September 29, 2006

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum **/RA/**
Assistant Inspector General for Audits

SUBJECT: PERSPECTIVE ON NRC'S PRA POLICY STATEMENT (OIG-06-A-25)

Attached is the Office of the Inspector General (OIG) report, *Perspective on NRC's PRA Policy Statement*. OIG conducted a review of historical documents and information surrounding the use of risk in regulation at NRC to more clearly understand how PRA fits into NRC's use of risk regulation. OIG's report identifies key historical underpinnings of risk-informed regulation at NRC. This report is being issued as a supplement to the Evaluation of NRC's Use of Probabilistic Risk Assessment (PRA) in Regulating the Commercial Nuclear Power Industry (OIG-06-A-24)

At an exit meeting on September 8, 2006, NRC officials basically agreed with the report and provided editorial suggestions, which OIG incorporated as appropriate.

We appreciate the courtesies and cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please feel free to contact me at 415-5915 or Tony Lipuma at 415-5910.

Attachment: As stated

Electronic Distribution

John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO
Michael R. Johnson, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Cynthia A. Carpenter, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Janet R. Schlueter, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV

AUDIT REPORT

Perspective on NRC's PRA
Policy Statement

OIG-06-A-25 September 29, 2006

EXECUTIVE SUMMARY

BACKGROUND

- Probabilistic risk assessment (PRA) is a tool for assessing, in a realistic manner, the strengths and weaknesses of plant design and operation. PRA has been used by the nuclear industry and the Nuclear Regulatory Commission (NRC) since the 1970s. To clarify its expectations on the usage of PRA, NRC issued a formal PRA policy statement in 1995, which has not been revised since its publication.

- The agency's PRA policy statement reflects a commitment to increasing the use of PRA technology. The following three aspects specifically referenced in the policy statement direct the increased use of PRA:

    1. to the extent supported by the state-of-the-art in PRA methods and data,

    2. in a manner that complements the NRC's deterministic approach, and

    3. that supports the NRC's traditional defense-in-depth philosophy.

PURPOSE

- To gain an in-depth perspective of NRC's use of PRA, OIG reviewed the development of the agency's PRA policy statement.

- From a historical basis, OIG synopsized the development of PRA and the resultant PRA policy statement. OIG reviewed the policy statement focusing on how PRA complements NRC's traditional deterministic approach and how PRA supports defense-in-depth. This report contains no recommendations.

INTRODUCTION

- NRC's policy statement identifies the importance of PRA in understanding "risk."

- Risk is the possibility of loss or injury.

- A "PRA" is a tool to identify severe accident vulnerabilities and provide specific quantitative results.

PRA POLICY STATEMENT

- The deterministic approach to reactor safety involves the selection of a prescribed limiting set of accidents. For each accident, the NRC requires a conservative means of evaluating the accident sequence in terms of methodology and assumptions used to evaluate the accident sequence. NRC's policy statement establishes the expectation that PRA expand on these traditional deterministic approaches.
- NRC's traditional defense-in-depth is composed of layers of protection associated with accident prevention, accident mitigation, containment, siting, and emergency response and the four fission product barriers. The fission product barriers are the fuel pellet, the fuel clad, the reactor coolant piping and containment. NRC's PRA policy statement establishes the expectation that PRA support these defense-in-depth concepts.

CHRONOLOGY

The detailed historical chronology is divided into three time periods:

- 1946-1969 – focuses on the initial uses of reactors, early reactor safety approaches, and industry concern with financial risk.
- 1970-1978 – focuses on the issuance of the Reactor Safety Study.
- 1979-1995 – focuses on the Three Mile Island accident as it affected the development of PRA up to the issuance of the PRA policy statement.

ABBREVIATIONS AND ACRONYMS

ACRS	Advisory Committee on Reactor Safeguards
AEC	Atomic Energy Commission
BWR	boiling-water reactor
CDF	core damage frequency
ECCS	emergency core cooling capability
EDO	Executive Director for Operations
LOCA	loss of coolant accident
LOSP	loss of offsite power
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
PRA	probabilistic risk assessment
PWR	pressurized-water reactor
TMI	Three Mile Island

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

I. BACKGROUND

Probabilistic risk assessment (PRA) is a tool for assessing, in a realistic manner, the strengths and weaknesses of plant design and operation. PRA has been used by the nuclear industry and the Nuclear Regulatory Commission (NRC) since the 1970s. To clarify its expectations on the usage of PRA, NRC issued a 1995 PRA policy statement, which has not been revised since its publication.

The agency's PRA policy statement reflects a commitment to increasing the use of PRA technology. The following three aspects specifically referenced in the policy statement direct the increased use of PRA:

1. to the extent supported by the state-of-the-art in PRA methods and data,

2. in a manner that complements the NRC's deterministic approach, and

3. that supports the NRC's traditional defense-in-depth philosophy.

II. PURPOSE

OIG conducted a review of historical documents and information relevant to the PRA policy statement to gain a full perspective of NRC's use of PRA. From a historical basis, OIG synopsized the development of PRA and the resultant PRA policy statement. OIG reviewed the policy statement focusing on how PRA complements NRC's traditional deterministic approach and how PRA supports defense-in-depth. This report does not contain observations, findings, or recommendations.

To evaluate NRC's use of PRA in relation to the "state-of-the art" aspect of its policy statement, OIG contracted with Scientech, LLC – a contractor with expertise in PRA methodology. Scientech evaluated NRC's internal PRA tools (i.e., PRA models and software) against prevailing good practices established in industry. Scientech used prevailing good practices as a surrogate for the PRA *Policy Statement* term "state-of-the-art" to avoid measuring NRC against leading

edge, not yet fully deployed methods. Prevailing good practices are generally accepted practices for conducting, reviewing, and documenting PRA. Scientech's report is issued under separate cover.[1]

III. INTRODUCTION

NRC's guiding principles for using PRA in regulatory decisions are reflected in the 1995 PRA policy statement. The policy statement states that traditional reactor safety[2] approaches implicitly treat "risk" by considering accidents of varying, yet non-quantitative, likelihoods of occurrence. The policy statement also identifies the importance of PRA in understanding "risk." However, the policy statement never explicitly defines "risk" in either context.

