The Structure and Evolution of Probabilistic Risk Assessment and Risk-Informed Regulation

PURPOSE

This document provides more detailed information on the structure and evolution of probabilistic risk assessment (PRA) and risk-informed regulation that led to the staff's original proposal for a scoping study to evaluate the feasibility of performing a new full-scope comprehensive site Level 3 PRA.

A separate document included as the first enclosure to the notation vote SECY paper provides more detailed technical information on (1) the basis for originally proposing to perform a scoping study to evaluate the feasibility of performing a new full-scope comprehensive site Level 3 PRA for a nuclear power plant (NPP)[1], (2) potential future uses for Level 3 PRAs, (3) three primary options for proceeding with future Level 3 PRA activities[2], and (4) the activities that supported development of items 2 and 3.

[1] As used in this document and the SECY paper to which it is enclosed, a full-scope comprehensive site Level 3 PRA is a PRA that includes a quantitative assessment of the public risk from accidents involving all site reactor cores and spent nuclear fuel that can occur during any plant operating state, and that are caused by all initiating event hazards (internal events, fires, flooding, seismic events, and other site-specific external hazards).

[2] This document and the SECY paper to which it is enclosed distinguish between "Level 3 PRA activities" and "Level 3 PRAs." The latter refers to a PRA that includes specific technical elements or analyses to assess the public risk from a NPP, while the former refers to activities (e.g., research and development) specifically related to or in support of Level 3 PRAs.

The Structure and Evolution of Probabilistic Risk Assessment and Risk-Informed Regulation

BACKGROUND

A Quantitative Definition of Risk

The traditional definition of risk involves the combination of the likelihood of and consequences associated with an adverse event. Kaplan and Garrick[3] advanced this definition and formalized risk as a set of triplets developed by answering the following three questions:

(1) What can go wrong?
(2) How likely is it that it will happen?
(3) If it does happen, what are the consequences?

To answer these questions, a set of possible scenarios or outcomes are identified, each with an associated probability and consequence measure. The total risk (R) is therefore captured by the set of all possible scenarios identified (s), the probabilities of those scenarios occurring (p), and the consequence measures of those scenarios (x). In equation form,

$$\mathbf{R = \{(s_i, p_i, x_i)\}, \qquad i = 1, 2, \ldots, N}$$

Probabilistic Risk Assessment (PRA)

PRA is a structured, analytical process that provides both qualitative insights and quantitative estimates of risk by (1) identifying potential sequences that can challenge system operations and lead to an adverse event, (2) estimating the likelihood of these sequences, and (3) estimating the consequences associated with these sequences, if they were to occur. By prioritizing significant risk contributors[4] and characterizing key sources of uncertainty and their impact on results, PRA serves as a useful decisionmaking tool that can help focus thinking and limited agency resources to ensure safety.

The Use of PRA in the Decisionmaking Process

In using PRA as a tool to support a regulatory decision, the following four-step process is typically followed:

(1) **Identify the results needed**. For many risk-informed applications, acceptance criteria or guidelines have been established in terms of numerical values of risk metrics. Therefore, when using PRA results to support a risk-informed decision, the first step is to identify which results are needed and how they are to be used to inform the decision.

(2) **Construct a PRA model to generate the required results**. Once identified, the next step is to develop a model, typically a quantitative PRA model that is of the appropriate scope and level of detail that can generate the needed results.

(3) **Compare PRA results to acceptance criteria or guidelines**. Once results are generated, they can be compared to the appropriate acceptance criteria or guidelines. Although this appears to be straightforward, this step involves more than

[3] Kaplan S. and Garrick B.J., "On the quantitative definition of risk." Risk Analysis, 1, 11-37 (1981).

[4] As used in this enclosure and the SECY paper to which it is enclosed, risk contributors include: radiological sources (e.g., reactor core, spent nuclear fuel); initiating event hazards (e.g. internal events, fires, flooding, seismic events, other site-specific external hazards); plant operating states; accident sequences; failure of structures, systems, and components; and operator actions.

just a simple comparison of numerical values. To ensure confidence in the decision, the PRA results need to be evaluated to determine their realism and to identify and address any key sources of uncertainty. Types and sources of uncertainty in PRA models and results are discussed in more detail below.

(4) **Document the results**. In this final step, the results of the comparison of the PRA results to the acceptance criteria or guidelines are documented, along with a statement characterizing the confidence in the results.

Characteristics of NPP PRA Models

To understand why future Level 3 PRAs would be beneficial, it is important to first understand some of the key characteristics of NPP PRA models that can influence their use in regulatory applications, including the scope, level of detail, structure, associated uncertainties, and the aggregration of PRA results from different hazards.

<u>The Scope of a PRA Model</u>

NPP PRA models can vary in scope, depending on their intended application or use. As summarized in Table 1 below, the scope of a PRA is defined by the extent which various options for the following five factors are modeled and analyzed:

(1) Radiological sources. NPP sites contain multiple sources that could potentially release radioactive material into the environment under accident conditions. Although current PRAs focus on the reactor core, other important sources that could be modeled in the PRA to estimate the public risk from NPP sites include spent nuclear fuel (both wet and dry storage), fresh fuel, and radiological waste storage tanks.

(2) Population exposed to the hazards. In determining the potential health effects associated with a nuclear accident, both onsite and offsite populations can be considered. Typical NPP PRA models have been developed to estimate the risk to the general public located offsite, and do not consider the risk to the onsite workers and immediate responders to a nuclear accident.

