NUCLEAR ENERGY RESEARCH INITIATIVE

Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants

(Cooperative Agreement DE-FC03-99SF21902)

Annual Report

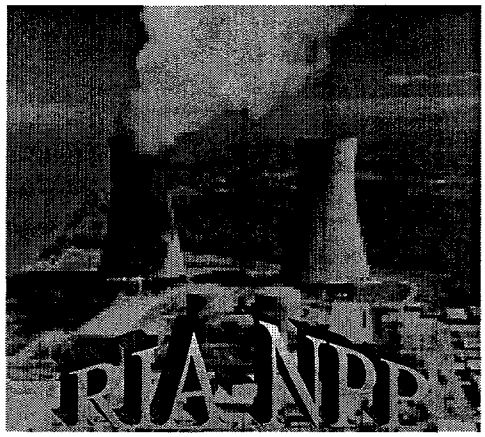
RISK-G-007-2000
Version 1.0
August 2000

NUCLEAR ENERGY RESEARCH INITIATIVE

Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants

(Cooperative Agreement DE-FC03-99SF21902)

Annual Report



RISK-G-007-2000
Version 1.0
August 2000

Issued by Westinghouse Electric Company, Nuclear Systems

Stanley E. Ritterbusch,
Principal Investigator and
Annual Report Editor

For copies of this document, contact Laurie White [(860) 285-3797, laurie.j.white@us.westinghouse.com] or Stanley Ritterbusch [860 285-5206, stanley.e.ritterbusch@us.westinghouse.com]

Table of Contents

Executive Summary

This document provides a status report to the Department of Energy (DOE) on each of the subtasks in this project, as of the end of Phase 1 (the first year). As such, the material presented herein is not finalized. Instead, each of the "Accomplishment" sub-sections and corresponding material in the appendices are snapshots of "works in progress" – some being almost complete and others requiring extensive effort and editing. As the subtasks are completed, final reports will be issued as deliverables to DOE, during Phases 2 and 3 of the project – including a summary report that ties the pieces together. These final reports will be suitable for wide distribution.

Background and Goal: The DOE established the Nuclear Energy Research Initiative (NERI) to address the barriers to long term use of nuclear-generated electricity in the United States. In addition, the Electric Power Research Institute has continued to perform studies on the cost of coal, gas, and nuclear-generated electricity. To be competitive, the cost for the nuclear option would have to decrease to the range of 3 cents/kilowatt-hour over the next two decades. Correspondingly, the total plant capital cost would have to decrease by about 35% to 40%, and the construction schedule would have to be shortened to about three years in order to ensure nuclear-generated electricity would be economically competitive.

In response to the above developments, Westinghouse Electric Company, Nuclear Systems (WENS, formerly ABB Combustion Engineering Nuclear Power) initiated a cooperative effort with Sandia National Laboratories and Duke Engineering & Services on an innovative research program proposal with the goal of meeting the above cost reduction targets for new nuclear power plant construction. The vision for this cooperative effort is to meet the cost-reduction goals through implementation of new technology and innovative approaches to the design and licensing of new nuclear power plants. Specifically, the cooperative proposal included (1) computer technologies already developed for other industries, (2) significant use of probabilistic safety assessments to reform plant design practices, and (3) risk-informed methods to develop a new design and regulatory process. DOE approved three separate projects which have similar overall objectives of reducing nuclear power plant costs. These three projects are "Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants" led by WENS, "Smart Nuclear Power Plant Program" led by Sandia National Laboratories, and "Design, Procure, Construct, Install and Test Program" led by Duke Engineering & Services. These projects are being coordinated by WENS to gain maximum benefit to each. The duration of the Risk-Informed Assessment project is approximately 2.6 years and DOE is expected to provide funding of $2.5 million. WENS partners in this project are Egan & Associates, Duke Engineering & Services, Massachusetts Institute of Technology, North Carolina State University, Sandia National Laboratories, and Idaho National Engineering & Environmental Laboratory.

Approach and Benefits: The Risk Informed Assessment of Regulatory Requirements project includes two basic tasks: (1) "Development of Risk-Informed Methodologies" and (2) "Strengthening the Reliability Database." The primary benefit of this project is

the development of methods for a new, highly risk-informed design and regulatory process. For the first task, specific subtasks are: (1) identify all applicable current regulatory requirements and industry standards; (2) identify systems, structures, and components (SSCs) and their associated costs for a typical plant; (3) develop a methodology for risk-informing the requirements and standards; (4) develop a methodology for risk-informing the design of SSCs; (5) identify those requirements, standards, and SSCs that should be given the highest priority; (6) demonstrate the methodologies by applying them to a sample SSC; (7) evaluate the current regulatory processes at the Nuclear Regulatory Commission (NRC); and (8) coordinate these activities with the currently ongoing efforts of the Nuclear Energy Institute (NEI), NRC, and industry.

The second basic task is the strengthening of the reliability database that will be needed to evaluate the safety and reliability of future nuclear power plant designs. Plant designers will need to demonstrate that their new plant designs satisfy NRC safety goals. This will require good, defensible reliability data for equipment. For example, there is limited data on the reliability and performance of the new, advanced "smart" equipment or other advanced technology equipment that may be introduced in new nuclear plant designs. Very little reliability data on domestic software used in SSCs is available, particularly for software used in critical safety systems. Further, there is not any significant amount of information from the nuclear industry that can be used to correlate equipment reliability to quality class or to the "goodness/completeness" of the testing performed on the equipment reliability. Specific subtasks for this effort are: (1) identify current sources of reliability data, (2) identify weaknesses in data sources, and (3) develop proposed programs for correcting the weaknesses.

Issues and Accomplishments: Shortly after initiating Phase 1 of this project, team members met to establish the principal strategies required to achieve the project's cost reduction goals. It was agreed that a very basic change to the current method of design and regulation was needed. That is, it was believed that the cost reduction goal could not be met by fixing the current system (i.e., an evolutionary approach) and a new, more advanced, approach for this project would be needed. It is believed that a completely new design and regulatory process would have to be developed – a "clean sheet of paper" approach. This new approach would start with risk-based methods, would establish probabilistic design criteria, and would implement defense-in-depth only when necessary to meet basic public policy issues (e.g., use of a containment building) and to address uncertainties in probabilistic methods and equipment performance. This new approach is different from the NRC's current risk-informed program for operating plants in that , for our new approach, defense-in-depth is subsidiary to risk-based methods whereas in the NRC's current approach, defense-in-depth remains the primary means of assuring protection of the public health and safety.

The primary accomplishments during Phase 1 included (1) the establishment of a new, highly risk-informed design and regulatory framework, (2) the establishment of the preliminary version of the new, highly risk-informed design process, (3) core damage frequency predictions showing that, based on new, lower pipe rupture probabilities, the

emergency core cooling system equipment can be reduced or eliminated without reducing plant safety, and (4) the initial development of methods for including uncertainties in a new integrated structures-systems design model. Other Phase 1 accomplishments included the conversion of an NRC database for cross-referencing NRC criteria and industry codes and standards to Microsoft 2000 software, an assessment of NRC's hearing process which concluded that the normal cross-examination during public hearings is not actually required by the U.S. Administrative Procedures Act, the identification and listing of reliability data sources, and interfacing with NRC at workshops for risk-informing regulations and other industry groups (NEI and IAEA).

Deliverable, Schedule, and Cost Summary: Status reports and documentation for Phase 1 were produced as planned. As a result of re-orienting the approach for this project, as summarized above, the start dates of tasks 1.1 and 1.2 were delayed by about six months and the start of tasks 1.3 – 1.6 were advanced by the same amount. Total project costs remained within budget limits and, at the end of Phase 1, all subcontractors were within their respective cost limits.

Next Year's Activities and Deliverables: In Phase 2, the tasks summarized above will be continued. The primary activities will be the fuller development of the new design and regulatory process, its demonstration with more cost reduction estimates, refinement of the new risk-informed regulatory framework, integration of the new structures-systems design model into the new design process, evaluation of existing reliability data against needs of the new design process, evaluation of NRC staff's design review process, and continued interactions with NRC and industry. This work will be documented primarily in the Phase 2 annual topical report, with supplementary documents, papers, presentations, and final reports produced as necessary for specific tasks.

1.0 Introduction

1.1 Background

The overall goal of this research project is to support innovation in new nuclear power plant designs. This project is examining the implications, for future reactors and future safety regulation, of utilizing a new risk-informed regulatory system as a replacement for the current system. This innovation will be made possible through development of a scientific, highly risk-informed approach for the design and regulation of nuclear power plants. This approach will include the development and/or confirmation of corresponding regulatory requirements and industry standards. The major impediment to long term competitiveness of new nuclear plants in the U.S. is the capital cost component -- which may need to be reduced on the order of 35% to 40% for Advanced Light Water Reactors (ALWRs) such as System 80+ and Advanced Boiling Water Reactor (ABWR). The required cost reduction for an ALWR such as AP600 or AP1000 would be expected to be less. Such reductions in capital cost will require a fundamental reevaluation of the industry standards and regulatory bases under which nuclear plants are designed and licensed. Fortunately, there is now an increasing awareness that many of the existing regulatory requirements and industry standards are not significantly contributing to safety and reliability and, therefore, are unnecessarily adding to nuclear plant costs. Not only does this degrade the economic competitiveness of nuclear energy, it results in unnecessary costs to the American electricity consumer. While addressing these concerns, this research project will be coordinated with current efforts of industry and NRC to develop risk-informed, performance-based regulations that affect the operation of the existing nuclear plants; however, this project will go further by focusing on the design of new plants.

1.2 Benefits

Meeting the above goal will enable both a more efficient and science-based regulatory process and improved plant designs. The resulting methods and tools will represent an advancement in the science of risk management. Further, the capability to rapidly evaluate designs and design changes will facilitate innovation in plant concept and design.

Regulatory requirements and industry standards will strongly determine the design bases for future nuclear energy plants – whether they be pressurized water reactors, boiling water reactors, gas cooled reactors, liquid metal reactors, molten salt reactors, proliferation-resistant reactors, passive reactors, or any other type that has yet to be conceived. Before any new nuclear plant designs are developed and licensed in the U.S., it is essential that appropriate regulatory requirements and industry standards be established so as to minimize costs and enable new technologies. Systematic, science-based processes need to be developed to evaluate the appropriateness of the existing requirements and standards, propose new design and regulatory criteria, and support design evaluations.

The current collection of nuclear industry standards and NRC regulatory requirements includes primarily deterministic criteria, based largely on qualitative risk assessments and engineering judgment that evolved over the last forty years of the nuclear energy industry. Many of the current industry standards and regulatory criteria are not significantly contributing to reliability and safety and, therefore, have needlessly driven the costs of new nuclear plants into a range that is not economically competitive in the U.S. market.

The state of the art for probabilistic safety assessment (PSA), including the database of operating experience, is now sufficiently mature that we should be able to develop a new, highly risk-informed design and regulatory process that maintains high levels of reliability and safety while decreasing plant capital and construction costs. Although humans must always make the final decisions, the decision process should now be able to rely much more heavily on risk-informed inputs. The Nuclear Energy Institute, the NRC, and the rest of the nuclear industry are already working together to apply risk-informed, performance-based regulation to the licensing of existing plants. Though still in the early stages, this industry/NRC effort is making progress and promises to offer substantial benefits. However, these efforts are focused only upon the requirements that affect operation and maintenance of existing nuclear plants.

What is needed, beyond the current effort, is to apply a more aggressive risk-informed approach to those issues that affect the design and licensing of new plants, rather than just the operation and maintenance of existing ones. This project is developing the methodologies needed for such an aggressive program. Since this research effort will be coordinated with the ongoing industry/NRC effort for existing plants, it is intended to complement that ongoing program, rather than duplicate it or compete against it.

1.3 Vision

To understand the need for a new, highly risk-informed design and regulatory process, it is worthwhile to first step back and look at an example of how the current design and regulatory requirements and standards evolved – and why they may no longer be appropriate. For such an example, let's look at the design of the Safety Injection System (SIS) and its design basis event, the loss of coolant accident. Beginning over thirty years ago, a great number of deterministic regulatory criteria have been developed for the SIS, based upon a postulated event that is now known to have a negligible chance of occurrence: an instantaneous double-ended guillotine pipe break, in the worst location, with the worst single failure, with the worst initial conditions, with the worst operator response, with the worst coolant-radioactivity conditions, with the worst containment leakage, etc., etc. Industry standards and NRC regulatory requirements for the SIS evolved in a patchwork of documents that were generated or revised every time someone thought of a new concern, there was a new problem at an operating plant, or something was found during maintenance. These requirements are found in a number of documents that include the Code of Federal Regulations, regulatory guides, standard review plans, IE bulletins, etc. In many cases, industry standards (e.g., portions of the ASME Code) were developed and referenced in the NRC documents. Because many of these

requirements were put in place many years ago, they were not subject to cost/benefit evaluation. Even if they had, they would have been evaluated separately, one by one. There has never been a complete assessment of how all of the requirements – taken together as a package – would be evaluated in a comprehensive cost/benefit analysis.

After the first full blown PRAs were performed in the 1970s (e.g., WASH-1400), it was recognized that the most catastrophic events imaginable were not the events most likely to threaten public safety. The double-ended guillotine pipe break was found to be of such low probability that, by the early 1980s, the NRC's Materials Branch acknowledged that ductile pipe would "leak before break" and, therefore, could not pose a real threat -- as long as there was a leakage detection system. On this basis, the NRC allowed "leak before break" to be credited, in satisfying some of the *new* requirements that NRC was then imposing (e.g., for asymmetric blowdown loads). However, the double-ended guillotine pipe break was still maintained as the basis for the already established NRC requirements -- which had served as the design basis for almost everything in the nuclear island (e.g., the SIS, containment, etc.). This obvious inconsistency in regulatory requirements was accepted by NRC and industry as providing an added safety cushion, to cover the unknown.

In a young industry -- lacking a wealth of operating experience and data -- an added safety cushion, to cover the unknown, was not unreasonable. Furthermore, in a regulated electricity industry, the added requirements could be tolerated because plant owners could usually pass along the costs of satisfying the NRC requirements to ratepayers. However, in the coming deregulated power market, continuing the use of design features that don't truly add to safety and reliability will result in nuclear plant designs that are not cost competitive against other electricity generating options -- and, therefore, will simply not be purchased.

If a significantly more risk-informed design and regulatory approach were applied to the SIS, then the design of the system could be greatly simplified. Based on PRA insights, a more realistic pipe break scenario could be established as the design basis event. At the same time, plant designers could introduce new advanced technologies into the SIS design – e.g., "smart" equipment (pumps and valves with self-diagnostic self-monitoring features built in) – to improve reliability at the component level. Coupled with the more realistic design bases, it is likely that the designers could develop a two-train SIS that is just as reliable as the four-train design currently found in the ALWR designs -- with each train being simpler than those in the ALWR designs. Even if each individual train turned out to be slightly more expensive, elimination of two trains would still reduce the overall cost of the SIS. Very importantly, elimination of two trains would also reduce the costs of the structures required to house the SIS, as well as the other systems that support it. Designers could also simplify the system's operating, maintenance, and testing procedures. Another possibility for providing the SI function would be to combine the SI function with the normal water makeup function, using "smart" pumps that would be more reliable and would always be available in case of an accident. A similar approach could be applied to the containment and throughout the entire plant design. Very

importantly, this new design approach could all be implemented without sacrificing safety.

Coordinated through NEI, the NRC and industry are already discussing how many of the NRC's overly prescriptive requirements can be streamlined via a risk-informed, performance-based assessment. However, they are focusing their discussions upon those issues that affect the operation of existing plants. Thus, in the example just discussed (the double-ended guillotine pipe break and the SIS design), the NRC and industry are most concerned about requirements that affect the plant's technical specifications. Since these plants have already been built, the current NRC and industry efforts are not concerned with changes that could determine the design of a new SIS or its combination with the normal water makeup system. Obviously, the potential cost savings related to the design, fabrication, and construction of the SIS for a new nuclear plant would be substantially greater than the cost savings likely to result from technical specification changes related to the operation of the SIS.

The SIS is but one of hundreds of Systems, Structures, and Components (SSCs) in a nuclear plant's design that could benefit from application of risk-informed methodologies. For example, risk-informing the quality assurance requirements for nuclear plant equipment (in Appendix B of 10CFR50) could save many millions of dollars in unnecessary paperwork that, in many cases, does not significantly add to safety. A thorough risk-informed assessment of the design and regulatory process and all of the SSCs in a nuclear plant design would likely result in a reduction of nuclear plant costs by hundreds of millions of dollars.

2.0 Project Goals and Organization

2.1 Goals

The overall goal of this research project is to support innovation in new nuclear power plant designs. This project is examining the implications, for future reactors and future safety regulation, of utilizing a new risk-informed regulatory system as a replacement for the current system. This innovation will be made possible through development of a scientific, highly risk-informed approach for the design and regulation of nuclear power plants. The major impediment to long term competitiveness of new nuclear plants in the U.S. is the capital cost component -- which may need to be reduced on the order of 35% to 40% for ALWRs such as System 80+ and ABWR. The required cost reduction for an ALWR such as AP600 or AP1000 would be expected to be less. Such reductions in capital cost will require a fundamental reevaluation of the industry standards and regulatory bases under which nuclear plants are designed and licensed. Fortunately, there is now an increasing awareness that many of the existing regulatory requirements and industry standards are not significantly contributing to safety and reliability and, therefore, are unnecessarily adding to nuclear plant costs. Not only does this degrade the economic competitiveness of nuclear energy; it results in unnecessary costs to the American electricity consumer. While addressing these concerns, this research project will be coordinated with current efforts of industry and NRC to develop risk-informed, performance-based regulations that affect the operation of the existing nuclear plants; however, this project will go further by focusing on the design of new plants.

The above goal is being achieved through the following two major tasks (objectives):

- **Task 1: Development of Risk-Informed Methodologies:** Many of the regulatory requirements and industry standards that form the bases for designing the current generation of nuclear plant designs are based upon subjective, deterministic assumptions that were limited by the knowledge-base and engineering tools that were available at the time that those requirements and standards were created. The research effort proposed for this project is to develop a set of risk-informed methodologies that can be used by future plant designers to (1) systematically develop and/or utilize all of the regulatory requirements and industry standards that would impact the design of new nuclear plants and (2) systematically develop designs for a nuclear plant's SSC's, by applying those methodologies. This research effort will be complementary to the current industry/NRC efforts to apply risk-informed, performance-based regulation to selected issues that affect operation of existing nuclear plants. The methodologies developed in this research project will then be demonstrated, by applying them to a sample problem. The methodologies may then be revised to apply the lessons learned from this sample.