A. Definition of Risk

A dictionary definition of risk indicates that risk is the "possibility of loss or injury." This definition indicates that risk is composed of two elements. The first element, "possibility," refers to the likelihood (probability) of some event. The second element of risk is "loss or injury" (consequence) flowing from the event. Although risk is frequently used to indicate probability alone or consequence alone, both elements are necessary for a proper description of risk.

An everyday example can be used to demonstrate the two elements of risk. The owner of an automobile may take actions to reduce the likelihood *(*probability*)* of accidents through preventative maintenance, safe driving practices, or reducing unnecessary trips. The automobile owner may use airbags and seatbelts to reduce the degree of injury *(*consequence 1*)* in the event of an accident. The owner may choose to have certain levels of collision and liability insurance to reduce the degree of financial loss *(*consequence 2*)* in the event of an accident. In this manner, the risk of injury and financial loss associated with automobile ownership can be managed.

[1] *Evaluation of NRC's Use of Probabilistic Risk Assessment (PRA) In Regulating the Commercial Nuclear Power Industry*, Scientech, LLC, September 2006.

[2] The term "traditional reactor safety" is used in this report as shorthand for the policy statements phrase "NRC's deterministic approach and the NRC's traditional defense-in-depth philosophy." Refer to the background section of *Federal Register* notice (60 FR 42622).

In the context of nuclear power, risk is composed of the same basic elements. In this context, risk is most often characterized as a combination of the "probability" of a reactor accident and the consequences arising from that accident. In current risk assessment frameworks, the following arithmetic relationship is frequently used:

Risk = Probability x Consequences[3]

NRC more generally characterizes risk in terms that can be applied to the entire range of activities involving NRC licensees. As such, the agency asks the following three questions to define risk:

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

NRC refers to these three questions as the *risk triplet*. The first question is typically answered in the form of a "scenario" or a set of scenarios. The second question refers to probability and uncertainties involved. Whereas, the third question deals with the consequence or outcomes.

In reactor safety applications, typical probabilities cited involve core damage scenarios and radionuclide release scenarios. Typical consequences cited are radiation dose, health impact, or property damage.

B. Definition of Probabilistic Risk Assessment (PRA)

A "PRA" is a tool used to identify severe accident vulnerabilities and provide specific quantitative results. There are three levels of PRA -- an individual PRA evaluation can be performed at any of these levels.

[3] The NRC has not explicitly treated societal perception of different risks (risk harmonization) associated with reactor accidents. Such approaches are addressed in risk literature, including the use of risk conversion factors (RCF), where Risk = probability x consequence x RCF. See for example different RCFs for prompt death or latent cancer death addressed in "The Analysis of Actual Versus Perceived Risk," Plenum Press, 1983, (pages 213-233).

1. Level One PRA - a systematic assessment of accident initiators and system/operator responses. It reports core damage frequency and contributors to core damage frequency. A level one is the most commonly used PRA in regulatory decision making.

2. Level Two PRA - an assessment of frequency and modes of containment failure. It reports categories and frequencies of radionuclides released to the atmosphere.

3. Level Three PRA - a radiological consequences assessment of public health consequences. It reports an estimation of economic and public health risks.

A PRA[4] calculates the probability of core damage for a specific reactor through the use of fault trees[5] and event trees.[6] Fault trees and event trees are analytical tools used to develop a near exhaustive summary of sequence of failures that will lead to core melt. The accident sequences are not limited to the design basis accidents used in traditional deterministic reactor safety.[7] Design basis accidents are the set of prescribed hypothetical accidents which a reactor is designed to mitigate by preventing significant core damage.

Equipment failure probabilities are incorporated into the logic models representing the trees. This data is employed in the models to calculate core damage frequency for a reactor under evaluation. The details surrounding fault tree and event tree construction and the methods are complex and beyond the scope of this report.

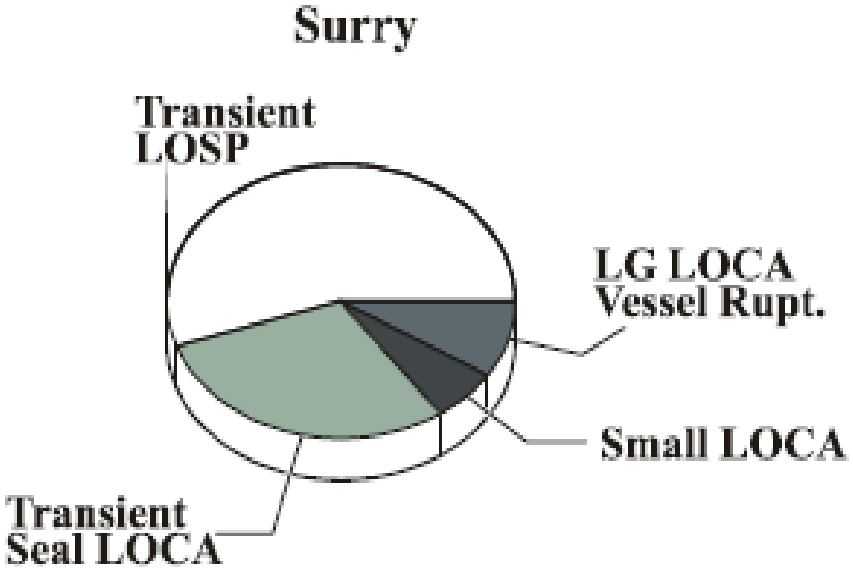
Core damage frequency provides a key risk metric for each reactor. In this manner, reactors can be compared on a risk basis using CDF.[8] Core damage frequency (CDF) is calculated from the probability of core damage. CDF represents the number of core damage events per reactor year of operation. Therefore, lower values represent lower "risk" values. For