(3) Initiating event hazard groups. Initiating events disrupt the steady state operation of the plant by challenging plant control and safety systems and operators whose failure could potentially lead to reactor core damage and/or the release of radioactive material to the environment. These events include failure of equipment from internal causes (e.g., transients, loss-of-coolant accidents, internal floods, internal fires) or external causes (e.g., earthquakes, high winds, tsunamis). In a NPP PRA model, similar causes of initiating events are organized by hazard groups, which are then assessed using common approaches, methods, and data to characterize their effects on the plant.

(4) Plant operating states (POSs). In determining the public risk from NPP operations, it is important to consider not only the response of the plant to initiating events occurring during at-power operation, but also its response to initiating events occurring while the plant is in other operating states, such as low-power and shutdown (LPSD). POSs are used to subdivide the plant operating cycle into unique states defined by various characteristics (e.g., reactor power; coolant temperature, pressure, and level; equipment configuration) so that the plant response can be assumed to be the same for all subsequent initiating events.

(5) End state (level of risk characterization). NPP PRA models can be used to calculate risk metrics at different end states. The three different end states or levels of risk characterization that have been traditionally used in NPP PRA models are discussed in more detail below.

Table 1. Scoping Options for Commercial NPP PRAs

Factor	Scoping Options for Commercial NPP PRAs
Radiological sources	Reactor core(s) Spent nuclear fuel (spent fuel pool and dry cask storage) Other radioactive sources (e.g., fresh fuel and radiological wastes)
Population exposed to hazards	Onsite population Offsite population
Initiating event hazard groups	Internal hazards • Traditional internal events (transients, loss-of-coolant accidents) • Internal floods • Internal fires
	External hazards • Seismic events (earthquakes) • Other site-specific external hazards (e.g., high winds, external flooding)
Plant operating states	At-Power Low-Power/Shutdown
End state/Level of risk characterization	Level 1 PRA: Initiating event to onset of core damage or safe state Level 2 PRA: Initiating event to radioactive material release from containment Level 3 PRA: Initiating event to offsite radiological consequences

When using PRA to support regulatory applications, all risk contributors relevant to the regulatory decision need to be included in the scope of the PRA model. In accordance with staff requirements memorandum (SRM) COMNJD-03-0002[5], the risk from each significant risk contributor should be addressed using a PRA model developed in accordance with a U.S. Nuclear Regulatory Commission (NRC) staff-endorsed consensus standard. In some cases, however, a conservative bounding assessment or qualitative screening analysis can be used to demonstrate that some risk contributors are not relevant to the regulatory decision, and can therefore be excluded from the scope of the PRA.

<u>Level of Detail of a PRA Model</u>

Much like scope, the level of detail of a NPP PRA model can vary, depending on its intended application or use. The level of detail is defined by the degree to which (1) the actual plant is modeled and (2) the unlimited range of potential scenarios is simplified. Although the goal of a PRA is to represent the as-designed, as-built, and/or as-operated plant as realistically as practicable, some compromise must be made to keep the PRA model manageable.

For each of the technical elements that comprise a PRA model, the level of detail may vary by the extent to which:

[5] SRM COMNJD-03-0002, "Stabilizing the PRA Quality Expectations and Requirements" (September 8, 2003).

(1) Plant systems and operator actions are credited in modeling plant-specific design and operation,

(2) Plant-specific operating experience and data for the plant's structures, systems, and components (SSCs) are incorporated into the model, and

(3) Realism is incorporated into analyses that predict the expected plant and operator responses.

In addition, to keep the PRA model manageable, the logic structures (e.g., event trees and fault trees) used in the model are simplified representations of the complete range of potential accident scenarios. Simplifications are made through underlying assumptions and approximations, such as the consolidation of initiating event causes into representative hazard groups and the screening out of certain equipment failure modes.

Although the level of detail needed for a NPP PRA model is largely dependent upon the requirements associated with its intended use, at a minimum, the model needs to be detailed enough to model the major system dependencies and to capture the significant risk contributors.

The Structure of a PRA Model

NPP PRA models are logic models constructed using logic structures such as event trees and fault trees. Event trees are used to model different plant and operator responses in terms of sequences of undesired system states that could occur following an initiating event. Fault trees are used to identify different combinations of basic events (e.g., initiating events, SSC failures, and human failure events) that could lead to the undesired system states. When linked together, these logic structures provide an integrated perspective that can capture major system dependencies.

As discussed in the previous section, these logic structures represent a simplification of the potentially unlimited range of scenarios by modeling a more manageable yet representative set that encompasses all of the potential consequences. Underlying assumptions and approximations made in the development of the PRA model give rise to uncertainty, a topic discussed in more detail below.

Uncertainties in PRA Models

When using PRA results as part of any regulatory decisionmaking process, it is important to understand the types, sources, and potential impact of uncertainties associated with PRA models and how to treat them in the decisionmaking process. NUREG-1855[6] was developed to address these issues.

Although there are several different sources of uncertainty in PRA models, there are two principal classes of uncertainty: aleatory and epistemic. Aleatory uncertainty arises from the random nature of the basic events modeled in PRAs. Because PRAs use probabilistic distributions to estimate the frequencies or probabilities of these basic events, the PRA model itself is an explicit model of the aleatory uncertainty.

---

[6] NUREG-1855, "Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making" (March 2009).