- **Task 2: Strengthen the Reliability Database:** To fully risk-inform the design bases for future nuclear plants, it is essential that the reliability database for the SSC's be complete. Current industry/NRC efforts to strengthen the reliability database are primarily focused upon issues that affect operation of the existing nuclear plants. The

research effort proposed for this project will identify where strengthening of the risk assessment database is needed to support the design of new plants – including identification of the reliability information that will be needed to support introduction of new, advanced "smart" technologies. The research effort will also recommend programs for collecting the information that will be needed by future plant designers, to provide this information.

2.2 Organization

Work for this project is organized according to the following work breakdown structure:

Task 1: Development of Risk-Informed Methodologies

- Subtask 1.1: Identify applicable current regulatory requirements and industry standards.
- Subtask 1.2: Identify systems, structures, and components (SSCs) and their associated costs for a typical plant.
- Subtask 1.3: Develop methodology for developing risk-informed requirements and standards.
- Subtask 1.4: Develop methodology for designing highly risk-informed SSCs.
- Subtask 1.5: Identify high priority requirements, standards, and SSCs.
- Subtask 1.6: Apply methodologies to a sample SSC.
- Subtask 1.7: Evaluate regulatory processes and develop recommended improvements.
- Subtask 1.8: Coordinate activities with ongoing efforts of NEI, NRC, and industry.

Task 2: Strengthen the Reliability Database

- Subtask 2.1: Identify current sources of reliability data for SSCs.
- Subtask 2.2: Identify weaknesses in sources.
- Subtask 2.3: Develop industry/government programs for correcting the weaknesses.

The primary technical responsibilities of each team participant are shown in the matrix of Table 2.2-1. The schedule for these tasks is shown in Figure 2.2-1 and the project organization is shown in Figure 2.2-2.

Table 2.2-1
Primary Responsibilities of Team Participants for the Risk-Informed Project

Participant / Task	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	2.1	2.2	2.3
Westinghouse		X		X	X	X		X			
Duke Engineering	X			X							
MIT			X	X	X	X					
NCSU				X	X	X					
Egan & Associates							X	X			
Sandia NL			X								
Idaho NEEL									X	X	X

Figure 2.2-1

DOE F 4600.3
(03-94)
Replaces EIA-459B

U.S. DEPARTMENT OF ENERGY
FEDERAL ASSISTANCE MILESTONE PLAN

OMB Control No.
1910-0400

OMB Burden Disclosure Statement

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of Information Resources Management Policy, Plans, and Oversight, Records Management Division, HR-422 - GTN, Paperwork Reduction Project (1910-0400), U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, DC 20585; and to the Office of Management and Budget (OMB), Paperwork Reduction Project (1910-0400), Washington, DC 20503.

1. Program/Project Identification No.	2. Program/Project Title	
DE-FC03-99SF21902	Risk-Informed Assessment of Design and Regulatory Requirements for NPPs	
3. Performer (Name, Address) ABB Combustion Engineering Nuclear Power, Inc. 2000 Day Hill Road Windsor, CT 06095-0500 Attn: PI Stanley Ritterbusch		4. Program/Project Start Date 8/20/99 5. Program/Project Completion Date 3/19/02

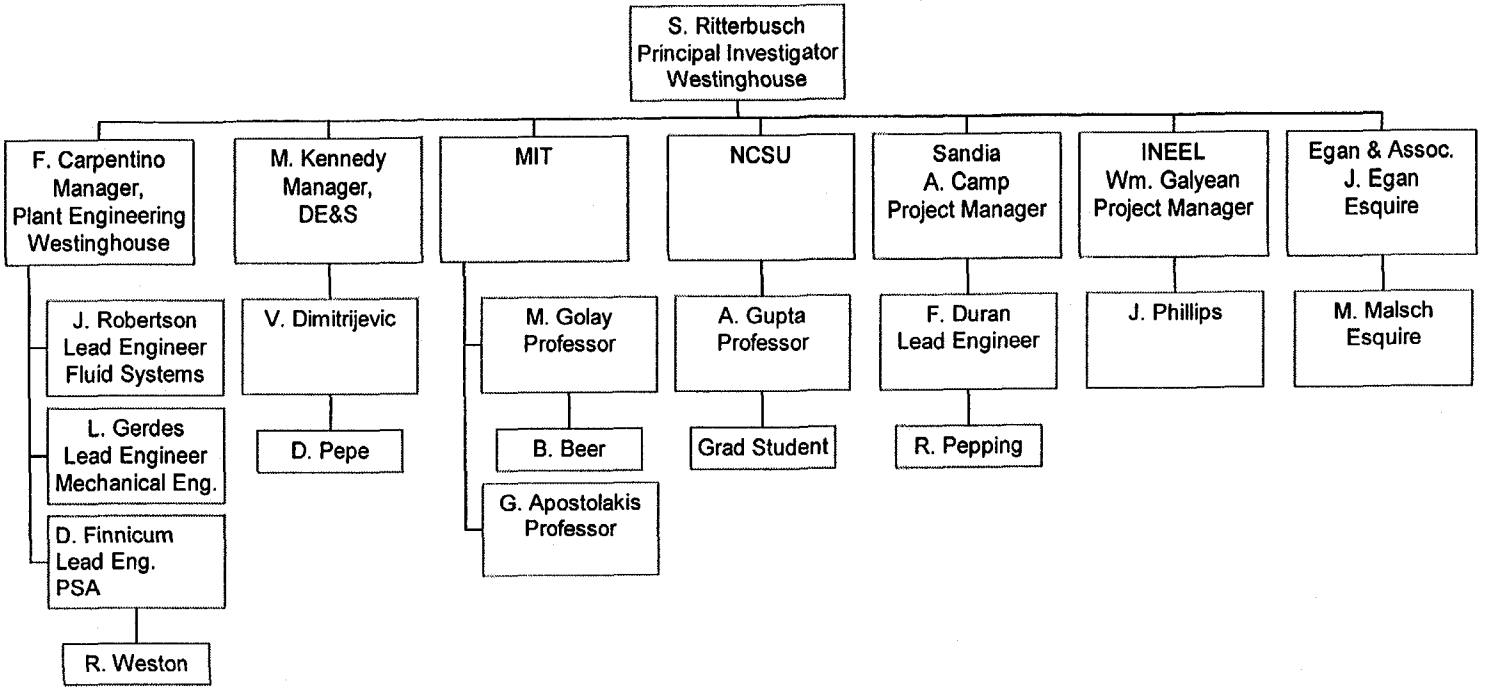
6. Identification Number	7. Planning Category (Work Breakdown Structure Tasks)	8. Program/Project Duration (1) 9/99 9/00 9/01 S N J M M J S N J M M J S N J M	9. Comments (Notes, Name of Performer)
1.1	Identify Reg. Requirements		ABB (2)
1.2	Identify SSCs & Costs		ABB (2)
1.3	Develop Reg. Methods		ABB (2)
1.4	Dev.Simplification Methods		ABB (2)
1.5	Identify Priority SSCs		ABB (2)
1.6	Apply Methods to Sample		ABB (2)
1.7	Evaluate Reg. Process		ABB (2)
1.8	Industry Coordination		ABB (2)
2.1	Identify Data Sources		ABB (2)
2.2	Identify Data Weaknesses		ABB (2)
2.3	Develop Corrective Programs		ABB (2)

10. Remarks
(1)Two months/box (2) ABB is lead organization; collaborating orgs are Sandia, INEEL, MIT, DE&S, NCSU, Egan & Associates

11. Signature of Recipient and Date	12. Signature of U.S. Department of Energy (DOE) Reviewing Representative and Date

Printed with soy ink on recycled paper

Figure 2.2-2
Risk-Informed Assessment Project Team Organization



3.0 Approach and Accomplishments

3.1 Task 1 Development of Risk-Informed Methodologies

3.1.1 Identify All Applicable Current Regulatory Requirements and Industry Standards

Approach

Before a new nuclear plant designer can begin to implement any methodologies for risk-informing the plant's design criteria, it is essential that the designer have a complete set of those criteria available. Thus, the objective of this task is to prepare a complete compilation of all NRC criteria and industry standards that are applied to the design and operation of a typical nuclear power plant. In addition to compiling a complete list of regulatory guidance, this task will also search for design criteria that are imbedded in other documents. For example, NRC Regulatory Guidelines often refer to IEEE or other industry standards. Many of the criteria are imbedded in documents that are not legal requirements but are, nevertheless, often applied by designers and regulators.

There are also a vast number of non-enforceable NRC guidance documents. These provide detailed descriptions of current NRC regulatory policies, interpretations, and practices, and they usually constitute *de facto* requirements because of the time and effort required to convince the NRC that an alternative policy, interpretation, or practice is acceptable. These include Commission Policy statements, Division 1 regulatory guides, standard format and review plans, NRC staff technical positions and other Commission announcements and technical reports (e.g., NUREG-series documents).

For this task, an assessment and compilation will be made of publicly available databases and other resources for the current body of nuclear plant regulatory documentation and industry codes and standards. In addition to searching publicly available resources for regulatory guidance documents, an assessment will also be made to determine the existence, capabilities and cost of any commercially available databases of nuclear plant regulatory information.

Accomplishments

The main accomplishment in this task has been the creation of an Access database of industry consensus codes and standards in NRC regulatory guidance. The database in NUREG/CR-5973, Rev. 2 (*Codes and Standards and Other Guidance Cited in Regulatory Guidance*) was converted into a searchable Microsoft® Access database. This database identifies codes and standards cited in the following types of documents:

- NRC Regulatory Guides
- Code of Federal Regulations
- NRC Bulletins
- NRC Circulars
- NRC Generic Letters

- NRC Inspection Manual
- NRC Information Notices
- Formal NRC Staff Publications (NUREGs)
- NRC Policy Statements
- Standard Technical Specifications
- Standard Review Plan (NUREG-0800)

This database can be used to identify the codes and standards referenced within a given regulatory document. For example, data queries showing codes and standards supporting Reg. Guide 1.118, Standard Review Plan 8.3.1, and Standard Review Plan 15.6.1 are shown in Tables 3.1.1-1, 3.1.1-2, and 3.1.1-3, respectively. This database can also be used to search the *titles* of the codes and standards for specific phrases such as "radiation protection" or "reinforced concrete." However, the database has the following limitations:

- It has not been updated since 1994.
- It only links codes and standards to specific regulatory guidance and does not show the relationship between various regulatory documents. For example, in addition to referencing the codes and standards shown on the attached sheet, Reg. Guide 1.118 also references several of the General Design Criteria contained in Appendix A of 10 CFR 50. The linkage between these two documents is not captured in the NUREG/CR-5973 database.
- Full text searches are not available for either the codes/standards or the regulatory documents.

An additional accomplishment of this task has been the assessment of publicly available NRC regulatory information resources. The NRC web site (http://www.nrc.gov) has a fully text searchable electronic archive of the following regulatory documents:

- Administrative Letters
- Commission Meeting Transcripts
- Federal Regulatory Notices
- Generic Letters
- NRC Bulletins
- NRC Inspection Manual
- NRC Legislation
- Title 10 of the Code of Federal Regulations
- SECY papers
- Staff Requirements Memoranda (SRM)
- Commission Action Memoranda (COM)

Additionally, the web site contains an archive of NUREGs published since 1997 and a partial archive of the Regulatory Guides. Notable in the NUREG archive is NUREG-0933, "A Prioritization of Generic Safety Issues" and Chapters 7, 13, and 15 of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants." Together, the NUREG/CR-5973 database and the NRC electronic archive provide a useful tool for navigating through the body of regulatory guidance that governs nuclear plant operation and design. A partial listing of the NUREG/CR-5973 database is contained in Appendix D.

Table 3.1.1-1: Standards Supporting Periodic Testing of Electric Power & Protection Systems (Reg. Guide 1.118, Rev. 2)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*TITLE*
reg1.118.r02	ANSI	ANSI N42.7	1972	Standard Criteria for Safety Systems for Nuclear Power Generating Stations
reg1.118.r02	IEEE	IEEE 279	1971	Standard Criteria for Safety Systems for Nuclear Power Generating Stations
reg1.118.r02	IEEE	IEEE 308	1974	Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
reg1.118.r02	IEEE	IEEE 338	1975	Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
reg1.118.r02	IEEE	IEEE 338	1977	Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

NUREG/CR-5973 Database Query Results

Table 3.1.1-2: Standards Supporting Standard Review Plan 8.3.1 (Onsite AC Power Systems)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*TITLE*
srp8.3.1	IEEE	IEEE 308	N/S	Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
srp8.3.1	IEEE	IEEE 317	N/S	Standard for Electric Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations
srp8.3.1	IEEE	IEEE 338	N/S	Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
srp8.3.1	IEEE	IEEE 379	N/S	Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems
srp8.3.1	IEEE	IEEE 384	N/S	Standard Criteria for Independence of Class 1E Equipment and Circuits
srp8.3.1	IEEE	IEEE 387	N/S	Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations

NUREG/CR-5973 Database Query Results

Table 3.1.1-3: Standards Supporting Standard Review Plan 15.6.1 (Inadvertent Relief Valve Opening)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*TITLE*
srp15.6.1	ANS	ANS N212	1974	Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants
srp15.6.1	ANSI	ANSI B95.1	1972	Terminology for Pressure Relief Devices
srp15.6.1	ANSI	ANSI N18.2	1974	Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants
srp15.6.1	ASME	ASME Section III	N/S	Rules for Construction of Nuclear Power Plant Components
srp15.6.1	ASME	ASME Sec. III, NB-7000	N/S	Overpressure Protection

NUREG/CR-5973 Database Query Results

3.1.2 Identify Systems, Structures, and Components (SSCs) and Their Associated Costs for a Typical Plant

Approach

Just as future plant designers will need a complete listing of design criteria for a new plant, they will also need a listing of the SSCs to which those criteria are applied. Thus, the objective of this task is to prepare such a listing for a typical nuclear plant. The list of SSCs will vary somewhat from one reactor technology to another. For example, a gas-cooled reactor would not have a Safety Injection System to pump coolant water into the reactor vessel following a pipe leak or break. To be manageable within the NERI funding levels available, the proposed research effort will need to focus upon a single type of nuclear plant, as a design that is considered typical. The regulatory requirements and industry standards (from Task 1.1) are based on Light Water Reactor (LWR) technology as are the SSCs for Task 1.2

To be able to perform a cost/benefit analysis of changes to the SSCs, future plant designers will need to know the approximate costs of the SSCs. Therefore, this task will also produce cost data for the typical nuclear plant, as needed, to support the efforts in the other tasks. Rather than create new cost data from scratch, this research effort will simply modify existing available cost data, to serve as typical. The results of this task will be used in Tasks 1.5 and 1.6, to identify the high priority SSCs and to apply the methodologies to a sample SSC.

Under Option 2 of SECY-98-300, the NRC staff proposes to "make changes to the scope of systems, structures, and components covered by those sections of Part 50 requiring special treatment." The current scope of SSCs covered by NRC regulations is based primarily on the evaluation of selected design-basis events, as they are analyzed in a plant's final safety analysis report. These postulated events are only a small fraction of the potential accident sequences that are identified in risk assessments. There has also been some confusion over the fact that some SSCs are considered "safety-related", some are considered "important to safety" and others are not considered in either of those categories.

Over the next several years, considerable resources will be expended by NRC and industry to use the risk-informed approach to reclassify the SSCs into just two categories: safety-significant and non-safety-significant, based on the importance of the SSC in preventing or mitigating accidents. The anticipated result is that most of the SSCs currently required to satisfy Part 50 requirements would be re-categorized as being non-safety-significant. The benefit will be that the re-categorized SSCs could then be purchased and maintained to commercial industry standards – which will be dramatically lower in costs than SSCs purchased and maintained to Part 50 requirements. In some areas, it is anticipated that costs could be reduced by as much as an order of magnitude.

The currently planned efforts of NRC and industry to re-categorize SSCs are not expected to be based upon a systematic review of all SSCs in a nuclear plant. Instead, they will focus upon selected SSCs that are anticipated to provide the most relief for plant operational issues. Therefore, the efforts in this task will go well beyond current industry efforts by listing all SSCs in the entire nuclear plant – which will be candidates for re-categorization. More importantly, in

future nuclear plants, all of the SSCs will be candidates for simplification, using the methodology being developed in Task 1.4.

For this task, lists of SSCs and their associated costs for a typical pressurized water reactor plant will be developed. This typical list will use WENS's System 80+ Standard Plant Design listing of SSCs as a starting point.

Cost data will be obtained from recent WENS NSSS projects and bids, but will be presented in a manner that will not compromise WENS's proprietary pricing and negotiating methods.

- Most costs will be presented on a system level basis, although component-level costs will be presented for systems and structures that are likely candidates for simplification, i.e., SSCs that may have redundant trains or components removed, but will not be eliminated completely.
- Cost comparisons will be provided for component types – pumps, tanks, valves, instrumentation and controls – that are available in both safety-related (10 CFR 50 Appendix B, ASME Boiler and Pressure Vessel Code Section III, Class 1E) and commercial grade variations.
- The impact on building/structures size, bulk material quantities, and construction time will be estimated for selected system simplification or deletion. These factors affect the base cost of the plant and the interest during construction (IDC). IDC can range from $5 million to $10 million per month for a single unit, using current US and international lending rates.

The product of this task will be a report which lists the systems, structures and components (SSCs) in a typical nuclear power plant whose design, analysis, procurement, construction, installation and testing are governed by the regulations and criteria identified in Task 1.1. This report will also provide a unitized/normalized estimate of the costs for each of the SSCs listed. To the extent practicable, the costs will be apportioned to engineering (design and analysis) costs, procurement costs, and construction/installation costs.

Accomplishments

Activities for this task during Phase 1 have focused on obtaining a comprehensive list of SSCs and some representative costs. The System 80+ listing of SSCs is presented in Appendix E. Cost data for an overall plant and for selected SSCs are presented below.

Overall Plant Cost

Recent estimates for the installed cost for an ALWR in the range of 1300-1400 MWe are between $2 and $3 billion. As a data point, the average cost for PWRs completed in the US between 1986 and 1993, the period when large plants (electrical output in excess of 1200 MWe) such as Palo Verde and the South Texas Project entered commercial operation, was about $2.8 billion. A significant portion of the costs for those plants was for high interest or carrying charges due to regulatory delays, and for regulatory backfits.

The current economic target for installed cost on a per kilowatt basis is in the range from 1400 to 1800 $/kWe. For outputs in the range of 1300-1400 MWe, the current estimated ALWR cost is toward the high end of the range ($1600-1800/kWe).