[4] PRA is used as shorthand for a "Level 1 PRA" in the remainder of the discussion.
[5] Fault tree analysis is an evaluation of a system, component, or function in the context of environment, dependencies, and operation in an effort to identify all credible ways in which an undesired state can occur.
[6] Event trees are used to identify accident sequences that result in a specific outcome of interest (e.g., core damage). An event tree consists of an initiating event (one per tree) followed by a number of top events with the tree structure below. The top events represent the systems, components, and operations that are identified by success criteria. Success criteria establish the performance requirements for the fundamental safety functions which will be challenged or are necessary to mitigate the accident initiator.
[7] Deterministic reactor safety is discussed in section IV.A.
[8] Within the limitations of the uncertainties of the respective PRA models.

example, 100 reactors operating for 10 years, represents 1,000 reactor years of operation (1,000 = 100 x 10). If the CDF for each of these 100 reactors was 10^{-03} (0.001), there would be one (1) expected core damage event in that 10 year period (1 = 1,000 x 0.001).

Contributors to core damage measure how various events contribute to an individual reactor's CDF. As an example, Figure 1 provides the principal initiating event contributors to CDF for seismic events at Surry Nuclear Station. The figure demonstrates that transient loss of offsite power (LOSP) and transient seal loss-of-coolant accident (LOCA) are the greatest sources of core damage risk during seismic events at that plant. This information could be useful for evaluating potential safety improvements at the plant. It would lead plant operators to review plant equipment that plays a role in such events.

Figure 1
Principal Contributors
Core Damage Frequency[9]



[9] Perspectives on Reactor Safety, NUREG/CR-6042, Rev. 2, March 2002.

IV. PRA POLICY STATEMENT

The overall objective of the PRA policy statement is increased use of PRA at the NRC. As such, the policy statement provides for an expanded use of PRA in a manner that complements the agency's deterministic approach and supports its traditional defense-in-depth philosophy.

A. Complement Deterministic Approach

The deterministic approach to reactor safety establishes requirements for engineering margin (design parameters) and for quality assurance in design, manufacture, and construction. It also assumes that adverse conditions can exist and establishes a specific set of design basis events (i.e., what can go wrong?). The traditional deterministic approach treats event likelihood in non-quantitative or semi-quantitative terms. Design basis event frequencies are not required to be calculated, but are estimated. These event frequencies are used to inform the overall decision-making process for evaluating the plant design, by putting design basis accidents into groups with acceptance criteria that increase in rigor as event frequency increases.

NRC establishes conservative limiting acceptance criteria for each design basis accident for parameters such as peak fuel clad temperature, peak containment pressure, and post accident radiological dose for an individual located at the site boundary. An analytical model is used to calculate results for specified parameters for each design basis accident. The calculated results must meet acceptance criteria[10] established by the NRC, thereby demonstrating that the plant will operate within the design basis accident requirements. In this manner the deterministic approach uses a rigorous quantitative approach for determining event consequences.

In terms of the risk triplet, the traditional deterministic approach treats the first question, "What can go wrong?" -- but treatment is limited to a prescribed set of design basis events. The second question, "How likely is it?" is treated in a non-quantitative or semi-quantitative approach. The third question, "What are the consequences?" is treated using a rigorous quantitative approach for determining event consequences.

[10] Or the licensee must demonstrate and the NRC must accept a basis for adequate protection for public health and safety on a case by case basis.

NRC's policy statement establishes the expectation that PRA expand on the traditional deterministic approach. Specifically, the policy statement compliments the 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.

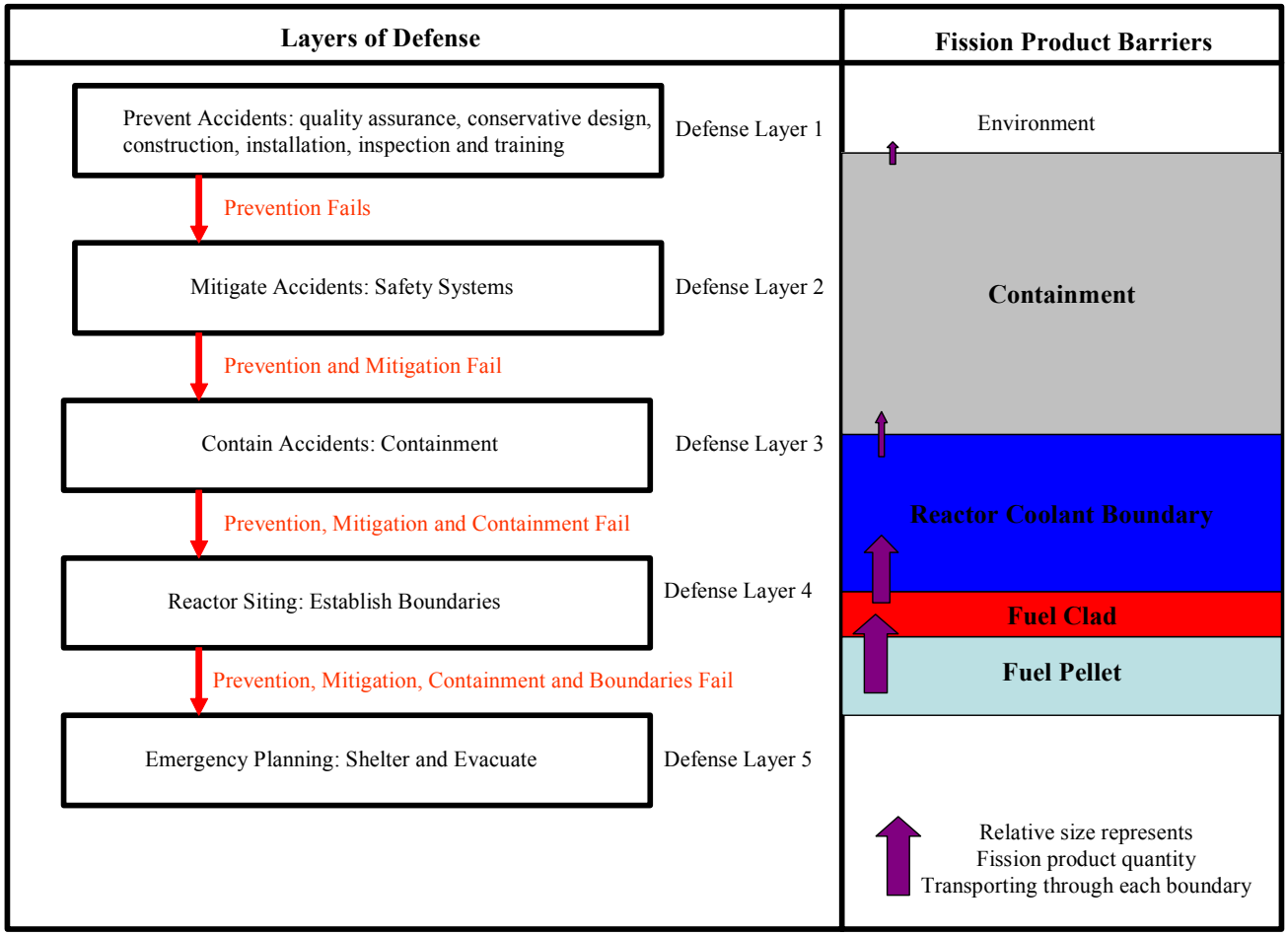
In this manner, PRA applications expand "what can go wrong" beyond those accidents prescribed in the deterministic approach. In addition, PRA develops a rigorous calculated basis for core damage frequency, "how likely is it." In this manner, PRA complements the traditional deterministic approach.