Epistemic uncertainties arise from incompleteness in the collective state of knowledge about how to represent plant behavior in PRA models. These uncertainties relate to how well the PRA model reflects the as-designed, as-built, and/or as-operated plant and to how well it predicts the response of the plant to various scenarios. Since these uncertainties can have a significant impact on the interpretation and use of PRA results, it is important that they be appropriately identified, characterized, and addressed. The three types of epistemic uncertainty associated with PRA models are:

(1) **Parameter Uncertainty.** Parameter uncertainty relates to uncertainty in the computation of input parameters for the probability distributions used to quantify the frequencies or probabilities of basic events in the PRA logic model. Importantly, this assumes that the selection of the probability distribution used to model the likelihood of the basic event is agreed upon; if uncertainty exists about this selection, it is more appropriately considered model uncertainty. Parameter uncertainty is typically characterized by using probability distributions to represent the degree of belief in the values of these input parameters.

(2) **Model Uncertainty.** Model uncertainty arises from a lack of knowledge of physical phenomena, failure modes related to the behavior of SSCs under various conditions, or other phenomena modeled in a PRA (e.g., the location and habits of members of the public in different exposure scenarios). This can result in the use of different approaches to modeling certain aspects of the plant and public response that can significantly impact the overall PRA model. Since uncertainty exists about which approach is most appropriate, this leads to uncertainty in the PRA results. Model uncertainty can also arise from uncertainty in the logic structure of the PRA model or in the selection of the probability distribution used to model the likelihood of the basic events in the PRA model. Model uncertainties are typically addressed by using sensitivity analyses to determine the sensitivity of the PRA results to any reasonable alternative modeling approaches.

(3) **Completeness Uncertainty.** Completeness uncertainty arises from limitations in the scope and completeness of the PRA model. Known risk contributors can be excluded from the PRA model due to technology or resource limitations or because their contribution to overall risk is believed to be negligible. These uncertainties can be addressed by supplementing the PRA with additional analyses to demonstrate their impact is not significant. Unknown risk contributors are excluded because their potential existence has not yet been recognized. These uncertainties are typically addressed through the use of defense-in-depth principles. Although it can be viewed as a special type of model uncertainty, completeness uncertainty is treated separately because it reflects an unanalyzed contribution to risk that is difficult, if not impossible, to quantify.

Skeptics of PRA question its usefulness due to the uncertainty in its results. Although PRA cannot account for the unknown and identify all unexpected event scenarios, it can identify some originally unforeseen scenarios, identify where some of the uncertainties exist in plant design and operation, and for some uncertainties, quantify the extent of the uncertainty. PRA is therefore a powerful tool that can lead to safer plant design by focusing attention and resources on those aspects important to safety and by identifying where defense-in-depth measures are needed to account for uncertainty.

<u>The Aggregation of PRA Results from Different Hazards</u>
PRA results can include more than just calculated risk metrics for comparison to acceptance criteria or guidelines. In fact, one of the most valuable insights from PRA can be the identification of the relative importance of various risk contributors.

For many regulatory applications, it is necessary to consider the contributions from several hazards to a specific risk metric. When considering multiple hazards, a PRA model can be a fully integrated model in which all hazards are combined into a single logic structure, a set of individual PRA models for each hazard, or a mixture of the two. When combining the results of PRA models for several hazards, the level of detail and level of approximation included in the PRA model may differ from one hazard to the next. Because of the unique methods and data used, a significantly higher level of conservative bias can exist in PRAs for internal fires, external events (seismic, high wind, and others), and low-power/shutdown conditions. In principal, this conservative bias could be reduced to some degree by developing models to the same level of detail and rigor associated with internal events, at-power PRAs. That said, the larger conservative bias can result in larger uncertainties in the results. Importantly, however, this does not preclude the aggregation of results from different hazards. Instead, it requires an understanding of the main sources of conservatism associated with any of the hazards that can potentially impact the regulatory application for which the PRA results are being used.

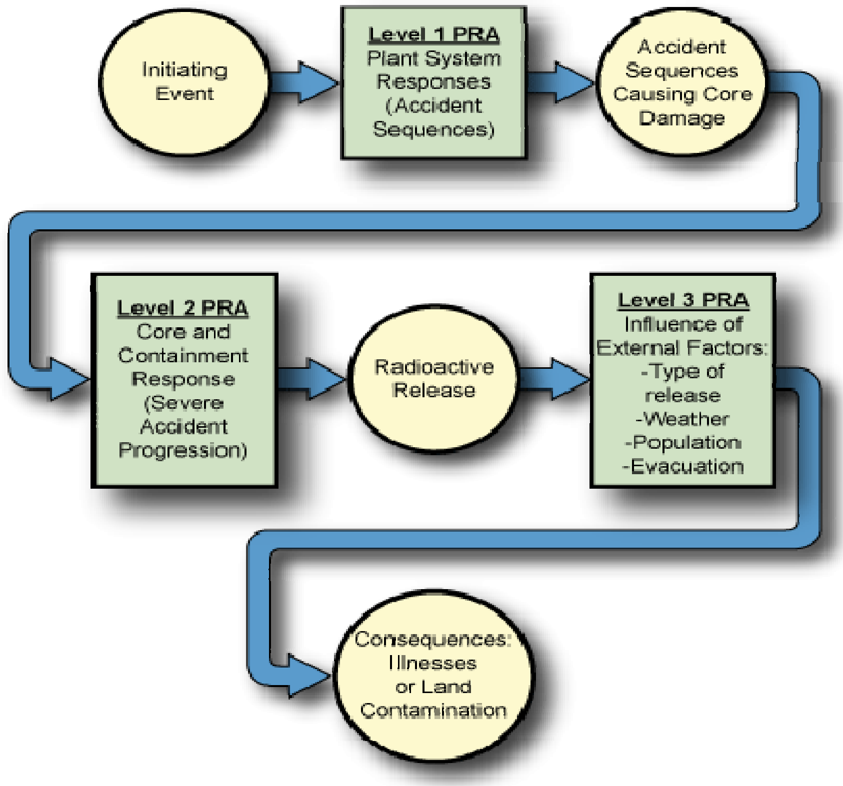
Therefore, when interpreting the results of the comparison of risk metrics to acceptance criteria or guidelines, it is important to not only focus on the aggregated numerical result, but also on the relative importance and realism of the main contributors to the risk metric.