The installed cost includes three major components:

- Overnight or Basic Cost (today's cost of all plant land, engineering, equipment, construction, startup and commissioning)
- Escalation (inflation effect)
- IDC

There are a few different models for rolling up or summing the costs for a plant, but generally, the overnight or basic cost is defined as the sum of direct, indirect and other costs. Direct costs include the costs to engineer, procure and construct the plant, that is:

- land,
- reactor equipment,
- turbine equipment,
- heat rejection equipment and structures,
- electrical and instrumentation and controls equipment
- miscellaneous plant equipment, and
- construction.

Indirect costs include the costs to manage the project and to startup, test and commission the plant. Other costs include owners' costs, spare parts and contingencies.

The escalation and IDC components will vary with the economic and financial conditions in the project countries and with the project schedule – both the duration and the timing with which expenses are incurred. Recent estimates have pegged IDC at between 12 and 23% of the plants installed cost.

Costs of SSCs

Previous studies have identified some significant contributors to the higher cost of nuclear power plants relative to other generation sources. These contributors include:

- Large robust buildings and maintenance areas. The requirements for building strength result in large quantities of bulk materials such as concrete and reinforcing steel, and significant construction labor.
- The "safety related" pedigree for nuclear components such as pumps, valves, chillers, and fans. The additional engineering, testing, qualification and documentation may increase the cost by *3 to 4 times* over the same commercial grade equipment.
- Redundant systems and components. The regulatory requirements for complete redundancy of some systems results in large quantities of piping and cabling with requirements for a safety-related pedigree.

For Phase 1, costs of selected SSCs were obtained. Since the sample application in Task 1.6 is based on the SIS, typical costs for components that would be used in a System 80+ SIS were

compiled. The cost data was obtained from vendors over the last several years. For one train of the SIS, the components and costs are:

Equipment	Quantity in One SIS Train	Typical Hardware Costs, US Dollars
Safety Injection Pump, Multistage Centrifugal, ASME "N" stamp, Class 1E Motor	1	1,000,000
Safety Injection Tank, Vertical, 2400 cubic foot, 700 psi design pressure, "N" stamp	1	650,000
Pipe, Fittings, Supports	Set ranging from 0.75 to 30 inch nominal	2,000,000
Valves	4 motor-operated 6 air/solenoid-operated 10 large bore manual/check Several small bore manual 2 relief	1,000,000
Support Systems (electrical, cooling water, HVAC) and instruments and controls	Numerous	450,000
TOTAL		5,100,000

The PSA model described in Task 1.6 uses a simplified SIS design which reduces the number of HPSI pumps and safety injection tanks from four to two, but maintains the hot leg injection piping and components. Effectively, two trains of the SIS are deleted. Based on the estimate above, plant cost savings could exceed 10 million dollars for equipment alone, before considering potential reductions in building size.

The advanced SIS design described in Task 1.6 also combines the HPSI function and the charging function, currently provided by the CVS system, into a hybrid pump, similar to the older U.S. plants. With this additional design change, equipment cost savings are expected to be even greater ($15-20 million).

While these potential savings are significant, they represent a small percentage of the overall plant cost. A savings of $20 million on SIS hardware reduces the estimated overall plant cost by less than one percent. However, the simplification of other safety systems, and the potential for reductions in the plant buildings, provides an opportunity for larger savings.

Future activities will develop costs for other plant SSCs to support further sample applications of the risk-informed design process.

3.1.3 Develop Methodology for Risk-Informing Requirements and Standards

Approach

The original objective for this task was to develop a set of procedures and guidelines that could be used for reviewing regulatory requirements and industry standards and revising them to be risk-informed. These procedures and guidelines would then provide a process for determining the extent to which the underlying bases for the regulation or standard are still applicable given the current state of knowledge. Further, they would provide a methodology and guidance for determining the extent to which the actual regulation or standard could be changed while still maintaining a level of safety appropriate to the underlying bases for the regulation or standard.

In the course of this year's activities, it was determined that the overall objective for the task could be more readily achieved by taking a "clean sheet of paper" approach to develop a framework for *risk-based* regulation and design. This approach to developing the framework has allowed us to focus more on applying PRA techniques to address requirements for new plants without the restrictions of current NRC assumptions and acceptance criteria. Additionally, this approach provides more innovation and differentiation from the NRC's efforts on risk-informing requirements for current plants.

Initially, the Project Team reviewed the NRC's approach to risk-informing 10 CFR 50 for current operating plants and considered how this approach could be applied to the regulation and design of future plants. Additionally, alternative approaches that might be more effective for developing risk-informed regulatory and design requirements for future plants were identified, discussed and evaluated. Three approaches were considered for developing the framework for risk-based regulation and design for new plants:

- a risk-informed, defense-in-depth approach similar to the NRC's effort for risk-informing 10 CFR 50 for current operating plants;
- a safety goal approach in which risk is evaluated against established quantitative safety goals with defense-in-depth used explicitly to address uncertainties; and
- variations of these two.

Key to the framework development effort were discussions on regulatory philosophy of adequate protection, consideration of alternative views of defense in depth, application of state-of-the-art PRA techniques, and treatment of uncertainties.

With regard to regulatory philosophy of adequate protection, the Project Team considered whether, for new plants, this should be determined in a quantitative manner. In the end, the Project Team decided against this and decided that our work would maintain the current subjective approach for adequate protection, that is meeting all regulations will remain presumptive evidence of adequate protection. However, requirements for new plant will be based as much as reasonable on meeting quantitative risk targets. Additionally, the project team made a preliminary judgement that the bases for regulatory decision-making for new plants

would include the following: (1) deterministic and probabilistic analyses; (2) tests; and (3) subjective judgements – by individuals or collectively by expert panels or review panels.

With regard to approaches to defense in depth, the NRC Advisory Committee on Reactor Safeguards (ACRS) has identified two schools of thought, labeled "structuralist" and "rationalist," and recommend an approach for risk-informed regulation. The two schools differ in the process used to deal with uncertainty in reaching an acceptable level of safety. The structuralist approach has evolved from the early days of nuclear power with a process of accumulating defense-in-depth features until a judgement was made that sufficient protection against uncertainty in performance had been achieved. With the development of PRA methods, the rationalist approach uses these tools to quantify uncertainty and to explicitly account for defense-in-depth features in reducing uncertainties to acceptable levels. The main difference is that the structuralist accepts defense in depth as a fundamental principle, while the rationalist would place defense in depth in a subsidiary role. Additionally, the structuralist does not deal with uncertainties in a quantitative manner, while the rationalist takes advantage of the fact that advances in PRA allow the quantitative estimation of some of these uncertainties. For new plants, the rationalist approach to defense in depth, employed within the context of PRA, is preferred to more effectively develop a body of regulations that eliminates requirements that do not contribute significantly to safety.

The rationalist relies on PRA methods to provide an integrated and systematic analysis of the plant that explicitly addresses sources of uncertainty. The process envisioned by the rationalist is: establish quantitative safety goals, such as health objectives, core damage frequency, and large release frequency; design and analyze the plant using PRA methods to establish that the safety goals are met; evaluate the uncertainties in the analysis, including those due to model inadequacies, system performance and reliability, and lack of knowledge; and determine what steps (i.e., defense in depth, new design features) to take to address those uncertainties. The quantification of uncertainties in terms of probability distribution functions provides a means for determining how much redundancy and diversity (i.e., defense in depth) is sufficient.

Accomplishments

The preliminary version of the framework or risk-based regulation and design has been developed and a detailed project report on the framework is also provided in Appendix B. A related conference paper to be presented at the International Conference on Probabilistic Safety Assessment and Management in Osaka, Japan, in November is also provided in Appendix B. A summary of the framework development and the issues being considered are presented below.

Summary of Framework Development:

The proposed framework for risk-based regulation and design is based on the evaluation of risk against quantitative safety goals. A top-down hierarchy is being used to define the goal, establish an overall approach, and develop and implement appropriate strategies and tactics. The framework is based on an application of PRA methods and reflects a rationalist approach to defense in depth. For new plants, a detailed plant-specific PRA for all operating modes, along with an explicit treatment of uncertainties, would confirm that established quantitative safety goals are met. Within the current capabilities of PRA methods, sources of uncertainty will be

quantified to gain as complete an understanding as possible about the range of risk and uncertainty before defense in depth is applied to address uncertainties. Within this framework, PRA provides the basis for both developing and evaluating compliance with requirements for risk-based design and regulation.

Regulations for NPPs are required to ensure adequate protection to the health and safety of the public. Accordingly, the *goal* of this effort is to provide a framework for developing and implementing risk-based regulations that meet this requirement. An *approach* based on evaluating risk against quantitative safety goals is proposed to achieve the stated goal. With respect to adequate protection, the NRC has established safety goals including Quantitative Health Objectives (QHOs) that state the Commission's expectations with respect to how safe is safe enough. Although the NRC's safety goals are not considered quantitative measures of adequate protection, for new plants, we will consider the determination of adequate protection using increased reliance on comparisons of PRA results to quantitative risk measures. The safety goals we will use for the framework have been adapted from the NRC's goals.

The *strategies* for developing and evaluating compliance with requirements for risk-based regulation and design are based on the use PRA to quantify risk and uncertainties. High confidence is achieved through explicit consideration of uncertainties, including modeling adequacy and equipment design and performance. These strategies include consideration of the risk information available from Level 1, Level 2, and Level 3 PRA analyses. Level 1 PRA evaluates the potential for accident initiators and the system response to prevent core damage. An estimate of core damage frequency (CDF) is compared to the corresponding goal. Level 2 PRA encompasses the response to and mitigation of core damage, including containment of fission products. Risk estimates here can be compared to goals for conditional probability of large release, both early and late. Level 3 PRA encompasses the response to and mitigation of radionuclide releases, including emergency response. These risk estimates can be directly compared to the QHOs or to subsidiary goals for conditional probability of early fatalities and latent cancer risks.

To develop risk-based regulations, *implementation* of the framework is achieved by defining functional system characteristics, within the context of how PRA is performed, to determine what areas need to be regulated to assure safety. Implementation for design is achieved by specifying design configurations and using PRA to evaluate the design, then iterating with subsequent design changes. A master logic diagram (MLD) is used to take a top-down approach to identify the safety functions, and systems, structures, and components (SSCs) that are required to maintain safety and to identify the accident initiators and system response failures that could compromise safety. The top event for the MLD is stated in terms of risk exceeding the safety goals. Intermediate events correspond to the Level 1, Level 2, and Level 3 PRA strategies, respectively. The sixth level of the MLD defines the system functions that are required to assure safety. The next level down indicates that initiating events and failure of mitigating systems, containment, and emergency response can compromise safety functions. The last level of the MLD indicates that internal initiators for all operating modes and external initiators will be considered for completeness. Further development of the MLD will determine the "regulatory risk space" for which regulatory and design requirements are needed.

Various *tactics* (e.g., design criteria, procedures, redundancy, emergency response, etc.) are applied to support the PRA strategies and implementation. Once the SSCs required to achieve safety have been identified, then decisions on appropriate tactics for regulation and design can be made. The specification of these tactics will be based on a systematic evaluation of the areas that need to be regulated for the purposes of assuring safety and will also evolve from this process.

Further development of the framework is required to determine specific procedures and guidelines that can be applied for risk-based regulation and design. Work in Phase II for this subtask will focus proceed to define one issue and proceed to regulate it using the framework. The preferred features of the issue are as follows:

- self-contained issue
- complementary focus to design tasks
- consideration of safety margins
- active and passive design features
- subjective probabilities for addressing uncertainties

The development of the framework will be updated as the specific application progresses.

3.1.4 Develop Methodology for Simplifying SSCs

Approach

Coincident with risk-informing the regulatory framework and design bases for future nuclear plants, plant designers need a methodology for systematically reviewing the design of each and every SSC in a nuclear plant and simplifying the design to take advantage of the new risk-informed design bases. The overall goal of this effort is to reduce the costs of future nuclear plants without sacrificing safety. Since the industry standards and regulatory requirements do not literally match up with the SSCs, it is important to provide future plant designers with a methodology for cross-referencing them and assuring that the potential interactions between them are fully understood. Furthermore, because there is so much diversity in the ways that the different SSCs are designed, it will be important to have a consistent set of methodologies available to the plant designers.

The objective of this subtask is to develop a set of procedures and guidelines (i.e., instructions) that can be used for evaluating plant SSCs and simplifying them, using the revised requirements and standards that would result from implementation of the risk-informed design bases and regulatory framework. Inherent within this task is the need to define simplification with respect to the design of an SSC. This definition will need to address the means that can be used to "simplify' the SSC design while considering the original deterministic bases for the SSCs' design and the extent of their current relevance with respect to the SSCs' importance to safety.

For this task, functions for power production will be defined, and design goals and challenges to functions identified. Keeping these requirements and considerations in proper perspective, a high level, risk-informed design process will be developed. The current design process will be evaluated to help identify existing deficiencies and areas where improvements are required. The design process will be refined and/or expanded in conjunction with Task 1.3 using feedback from the sample application (Task 1.6).

In addition to developing a high level, risk-informed design process, improved and risk based design methods for simplifying structural design will also be defined and developed.

Accomplishments

Risk-Informed Design Process: Figure 3.1.4-1 provides a simplified illustration of the current plant design process. A key point about the current process is that it is highly dependent upon past experience to establish design parameters and SSC requirements. The deterministic defense in depth requirements and design margins are implicitly incorporated via the regulations, codes and standards. While there is some flexibility in system layout and SSC selection, much of the process is evolutionary in that each design is based on the previous one with some limited changes. The design analysis also tends to follow the "cookbook" approach. Thus, with the existing design approach, the underlying bases are not critically re-evaluated to understand their relevance.

The risk-based regulatory framework described by Task 1.3 suggests a parallel "top-down" risk informed design process that can be used to develop new plant designs. Conceptually, this

process can be used for evolutionary plant designs or for more radical new designs. Figure 3.1.4-2 presents the high level framework for this risk-informed design process.

The first step (Step 1, Figure 3.1.4-2) in the overall risk-informed design process is to set the goals for the plant design. These goals need to address both the power production aspects of the plant and the safety aspects of the plant. It is anticipated that the highest level safety goal for the plant will most likely be regulatory in nature and will encompass the qualitative goal to provide adequate protection of the public safety and health. It is assumed that this qualitative goal will be further defined by the QHOs. As illustrated in the regulatory framework discussion, lower level quantitative surrogate goals such as Large Early Release Frequency (LERF) CDF. The risk-informed design process is predicated on two assumptions: (1) the quantitative surrogate goals are goals and not required upper limits and (2) the designers have flexibility in how they achieve these goals. The power production goals are the basic economic goals of the plant. These goals will probably include: (1) plant power output (x megawatts electric), (2) plant capacity factor, (3) plant availability, (4) plant cost, (5) plant construction schedule, and (6) plant maintainability.

The next step (Step 2, Figure 3.1.4-2) in the design process is to identify the functions that need to be accomplished in order to meet the goals that were established. Conceptually, the designers would establish a set of power production functions and a set of safety functions. However, at the highest level, these functions are essentially the same. The power production functions are to establish and control the processes needed to produce power and the safety functions are basically those needed to prevent or mitigate challenges to the power production function. (Two underlying assumptions are: A) steady state power production operation is a safe state, and B) perturbations to the steady state operation of the plant can lead to challenges to public safety and health.) Integral to establishing the functions is defining control parameters and establishing bounds on the function control parameter. Table 3.1.4-1 suggests a set of high level functions that encompass both power production and safety. While these functions were developed based on a knowledge and understanding of current LWR technology, they are, in general, applicable to other technologies such as heavy water reactors and liquid metal cooled reactors. The designers should consider this set of functions as a starting point for defining the specific set of functions for their design, especially if it is a significant departure from the current LWR technologies. This step is the start of an iterative process in which the plant design is developed in increasing levels of detail. With each iteration, the power production elements would be addressed first, then the safety aspects would be evaluated.

The next step (Step 3, Figure 3.1.4-2) in the iterative portion of the risk-informed design process is to identify the systems needed to accomplish the functions identified in the previous step. Initially, the designers need to identify the systems that are needed to accomplish the power production functions. In doing so, the designers need to consider the full range of anticipated plant standard operating conditions. These would include steady-state, full-power operation, steady-state, reduced-power operation, plant shutdown conditions (including refueling if appropriate), power escalation and power descent. It is in this step that the basic plant design and configuration is established. The third column in Table 3.1.4-1 provides high level examples of systems associated with each of the high-level power production functions previously defined.

The following step (Step 4, Figure 3.1.4-2) in the process is to identify challenges to the power production functions. At the very highest level, a challenge is defined to be failure to maintain the function. The next level of refinement is to define the challenge with respect to the function control parameter limits established for each function. (Note: In some cases the high level control parameter may be just maintain function and the challenge is failure to maintain function.) The third level of refinement in identifying the challenges is to link faults in the systems needed to accomplish the function to function challenges. The examples provided in Table 3.1.4-2 illustrate this refinement of the definition of the functional challenges. Once the challenges have been identified, the next step (Step 5, Figure 3.1.4-2) is to identify SSCs needed to prevent or mitigate the challenges. In general, preventing challenges will be associated with the design and operation of the SSCs associated with performing a given function. Mitigating a challenge has a much broader scope because a nuclear power plant is a highly coupled system. A challenge to one function will affect the conditions associated with other functions and may lead to challenges to these other function. Thus, when one function is challenged, the challenge must be mitigated for the affected function, and the other functions must be maintained in the face of changing conditions which may challenge these functions. For example, a failure in the turbine control system results in a trip of the turbine, resulting in loss of the "Energy Conversion and Transmission" function. At the time of this initial challenge, the reactor will still be generating energy under conditions associated with full-power operation. The turbine trip will result in a mismatch between the energy being generated and the energy being removed. This is a challenge to the "Heat Generation and Control" function, the "Primary System Pressure Control" function and the "Heat Transfer" function. While not directly challenged in this scenario, the "Primary System Inventory Control", Maintenance of Vital Support Systems" and "Radioactive Materials Control" functions must be maintained as part of the mitigation of the original challenge.

Any given challenge to a function can be characterized by a frequency of occurrence and by the nature and magnitude of the impact on the plant processes and SSCs, that is, what happens to the thermal-dynamic processes in the plant and how are the normal operating systems affected. Thus, the first step in determining what SSCs are needed to mitigate a challenge to a given function is to evaluate the nature, magnitude and scope of the impact of the challenge on the process parameters and SSCs associated with all of the functions. Then, for all functions, the designer would ascertain whether the normal complement of equipment associated with that function is capable of maintaining (or re-establishing) the function given the conditions resulting from the original challenge and any normal consequential challenges to other functions resulting directly from the original challenge. Where the normal SSCs are not capable of mitigating the challenge and/or maintaining the function being evaluated for the challenge, additional equipment may be needed. Conceptually, this process is repeated until all functions have been evaluated for all challenges to any function. The results of this evaluation are a definition of the conditions that must be mitigated/controlled for each challenge and a preliminary assessment of the SCCs that are needed to mitigate the full spectrum of challenges. This information is then used to establish initial performance requirements for the set of SSCs identified by the evaluation (See Step 6, Figure 3.1.4-2). This information would then be factored into the preliminary system designs.