These policy statement expectations require that, PRA be used to characterize the risk posed by severe accidents and establish a means of prioritizing them for eventual resolution. In addition, resources beyond those credited in design basis accident analysis are allowed in PRA applications.

B. Support "Defense-In-Depth"

The principles of defense-in-depth dictate layers of safety in plant design and in operating practices. Defense-in-depth also stands for the principle that reactor safety should not focus on any single layer. Principles of defense-in-depth have evolved over a period of years. Defense-in-depth consists of two distinct complementary approaches. The first approach involves layers of barriers; where each barrier is focused on mitigating the consequences of the failure of other barriers. The second approach to defense-in-depth is embodied in specific plant components. Each component is an immediate physical barrier, preventing the release of radioactive fission products; these are known as fission product barriers. The fission product barriers are arranged so that radioactive material must penetrate all of the fission product barriers before reaching the environment. These two distinct approaches are described in more detail below, and represented in Figure 2.

Figure 2 Defense-in-Depth



Defense-in-Depth

Defense-in-depth principles start with accident prevention measures such as quality assurance, conservative design, construction, installation, inspection, and training -- each designed to reduce the likelihood of a reactor accident. Defense-in-depth principles postulate that these prevention measures may fail and accidents may still occur. Therefore, safety systems are required to mitigate the consequences of accidents. To exemplify defense-in-depth principles, the Federal Register Notice (60 FR 42622) for the policy statement provides that "safety cannot be placed on any single element of the design, maintenance, or operation of a nuclear power plant."

For example, power plants include a containment to reduce the likelihood of uncontrolled radioactive releases. However, defense-in-depth principles assume that containment can fail. As a result, siting criteria along with exclusion areas and low population zones are employed to reduce the potential dose received by the public in the event of an accidental radiological release from containment. Finally, emergency plan requirements further provide protection for individuals in the vicinity of nuclear plants through sheltering and evacuation actions.

V. CHRONOLOGY OF RISK DEVELOPMENTS AND KEY INFLUENCING EVENTS

External influences, circumstances, and events play a role in the formulation of agency policy. Policy statements can also be traced to predecessor activities. NRC's 1995 policy statement contains an expectation that PRA applications be developed consistent with certain traditional reactor safety practices. As a result, a historical chronology leading to the PRA policy statement is useful in understanding NRC's PRA policy statement. [See Appendix B for a timeline.]

The detailed chronology is divided into the following three time periods:

- 1946-1969 – focuses on the initial uses of reactors, early reactor safety approaches, and industry concern with financial risk.
- 1970-1978 – focuses on the issuance of the Reactor Safety Study.
- 1979-1995 – focuses on the Three Mile Island accident as it affected the development of PRA up to the issuance of the PRA policy statement.

A. Early Reactors, Financial Risks, and Early Public Concerns (1946-1969)

The Atomic Energy Act of 1946 established a government monopoly over reactor ownership and operation. From 1946 to 1954 reactors were owned and operated by the government for purposes of research (research reactors) or for the production of plutonium (production reactors) for use in nuclear weapons.

In 1954, the Atomic Energy Commission (AEC) was statutorily mandated to stimulate private sector interest in commercial nuclear power plants. Initial industry interest was tempered by concern over liability associated with potential catastrophic reactor accidents.

Early Responsibilities of Atomic Energy Commission

In 1954 when the Atomic Energy Act was amended, it abolished the government monopoly and gave the AEC two new mandates. First, the AEC was statutorily charged with stimulating interest in the private sector for commercial uses of atomic energy, including nuclear reactors for electrical power generation. Second, the AEC was responsible for regulating the use of atomic energy to ensure adequate protection of public health and safety, and for common defense and security.

The AEC worked to stimulate interest in the use of nuclear reactors for electrical power generation including a joint project between government and industry to build the first large scale electricity generating station. Industry officials were concerned with the liability that might exist in the event of an unlikely, but catastrophic reactor accident. This concern represented an impediment to increased use of nuclear reactors for electrical power generation.