PRA End States: The Significance of Level 3 PRAs
As shown in Table 1 and Figure 1 below, NPP PRAs that have traditionally focused on accidents involving the reactor core can estimate risk metrics at three different levels of characterization by using sequential analyses in which the output from one level serves as a conditional input to the next.

<u>Level 1 PRA</u>
Using event trees and fault trees, a Level 1 PRA models system and operator responses to various initiating events that challenge plant operation to identify sequences (combinations of system and operator action successes and failures) that result in either the achievement of a safe state or the onset of core damage. The estimated frequencies of those sequences that result in the onset of reactor core damage are summed to calculate the total core damage frequency (CDF) for the analyzed plant.

<u>Level 2 PRA</u>
A Level 2 PRA includes Level 1 PRA analyses and in addition estimates conditional containment failure probabilities (CCFPs), radioactive material release frequencies, and various source term characteristics by modeling the progression of those accident sequences resulting in core damage (otherwise known as “severe accidents”) and evaluating the response of both plant systems and the containment to the harsh accident environment. For those sequences resulting in containment failure or bypass, the frequency, type, amount, timing, and energy content of the radioactive material released to the environment is estimated.

Figure 1. PRA End States: The three sequential levels of risk characterization.



Level 3 PRA

A Level 3 PRA includes Level 2 PRA analyses and in addition models atmospheric transport and dispersion phenomena to estimate various offsite health and economic consequence measures, Inputs to the Level 3 PRA include the source term characteristics from a Level 2 PRA and several other factors, to include site-specific meteorology, demographics, emergency response, and land use. Outputs from the Level 3 PRA include estimates of offsite radiological consequences in terms of various consequence measures such as early fatalities and injuries and latent cancer fatalities resulting from the radiation doses to the surrounding population, and economic costs associated with evacuation, relocation, property loss, and land contamination.

Importantly, by combining the radioactive material release frequencies obtained from a Level 2 PRA with the offsite radiological consequences associated with each release, only a Level 3 PRA can estimate the public risk from all analyzed risk contributors associated with a NPP. More importantly, a full-scope comprehensive site Level 3 PRA that includes an assessment of not only accidents involving the reactor core, but also accidents involving other site radiological sources—such as spent fuel pools (SFPs), dry storage casks, and other units[7] on site–can provide valuable insights into the relative importance of various site risk contributors. These insights can be used to enhance regulatory decisionmaking and to help focus limited agency resources on issues most directly related to the agency's mission to protect public health and safety. Although a PRA that includes an assessment of other site radiological sources could conceivably be done using only a Level 1 or Level 2 PRA, such an assessment would not

[7] As used in this enclosure and the SECY paper to which it is enclosed, a unit refers to a reactor core and, if applicable, an associated spent fuel pool.

necessarily yield information about issues most directly related to the agency's mission to protect public health and safety.

A common misconception is that a Level 2 PRA is limited to the accident progression and source term analyses, while a Level 3 PRA is limited to the accident consequence analyses. To be clear, a Level 2 PRA includes the analyses from a Level 1 PRA, and a Level 3 PRA includes the analyses from a Level 2 PRA. A Level 3 PRA therefore analyzes from initiating event to offsite radiological consequences for accident sequences involving core damage and containment failure or bypass. The analyses that are included in each PRA level are summarized below in Table 2.

Table 2. Analyses Included in Each PRA Level

Analysis	Level 1 PRA	Level 2 PRA	Level 3 PRA
Accident Frequency Analysis	X	X	X
Accident Progression Analysis		X	X
Source Term Analysis		X	X
Consequence Analysis			X
Risk Integration Analysis			X

Historical Perspective: The Evolution of PRA Technology and Risk-Informed Regulation

Pre-PRA Policy Statement Era (1946 – 1995)

From 1946 to 1954, nuclear regulation was the responsibility of the NRC's predecessor, the Atomic Energy Commission (AEC). The Atomic Energy Act of 1946 established the AEC to maintain strict control of atomic technology and to further exploit it for military applications. By 1954, the need for commercial nuclear power became an urgent national goal, and a new Atomic Energy Act was passed. Under this Act, the AEC had responsibility for the development and production of nuclear weapons and for both the development and the safety regulation of the civilian uses of nuclear materials.

In the development of early nuclear safety regulations, the AEC ensured adequate protection of public health and safety by using a conservative deterministic approach to demonstrate that NPPs could withstand a set of worst-case design basis accidents (DBAs) involving single failures in independent systems following certain initiating events. In addition, the AEC relied on the concept of defense-in-depth, which originated in the design of nuclear weapons facilities to account for uncertainties in safety system design margins. This concept, which promotes the use of safety margins and multiple, independent layers of defense mechanisms, would theoretically mitigate the consequences of a severe accident resulting in core damage, or "beyond-DBA," should one occur.

Prior NRC-Sponsored Studies to Estimate Public risk

As NPP designs and PRA techniques evolved over time, the NRC and its predecessor, the AEC, periodically sponsored studies to obtain updated estimates of the public risk from severe reactor accidents.