Once the basic requirements for the SSCs have been established, the designers develop and evaluate the system designs to ensure that they meet the performance requirements and the safety and reliability goals. This basic evaluation process is illustrated on sheet 2 of Figure 3.1.4-2. The following paragraphs further discuss some of the issues that are considered in this process.

In the current deterministic design process, the designers must demonstrate that the plant has sufficient equipment to mitigate any and all challenges assuming the worst single failure for each challenge and the unavailability of most normally operating SSCs. The end result of this process has been the proliferation of "Safety Systems" which are in standby during normal operation. These systems are designed to respond to a spectrum of challenges with no distinction as to whether any given challenge is credible or not. In the risk-informed design process, the designers must demonstrate that the plant is capable of meeting the specified safety goals over the spectrum of potential challenges. Given that the challenges have been identified, one way to accomplish this goal is to apportion the safety goal over the challenges.

The apportionment process looks at the frequency of the challenge as well as the scope and severity of the challenge. This process will also factor the cost of preventing/mitigating challenges into decisions as to how to deal with individual challenges. The starting point in the apportionment process is to list the challenges and their anticipated frequencies of occurrence. Table 3.1.4-3 is an example of the initial risk apportionment for a Pressurized Water Reactor (PWR) type design. The first ten challenges in this table are consistent with those presented in Table 3.1.4-2 and, in general, cover the spectrum of challenges initiated internal to the plant (internal initiating events). The eleventh challenge covers a spectrum of other initiators related to internal fires, floods or support system faults which tend to be design specific. The twelfth category is titled "Margin" and is included to cover other challenges that may not have been identified in the initial process or that arise as the plant design evolves. It also covers risk contributions from external challenges (seismic, hurricanes, etc.) and other modes of operation and general uncertainty about all challenges. As the apportionment process proceeds, the specific list of challenges and their allocated CDF contributions will grow and the CDF allocated to the "Margin" category will decrease correspondingly. The third column in Table 3.1.4-3 presents the initial sample risk allocation in terms CDF contribution for each challenge. An actual risk allocation would need to address all agreed-upon safety goals from Step 1. The initial allocations are more or less arbitrary but do involve some general considerations: (a) Incredible severe challenges (i.e. those whose frequency is less than about 1E-07/yr) do not need to be mitigated, (b) no single challenge should dominate the risk, that is each challenge would have about the same risk contribution, (c) challenges that breach the primary boundary should have a somewhat lower initial risk allocation, (d) challenges that may encompass a number specific initiators would have a somewhat higher initial risk allocation and (e) the initial risk allocation for high frequency challenges (i.e., those with frequencies approaching 1 per year) should reflect achievable reliabilities for mitigation systems. The final column in Table 3.1.4-3 is the maximum mitigation system unavailability that is needed to achieve the allocated risk goal for each challenge. In developing system designs that will meet the overall safety goals, the designers can design mitigation systems that meet the requisite unavailability, they can modify the normally operating systems to reduce specific challenge frequencies or they can trade risk allocations with other challenges that are easier to mitigate or prevent. This whole process is performed in an iterative fashion until the final design is established.

In the risk-informed design process, the designers will be able to consider the use of normal power production systems, separate "mitigation" systems or some combination thereof when establishing the "mitigation" approach for the various challenges. The first option will be to use one or more of the power production systems to perform the mitigation function if it can be demonstrated that the power production systems have sufficient physical capabilities to meet the full range of required responses such as flow rates or pressures and that the selected power production systems can be reasonably expected to be available to respond to the challenge. As an example, consider the turbine trip challenge. Because of the power mismatch, the turbine trip will lead to a reactor power cutback or reactor trip, depending on design. In either case, feedwater flow will be needed to remove heat from the core albeit at a lower level than at full power. In this scenario, the main feedwater is not failed and could be used to provide the requisite flow if it can be throttled to meet the lower flow required in this case. However, if the challenge was a failure of the main feedwater system, the required feedwater flow would have to be supplied by some other system.

The second main option will be to incorporate separate mitigation systems to handle some or all aspects of given challenges. The design of these systems would be governed by the physical capabilities needed to mitigate the challenge and the system reliability needed to meet the mitigation system unavailability goals. For relatively low goals, single train systems may be sufficiently reliable to meet the goal. For more stringent goals redundant or diverse system designs may need to be considered.

The overall goal of the risk–informed design process is to meet the safety goals in the most cost-beneficial manner. This allows the designer to consider cost as well as system reliability when developing the system design to meet the unavailability goals. Given this increased flexibility, the designers have a number of options to consider when establishing the mitigation capability for the defined challenges as long as the safety goals are met. These include:

- Utilizing power production systems/subsystems that are available and capable of mitigating the challenge;
- Expanding the capabilities of power production systems so that they can mitigate challenges;
- Replacing N-stamp components with non N-stamp components (i.e., using components with fewer QA requirements);
- Replacing active components with passive components;
- Reducing the degree of redundancy by use of more reliable equipment, e.g., "smart" equipment with self-monitoring, self-diagnostic features built in;
- Using diverse components in combination with redundancy;
- Using fewer components to achieve the same function;
- Using single train systems where a high level of reliability is not required;

- Elimination of unrealistic design requirements related to capacities (discharge pressures, discharge flows, etc.), timing (start time, open time, close time, etc.), design load combinations (e.g. blowdown loads plus seismic loads) or environmental qualification requirements; and

- Reducing inherent conservatism from existing structural design methods and codes.

Simplifying structural design through use of improved and risk-based design methods and the status of efforts supported by this task are presented in detail in Appendix F.

At this point, the risk-informed design process is still fairly general and needs to be further refined and expanded to cover more detail. Some areas that need to be addressed in more detail include:

- Incorporate all quantitative safety goals in the risk allocation process;

- Develop rules/guidance for risk allocation trade-offs between challenges;

- Develop a process for evaluating how to include challenge frequency in the trade-off analyses;

- Explicitly factor a process for establishing the process parameters at the function, system and sub-system level into the risk informed design process;

- Establish more detailed guidance for evaluating mitigation system performance requirements;

- Prepare guidance for how to address the structural design process within the overall risk-informed design process;

- Establish guidance for explicit treating support systems in the overall design process and the risk allocation process; and

- Determine whether or not the risk-informed process should include "Design Basis Events" and if so how are these events defined and how are they to be evaluated.

The preliminary risk-informed design process described above is actually more a risk-based, performance-based design process and does not explicitly address regulatory constraints beyond the safety goals. It is recognized that a risk-based, performance-based design process is not likely to be accepted by the regulatory agencies. Therefore, as the process is refined, it will incorporate guidance on identifying regulatory requirements that need to be revised to remove unwarranted constraints and requirements that are impediments to a risk-informed system design.

The performance of structural systems depends upon the structural behavior of individual components and the interaction between them. Structural failure of a particular component or sub-system may not necessarily produce a system malfunction. Therefore, it is desirable to

consider the benefits in a system as a whole when evaluating the benefits obtained from a component risk reduction. Current risk assessment methodologies do not account for correlation between component failures, nor do they consider multi-state failures. Two primary barriers in optimizing the design consistency with the safety goals are: (i) unavailability of risk assessment methodologies capable of incorporating detailed structural behavior models, and (ii) lack of tools capable of accurately predicting structural performance of components and systems. One may reduce the cost of the plant by avoiding wasteful conservatism in the structural systems that do not significantly contribute to the overall risk, and by reducing the uncertainties in the evaluation of performance and failure modes of structural systems that do contribute to the overall risk. Consequently, the definition and the identification of significant failure modes for various structural systems and their interdependencies is a very important task in developing a consistent risk system. For example, failure mode is typically defined as the collapse of a component. However, a serviceability failure may be more critical to the overall system risk. In such a situation, definition of failure mode by the collapse of component will not only introduce uncertainties in the system risk it will also lead to excessive conservatism in the design of the particular component. Improvements in fragility evaluations for identifying component failure modes and mechanistic models in structural systems would contribute to reducing the uncertainty, simplifying the design process and assigning appropriate margins for each component. Simple and easy-to-use design tools can assist in reducing the high engineering costs. Unnecessary conservatism can be eliminated depending upon the contribution of individual component to the overall risk leading to significant cost reductions.

The current practices of structural analysis and design do not use an integrated approach at systems level. They consider design and construction of various components separately. Individual components interact and significantly affect each other's performance. For example, several piping failures have been associated with large displacements of attached equipment or interaction of large diameter and small bore piping systems. This is so because interaction between the piping system and attached equipment is rarely included in the conventional piping analysis. Similarly, the large diameter and small bore piping systems are modeled separately and the interaction between them neglected. Ignoring interaction has also resulted in failures due to impacting of adjacent equipment and systems.

Uncertainties are associated with modeling the behavior of each individual sub-system or component. Conservatism is introduced to account for these uncertainties in each component even though the performance of a particular component may not be critical to the system performance. Conservatism introduced at the design and fabrication stages of each component accumulates, resulting in excessively high conservatism for most systems in a plant. Therefore, separate modeling of individual sub-systems results in high capital and operating costs. For example, the supporting structures and the attached piping are modeled separately. Consequently, the analyst or designer cannot account for the interaction between them and the phasing between various support motions of a piping system. This leads to adoption of conservative methods that yield a design with several unnecessary supports thereby increasing the design, hardware, engineering and maintenance costs.

Development of large three dimensional computer models can be impractical because the properties of various interacting sub-systems can be significantly different from each other. For

example, the stiffness, the mass and the damping characteristics of a piping system are significantly different from that of a building with which it interacts. Further, a detailed model of the complete building-piping system becomes excessively large and takes large computer time. In the proposed study, advantage will be taken of the new approaches developed in the recent past which use modular techniques to represent the large models, take significantly less computer time and give accurate behavior as would be given by the large model. One such example is the computer program CREST, developed by Center for Nuclear Power Plant Structures, Equipment and Piping (C-NPP-SEP) at North Carolina State University. This computer program models accurate behavior of coupled building-piping system and accounts for interaction between them. It does not require creation of a large computer model. Instead, separate computer models can be created for evaluating the properties of individual piping and building systems. CREST then takes the information on the properties of two individual systems and creates a much reduced coupled model which is computationally efficient and gives accurate behavior for the coupled system. Brookhaven National Laboratory, under contract to US Nuclear Regulatory Commission, conducted a benchmark study for validating the methods for seismic analysis of non-classically damped building-piping systems. We participated in this study and the outcome of this study is published in a NUREG report (NUREG/ CR 6661, January 2000). This study finds these methods appropriate for modeling building-piping systems. The conclusions are expected to facilitate the use of these methods in the design and operation of piping systems for future nuclear power plants.

Electrical and mechanical equipment are seismically qualified by vibration tests. Either an in-situ test or a shake table test may be conducted. Often, it is observed that the same component exhibit completely different characteristics during different testing conditions. One such example is the differences in dynamic behavior exhibited by electrical control panels and switchgear during an in-situ (low magnitude input) test and a shake table (high magnitude input) test. Further, it is impractical and costly to evaluate cabinet's dynamic behavior by large scale modeling or testing for each cabinet in a plant. Recent studies conducted at NC State University have validated the analysis results for cabinets with the experimental data. Validated models have been used to explain the differences in the cabinet behavior exhibited during low and high level input tests. These detailed models are then used to study the typical patterns in cabinet dynamic behavior and develop a simple method. This new procedure takes only limited information on cabinet properties and gives accurate dynamic characteristics.

Effect of Uncertainty in Building Models on Piping Behavior

In a conventional piping (or equipment) analysis, an uncertainty in the building model is accounted for by modifying the earthquake input floor motion at the supports of piping system. The two widely used methods for modification of floor motion are called Peak Broadening and Peak Shifting. In Peak Broadening, the spectral peaks associated with the structural frequencies of the building are broadened within a specified frequency region, typically ± 15%. In Peak Shifting, multiple analyses of the piping system are performed by shifting the floor spectra within a ± 15% frequency region. The responses from these multiple analyses are enveloped to obtain the final responses. Both these methods are excessively conservative as they evaluate maximum possible response values.

An analysis of the coupled building-piping system is superior to the conventional uncoupled analysis. An uncertainty in the building frequency can either increase or decrease the tuning (resonance condition) between the modes of piping and building, i.e. tuned modes can become detuned and vice versa. The degree of tuning between the vibration modes of the two individual sub-systems can significantly affect the behavior of piping systems. However, the methods like Peak Broadening and Peak Shifting cannot be used to account for an uncertainty in the building model in a coupled system analysis. This is so because a coupled system analysis uses the input ground spectra at the base of building directly and the floor spectra at piping supports are neither generated nor required. We studied the effect of uncertainty in building frequencies on the coupled building-piping response. The following sections describe this study and summarize its outcome.

Monte Carlo Simulation: According to the current design philosophy, the earthquake input for the design of structural systems and components in a nuclear power plant is defined by a ground response spectrum in which the spectral accelerations correspond to eighty four percent (84%) non-exceedence probability. Alternatively, one may use multiple acceleration time histories as input in a Monte Carlo simulation. Responses obtained from these multiple time history analyses are then used to obtain the design values corresponding to eighty four percent non-exceedence probability. We conducted a similar Monte Carlo study in which not only multiple time history inputs were considered but the building frequencies were also varied within a ± 15% frequency region. For n time history inputs (normalized to same value of peak accelerations) and m variations in the building frequency, a total of $n \times m$ analyses were performed and the design responses evaluated. Assuming the responses to be normally distributed (a conventional practice), the eighty four percent non-exceedence values are given by mean plus one standard deviation. We considered several representative building-equipment and building-piping systems in this study. However, for illustration purposes let us consider a single story (single degree of freedom) building and simple single degree of freedom equipment attached to this building, as shown in Fig.3.1.4-3. To start with, the building and the equipment models are considered to be perfectly tuned with each other, i.e. both the building and the equipment have a frequency of 5 Hz. An uncertainty in the building frequency results in the detuning of the two systems. For 11 input time histories and 31 variations in the building frequency within a ± 15% frequency region, a total of 341 values exist for seismic force in the equipment. Fig.3.1.4-4 shows the variation in this force for each input motion considered. The design value for 84% non-exceedence probability is 73 kips.

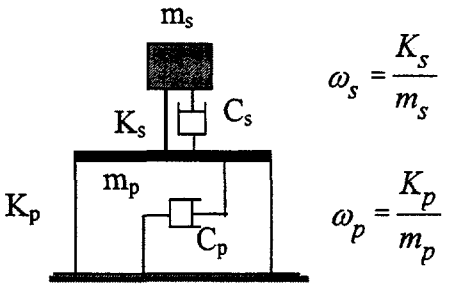


Figure 3.1.4-3: SDOF Building - SDOF Equipment System

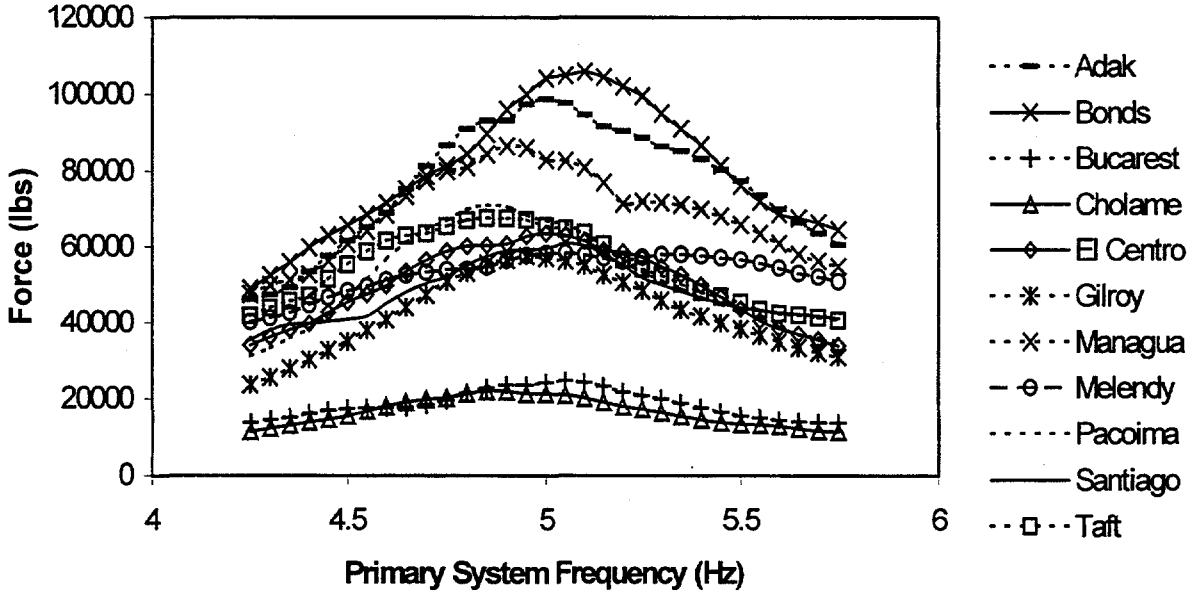


Figure.3.1.4-4: Seismic Force in Equipment, Eleven Actual Earthquake Inputs

Response Spectrum Method: The procedure of using multiple time histories, as discussed above, cannot be adopted directly as a design rule because a design earthquake input is typically defined in terms of a response spectrum curve and not multiple time histories. For a design spectrum input, *n* variations in the building frequency gives as many responses. However, an eighty four percent non-exceedence probability value over these *n* quantities will be excessively conservative because the input spectral accelerations are themselves defined at the same probability of non-exceedence. We used the observations made from the detailed studies conducted with multiple time history inputs for developing a method to account for the effect of uncertainty in the building frequency in a response spectrum method. First, let us describe the procedure for evaluating a design input spectrum curve at eighty four percent non-exceedence

probability corresponding to m time histories. Each of the m time history inputs, normalized to same value of peak acceleration, gives one response spectrum curve. At each oscillator frequency in the response spectrum curves, the m values for spectral accelerations can be used to evaluate a spectral acceleration value corresponding to eighty four percent non-exceedence probability. All such spectral values at each oscillator frequency constitute the design spectrum curve. Consistent with this approach, m responses obtained from as many time history analyses at each of the n frequency variations, as shown in Figure 3.1.4-4, can be used to evaluate the design response corresponding to eighty four percent non-exceedence probability. Figure 3.1.4-5 gives the design values for a variation in the building frequency. The n values obtained from the corresponding response spectrum analysis should be very close. Any difference between the two set of results is due to the inherent differences between the two analyses methods.