The Price Anderson Act: Industry Concern for Financial Liability

The AEC undertook a study to assess the potential liability posed by a nuclear plant. The results were published in "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants" (WASH-740) in 1957. The study looked at hypothetical worst case scenarios that would cause the most damage in the event of a nuclear incident. WASH-740, in combination with the persuasive efforts of industry and the AEC, convinced Congress to pass liability legislation. As a result, in 1957 Congress enacted the Price-Anderson Act to limit the liability faced by operators of nuclear reactors.

During the 1960s, reactor applications and construction activities accelerated in response to liability protection, projected electrical generation growth, and general public support for nuclear power. By the late 1960s, public opposition to nuclear power began to grow.

B. Safety Concerns and Need to Quantify Risk (1970-1978)

By the beginning of the 1970's, anti-nuclear sentiment had grown and gained momentum. Significant concerns were raised by research tests of the emergency core cooling systems suggesting that these key safety systems may be inadequate.

Emergency Core Cooling Capability Safety Concern

The AEC sponsored emergency core cooling capability safety (ECCS) research efforts to more fully understand the effectiveness and capability of the ECCS. A series of small scale tests were conducted in 1970 and 1971 at a reactor testing facility in Idaho. These tests simulated the effects of breaks in reactor coolant pipes. Some of the test results indicated that increasing steam pressure in the reactor vessel following certain loss of coolant accidents could significantly slow down core cooling. In addition, some tests suggested that there could be significant losses of ECCS flow out of a pipe break.

Earlier work had determined that a failure of ECCS represented a potential mechanism for breaching containment.[11] The ECCS results in combination with the concerns over the potential for containment breaches represented a significant potential reactor safety concern. The AEC attempted to keep the information regarding the test results away from the public and congressional oversight. However, the information and AEC's attempt to suppress it became public knowledge. As a result, emergency core cooling moved reactor safety to the center of public controversies over nuclear power. The issue became of such significance that it was the subject of congressional hearings before the Joint Committee on Atomic Energy.

Senator Requests Comprehensive Assessment of Reactor Safety

During the ECCS controversy, Senator Pastore wrote a letter to the AEC Chairman requesting a quantifiable and probabilistic evaluation of reactor safety.[12] This letter appears to have been

[11] Concerns emerged in the late 1960s that containment failure may be conceivable under certain severe accident conditions. In a report from Oak Ridge National Laboratory in October of 1967, it was concluded that containment breaches were possible in reactor accident scenarios involving a failure of ECCS. The possibility of a containment breach represented a potential safety issue of great significance.

[12] Nuclear Reactor Safety: On the History of the Regulatory Process, David Okrent, University of Wisconsin Press, 1981, (page 316).

the impetus for a 1972 study, "The Safety of Nuclear Power Reactors (Light Water-Cooled) and Related Facilities," (WASH-1250) was circulated as draft for comments in late 1972 and later published in 1973.[13] Because the study did not provide the quantifiable and probabilistic evaluation that was requested by the Senator, an evaluation of reactor safety was initiated in the summer of 1972.

Rasmussen Report: Reactor Safety Study (WASH 1400)

A project was initiated in the summer of 1972, led by Professor Norman Rasmussen of the Massachusetts Institute of Technology. The project report titled "The Reactor Safety Study" (WASH-1400) was published in 1975 and is also commonly referred to as the "Rasmussen Report." The report identifies potential reactor accidents and accident sequences, and estimates the likelihood of fission product release during an accident sequence. The report also estimates the health effects due to the radiological release, and compares nuclear risks with other more common risks. The project was initiated under the auspices of the AEC; however, it was not published until after the NRC was formed in 1975 as part of the Energy Reorganization Act.

This study was the first PRA used in reactor safety and established core damage frequency as a key new quantitative metric for reactor safety. The study employed fault tree and event tree methodology and extensive data to estimate failure rates of equipment. One important result of the study was identifying significant contributors to core damage, including small LOCAs and transients as dominant contributors to core damage frequency.[14] The study represented a major milestone for using PRA in NRC regulatory programs and laid the foundation for risk quantification using a structured quantitative framework.

Lewis Committee Review of Reactor Safety Study

The Reactor Safety Study did not go without criticism. In 1978, Congressman Udall requested a reevaluation of its executive summary. In response, the NRC created the Risk Assessment

[13] Ibid.
[14] Nuclear Reactor Safety: On the History of the Regulatory Process, David Okrent, University of Wisconsin Press, 1981, (page 319).

Review Group, also known as the Lewis Committee, and charged them to review the Reactor Safety Study. The committee determined that WASH-1400 was successful in the following three ways:

1. making the study of reactor safety more rational,

2. establishing many of the potential accident sequences, and

3. creating methods and procedures for finding quantitative estimates of risk, using accident sequences and a data base.

The Lewis Committee cited two primary problems with the Reactor Safety Study. First, the Committee stated that error bounds on the probabilities for accident sequences were extremely understated. The Lewis Committee claimed that this weakness was due to inadequate data, an inability to quantify common cause failures, and finally due to problematic procedures and statistical methods.

The second primary problem reported by the Lewis Committee was the executive summary of The Reactor Safety Study. The Committee concluded that the executive summary was not adequately representative of the full report. The [NRC] Commission accepted the Committee's findings and issued a statement directing the NRC staff not to use the results of WASH-1400 uncritically in regulatory decision-making. In addition, the Commission did not endorse the executive summary of the Reactor Safety Study.

C. TMI: Increased Need for PRA Applications (1979-1995)

On March 28, 1979, a series of design problems and human errors converged in a sequence of events that resulted in a partial core meltdown at the Three Mile Island (TMI) nuclear plant near Harrisburg, Pennsylvania. The accident occurred as public support for nuclear power was low, and only 4 years following the formation of the NRC.