WASH-740[8]

Published in March 1957 by the AEC, the purpose of this first major study was to provide an estimate of the upper limit consequences of severe reactor accidents to inform Congressional deliberation on the Price-Anderson Act. The study was conservative in nature, focusing on large loss-of-coolant accidents (LOCAs) as the leading source of worst-case radioactive material release to the environment. Although this was a non-probabilistic consequence study instead of PRA study, the scientists involved were willing to offer rough order-of-magnitude estimates of the probability of a severe reactor accident that ranged from 10^{-5} – 10^{-9} per reactor-year of operation.

WASH-1400[9]

During the late 1960s and early 1970s, the size and number of commercial NPPs rapidly increased. In addition, a series of loss-of-fluid tests (LOFTs) conducted using a small-scale reactor mockup suggested that steam buildup during an accident scenario could prevent the Emergency Core Cooling System (ECCS) from injecting water into the reactor core, thereby leading to core damage. In the midst of these concerns with ECCS performance and an upcoming extension of the Price-Anderson Act, the AEC initiated a study in 1972 to obtain a more realistic estimate of the public risk from severe nuclear accidents.

In October 1975,18 years after the publication of WASH-740, and after considerable progress in the use of reliability techniques and increased use of commercial NPPs, the NRC published WASH-1400. This Level 3 PRA study marked the first U.S. attempt to systematically evaluate a large spectrum of accidents and to use quantitative techniques to evaluate severe accident probabilities, source terms, and offsite radiological consequences in an integrated manner to obtain a more realistic estimate of severe accident public risk.

The WASH-1400 study demonstrated that although the CDF and the CCFP, given the occurrence of accident sequence that releases radioactive material into the containment atmosphere, were both higher than previously estimated, the offsite radiological consequences associated with these severe reactor accidents were much smaller.

More important than the actual risk estimates were the risk insights that were gained. The WASH-1400 study challenged the concept that conservative safety analyses of DBAs could establish an upper limit on public risk. Small-break LOCAs and other accident sequences involving multiple failures were found to contribute much more significantly to risk than the large-break LOCA DBAs involving single failures.

Although the PRA methodology used in WASH-1400 was broadly endorsed as the best available at the time, the study was widely criticized for its treatment of uncertainties in its estimates of severe accident probabilities. In fact, in January 1979, the Commission withdrew its support of the WASH-1400 results stating, "In particular, in light of the [Risk Assessment] Review Group conclusions on accident probabilities, the Commission does not regard as reliable the Reactor Safety Study's estimate of the overall risk of a reactor accident." Three months after the Commission released this statement, the accident at Three Mile Island (TMI)

---

[8] WASH-740, "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants" (March 1957).

[9] WASH-1400, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants" (October 1975).

occurred. This seminal event, which substantiated the WASH-1400 insight that small-break LOCAs were more significant contributors to risk than large-break LOCA DBAs, led to the initiation of a substantial research program on severe accident phenomenology and the increased use of PRA to identify plant vulnerabilities in the nuclear industry.

NUREG-1150[10]
As part of its integration plan for closure of severe accident issues[11], the NRC staff initiated a follow-on Level 3 PRA study in 1986 to update WASH-1400 using advanced PRA technology that could include quantitative estimates of risk uncertainty. Published in December 1990, 15 years after WASH-1400, the NUREG-1150 study provided a set of PRA models and a snapshot-in-time assessment of the severe accident risks associated with five commercial NPPs of different reactor and containment designs. The reactor and containment design for each of the sites involved, as well as the scope of initiating event hazard groups analyzed in each PRA are summarized below in Table 3. These "full-scope" PRAs were limited to the assessment of single-unit reactor accidents initiated primarily by internal events occurring during at-power operations, with only a partial treatment of fires and seismic events for two of the five analyzed plants. A later study evaluated the risk associated with accident sequences occurring during low-power/shutdown operations for two of the five analyzed plants (Grand Gulf[12] and Surry[13]).

Table 3. NUREG-1150 Reactor/Containment Design and Initiating Event Hazard Groups

Reactor/Containment Design	Level 1 PRA Scope	Level 2 PRA Scope	Level 3 PRA Scope
Surry-1 • Westinghouse 3-loop • Subatmospheric	Internal Events Fires Seismic Events	Internal Events Fires Seismic Events	Internal Events Fires
Zion-1 • Westinghouse 4-loop • Large dry	Internal Events	Internal Events	Internal Events
Sequoyah-1 • Westinghouse 4-loop • Ice condenser	Internal Events	Internal Events	Internal Events
Peach Bottom-2 • BWR-4 • Mark I	Internal Events Fires Seismic Events	Internal Events Fires Seismic Events	Internal Events Fires
Grand Gulf-1 • BWR-6 • Mark III	Internal Events	Internal Events	Internal Events

Primarily through the use of improved data and sophisticated models, the NUREG-1150 PRAs showed that estimates of severe accident risks were even lower than those provided by the WASH-1400 PRAs. More importantly, as a landmark study that advanced the state-of-the-art in

[10] NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants" (December 1990).

[11] SECY-88-147, "Integration Plan for Closure of Severe Accident Issues" (May 25, 1988).

[12] NUREG/CR-6143, "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1" (March 1995).

[13] NUREG/CR-6144, "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1" (July 1994).

PRA, particularly in terms of the uncertainty analysis, the NUREG-1150 models, results, and risk perspectives would subsequently be used in a variety of regulatory applications including, but not limited to:

- Development and implementation of the PRA Policy Statement
- Validation of regulatory analysis guidelines
- Validation of subsidiary numerical objectives
- Support for risk-informed rulemaking
- Prioritization of generic safety issues and nuclear safety research programs
- Individual Plant Examination of External Events (IPEEE) Program

Safety Goal Policy Statement[14]

In 1986, still in the aftermath of the TMI accident, the Commission issued the Safety Goal Policy Statement, in which it broadly defined an acceptable level of public risk due to NPP operations by establishing two qualitative safety goals, each supported by an associated quantitative health objective (QHO). These safety goals and their supporting QHOs are summarized below in Table 4.