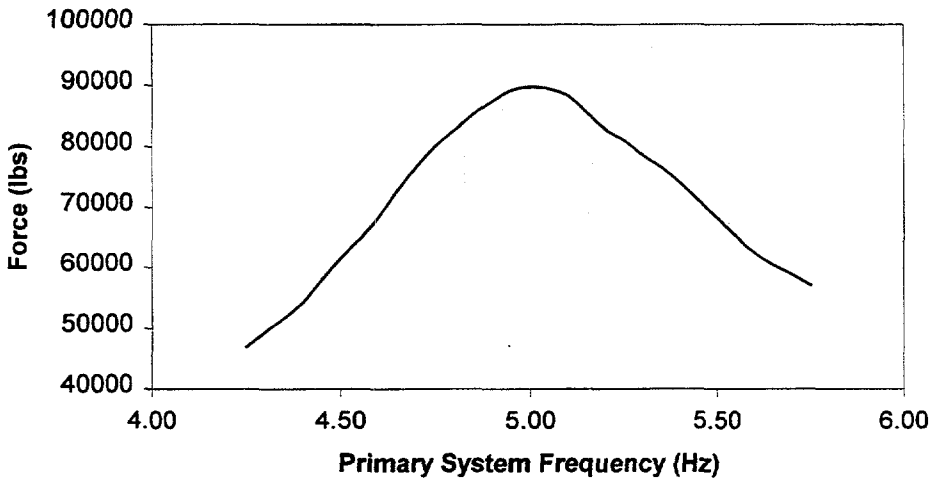


Figure 3.1.4-5: Seismic Force in Equipment Corresponding to Eighty Four Percent Non-Exceedence Probability, Eleven Actual Earthquake Inputs

We conducted detailed studies using several representative building-equipment and building-piping systems. It was observed that the systems in which the building frequencies are much smaller relative to the highest frequency of the input earthquake motion (also known as rigid frequency) the coefficient of variation over $n \times m$ response values is nearly equal to the coefficient of variation due to an uncertainty in the input motion alone and the effect of coefficient of variation due to an uncertainty in the building frequency is insignificant. For such systems, the response is primarily damped periodic and the design response is very nearly equal to the mean over n values in the corresponding response spectrum analysis. On the other hand, for systems in which the building frequencies are nearly equal to or higher than the rigid frequency of the input motion, there is no variation in response due to a variation in the input ground motion and the coefficient of variation over $n \times m$ values is equal to the coefficient of variation due to an uncertainty in the building frequency. The design response in such systems is given by the eighty four percent non-exceedence probability value over n response quantities in a response spectrum method because the periodic part of response is negligible and most of the response comes from rigid part. In actual building models the frequencies of vibration lie in a range that vary from a low frequency region to very high frequency region. In such systems, the

response in each mode is separated into the periodic and the rigid part. The periodic and the rigid parts of the modal responses are combined separately and the design response is evaluated as a mean over *n* values of the periodic part and mean plus one standard deviation over *n* values of the rigid part, obtained by a variation in the building frequency. For a building-piping system shown in Fig.4, the force in piping system at a particular location is equal to 11 kips when an uncertainty in the building frequency is not considered. For a ± 15% variation in the building frequency, this force varies between 1.5 kips and 14 kips when 11 different actual earthquake inputs are considered. The design response corresponding to eighty four percent non-exceeedence probability is 9.5 kips. It is close to the corresponding value obtained from a response spectrum method, equal to 10.2 kips.

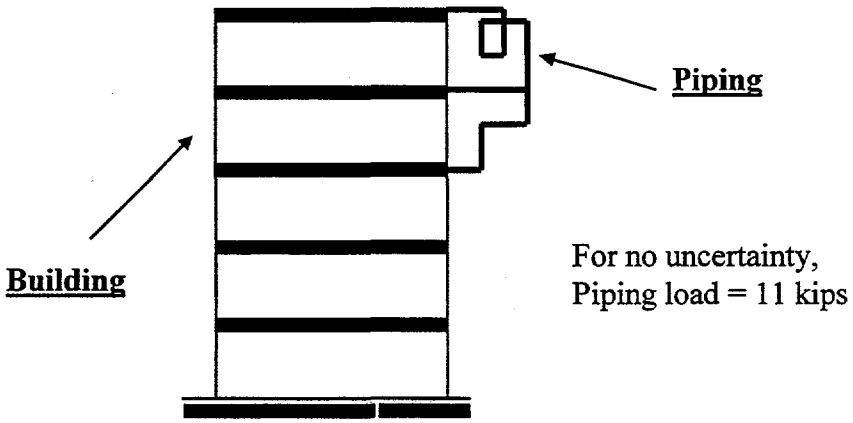


Figure 3.1.4-6: Multiply Connected Building-Piping System

Risk-Based Design Using ASME Code Equations

The ASME code provide rules for the design of pressure vessels and piping. It uses deterministic safety factors for loads, whereas, the allowable stresses are based on experience and test data. The ASME code has served its purpose well over the years. However, the reliability of a code designed piping system can vary considerably from one situation to another. For increasing the consistency in design, the code equations should provide the flexibility to design the piping system to a specified level of reliability. Some of the civil engineering codes (such as that for the design of steel structures) are based on this concept. To develop risk-based design rules these design codes employ the concept of Load Resistance Factor Design (LRFD). A design code developed using LRFD method provides risk consistency, is likely to result in economical use of materials, provides compatibility in design across different structural materials, and permits future modifications due to increased knowledge of failure mechanisms, material characterization, and loading environment. It also provides a framework to account for time-dependent degradation within a risk-based framework. Such a framework is useful in developing strategies for not only inspection and maintenance but also for life extension and license renewal. Other advantages include but are not limited to simplifications in system reliability analysis, and management of uncertainty in strength, loads and analytical models.

An equation in a design code which is based on the LRFD priciples is very similar in appearance to the one that is based on deterministic factors of safety. However, the deterministic factors for the loading and the strength terms in the equation are selected depending upon an acceptable level of reliability. To develop risk-based design equations, the first step lies in the definition of failure modes. These failure modes are then used to develop a performance function. For example, if S denotes the strength and L the load, the reliability can be defined as the probability when $S > L$. Mathematically,

$$R = P(S > L) \tag{1}$$

The performance function can be written as

$$Z = S - L \tag{2}$$

or in general,

$$Z = g(X_1, X_2, \ldots, X_n) \tag{3}$$

where X_i represents a probabilistically defined variable for load and resistance. Therefore, in LRFD method, the load and resistance are defined in probabilistic terms. The function $g(-)$ is a limit state function that describes the failure criterion. Mathematically, we can write

$$g(-) < 0 \qquad \textit{failure state} \tag{4a}$$
$$g(-) = 0 \qquad \textit{limit state} \tag{4b}$$
$$g(-) > 0 \qquad \textit{survival state} \tag{4c}$$

The reliability is defined in term of an index β, which is defined using the mean and variance of Z.

$$\beta = \frac{\mu_Z}{\sigma_Z} \tag{5}$$

If Z is assumed to be have normal probability distribution, the failure probability is given by

$$P_f = 1 - \Phi(\beta) \tag{6}$$

where Φ is the cumulative probability distribution of the standard normal variate.

For a given value of reliability (or probability of failure) and specified distribution of loads and strength variables, the resulting design equations have the following form

$$\gamma_1 L_1 + \gamma_2 L_2 + \ldots + \gamma_n L_n \geq \phi S \tag{7}$$

in which γ are the load factors (load amplifiers) and ϕ is the resistance factor (strength reducers). For illustration, let us consider the following design equation for a pipe of diameter D_o and section modulus Z, subjected to internal pressure P and bending moment M:

$$B_1 \frac{PD_o}{2t} + B_2 \frac{M}{Z} \leq 1.5 S_m \tag{8}$$

For a straight pipe, the deterministic values of the coefficients are $B_1 = 0.5$ and $B_2 = 1.0$. In LRFD method one can consider different ranges of internal pressure and ratio D_o/t. For these ranges and specified probability distributions of *P, M, Z* and S_m, the resulting equation will have the following form

$$\gamma_1 \frac{PD_o}{2t} + \gamma_2 \frac{M}{Z} \leq \phi S_m \tag{9}$$

in which different values of the load and the resistance factors represent designs for different values of reliability.

It should be noted that Eq.8 represents a performance function in which the failure is defined by the material yielding in extreme (outer) fiber of the pipe. The performance function will itself be different if the failure is defined as the yielding of the complete cross-section (formation of plastic hinge) to result in a leak. Several organizations such as ASME code committees and other task groups are involved in studying the risk-based modification of ASME code. We are collecting information on the outcome and progress of all these studies and also performing independent studies. So far we have studied the LRFD method for a couple of design equation by considering assumed distributions of loads and the correlation among them to generate the curves for load and resistance factors.

Table 3.1.4-1
Sample Set of
Power Production/Safety Functions

High Level Function	Description/Comment	Example Systems Structures and Components
Reactor Heat Generation and Control	Primary Source of Energy is the heat generated by the nuclear reactions in the fuel. This must be controlled for power production and safety.	• Fuel (Pellets, Fuel Rods, Fuel Assemblies) • Reactivity Control (Control Elements, Poison Systems, etc.)
Primary System Inventory Control		• Primary system pressure boundary • Primary system level control/makeup system
Primary System Pressure Control		• Primary system pressure boundary • Primary system pressure control system (e.g. pressurizer, heaters) • Primary system safety valves
Heat/Energy Transfer	This function includes transfer of the heat from the fuel to the primary coolant, plus, if applicable for a given design, transfer of the energy from the primary coolant to the secondary coolant. This is required for power production and must be maintained under all conditions to prevent damage to the fuel and potential release of radioactive materials	• Primary coolant circulation devices/pumps • Primary to secondary heat exchangers (e.g. steam generators) • Main feedwater/condensate system • Main steam system • Condenser and circulating water system

Table 3.1.4-1 (continued)
Sample Set of
Power Production/Safety Functions

High Level Function	Description/Comment	Example Systems Structures and Components
Energy Conversion and Transmission	The heat energy generated by the nuclear chain reaction must be converted to electrical energy. This must be controlled to maintain the required balance between energy generation and energy conversion.	• Turbine Generator and controls • High voltage switchgear/transformers
Maintenance of Vital Support Systems	Support systems such as motive power, control power, instrumentation and HVAC are needed for the proper operation and control of the power production systems and any non-passive safety systems (Note: instrumentation is required for monitoring the operation of passive safety systems.)	• High Voltage AC Power (motive power for equipment) • Low Voltage AC and DC power (instrumentation and control power) • Equipment cooling • Instrument air • HVAC
Control Of Radioactive Materials	To facilitate and control the energy generation the nuclear materials must be contained. These materials must also be contained to protect public safety and health	• Fuel Cladding • Primary Pressure Boundary • Containment

Table 3.4-2
Example Challenges to Power Production Functions

High Level Function	General Challenge	Specific Challenge
Reactor Heat Generation and Control	Positive Reactivity Insertion	• Control Rod Ejection • Uncontrolled Control Rod Withdrawal • Uncontrolled Poison (Boron) Dilution
	Negative Reactivity Insertion	• Control Rod Insertion • Excess Poison (Boron) Insertion
Primary System Inventory Control	Loss of Primary System Inventory	• Very Large Loss of Coolant Accident (LOCA) – Vessel Rupture • Large LOCA – Piping • Medium LOCA – Piping, Valves • Small LOCA • Interfacing System LOCA • Leak
	Excess Primary System Inventory	• Excess Inventory Makeup
Primary System Pressure Control	Loss of Primary System Pressure Control	• Loss of Pressurizer Heaters • Spurious Opening of Primary System Relief Valves
Heat/Energy Transfer	Insufficient Heat Transfer from Fuel to Primary System Coolant	• Loss of One or More Primary Coolant Circulating Pumps • Flow Blockage
	Insufficient Heat Transfer from Primary System Coolant to Secondary System	• Loss of Main Feedwater Flow • Loss of Main Steam Flow
Energy Conversion and Transmission	Loss of Energy Conversion/Transmission Equipment	• Loss of Turbine Generator • Loss of High Voltage (Main) Transformer
Vital Support Auxiliaries	Loss of Vital Support Systems	• Loss of Electrical Power • Loss of Equipment Cooling

Table 3.1.4-3
Example of Basic Risk Apportionment Process

No.	Challenge	Challenge Frequency	Apportioned Safety Goal (CDF Contribution)	GOAL (Failure to Mitigate)
1	Very Large LOCA	5 E-08/yr	5.0E-08	1
2	Large LOCA	5 E-06/yr	1.0E-07	2.0E-2
3	Medium LOCA	4 E-05/yr	1.0E-07	2.5E-03
4	Small LOCA	5 E-04/yr	5.0 E-07	1.0E-03
5	Steam Generator Tube Rupture	5 E-03/yr	5.0E-07	1.0E-04
6	Very Small LOCA/Leak	6 E-03/yr	5.0E-07	8.0E-05
7	Loss of Offsite Power	5 E-02/yr	5.0E-07	1.0E-05
8	Loss of Main Feedwater	1 E-01/yr	1.0E-06	1.0E-05
9	Loss of Condenser Vacuum	1 E-01/yr	1.0E-06	1.0E-05
10	General Transients (Turbine Trips, etc.)	1/yr	1.0E-06	1.0E-06
11	Other (Support System Induced, Fire, Flood, etc)	1 E-01/yr	1.0E-06	1.0E-05
12	*Margin*		3.0E-06	
TOTAL CDF GOAL			1.0E-05	

Figure 3.1.4-1
Typical Design Process (Current)

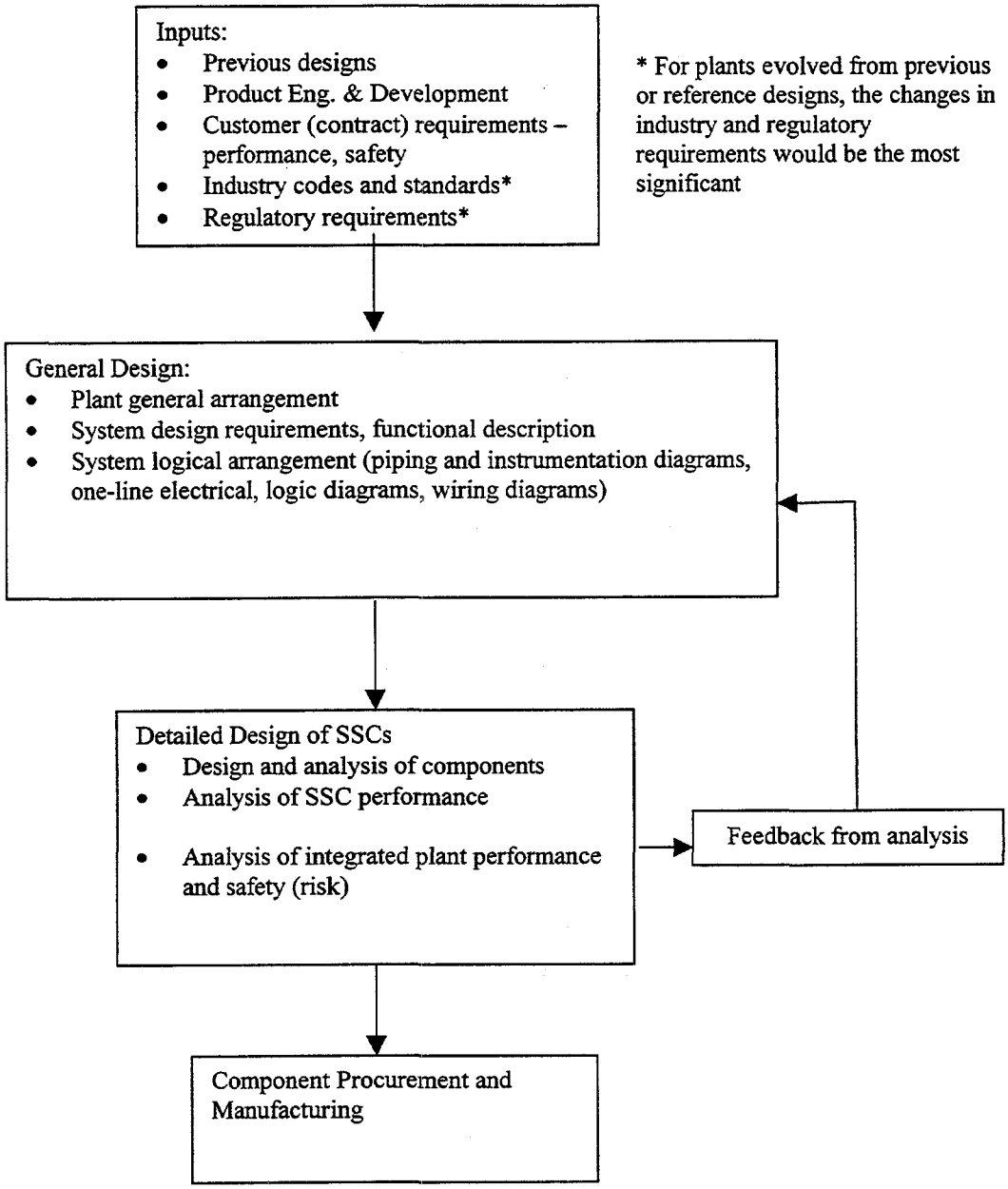


Figure 3.1.4-2
Overall Risk Informed Design Process
(Sheet 1 of 2)