The accident sequence at TMI was the type of accident that the Reactor Safety Study had identified as a significant contributor to core damage frequency. Subsequent investigations into the TMI accident, recognized the safety insights provided by the PRA techniques in the Reactor Safety Study and recommended the agency more fully explore the applications of this methodology.

Kemeny Report

Following the March 1979 TMI accident, President Carter issued an Executive Order[15] on April 11, 1979, creating an independent review commission. The commission was chaired by John G. Kemeny, who was president of Dartmouth College at the time. The commission and the resulting report are commonly referred to as the Kemeny report. The commission was tasked with conducting a comprehensive review of the accident at TMI. The executive order directed, among other things, that the commission's study and investigation include causes of the event and provide recommendations based on the commission's findings.

The Kemeny report recommendations were wide ranging, including NRC organizational structure and statutory mandate. One recommendation called for increased safety research to be coordinated with the regulatory process, to assure maximum application to the nuclear power industry.

The report recommended continuing in depth studies of the probabilities and consequences of nuclear power plant accidents, including consequences of meltdown. The report stated that these studies should be used to help with planning event recovery and cleanup, as well as identifying desirable modifications to help prevent accidents, and mitigate their consequences.

Rogovin Report

At the same time of the Kemeny report, NRC created a special inquiry group and published a report titled "three mile island: A Report to the Commissioners and to the Public." The special inquiry group was headed by Mitchell Rogovin. The Rogovin report made many recommendations parallel to those in the Kemeny report, covering a wide range of regulatory programs and processes. The report includes a specific section on improving reactor safety by increasing the use of quantitative risk assessment.

The Rogovin report called for quantitative risk assessment as a supplement to conceptualization of reactor safety beyond the limiting design basis approach. The report also noted that techniques involved in risk assessment had improved since

[15] Executive Order 12130, "President's Commission on the Accident at Three Mile Island," April 11, 1979.

WASH 1400, but the agency has been slow in putting these methods into practice. The report discussed specific examples of limitations in the traditional regulatory approach to reactor safety. The report noted that The Reactor Safety Study had identified accident sequences like those at TMI as dominant contributors to core damage, and that the report preceded the accident by 4 years.

PRA Related TMI Actions (1983-1989)

NRC took extensive actions in response to the TMI accident and inquiries in the years following the accident. Many of these actions are related to recommendations that NRC increase the use of PRA in regulatory programs.

Policy Statement on Safety Goals (1983)

NRC published its policy statement on Safety Goals in the Federal Register on March 14, 1983. The final Federal Register notice stated that the NRC was moving forward with the explicit policy statement on safety philosophy in response to the TMI accident and recommendations of the Kemeny report.

The policy stated that the regulatory practices in place at the time were sufficient for adequate protection of public health and safety. The statement added, "some probabilistic risk analyses have already been performed for individual nuclear plants and that safety inference might be made" by comparing these results to the proposed safety criteria. The Commission directed caution in making ultimate safety conclusions on that basis, noting that collections of PRA analysis had not been consistently performed, and large uncertainties were inherent in existing probabilistic risk assessments.

NUREG 1050 State of Art of PRA (1984)

In the plan for evaluating the Safety Goal Policy Statement, NRC's Office of Nuclear Regulatory Research was tasked to collect information on PRA studies. This assignment included the task of preparing a report available to the staff and the public. The stated purpose of the report was to develop a common understanding of the dominant contributors and the probability of core melt. In addition, the report addresses the public risk due to radiation from nuclear accidents.

NUREG-1050 "Probabilistic Risk Assessment (PRA) Reference Document" was published in September 1984 in response to that assignment. The report discussed the purpose and content of PRA, the level of development that existed in PRA at that time, as well as the uncertainties associated with PRA. Potential uses of PRA are also discussed along with results of PRAs performed as of the date of the report.

The report defined a PRA as an analysis that --

1. identifies and delineates the combinations of events that will lead to severe accidents (severe core damage or core melt),

2. estimates the frequency of occurrence of each combination, and

3. estimates the consequences.

The report found that qualitative systems analysis (logic modeling) for internal accident initiators had reached a highly developed state; external initiators (seismic, fire, flood) were less well developed. Also, the report found that the database for events of high frequency was fairly good, but poor for events of low frequency. For example, there was very limited data for events initiated by highly reliable systems, because of their reliability.

In addressing uncertainties, the report stated that the uncertainties in core melt frequency for internal events are generally an order of magnitude without considering modeling assumptions. Uncertainties for core melt frequency for external events were generally estimated to be between a factor of 10 to 30 above or below the point estimate. The report also indicated that questions remained regarding the appropriateness in the manner in which, statistical methods had been employed in PRAs.

The report stated that "the frequency estimated for severe core-damage accidents is usually low (on the order of once in 10,000 reactor-years). It is not possible to validate the results directly because sufficient data does not exist." It also noted that plant specific design or operational features can have an important influence on dominant accident sequences, making generic validation difficult.

Severe Accident Policy (1985)

NRC issued a final policy statement for severe accidents on August 8, 1985.[16] The policy statement noted that many changes had been implemented in existing plants as a result of the TMI Action Plan (NUREG-0660 and NUREG 0737). The Commission also concluded that the currently operating plants posed no undue risk to public health and safety, and that no immediate actions were necessary based on severe accident risk.

The policy statement established the definition of severe accident as one in which, there is substantial core damage whether or not there are serious offsite consequences. The policy statement identified PRAs as an important source of new information regarding the current position that reactors pose no undue risk. The policy statement credited PRAs as identifying unique vulnerabilities to severe accidents resulting in low cost changes to procedures and minor design changes. The statement indicated the Commission's intent to engage in a systematic review of each nuclear plant operating and under construction; including a review of significant risk contributors that might be missed, absent a systematic plant specific search.