Table 4. The Commission's Safety Goals for the Operations of NPPs

Qualitative Safety Goal	Associated QHO
Individual members of the public should be provided a level of protection from the consequences of NPP operation such that individuals bear no significant additional risk to life and health.	The risk to an average individual in the vicinity of a NPP of prompt fatalities that might result from reactor accidents should not exceed 0.1% of the sum of prompt fatality risks resulting from other accidents to which the members of the U.S. population are generally exposed.
Societal risks to life and health from NPP 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 risk to the population in the area near a NPP of cancer fatalities that might result from NPP operation should not exceed 0.1% of the sum of cancer fatality risks resulting from all other causes.

In its guidelines for regulatory implementation, the Commission directed the staff to develop specific guidance for use as a basis for determining whether a level of safety ascribed to a plant is consistent with the safety goal policy. The Commission indicated that this guidance would be based on the following general performance guideline proposed for further staff examination:

> *"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."*

In response, the NRC staff proposed that the safety goals and QHOs be partitioned into further subsidiary objectives that could utilize the risk metrics from Level 1, Level 2, and Level 3 PRAs as a basis for comparison. Although the Commission rejected this proposal in the associated

[14] 51 FR 30028, "Safety Goals for the Operations of Nuclear Power Plants" (August 21, 1986).

SRM[15], it supported the use of subsidiary quantitative core damage frequency and containment performance objectives through partitioning of the proposed large release guideline. Consistent with the defense-in-depth philosophy, these subsidiary objectives could be used as minimum acceptance criteria for prevention (core damage frequency) and mitigation (containment performance).

Direct comparison with the existing QHOs requires a Level 3 PRA that estimates the risk from all analyzed risk contributors associated with NPP operations. However, when progressing from determining the frequencies of accident sequences to estimating offsite radiological consequences, the calculations become more complex and costly, with increasing uncertainty in the end results. With Commission support, the staff therefore utilized NUREG-1150 results to develop and adopt the following subsidiary numerical objectives that could be compared with the results of Level 1 and Limited Level 2 PRAs:

- Core damage frequency (CDF) < 10^{-4} per reactor-year (surrogate for cancer fatality QHO)
- Large early-release frequency (LERF) <10^{-5} per reactor-year (surrogate for prompt fatality QHO)

The development of these subsidiary numerical objectives played an important role in the implementation of risk-informed regulation, and is germane to some of the issues that exist within the current risk-informed regulatory framework.

<u>Individual Plant Examination (IPE) Program</u>
On August 8, 1985, the Commission issued its policy statement on "Severe Reactor Accidents Regarding Future Designs and Existing Plants" (50 FR 32138), which introduced the Commission's plan to address severe accident issues for existing commercial NPPs. During the next few years, the Commission formulated an approach for systematically evaluating the safety of NPPs to identify particular accident vulnerabilities and cost-effective changes to ensure no undue risk to public health and safety.

To implement this approach, the NRC issued Generic Letter (GL) 88-20[16], requesting that each licensee perform a plant examination to "*identify plant-specific vulnerabilities to severe accidents that could be fixed with low-cost improvements*." The specific objectives of the IPE program were for each utility to:

(1) Develop an overall appreciation of severe accident behavior;

(2) Understand the most likely severe accident sequences that could occur at its plant;

(3) Gain a more quantitative understanding of the overall probability of core damage and radioactive material releases; and

(4) If necessary, reduce the overall probability of core damage and radioactive material release by appropriate modifications to procedures and hardware that would help prevent or mitigate severe accidents.

[15] SRM SECY-89-102, "Implementation of the Safety Goals" (June 15, 1990).

[16] Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities, 10 CFR 50.54(f)" (November 23, 1988).

In GL 88-20, the NRC identified PRA as one acceptable approach for conducting an IPE and further identified a number of potential benefits associated with performing PRAs on those plants without one. Examples of benefits included (1) support for licensing actions, (2) license renewal, (3) risk management, and (4) integrated safety assessment. As a result, licensees elected to perform PRAs for their IPEs.

The NRC staff received and evaluated 75 IPE submittal PRAs covering 108 NPP units. Based on guidance provided in GL 88-20, the scope of these Level 1 and Level 2 PRAs was limited to internal initiating events (including internal flooding) occurring during at-power operations. Even with these scope limitations, the NRC staff concluded that licensees had generally developed internal capability with an increased understanding of PRA and severe accidents and that the IPE Program had served as a catalyst for further improving NPP safety. Perspectives gained from the IPE Program are summarized in NUREG-1560[17].

Individual Plant Examination of External Events (IPEEE) Program

In June 1991, the NRC issued Supplement 4 to GL 88-20[18], requesting that "each licensee perform an individual plant examination of external events to identify vulnerabilities, if any, to severe accidents and report the results together with any licensee-determined improvements and corrective actions to the Commission." The external events considered in the IPEEE program included: internal fires; seismic events; and high winds, floods, and other (HFO) external initiating events involving accidents related to transportation and nearby facilities. Deliberate malevolent acts (e.g., sabotage, terrorism) were not included in the set of events considered. The objectives of the IPEEE Program were consistent with those of the IPE Program.