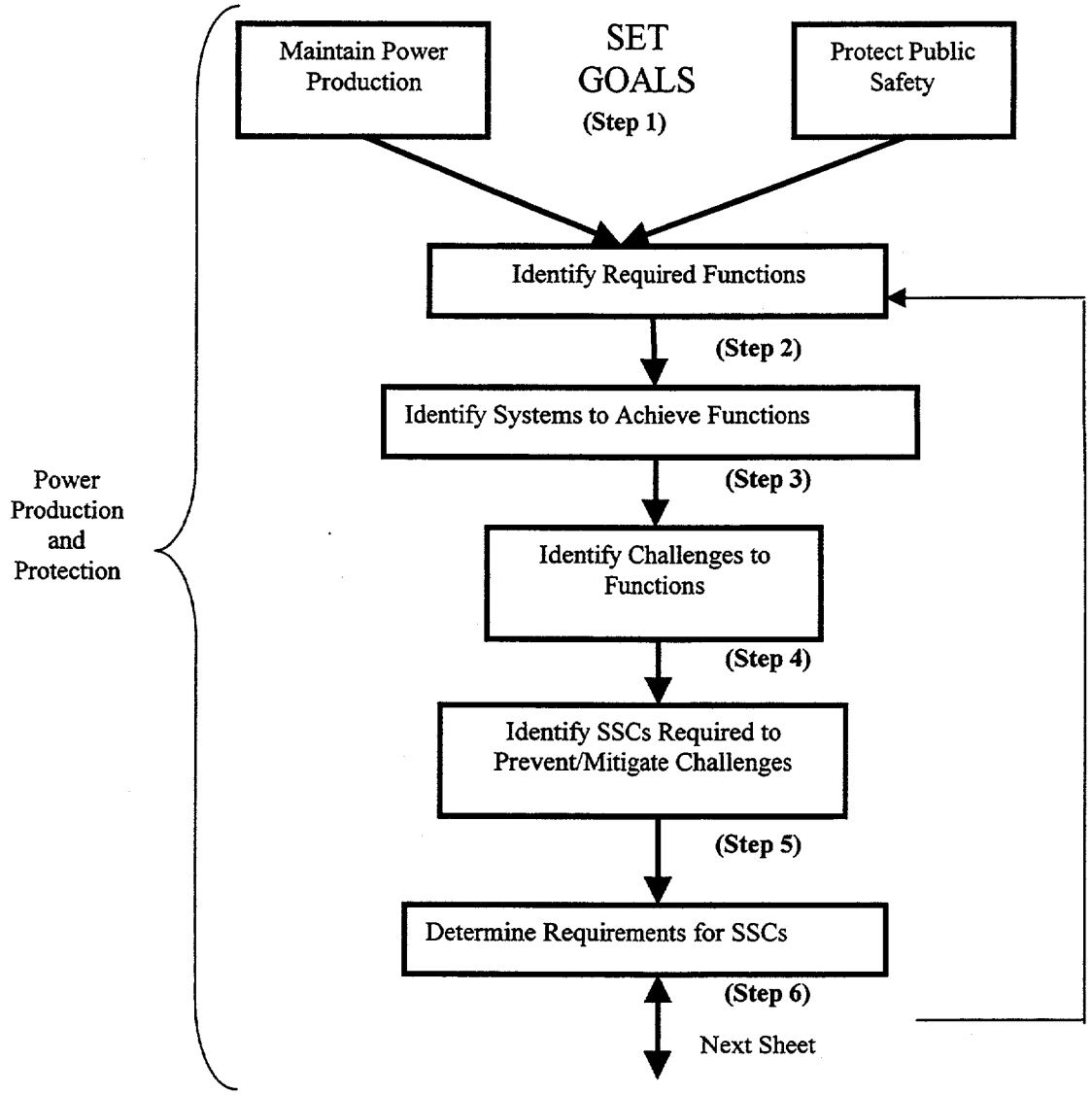
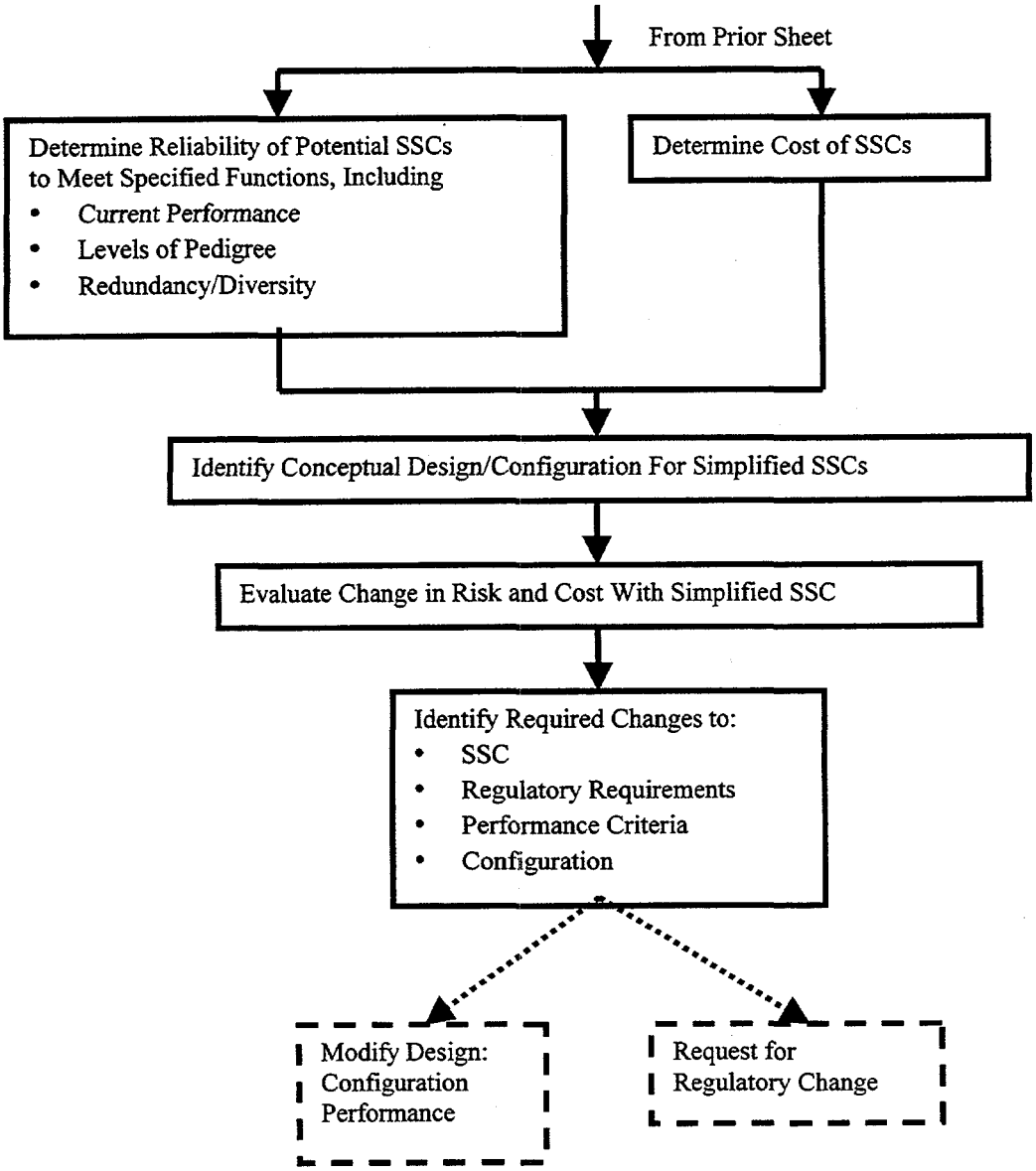


Figure 3.1.4-2 (Continued)
Overall Risk Informed Design Process
(Sheet 2 of 2)



3.1.5 Identify High Priority Requirements, Standards, and SSCs

Approach

Currently the NRC and industry are working to identify the regulatory requirements and SSCs that would likely yield the greatest cost savings through application of risk-informed regulation. However, these ongoing efforts are focused upon the areas that are most beneficial to reducing the operating costs of current plants. Moreover, the most beneficial areas in one nuclear plant do not necessarily match the most beneficial areas of another nuclear plant. This relates to differences in the plants' designs, as well as differences in the risk assessments that were previously performed for each of the plants.

Future plant designers, however, will need to apply the methodologies developed in Tasks 1.3 and 1.4 to all of the requirements, standards, and SSCs in a nuclear plant which are being identified in Tasks 1.1 and 1.2. This is a major undertaking and would require a budget that is well beyond the funding level of this project. This task, therefore, is intended to limit itself to a review and identification of the major requirements and standards that should be given the highest priority for risk-informed revision in the future based upon their relationships to the SSCs that will provide the greatest opportunities for cost reduction through simplification.

Originally, this task was to perform a high level review of the lists of SSCs, standards and regulations developed in Tasks 1.1 and 1.2 and identify the major requirements, standards and SSCs that should be given the highest priority for review and risk-informed revision in the future. This was to be accomplished by developing a methodology for ranking and prioritizing SSCs, standards and regulations based on their importance to safety, the potential for significant simplification of design and the potential magnitude of the cost reduction that could be achieved without jeopardizing the requisite level of safety. Application of this ranking methodology to the lists of SSCs, standards and regulations developed in Tasks 1.1 and 1.2 would then yield an estimate of the potential overall savings if the risk-informed methods were applied to an entire nuclear power plant. This prioritization methodology would also be used to select a more detailed sample application of the methodologies being developed in Tasks 1.3 and 1.4.

A key issue arose early in the project. It was recognized that the concept of "simplifying designs" was primarily an evolutionary concept that was dependent upon the current technologies. This creates the potential danger of inadvertently excluding other viable nuclear technologies or overlooking the potential for major system design changes that go beyond the "simplification" level. Thus, the methodologies being developed in Tasks 1.3 and 1.4 began looking at a more global approach, essentially starting with a "clean sheet of paper". With the initial evolution of the risk-informed design methodology, it was quickly recognized that the methodologies needed to be developed in conjunction with a sample application in order to identify potentially weak areas in the methodologies and to provide the basis for the details of the methodologies. Thus, the focus of this task during this phase of work was changed to select a sample application to support Tasks 1.3 and 1.4. The set of criteria established for selecting the sample application is:

- The application should be simple enough to accomplish within the resources and schedule of this project.

- The selected application should support the other tasks, for example:
  - exercise the new regulatory philosophy (Task 1.3)
  - provide a reasonably detailed application for the design methodologies (Task 1.4)
  - attract the interest and reaction of industry stakeholders - Task 1.8 (i.e., high profile, recognizable)
  - produce high potential cost reduction (Tasks 1.1, 1.2, 1.4)
  - address a reasonably significant function with potential design margin
  - be consistent with common sense/judgement

- The problem should have potential synergy with the DE&S Design/Construction NERI project and the Sandia Smart Equipment project.

- The problem should be consistent with/supportive of other on-going industry activities associated with risk informed regulation.

Accomplishments

The sample application selected based on these criteria was the RCS inventory control function. In the current plant designs, this general function encompasses a non-safety related function, the RCS makeup systems, and a safety related function, the Emergency Core Cooling System (ECCS). The ECCS design and analyses are covered by a number of standards and regulations so it provides a reasonable exercise for the risk-informed regulation methodologies from Task 1.3. The systems currently used to perform the two sub-functions have easily defined boundaries, are relatively small in scope and , as shown in Table 3.1.5-1, the ECCS is a relatively risk important system. There is a large body of knowledge available for the performance capabilities of the constituent SSCs and there is a reasonable belief that there is margin available for system simplification/refinement. Finally, there is an ongoing industry effort aimed at removing large break LOCA from the system design basis based on leak-before-break analysis. This type of design basis change would have a major impact on the design requirements for the ECCS that can be capitalized on in this project.

Table 3.1.5-1
System Risk Importance Measures For System 80+

System Name	Risk Achievement Worth*	Risk Reduction Worth+
Emergency Feedwater System	5.01×10^5	2.36
Electrical Distribution System	4.01×10^5	1.05
Component Cooling/Station Service Water System	7.99×10^4	1.00
Safety Injection System	3.95×10^4	2.16
Safety Injection Tanks	5.01×10^1	1.01
Chemical and Volume Control System	1.53×10^1	1.02
Engineered Safety Features Actuation System	4.31×10^3	1.01
Shutdown Cooling System	1.27×10^3	1.09
Safety Depressurization System	2.89×10^2	1.34
Containment Spray System	1.00×10^2	1.00
Steam Removal System	8.85×10^1	1.02
Startup Feedwater System	2.82×10^0	1.00
Instrument Air System	1.45×10^0	1.00
RCS Pressure Control System	1.00×10^0	1.00

* The Risk Achievement Worth for a system is the ratio of the Core Damage Frequency if the system is assumed to be always failed to the base Core Damage Frequency. It is a measure of the benefit of the system or a measure of the impact of taking the system out of service

\+ The Risk Reduction Worth for a system is the ratio of the Core Damage Frequency if the system is assumed to be always available to the base Core Damage Frequency. It is a measure of the maximum potential benefit making the system perfectly reliable.

3.1.6 Apply Methodologies to a Sample SSC

Approach

In addition to providing a broad assessment of what can be accomplished by risk-informing the requirements and standards for future nuclear power plants, and then simplifying the SSCs to which they apply, an in-depth evaluation of what can be achieved must also be provided. The objective of this task is to evaluate the efficacy of the methodologies developed in Tasks 1.3 and 1.4 via a detailed trial application to a high priority SSC identified in Task 1.5. The insights gained from the trial implementation of these methodologies will then be fed back into the methodologies to improve them.

The selected SSC will have a high potential for significant changes in design with the attendant reduction in costs and the anticipated impact of the design changes should be minimal. The selected SSC should, to the extent practical, cover systems aspects, component aspects and structural aspects so that the methodologies receive a comprehensive test.

An advanced conceptual system design that would be capable of satisfying the Reactor Coolant System (RCS) Level Control safety function was selected to evaluate the effectiveness and feasibility of the methodologies being developed in Tasks 1, 3 and 1.4. The conceptual system is required to achieve and maintain RCS Level Control over a wide range of plant operations, from normal power operations to shutdown conditions initiated by a loss of coolant accident (LOCA) or a transient event.

For this task, the advanced conceptual system will be defined, potential benefits established, and design or regulatory issues that need to be addressed identified. A surrogate system based on the Certified System 80+ design will be used to estimate the risk impact on core damage frequency (CDF).

Accomplishments

Definition of Advanced Conceptual System Function: The primary function of the advanced conceptual system design is to provide RCS makeup in order to achieve and maintain the RCS Level Control safety function. By satisfying the RCS Level Control safety function, the stored and fission product heat from the reactor core is removed following a LOCA. This will limit or prevent fuel damage so as to maintain a coolable core geometry, limit the cladding metal-water reaction, and will maintain the reactor core subcritical during the extended period of time following a LOCA.

The advanced conceptual system accomplishes its function by use of redundant active and passive subsystems. The active portion of the advanced system consists of the charging pumps and associated valves while the passive portion consists of the Safety Injection Tanks (SITs) (or accumulators)

The advanced conceptual system design is used to control and maintain RCS level during normal plant operation, or for the following events:

- LOCA including a pipe break or other related breach of the RCS pressure boundary,
- Steam Generator Tube Rupture (SGTR), or
- Feed and Bleed operations

Definition of Advanced Conceptual System Configuration: The advanced conceptual system consists of active and passive subsystems, as shown in Figure 3.1.6-1. The passive subsystems (i.e., the SITs) do not depend on support systems or operator action to perform their safety-related function. There are two SITs with sufficient inventory for rapid RCS makeup following a large LOCA. The SITs contain borated water and are pressurized with a cover gas. Redundant level and pressure instrumentation is provided to monitor the conditions of the SITs. The SIT flow paths are equipped with check valves and motor-operated valves in the open position to facilitated a rapid discharge of inventory to RCS.

The active subsystems consist of two charging pump trains, each of which relies on support systems or operator actions to perform its safety related function. Redundant injection motor-operated valves are included in each train. These valves are normally closed during normal plant operation and require an engineered safety feature actuation signal (ESFAS) or operation action to open following an accident condition. Motor-operated suction valves are also included. These valves are closed during normal plant operation and also require an ESFAS or operator action to realign the charging pumps to the makeup source. Each train of the active subsystems includes a single charging pump. Each pump is capable of delivering a nominal flow of approximately 150 gpm at normal operating RCS pressure (i.e., 2250 psia). This makeup flow rate accommodates step changes in power and reactivity control during normal power operation. A makeup flow path via the regenerative heat exchanger is used during normal plant operation. During accident conditions, each charging pump is capable of delivering a run-out flow of approximately 1500 gpm. The delivery of makeup during accident conditions is via either or both injection paths. Adequate instrumentation is provided to monitor pump operability and the delivery of flow to the RCS.

System Operation: The advanced conceptual system design is used to perform RCS inventory makeup during all modes of plant operation (i.e., normal and abnormal operations). Hence, a portion of the system is continually operating. During normal plant operation, the passive subsystem portion of the advanced conceptual system design is in standby. During an accident, such as a LOCA, when the RCS pressure falls below the pressure of the SITs, the check valves in the SIT flow paths open to discharge the contents of the SITs into the RCS.

During normal operation one of the two charging pumps is aligned to provide RCS makeup. During this mode of operation, the processed RCS letdown flow from the volume control tank is returned to the RCS via the regenerative heat exchanger flow path. Because both charging pumps can deliver significantly more makeup flow than required during normal power operation, the discharge path for one of the pumps is isolated and the associated pump is secured. However, the design is such that either pump may be used to satisfy makeup requirement during normal power operation. During an accident condition such as a LOCA, the injection flow paths are automatically actuated by ESFAS so that makeup flow can be delivered to the RCS. This involves the opening of the motor-operated injection and suction valves in each train. The

standby charging pump is also started automatically by ESFAS. Although one of the charging pumps is operating is receives a confirmatory ESFAS to start. The refueling water storage tank, which contains borated water, is the RCS makeup source during accident conditions.

The advanced conceptual system design is also used to satisfy the feed portion of "Feed and Bleed" operation. This is accomplished by manually opening the motor-operated injection and suction valves in the flow path of the operating charging pump. The bleed portion is accomplished by depressurizing the RCS as necessary to provide the required makeup.

The advanced conceptual system is designed to meet its functional requirements even with the failure of a single active component, except for a limited range of LOCA events. Physical and electrical separation of the trains assures that a single failure in one train cannot preclude the other train from performing its safety function.

Success Criteria: The advanced conceptual system design is used for RCS makeup and inventory control, and the success criteria varies for the initiating event of concern. For very large LOCAs of the order of a double-ended guillotine break in the RCS hot and cold leg, the advanced conceptual system design would not be capable of mitigating such an accident. Without mitigation, these types of very large LOCAs would lead directly to core damage. However, it should be noted that the frequency of such pipe breaks is of the order of the frequency of a vessel rupture. Such very large LOCAs are not expected to be key contributors to the risk profile.

For large LOCAs, which include pipe break of 10-inch nominal diameter and less than the very large LOCA break sizes identified above, both charging pumps and both SITs are required for mitigation. The single failure criterion requirement for the advanced conceptual system design would not be applicable for this type of large LOCA.

For all other types of LOCAs, which are not included above, successful mitigation can be accomplished by one of the two trains of charging pumps. The passive portion (i.e., SITs) of the advanced conceptual system design would not be required for mitigating these types of LOCAs. A single train of charging pump is also required for mitigating "Feed and Bleed" events.