Individual Plant Examinations (1988)

In furtherance of the severe accident policy, NRC issued generic letter 88-20[17]. The generic letter requested each plant to perform an Individual Plant Examination (IPE), to identify any plant-specific vulnerability to severe accidents. The staff listed four specific purposes for issuing this generic letter: (1) develop an appreciation of severe accident behavior, (2) understand the most likely severe accident sequences at each plant, (3) gain a more quantitative understanding of the overall probabilities of core damage and fission product releases, and (4) where necessary, reduce these probabilities by modifying hardware or procedures.

A level one PRA was acceptable for the generic letter 88-20 response, along with a variety of other methods. The use of PRA was strongly encouraged. The initial generic letter did not require the evaluation of external events (e.g., fires,

[16] The proposed policy was promulgated in the Federal Register on April 13, 1983, 48 FR 16014.

[17] U.S. Nuclear Regulatory Commission, Generic Letter 88-20, dated November 23, 1988, *Individual Plant Examination for Severe Accident Vulnerabilities*.

earthquakes, etc.). Later supplements did require evaluation of external events. In furtherance of the Severe Accident Policy Statement, the staff proposed and the Commission approved a severe accident integration plan in 1988.

NUREG-1150 "Severe Accident Risks: An Assessment of Five U.S Nuclear Power Plants" (1990)

An element of the severe accident integration plan was the development by NRC of an updated, modern PRA of five reactors. This set of PRA evaluations was completed and published as NUREG 1150[18] in 1990.

NUREG-1150 was an effort to update the Reactor Safety Study, incorporating new information. This report summarized detailed PRAs performed on five plants, including Peach Bottom and Surry, which were analyzed in the Reactor Safety Study. NUREG 1150 employed more comprehensive data sets, and employed improvements in risk assessment techniques in comparison to what was available for the Reactor Safety Study. The results of NUREG 1150 estimated the likelihood of core melt between 1 in 10,000 (10^4) and 1 in 100,000 (10^5) per plant per year.

ACRS PRA Quality Concerns and PRA Working Group (1991-1993)

In 1991, the Advisory Committee on Reactor Safety (ACRS) wrote a letter to the Chairman of the NRC. The letter acknowledged the potential usefulness and value of PRA as a risk assessment tool. The ACRS noted that PRA was beginning to be used with increasing frequency by the NRC staff. The memo expressed concern that PRA was not being used in a consistent manner specifically pointing to issues regarding treatment of uncertainties in calculated results and appropriate levels of conservatism.

In response to the ACRS, the Executive Director for Operations (EDO) chartered a PRA Working Group in October of 1991. The Working Group completed its work in 1993 and issued a final report. The final report identified the need for improvements in PRA guidance, training, methods, and data bases.

[18] Severe Accident Risks: An Assessment of Five U.S Nuclear Power Plants, NUREG 1150, December 1990.

In addition, the Regulatory Review Group report was chartered to review processes, programs, and practices to identify the feasibility of substituting performance based requirements and guidance founded on risk insights in place of prescriptive requirements. In 1993, the Regulatory Review Group completed its work and issued a report.

In November 1993, the directors of the four major offices at NRC collectively sent a letter to the Executive Director for Operations, summarizing information from the Regulatory Review Group and the PRA Working Group. This memo suggested developing an integrated agency approach for increased PRA use considering the work of the review groups and ACRS criticisms regarding PRA. This memo, the Working Group report, and the work of the ACRS provided the direction for developing a 1994 SECY paper proposing the 1995 policy statement on PRA use.

Development of PRA Policy Statement (1994-1995)

SECY 94-128[19] proposed that the Commission adopt and publish a policy statement on the use of PRA. The SECY paper stated that policy, legal, and technical issues would be raised in adopting increased use of PRA. The SECY paper identified several technical issues including uncertainties with calculated probabilities, limitations in data and modeling, difficulties in addressing design or construction errors, and difficulties in modeling human error and safety culture issues.

The discussion contained in the SECY noted that NRC requirements, associated with defense-in-depth and with deterministic evaluation of design basis accidents had been effective in protecting public health and safety. The paper also noted that PRA, up to that point in time had been used to "complement" these traditional methods by facilitating an assessment of a broad range of beyond design basis accident, conditions involving multiple and complex failures, and system interactions. The paper also recommended the increased use of PRA, to the extent it is "supported by the state-of-the-art" in PRA methods, and tools in a manner "supportive" of the NRC's traditional defense-in-depth philosophy.

[19] U.S. Nuclear Regulatory Commission, *Proposed Policy Statement on the Use of Probabilistic Risk Assessment (PRA)*, August 18, 1994.

The Commission proposed minor modifications in approving the proposed PRA policy statement later in 1994. The final policy statement was published in the Federal Register in August 1995 and has not been revised since that date.

The policy suggests that the use of PRA should be increased, but this increase should be tempered in two particular ways. First, PRA should only be implemented to the extent that the tools and data are the state-of-the-art. Second, PRA should "complement" the deterministic approach and be supportive of defense-in-depth. This can be achieved by --

1. considering 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.

Along with the PRA policy statement, the staff developed and issued a PRA implementation plan to carry forward initiatives in support of the policy.

Appendix A

PRA POLICY STATEMENT

On August 16, 1995, the NRC issued a Final Policy Statement[20] regarding the use of PRA at the Nuclear Regulatory Commission. The Policy Statement has not been revised since that time and continues to represent the written expression of Commission policy regarding the use of PRA. The Policy statement provides key guiding principles regarding PRA applications. The actual statement of the Policy in section IV of the Federal Register Notice is repeated in full below:

"Therefore, the Commission adopts the following policy statement regarding the expanded NRC use of PRA:

1. 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.