The NRC staff received and evaluated 70 IPEEE submittal PRAs covering all operating U.S. NPPs at the time. Through its review and evaluation, the NRC staff concluded that the perspectives and insights gained from the IPEEE program would be particularly useful in (1) NRC and industry risk-informed regulatory initiatives and activities, (2) guidance for future external events standards and PRAs, and (3) prioritization of research to improve risk analysis methods. Perspectives gained from the IPEEE program are summarized in NUREG-1742[19].

Post-PRA Policy Statement Era (1995 – Present)

As PRA technology matured and as confidence in the nuclear industry's use of PRA to positively impact NPP safety increased through the IPE Program, the NRC gradually refined its deterministic regulatory framework by incorporating the use of risk information and insights in a risk-informed regulatory framework. In 1994, the NRC developed the PRA Implementation Plan[20] to focus its efforts on increasing the use of PRA in regulatory activities. This plan was

---

[17] NUREG-1560, "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance" (December 1997).

[18] Supplement 4 to Generic Letter 88-20, "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, 10 CFR 50.54(f)" (June 28, 1991).

[19] NUREG-1742, "Perspectives Gained from the Individual Plant Examination of External Events (IPEEE) Program" (April 2002).

[20] SECY-94-219, "Proposed Agency-wide Implementation Plan for Probabilistic Risk Assessment" (August 19, 1994).

superseded in 2000 by the Risk-Informed Regulation Implementation Plan (RIRIP)[21], which was developed to more clearly describe the NRC's risk-informed activities and to provide links between those activities and the NRC's Strategic Plan. Finally, in April 2007, the NRC replaced the RIRIP with the Risk-Informed, Performance-Based Plan (RPP)[22], an integrated master plan for initiatives designed to help the NRC achieve the Commission's goal of a holistic, risk-informed and performance-based regulatory framework. Each of these plans has guided the NRC in developing risk-informed, performance-based regulations.

In this section, some of the more important activities that have shaped the development and implementation of the existing risk-informed regulatory framework are highlighted. In addition, to further set the stage for providing a basis for proposing new Level 3 PRA activities, an overview of how risk-information is currently used in regulatory activities is provided.

PRA Policy Statement[23]
On August 16, 1995, the Commission issued its PRA Policy Statement, which effectively introduced the risk-informed regulatory paradigm. Established to promote regulatory stability and efficiency through consistent and predictable implementation of potential PRA applications, this Commission policy included the following four main statements:

(1) The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art and in a manner that complements the NRC's deterministic approach and traditional defense-in-depth philosophy.

(2) Where practical within the bounds of the state-of-the-art, PRA should be used to reduce unnecessary conservatism in current regulatory requirements and to support proposals for additional regulatory requirements in accordance with 10 CFR 50.109 (Backfit Rule).

(3) PRAs used in support of regulatory decisions should be as realistic as practicable.

(4) The Commission's safety goals and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory decisions.

Regulatory Guide (RG) 1.174[24]
Although it was developed to address the use of PRA in only a specific subset of the applications identified in the PRA Implementation Plan, RG 1.174 establishes a framework for risk-informed integrated decisionmaking that has been generalized to apply to a wide variety of applications, including other application-specific regulatory guides developed to risk-inform inservice testing[25], technical specifications[26], and inservice inspection of piping[27].

---

[21] SECY-00-0062, "Risk-Informed Regulation Implementation Plan" (March 15, 2000).

[22] SECY-07-0191, "Implementation and Update of the Risk-Informed and Performance-Based Plan" (October 31, 2007).

[23] 60 FR 42622, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities" (August 16, 1995).

[24] Regulatory Guide 1.174, Rev. 2, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis" (May 2011).

[25] Regulatory Guide 1.175, "An Approach for Plant-Specific Risk-Informed Decisionmaking: Inservice Testing" (August 1998).

This risk-informed integrated decisionmaking framework, which consists of five key principles, was developed to improve consistency in regulatory decisions where PRA results are used to supplement traditional deterministic and defense-in-depth approaches. The five key principles include:

(1) **Current Regulations Met.** The proposed change meets the current regulations unless it is explicitly related to a requested exemption or rule change.

(2) **Consistent with Defense-in Depth.** The proposed change is consistent with the defense-in-depth philosophy.

(3) **Maintains Safety Margins.** The proposed change maintains sufficient safety margins.

(4) **Acceptable Risk Impact.** When proposed changes result in an increase in CDF or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement.

(5) **Monitor Performance.** The impact of the proposed change should be monitored using performance measurement strategies.

Principle 4 relates specifically to the use of PRA results. For the purposes of RG 1.174, the proposed change is considered to have met the intent of the Commission's Safety Goal Policy Statement if the PRA results meet established acceptance guidelines based on a comparison of the change in CDF and LERF to the total baseline CDF and LERF, respectively. Taken from RG 1.174, figures 2 and 3 below illustrate the CDF and LERF acceptance guidelines, respectively.

---

[26] Regulatory Guide 1.177, Rev. 1, "An Approach for Plant-Specific Risk-Informed Decisionmaking: Technical Specifications" (May 2011).

[27] Regulatory Guide 1.178, Rev. 1, "An Approach for Plant-Specific Risk-Informed Decisionmaking for Inservice Inspection of Piping" (September 2003).