Potential Benefits: The advanced conceptual system design shown in Figure 3.1.6-1 is used for RCS makeup during normal and accident conditions. This concept is quite a departure from current light water reactor designs, which in general utilize two different systems to accomplish RCS makeup. For current designs, the Chemical and Volume Control System (CVCS) is used to provide RCS makeup during normal power operation. The CVCS is a high head low volume system, and therefore cannot provide the high flow rates required for mitigating a large LOCA. The Emergency Core Cooling System (ECCS), which is different from the CVCS, is used for RCS makeup during accident conditions. The ECCS provides a much higher flow rate that is required for mitigating a LOCA.

Even though the advanced conceptual system design is a departure from current designs, it exhibits potential benefits in terms of reduced equipment and cost savings that may not have an

adverse impact on risk. The reduction in equipment is based on a comparison of the System 80+ Certified Design. The potential benefits are identified as follows:

- Elimination of all four high pressure safety injection (HPSI) pumps
- Elimination of two HPSI lines and associated valves with the remaining two HPSI lines connected to the two charging pumps
- Elimination of two SITs
- Elimination of both hot leg injection lines
- Elimination of support system connections for four HPSI pumps, including:
  - Electric power (i.e., 4.16 KV, 480 VAC, & 125 VDC)
  - ESFAS and controls
  - Component cooling piping and valves
  - Heating, ventilating and air conditioning dampers and ductwork
- Reduction of the loads on the emergency diesel generators, which may lead to a smaller size and reduction in physical space allocation
- Better utilization of equipment (i.e., the charging pumps are used for RCS makeup during normal and accident conditions)
- Utilization of smart equipment and controls for boration

Design and Regulatory Issues: In order to realize the potential benefits identified above for the advanced conceptual system design, there are several design and regulatory issues that need to be addressed and resolved. The design issues are summarized below:

- Utilization of Smart Equipment – The conceptual design calls for charging pumps that are capable of delivering a wide range of makeup flow. A larger than normal flow rate during a boron dilution event will exacerbate the problem. Hence, design features and enhancements should be in place to limit boration flow rate during normal power operation. This may include smart equipment and controls to isolate the boron dilution source in the event that the required flow rate is exceeded.

- Demonstration of Spillover/Mixing Capability – Current light water reactors are designed to mitigate long term boron precipitation in the reactor vessel following a large LOCA. This is accomplished by performing simultaneous hot and cold leg injection to ensure mixing within the reactor vessel. For the advanced conceptual system design the hot leg injection piping and associated valves are eliminated. Adequate mixing within the reactor vessel to preclude boron precipitation via the makeup process or other means must therefore be demonstrated for the advanced conceptual design.

- Operating Charging Pumps without Isolating Normal Suction – The makeup source for the advanced conceptual design depends on the plant operating condition. For normal plant operation, the makeup is obtained from the volume control tank. During accident conditions, the makeup source is realigned to the refueling water tank. Isolation of the volume control tank during accident conditions is not credited. The issue regarding whether or not the charging pumps can deliver the required makeup flow during accident conditions without isolating the volume control tank should be assessed.

- Aggressive RCS Depressurization – For the System 80+ Certified design, aggressive depressurization of the RCS is credited. This feature allows for an alternate means of providing makeup to the RCS by low head pumps (i.e., shutdown cooling pumps) in the event of a small LOCA and failure of high pressure injection pumps. All four SITs were credited for aggressive RCS depressurization. Since the advanced conceptual system design includes a reduction in the number of SITs, the feasibility of aggressive RCS depressurization using equipment on the primary and secondary sides should be explored.

In addition to the design issues identified above, certain regulatory issues that impact the advanced conceptual system design should also be addressed. These regulatory issues are listed below:

- Leak Before Break – Leak before break is currently not used to support the removal of large LOCAs from the design basis. By crediting leak before break in the advanced conceptual system design, a full spectrum of LOCAs can be removed from the design basis.

- Single Failure Criterion for LOCA – Mitigating system(s) for all types of LOCAs in current light water reactor designs are required to meet the single failure criterion. This ensures that the mitigating system can accommodate a single failure and still perform its safety-related function. Although leak before break is used to eliminate a full spectrum of LOCAs from the design basis for the advanced conceptual system, the risk impact of such LOCAs would still be assessed. However, the mitigating systems for such LOCAs would not be required to meet the single failure criterion.

- Qualification of Charging Pumps – The charging pumps for the advanced conceptual design are required to operate during normal and abnormal plant conditions. Hence, these pumps should be qualified to perform their safety-related function over a wide range of flow rates.

- Boron Dilution – The utilization of charging pumps with significantly higher flow rate capabilities increases the severity of a boron dilution event. To minimize the severity of such an event, the feasibility of using smart equipment and controls should be assessed.

Surrogate System: Recognizing the fact that the support systems for the advanced conceptual system design is not defined or identified in this phase of the program and the modeling complexity without such well defined interfaces, a surrogate system was used to assess the risk impact on the RCS Level Control safety function. The core damage frequency (CDF) was used as a measure of risk. The Safety Injection System (SIS) of the System 80+ Certified design, as shown in Figure 4.1.6-2, was used as the basis for the surrogate system. A train of HPSI pump and the associated SIT were eliminated from each of the two SIS divisions to form the surrogate system. Hence, the surrogate system consisted of two HPSI pump trains and two SITs, which are used to provide RCS makeup for mitigating LOCA events.

The System 80+ Probabilistic Risk Assessment (PRA) model was used as the basis for the evaluation of the surrogate system. The PRA model was modified to reflect the reduction in the number of HPSI pumps and SITs described above. The support systems for the remaining two HPSI pumps and the other systems used in the PRA remained unchanged. Current data for RCS pipe break frequency as described in NUREG/CR-5750 was used in assessing the risk impact of the surrogate system. All other reliability data as used in the System 80+ PRA was used in this assessment.

The surrogate system was used to assess the risk impact of LOCA (i.e., large, medium, and small) events, which challenge the RCS Level Control safety function. Although steam generator tube rupture is generally categorized as a type of LOCA, this initiating event was not included in the assessment because it is a significant contributor to large early release risk rather than core damage risk. The surrogate system is also used to mitigate "Feed and Bleed" events, which challenge the RCS Heat Removal safety function and therefore these types of events are excluded from this assessment.

After modifying the System 80+ PRA model to reflect the surrogate system, the LOCA initiating event core damage sequences were re-quantified to determine their contributions to CDF. The resulting CDFs are shown in Table 3.1.6-1. The corresponding System 80+ LOCA CDFs are also provided in this table for comparison purposes. In crediting the current lower initiating event frequencies for pipe break, the surrogate system CDF for large LOCA increased slightly. However, the CDF for medium LOCA decreased by an approximate factor of 3, while the CDF for small LOCA increased by slightly more than a factor of 2. The total System 80+ CDF for LOCA initiating events is 6.1E-7 per year. The corresponding total CDF for the surrogate system is 7.1E-7 per year. Hence, the overall the difference between the CDFs for the System 80+ design and a modified System 80+ design, which uses the surrogate system, is 1.0E-7 per year. For the three types of LOCAs (i.e., Large, Medium, and Small) considered in this evaluation, the dominant contributor to their respective CDF involves the initiating event followed by failure of the safety injection system to perform its function.

The quantified CDF for each type of LOCA included in this evaluation was compared with the apportioned safety goal contribution to the overall CDF. For convenience, the apportioned CDFs for LOCAs are also shown in Table 3.1.6-1. The results show that the quantified CDFs for large and medium LOCAs are slightly above their respective allocated goals, and the quantified CDF for small LOCA is slightly below its allocated goal. This illustrates that the initial safety goal allocation for LOCA CDF is reasonable. Although initial CDFs for large and medium LOCAs

are slightly above their apportioned safety goals, it is expected that as the system designs become more solidified and the appropriate issues are resolved the mitigating goals for the systems will be met. By meeting the system mitigating goals the apportioned safety goal contribution to CDF will also be met. The methodology described in Task 1.4 outlines an iterative process for risk-informing the design. As the systems for simplifying the design become better defined, their impact on CDF and large early release frequency will also have to be re-evaluated. The iterative re-evaluation process will focus on the cost benefit of the systems and the feasibility of meeting the mitigating goals outlined in Table 3.1.4-3.

Table 3.1.6-1

LOCA CDF Comparison

Initiating Event	System 80+		Surrogate System		
	IE Freq [1] [Per Year]	CDF [Per Year]	IE Freq [2] [Per Year]	Quantified CDF [Per Year]	Allocated CDF [3] [Per Year]
Large LOCA	6.97E-05	1.09E-07	5.00E-06	1.49E-07	1.00E-07
Medium LOCA	1.49E-04	3.02E-07	8.92E-05	1.18E-07	1.00E-07
Small LOCA	3.00E-03	1.97E-07	5.00E-04	4.44E-07	5.00E-07
		6.08E-07		7.11E-07	7.00E-07

1. EPRI KAG Data
2. INEEL Data (NUREG/CR-5750)
3. Apportioned Safety Goal Contribution from Table 4.1.4-3

ΔCDF = 1.0E-7 per year

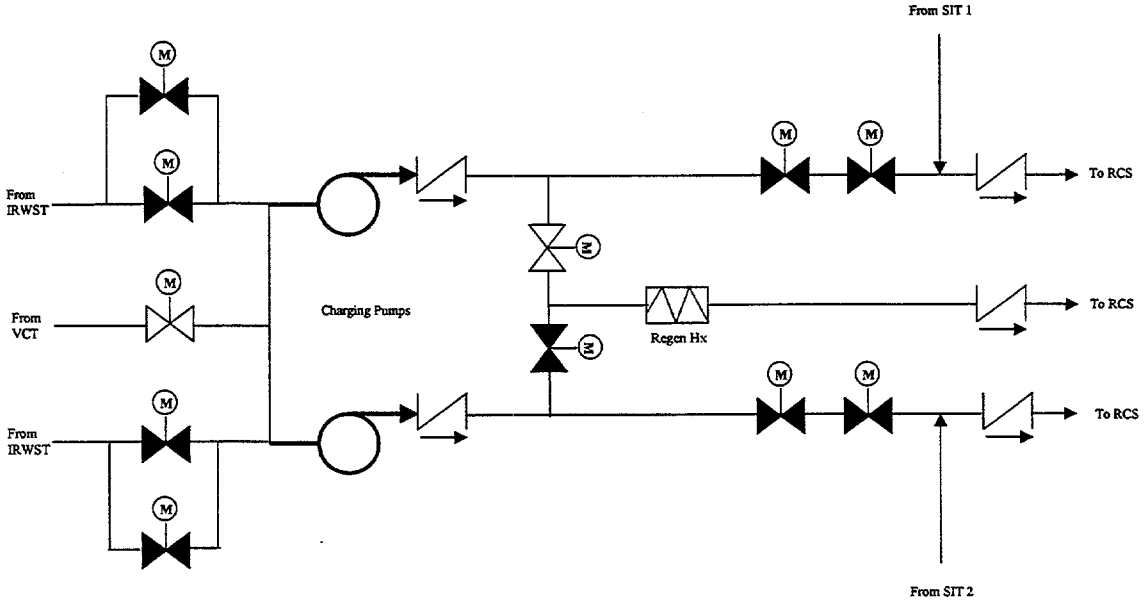


Figure 3.1.6-1

Advanced Conceptual System
Makeup System Schematic (High Pressure)

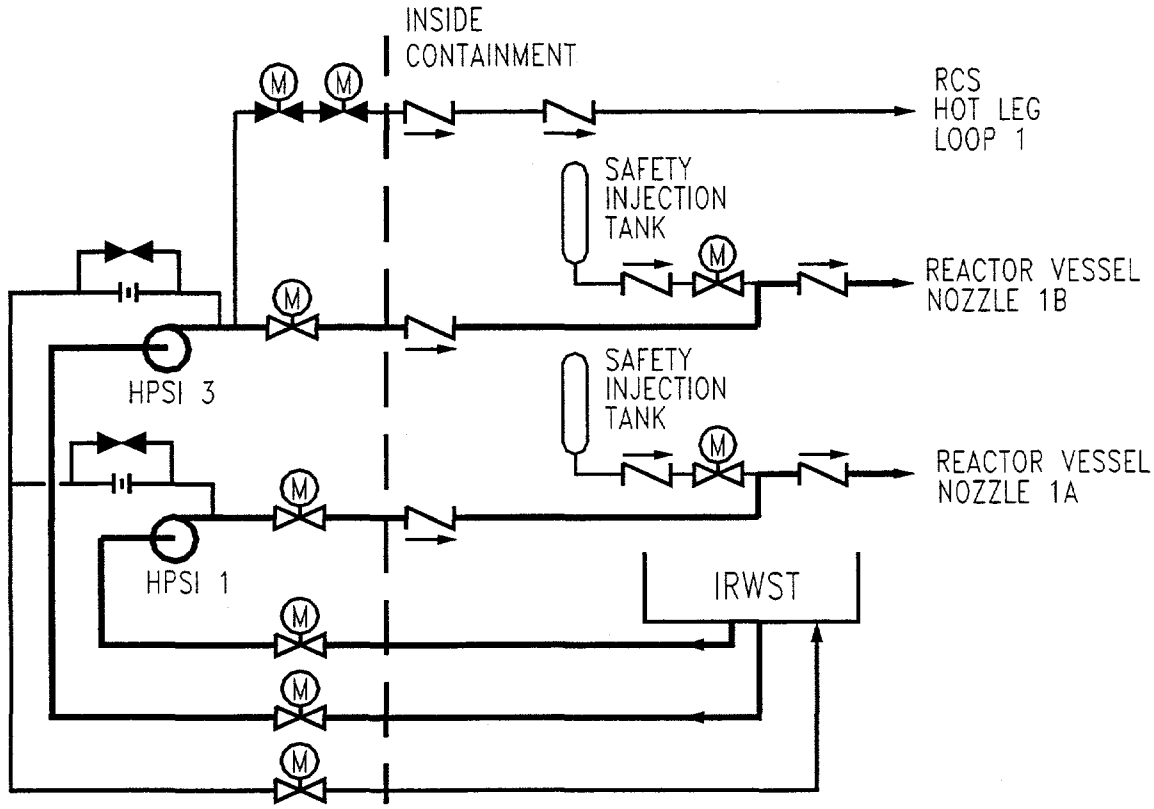


Figure 3.1.6-2

System 80+ Certified Design
Safety Injection System (One of Two Divisions)

3.1.7 Evaluate Regulatory Processes and Develop Recommended Improvements

Approach

The "Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Plants" project has as one of its objectives the development of a scientific, risk-informed approach for identifying and simplifying deterministic Nuclear Regulatory Commission (NRC) requirements for nuclear power reactors that do not contribute significantly to safety. It envisions a new substantive regulatory framework that uses quantitative risk criteria and probabilistic safety assessments (PSAs).

Task 1.7 addresses how the NRC hearing process might be reformed to accommodate extensive use of PSAs. This task will examine formal NRC hearings, including the most extensive NRC formal hearing on a full-scope PSA (the Indian Point case in the mid-1980s), and also hearing alternatives that would assure due process and the correct ultimate decision but in a more efficient and timely way.

Accomplishments

The following provides a summary for the Task 1.7 evaluation of the regulatory processes and recommended improvements. A detailed description is provided in Appendix B.

An evaluation of formal NRC hearings which are consistent with existing practice concludes that the use of PSAs and quantitative probabilistic criteria will likely add delay and expense to licensing hearings that are incommensurate with the likely contribution to safety. Therefore, it becomes imperative that change to the existing regulatory process must be invoked if full benefit is to be achieved from risk-based design and regulation.

The law is unclear whether the Atomic Energy Act requires formal, on-the-record hearings in nuclear power reactor initial (or renewal) licensing cases. The study assumes conservatively that formal hearings are required, but finds nevertheless that the law (the federal Administrative Procedure Act of 1946) offers flexibility in the conduct of formal hearings that NRC's rules in 10 CFR Part 2, Subpart G do not now include. The study examines how oral hearings with examination and cross-examination of witnesses are not required to resolve legal and policy issues, and recommends that these issues, including essential quantitative risk criteria in the new licensing framework, be resolved in any event by rules which create the new framework. The study concludes that use of PSAs will likely involve the need to resolve some case-specific issues of expert scientific opinion, and that formal hearings with examination and cross-examination of witnesses may not be required even when there are such disputes. It concludes that, contrary to NRC practice, written submissions (a so-called paper hearing) will comply with formal hearing requirements provided that all of the bases for the applicant's expert opinions are fully disclosed so that an opposing expert can prepare rebuttal. Formal hearings, with examination and cross-examination of witnesses, should be reserved for cases where there are disputes over motive, intent, credibility, or past events, like typical enforcement cases.

The task study also examines how scientific peer review, expert elicitation, and NRC Staff review processes offer suggestions on how the hearing process might be reformed. It concludes that some kind of additional process, beyond a simple paper hearing, will likely be necessary because in many cases this will be required as a practical matter for experts to understand fully the bases for opposing opinions. However this need only include opportunity to meet informally with opposing experts and to submit written questions, under the control of the NRC Staff, much like the interaction between applicant and NRC Staff in the current NRC Staff review process. Once the bases for applicant's expert opinions are fully disclosed, intervenor could be required to proceed with the filing of its own expert's opinion or be dismissed from the hearing. Current NRC practice of allowing an intervenor to attempt to prove its case without offering its own experts would be disallowed.

The study makes recommendations on special problems that are posed by the introduction of the results of expert elicitation in licensing hearings. It also recognizes that the hearing process it envisions will require a level of resources and access to scientific expertise that will not be available to many concerned citizens and groups. It suggests that NRC should allow these citizens and groups to play a role, early in the licensing process, in the formulation of issues of special concern that would be required to be addressed by the NRC Staff and the applicant in the review process (the Safety Analysis Report and Safety Evaluation Report).

3.1.8 Coordinate Activities with Ongoing Efforts of NEI, NRC, and Industry

Approach

NEI, NRC, and the remainder of the nuclear industry already have underway a substantial program to develop and apply risk-informed, performance-based regulation to issues that affect the operation of the existing nuclear plants. Since the research effort for this project is intended to identify and focus on those issues that relate to the design, regulation and construction of new nuclear plants, it is essential that this project be coordinated with the already ongoing effort. Therefore, the purpose of this subtask is to interface with the NEI, NRC, and the rest of the nuclear industry. Such coordination offers several benefits. First, it avoids any unnecessary duplication of efforts between existing plant programs and new plant programs. Second, it provides access to the information on existing plant activities by the research team for this project; thus, allowing it to work more efficiently. Third, it assures that NRC, NEI, and industry consider new plant issues, in their planning. Finally, it allows the results of this proposed research effort to be used, where appropriate, to supplement activities for the existing plants.