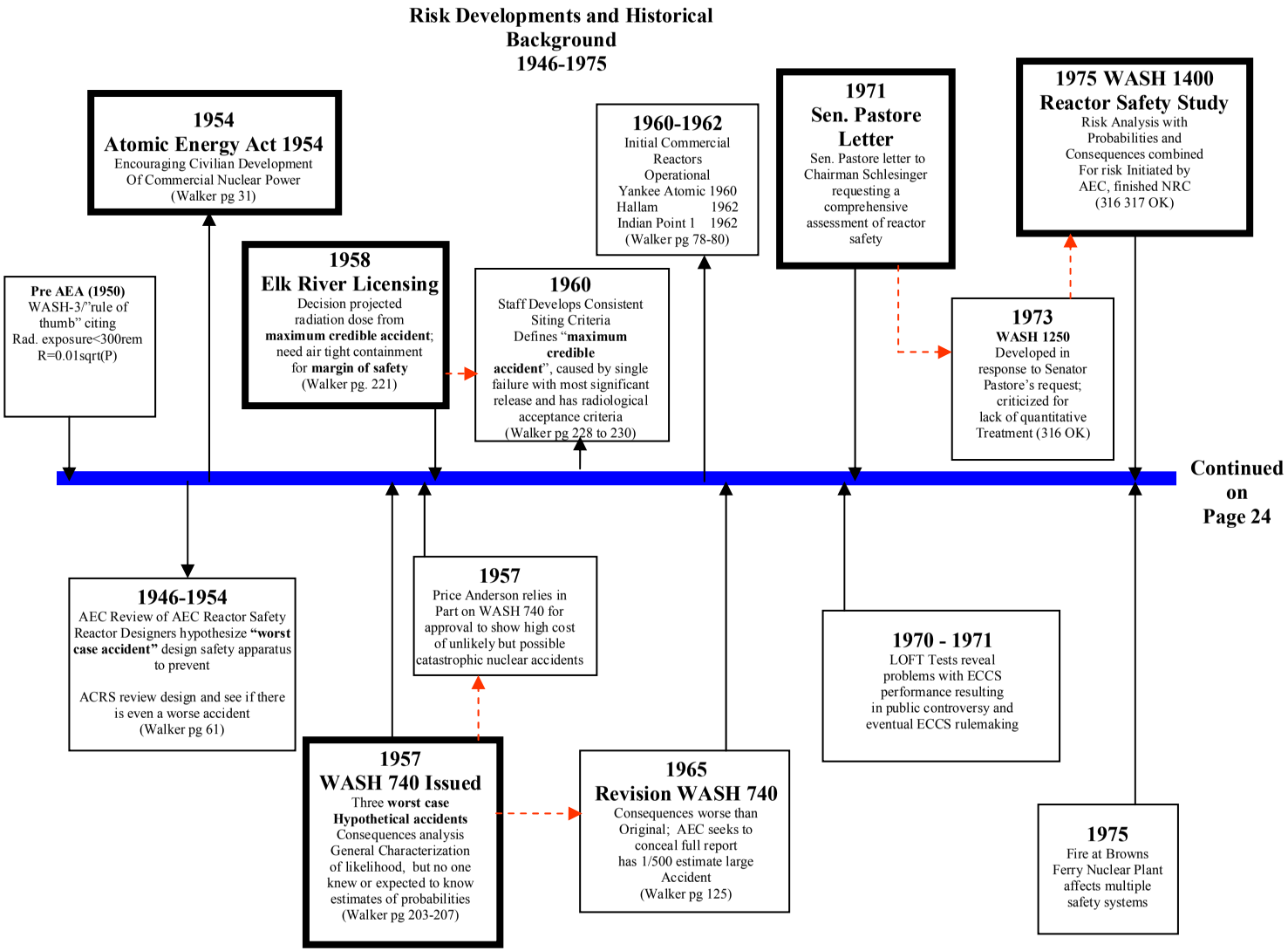
2. PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal for 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, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.

3. PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.

[20] Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement, August 16, 1995, *60 FR 42622*.

4). The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees."

Appendix B


Risk Developments and Historical Background 1946-1975
1954
Atomic Energy Act 1954
Encouraging Civilian Development Of Commercial Nuclear Power
(Walker pg 31)
1960-1962
Initial Commercial Reactors Operational
Yankee Atomic 1960
Hallam 1962
Indian Point 1 1962
(Walker pg 78-80)
1971
Sen. Pastore Letter
Sen. Pastore letter to Chairman Schlesinger requesting a comprehensive assessment of reactor safety
1975 WASH 1400
Reactor Safety Study
Risk Analysis with Probabilities and Consequences combined For risk Initiated by AEC, finished NRC
(316 317 OK)
Pre AEA (1950)
WASH-3/"rule of thumb" citing
Rad. exposure<300rem
R=0.01sqrt(P)
1958
Elk River Licensing
Decision projected radiation dose from maximum credible accident; need air tight containment for margin of safety
(Walker pg. 221)
1960
Staff Develops Consistent Siting Criteria
Defines "maximum credible accident", caused by single failure with most significant release and has radiological acceptance criteria
(Walker pg 228 to 230)
1973
WASH 1250
Developed in response to Senator Pastore's request; criticized for lack of quantitative Treatment (316 OK)
Continued on Page 24
1946-1954
AEC Review of AEC Reactor Safety
Reactor Designers hypothesize "worst case accident" design safety apparatus to prevent
ACRS review design and see if there is even a worse accident
(Walker pg 61)
1957
Price Anderson relies in Part on WASH 740 for approval to show high cost of unlikely but possible catastrophic nuclear accidents
1970 - 1971
LOFT Tests reveal problems with ECCS performance resulting in public controversy and eventual ECCS rulemaking
1957
WASH 740 Issued
Three worst case Hypothetical accidents
Consequences analysis
General Characterization of likelihood, but no one knew or expected to know estimates of probabilities
(Walker pg 203-207)
1965
Revision WASH 740
Consequences worse than Original; AEC seeks to conceal full report
has 1/500 estimate large Accident
(Walker pg 125)
1975
Fire at Browns Ferry Nuclear Plant affects multiple safety systems

Appendix B

Risk Developments and Historical Background
1975-1995