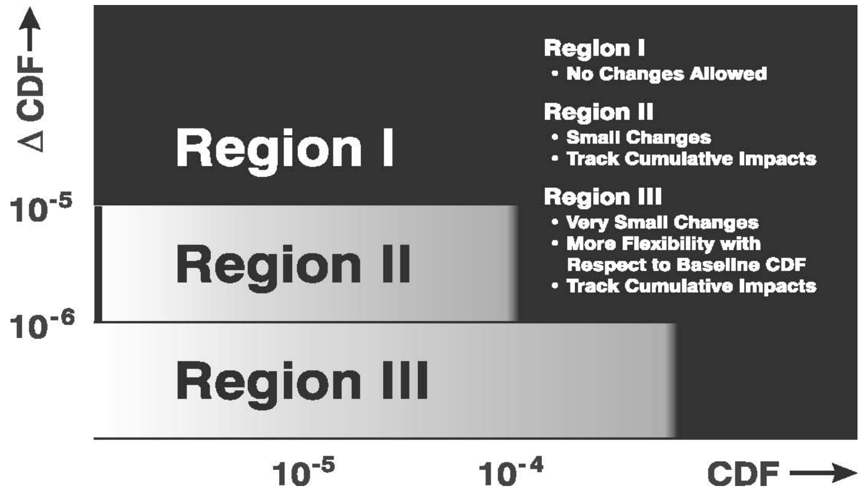


Figure 2. RG 1.174 Acceptance Guidelines for CDF

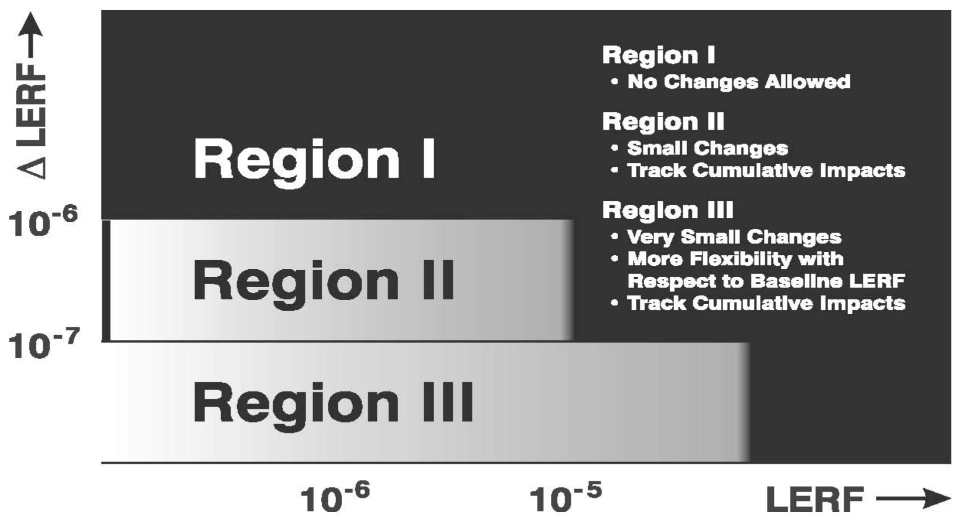


Figure 3. RG 1.174 Acceptance Guidelines for LERF

Although RG 1.174 allows for the use of the Commission's safety goal QHOs in lieu of LERF, it acknowledges that this would require an extension to a Level 3 PRA, and therefore would require additional consideration of the methods, assumptions, and associated uncertainties. Moreover, the acceptance guidelines are intended for comparison with the results of a full-scope PRA that includes all risk contributors. When a limited-scope PRA is used, the contribution of out-of-scope items to risk must be assessed based on the margin between the PRA results and the acceptance guidelines. When the margin is significant, qualitative analyses may be sufficient. When the margin is small, additional PRA analyses may be required.

Importantly, in developing this risk-informed integrated decisionmaking framework, the NRC staff acknowledged that assurance of adequate protection of public health and safety encompasses more than simply demonstrating an acceptable level of overall risk by stating:

> *"…NRC has chosen a more restrictive policy that would permit only small increases in risk, and then only when it is reasonably assured, among other things, that sufficient defense-in-depth and sufficient margins are maintained. This policy is adopted because of uncertainties and to account for the fact that safety issues continue to emerge regarding design, construction, and operational matters notwithstanding the maturity of the nuclear power industry. These factors suggest that nuclear power reactors should operate routinely only at a prudent margin above adequate protection. The safety goal subsidiary objectives are used as an example of such a prudent margin."*

RG 1.174 establishes acceptance guidelines based on CDF and LERF that reasonably assure a prudent margin above adequate protection exists.

<u>Overview of Risk-Informed Regulation in Practice</u>
The NRC now routinely uses risk information to complement traditional deterministic engineering approaches in several components of the NRC's regulatory process, including: licensing and certification, regulations and guidance, oversight, and operational experience. Some of the more significant risk-informed applications involving NPPs within each of these components are highlighted below:

Licensing and Certification
- 10 CFR 52, Licenses, certifications, and approvals for NPPs (includes PRA requirements)

Regulations and Guidance
- 10 CFR 50.44, Combustible gas control for nuclear power reactors
- 10 CFR 50.48(c), Fire protection – National Fire Protection Association Standard 805
- 10 CFR 50.62, Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled NPPs
- 10 CFR 50.63, Loss of all alternating current power (Station blackout rule)
- 10 CFR 50.65, Requirements for monitoring the effectiveness of maintenance at NPPs (Maintenance rule)
- 10 CFR 50.69, Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors

Oversight: Risk-Informed Aspects of the Reactor Oversight Process (ROP)
- Risk-informed baseline inspections
- Risk-informed performance indicators (e.g., Mitigating Systems Performance Index)
- Significance Determination Process (SDP)

Operational Experience: Risk-Informed Programs
- Incident response – Management Directive 8.3[28]
- Event assessment – Accident Sequence Precursor (ASP) Program

[28] Management Directive 8.3, "NRC Incident Investigation Program" (March 27, 2001).