no. 3 (1986). http://www.osti.gov/scitech/biblio/5407889.

Starr, Chauncey. "Radiation in Perspective." *Nucl. Safety* 5 (1964). http://www.osti.gov/scitech/biblio/4004706.

———. "Social Benefit versus Technological Risk." *Readings in Risk*, 1969, 183–194.

"Technique for Human Error-Rate Prediction." *Wikipedia*, April 15, 2015. https://en.wikipedia.org/w/index.php?title=Technique_for_human_error-rate_prediction&oldid=656627365.

Tennessee Valley Authority. "Comments on Draft NUREG-1150 (Reactor Risk Reference Document)," September 28, 1987. http://www.nrc.gov/docs/ML1111/ML111151348.pdf.

Travers, William D. "SECY-00-0009 - Rulemaking Plan, Reactor Fire Protection Risk-Informed, Performance-Based Rulemaking (WITS Item 199900032)," January 13, 2000. http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2000/secy2000-0009/2000-0009scy.pdf.

———. "SECY-02-0057 - Update To SECY-01-0133, 'Fourth Status Report On Study Of Risk-Informed Changes To The Technical Requirements Of 10 CFR Part 50 (Option 3) And Recommendations On Risk-Informed Changes To 10 CFR 50.46 (ECCS Acceptance Criteria),'" March 29, 2002. http://pbadupws.nrc.gov/docs/ML0206/ML020660607.pdf.

———. "SECY-99-007: Recommendations for Reactor Oversight Process Improvements," January 8, 1999. http://www.nrc.gov/reading-rm/doc-collections/commission/secys/1999/secy1999-007/1999-007scy_attach.pdf.

———. "Staff Requirements - SECY-00-0009 - Rulemaking Plan, Reactor Fire Protection Risk-Informed, Performance-Based Rulemaking (WITS Item 199900032)," February 24, 2000. http://www.nrc.gov/reading-rm/doc-collections/commission/srm/2000/2000-0009srm.pdf.

True, D., K. Fleming, G. Parry, B. Putney, and J. P. Sursock. "PSA Applications Guide. Final Report." Electric Power Research Inst., Erin Engineering and Research, 1995. http://inis.iaea.org/Search/search.aspx?orig_q=RN:27015409.

Union of Concerned Scientists (UCS). "Petition for Decommissioning of Indian Point Unit 1 and Suspension of Operation of Units 2 and 3," 1979.

United States Nuclear Regulatory Commission. "An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions on Plant Specific Changes to The Licensing Basis," May 2011.

———. "Policy Statement on Safety Goals for the Operation of Nuclear Power Plants." Washintong DC: Nuclear Regulatory Commission, August 21, 1986.

U.S. Nuclear Regulatory Commission. "Regulatory Guide 1.155 (Task SI 501-4) Station Blackout." Washintong DC: Nuclear Regulatory Commission, August 1988.

Vietti-Cook, Annette. "SECY-98-300: Options for Risk-Informed Revisions to 10 CFR Part 50 - Domestic Licensing of Production and Utilization Facilties.," June 8, 1998. http://www.nrc.gov/docs/ML0037/ML003751348.pdf.

———. "Staff Requirements - SECY-02-0057 - Update To SECY-01-0133, 'Fourth Status Report On Study Of Risk-Informed Changes To The Technical Requirements Of 10 CFR Part 50 (Option 3) And Recommendations On Risk-Informed Changes To 10 CFR 50.46 (ECCS Acceptance Criteria),'" March 31, 2003. http://www.nrc.gov/docs/ML0309/ML030910476.pdf.

"Voluntary Fire Protection Requirements for Light Water Reactors; Adoption of NFPA 805 as a Risk-Informed, Performance-Based Alternative." *Federal Register*, November 1, 2002. https://www.federalregister.gov/documents/2002/11/01/02-27701/voluntary-fire-protection-requirements-for-light-water-reactors-adoption-of-nfpa-805-as-a.

Watson, H. A. "Launch Control Safety Study." *Bell Labs*, 1961.

Westinghouse Energy Systems. "Westinghouse Owners Group Application of Risk Informed Methods to Piping Inservice Inspection Topical Report," 1999.

Willis, C. A. "Statistical Safety Evaluation of Power Reactors." Memo. Atomics International, 1965.

"Zion Probabilistic Safety Study." Prepared for the Commonwealth Edison Company. Chicago, Ilinois: Pickard Lowe and Garrick Incorporated (PLG), 1981.