Activities under this subtask includes participation in NEI programs and meetings related to risk-informed, performance-based regulation. Meetings held with the NRC present the research team's progress and solicit NRC feedback. The research team may also need to interface with utilities that are participating in the risk-informed, performance-based regulation development efforts. This is be aided by the fact that two of the three pilot nuclear plants, so far identified for leading the current plant demonstration effort, have nuclear steam supply systems that were originally provided by Westinghouse Electric Company, Nuclear Systems (WENS).

NEI has established the Risk-Informed Regulation Working Group (RIRWG), as a policy level committee to coordinate industry efforts to work with NRC to implement risk-informed regulatory changes. The Working Group is composed primarily of senior utility executives, with some participation by engineering companies, e.g., WENS. The primary focus of the Working Group is directed to regulatory issues that affect the operation of current plants. This project, however, focuses on issues that affect the design and construction of future nuclear plants. WENS's participation in the Working Group assures that the efforts in this project are well integrated with the ongoing effort on operating plants.

Activities under this subtask are compiled into status reports that to be issued at the end of each yearly phase of the project. These reports include a summary of the major interactions that have occurred between the project team, NRC, NEI, and other industry participants.

Accomplishments

NRC Workshops: WENS represented this project at two NRC workshops on risk-informing the current regulations for current plants (September 1999 and February 2000). The purpose of the presentation at the first workshop was to introduce our project, state its purpose of developing new methods for design and regulation of future plants, and state the importance of coordinating our project with other industry and NRC initiatives. NRC supported the desire to coordinate related programs.

At the second workshop, our draft regulatory framework document was summarized, with emphasis on differences (not conflicts) with the current NRC program for operating reactors. NRC Research personnel encouraged our project to think "boldly" in terms of challenging current regulatory assumptions even though future review and approval of NRC staff might be difficult.

NRC Research Management Meeting: At the Regulatory Information Conference in March 2000, WENS met with representatives of NRC Research to summarize the status of our project. Again, we were encouraged to proceed as planned and it was agreed that at some undetermined future time (possibly during Phase 2 of this project) a briefing should be provided to the Commissioners.

NEI Risk-Informed Working Group: WENS attended two meetings of this working group. This project's plans were summarized and the intent to closely coordinate activities with the ongoing NRC effort were summarized. Other NEI working group members supported this project and its approach.

IAEA Consultancy Group: WENS represented this project at two meetings of this working group. The purpose was to draft a report on optimizing water-cooled reactor technology. This draft was accomplished and it is consistent with and supportive of DOE's NERI program, specifically including this Risk-Informed Assessment project and its two related NERI projects for "Smart" Equipment and Improved Design and Construction methods. Another meeting is scheduled for December 2000 to further coordinate these projects.

Electric Power Research Institute: EPRI is initiating an effort to coordinate utility interests in risk-informing regulations for future reactors, with emphasis on the ALWRs. In July 2000, this project began discussions with EPRI to ensure that our projects would be complementary, non-conflicting, and synergistic. While discussions were only initiated, it was agreed that our programs would meet these coordination goals and that details would be worked out as their program developed.

Korean Organizations: WENS made two status presentations to Korea Electric Power Company and Korea Power Engineering Company. An invitation was made to participate in our NERI projects at no cost to DOE, and as long as Korean detailed information and labor were contributed to our projects. This cooperation is being coordinated via DOE management and may be initiated in Phase 2.

3.2 Task 2 Strengthening the Reliability Database

3.2.1: Identify Current Sources of Reliability for SSCs

Approach

Current databases or published sources of reliability data that can support the development and simplification of new reactor plant designs need to be identified. The objective of this task is to identify these sources by surveying the traditional sources of data used for evaluating nuclear power plant performance and examining potential new sources of data that have not been applied to previous plant-wide risk assessments. Sources of reliability data will be identified that can be applied to new advanced technologies which will likely be utilized in new nuclear plant designs.

Reliability data sources/databases are being identified by accessing the internet and using various search engines to locate subject matter via "keyword" searches. Search engines currently being used are Alta Vista, Excite, Metacrawler, and Mamma. Since the use of these engines provides voluminous hits on the web, making identification of relevant information somewhat tedious, the choice of keywords plays an important role in narrowing the number of documents found.

Each source of data will be reviewed and annotated with respect to its applicability to the current effort. Initially this effort will consist of identifying the years of experience, specific types of reliability data collected (raw data versus estimated reliability parameters), characteristics of the reliability data (failure mode, environment, quality level, unavailability versus reliability information, etc.), and applicability of data to meet NERI needs.

Accomplishments

Reliability Data Sources: Searches on reliability data associated with equipment have identified the traditional U.S. nuclear reactor failure rate databases as well several foreign database/publications. Sources of non-nuclear data have also been identified although data sources pertaining to the non-nuclear commercial sector appear to be limited. Keyword searches of the chemical and petroleum industries have turned up little information on equipment reliability databases.

Searches have been performed to specifically identify digital equipment (software/hardware) reliability data. Several publications were identified that contained digital I&C reliability information, however, software reliability data appears to be very sparse. (Many references can be found that discuss methods for evaluating software reliability but there seems to be little data.)

With regard to software reliability, several potential sources of reliability data may exist in either Canadian reactors (CANDU) or British reactors (Sizewell B). There appear to be probabilistic safety assessments performed and documented on these designs. Sizewell B uses a 100,000 line computer code to automate the primary protection system, while some CANDU designs (Darlington) use software that is roughly 20 times smaller in length than the Sizewell B source code. Efforts to obtain references and documents on these systems continue.

The review and applicability of identified sources is underway and applicable sources are being documented in an annotated bibliography, "Reliability Databases/Reports," Appendix B. As noted in Appendix B, reliability data information obtained can be grouped into three categories: nuclear reactor component reliability data, non-reactor component reliability data, and digital system reliability data.

Future activities include additional searching of the internet for identification of software reliability databases as well as further equipment searches, review of these additional potential sources and completion of the annotated bibliography.

Reliability Database: In order to provide an efficient mechanism for users to access and perform statistical analyses using the reliability information identified, a electronic database is necessary. Some years ago the U. S. Nuclear Regulatory Commission sponsored reliability data database development effort called the Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR). Originally, NUCLARR was developed using the Modula-II programming language. Currently, the NUCLARR database is being converted into Microsoft Access format and a new user interface is being developed specifically for the NERI program application. The converted NUCLARR database contains all the information (hardware and human error data) found in the original database (see NUREG/CR-4639), and will be expanded to include the data sources identified through the current effort. The NUCLARR package provides a tool that, with some modifications, will provide an analytical capability (both query capability, data aggregation, and Bayesian updating) to assess the data according to various reliability attributes.

The NUCLARR database is being transformed into a relational database and the existing data is being moved to the new database. The overall database design is 95% complete and the qualitative portion of the database is 90% complete with 85% of the data moved to the new database. The quantitative portion of the database is 10% complete.

Numerical methods for computing the F and Chi-squared distributions have been evaluated for precision and feasibility. These methods will be use to perform initial statistical calculation for verification of existing data and allow for entry of new data.

4.0 Expected Results Next Year

During the execution of Phase 2, the work described in Section 3 will be continued and expanded. The primary focus of the work will be refining and applying the risk-based and regulatory design process and updating the regulatory framework document. The program tasks and subtasks, the following specific efforts and results are planned

Task 1: Development of Risk-Informed Methodologies

- Task 1.1 - The design criteria database prepared at the very end of this year will be reviewed for completeness. Also, commercially available NRC regulatory information resources will be assessed and an evaluation summary will be prepared.

- Task 1.2 - Costs for other plant SSCs to support further sample applications of the risk-informed design process, beyond the Phase 1 sample application to the ECCS, will be determined. A cost summary for an entire plant will be prepared.

- Task 1.3 – An example regulatory "issue" will be defined and a sample regulation will be developed to "test" the new framework. The preferred features of the issue are that it be self-contained, complementary to the design tasks, consider safety margins, and have both active and passive design features. Subjective probabilities will be used for addressing uncertainties. A suggested role for Design Basis Accidents within the risk-informed design will be developed. The regulatory framework document will be updated as development progresses.

- Task 1.4 – The risk-informed design process will be refined and expanded in conjunction with task 1.3 using feedback from sample applications in task 1.6. Development of methods for simplifying design of SSCs for new plants will be continued, including investigation of applicability to designs such as the Pebble Bed Modular Rector (PBMR) and AP1000 designs.

- Task 1.5 - The prioritization process will be refined in conjunction with Tasks 1.4 and 1.6, resulting in a final version of the process.

- Task 1.6 – The ECCS sample application from Phase 1 will be refined (iterated). Additional sample applications will be prepared. The investigation of risk-informed structural design methods will be integrated with the cost-benefit assessments. Design changes that result from the sample applications will be summarized.

- Task 1.7 – The NRC staff review process will continue to be evaluated and an assessment will be made of the feasibility of revising that process to facilitate new design and regulatory process.

- Task 1.8: - The investigators will continue to coordinate activities with ongoing efforts of NEI, NRC, and industry.

Task 2: Strengthen the Reliability Database

- Task 2.1: The lists of reliability data for SSCs was essentially completed in Phase 1, but will be updated as necessary in Phase 2.

- Task 2.2: The weaknesses in reliability data sources will be identified and summarized.

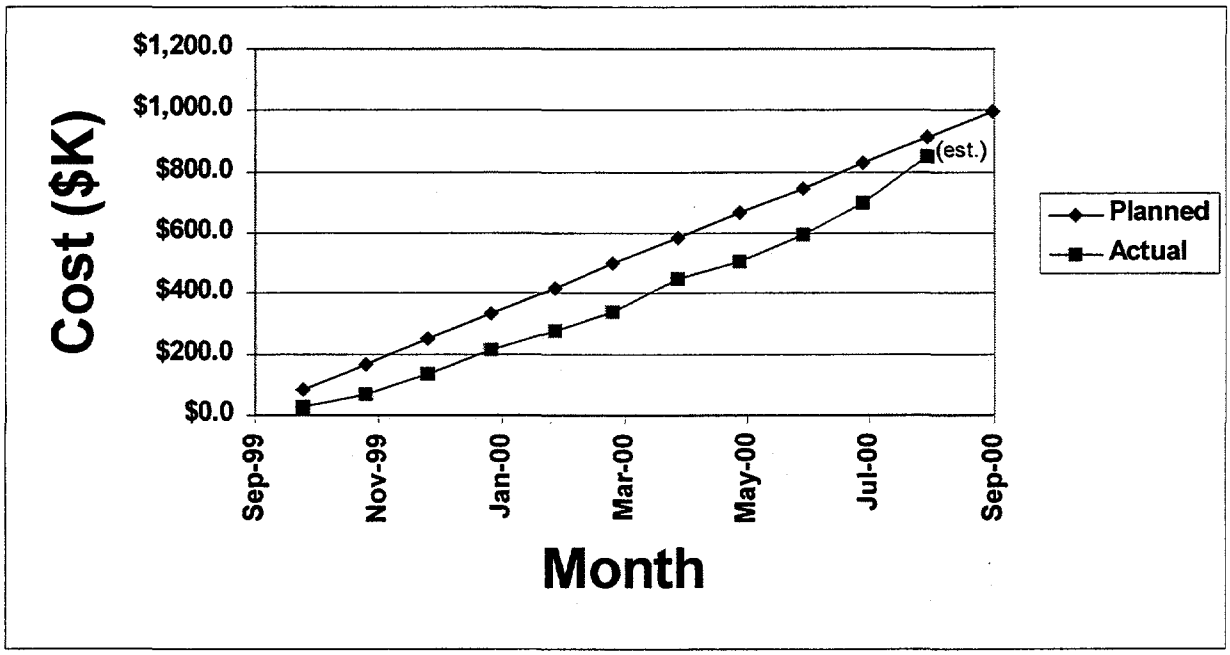
- Task 2.3: Start defining industry/government corrective programs for correcting the weaknesses in reliability data.

5.0 Schedule and Cost Summary

The budget for the Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants project is summarized in the table below.

	WENS	DE&S	Egan	MIT	NCSU	SNL	INEEL	Total
Year 1	$386,993	$113,675	$70,453	$84,763	$59,975	$131,704	$150,382	**$997,945**
Year 2	$319,472	$74,077	$46,260	$130,019	$50,784	$216,345	$192,629	**$1,029,587**
Year 3	$152,446	$37,248	$26,951	$37,217	$24,316	$84,227	$87,099	**$449,504**
Total	**$858,911**	**$225,000**	**$143,665**	**$252,000**	**$135,075**	**$432,276**	**$430,110**	**$2,477,036**

The graph below shows that the actual costs for this project are expected to be "on budget" by the end of Phase 1.



The milestone chart on the next page shows the overall schedule for this project and that task progress is on schedule.

DOE F 4600.3
(03-94)
Replaces EIA-459B

U.S. DEPARTMENT OF ENERGY

FEDERAL ASSISTANCE MILESTONE PLAN

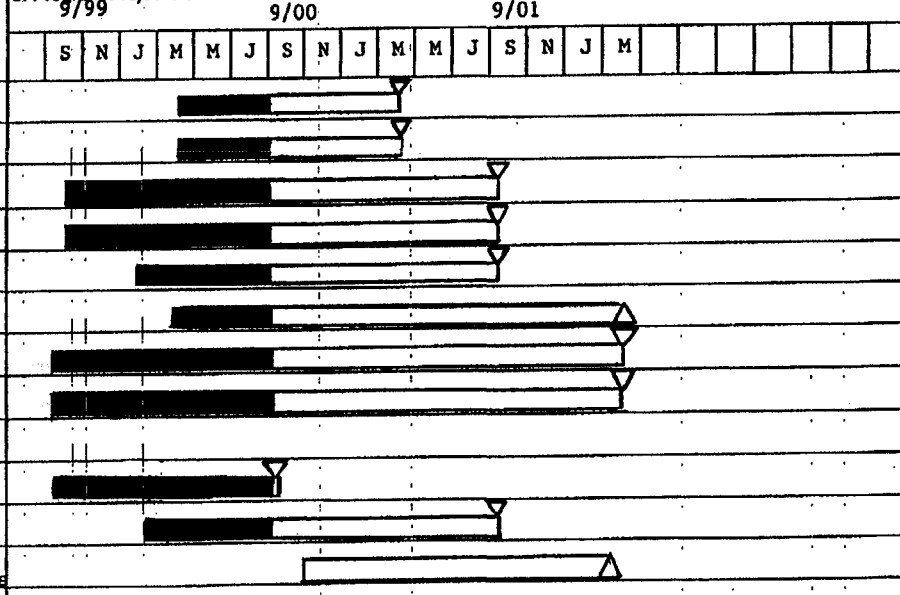
OMB Control No.
1910-0400

OMB Burden Disclosure Statement

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of Information Resources Management Policy, Plans, and Oversight, Records Management Division, HR-422 - GTN, Paperwork Reduction Project (1910-0400), U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, DC 20585; and to the Office of Management and Budget (OMB), Paperwork Reduction Project (1910-0400), Washington, DC 20503.

1. Program/Project Identification No.	2. Program/Project Title
DE-FC03-99SF21902	Risk-Informed Assessment of Design and Regulatory Requirements for NPPs
3. Performer (Name, Address) ABB Combustion Engineering Nuclear Power, Inc. 2000 Day Hill Road Windsor, CT 06095-0500 Attn: PI Stanley Ritterbusch	4. Program/Project Start Date 8/20/99 5. Program/Project Completion Date 3/19/02

6. Identification Number	7. Planning Category (Work Breakdown Structure Tasks)	8. Program/Project Duration (1)	9. Comments (Notes, Name of Performer)
1.1	Identify Reg. Requirements		ABB (2)
1.2	Identify SSCs & Costs		ABB (2)
1.3	Develop Reg. Methods		ABB (2)
1.4	Dev.Simplification Methods		ABB (2)
1.5	Identify Priority SSCs		ABB (2)
1.6	Apply Methods to Sample		ABB (2)
1.7	Evaluate Reg. Process		ABB (2)
1.8	Industry Coordination		ABB (2)
2.1	Identify Data Sources		ABB (2)
2.2	Identify Data Weaknesses		ABB (2)
2.3	Develop Corrective Programs		ABB (2)



10. Remarks
(1) Two months/box (2) ABB is lead organization; collaborating orgs are Sandia, INEEL, MIT, DE&S, NCSU, Egan & Associates

11. Signature of Recipient and Date	12. Signature of U.S. Department of Energy (DOE) Reviewing Representative and Date
S.E. Ritterbusch 7/31/00	

Printed with soy ink on recycled paper

Appendix A

Project Participants

Appendix A
Project Participants

The team for this project comprises the following representatives from industry, labs and universities:

- Westinghouse Electric Company, Nuclear Systems (WENS), as the lead organization, provides overall coordination and project management. It also provides expertise on the design and analysis of systems for nuclear plants and the licensing of nuclear plants.

- Sandia National Laboratories (SNL) provides expertise in risk methodology development, especially as it affects structures, low power and shutdown operations, fire risk, and object oriented risk and reliability analysis methodology.

- Idaho National Engineering & Environmental Laboratory (INEEL) provides expertise in risk methodology development, risk analysis tool development, and data collection and assessment methodology development.

- Massachusetts Institute of Technology (MIT) provides expertise in structuring the approach to risk-informed, performance-based regulation and the strategy for building the needed PRA database.

- North Carolina State University (NCSU) provides expertise in aging and structural analysis.

- Duke Engineering and Services (DE&S) provides expertise on the design and construction of systems and structures for nuclear plants and the evaluation of performance data.

- Egan & Associates, P.C. provides expertise in nuclear law, nuclear licensing and nuclear regulation.

The participants in this project are currently involved – or have recently been involved -- in a number of ongoing studies related to PRA and risk-informed assessments. These activities will provide a substantial base of experience from which to launch the proposed research project. The recent and current activities of each team member, which are relevant to the proposed research, are summarized below.

Westinghouse Electric Company, Nuclear Systems(WENS)

WENS has made extensive use of reliability analysis and PRA methodology in the design and licensing of its nuclear steam supply systems and has supplied risk assessment services to the power generation and chemical processing industries. The projects that WENS has conducted include:

- Providing Level 1 - Level 3 PRA support to individual utilities and to the Combustion Engineering Owners Group for their Individual Plant Examination (IPE) Studies

- Providing PRA-based licensing and operational support to PWR and BWR owner utilities
- The performance of a Level 3 PRA for the System 80^+ ALWR design, in support of Design Certification. This included extensive review by the NRC.
- The performance of a Level 1 PRA for the Korea Electric Power Company (KEPCO), Yonggwang Units 3 & 4.
- Availability analyses for five different fluidized bed combustion fossil power plant designs.
- The performance of Reliability Availability and Maintainability (RAM) analyses on several chemical production plant designs
- The performance of RAM analyses for the preliminary design of DOE's Heavy Water New Production Reactor design.
- The assembly of fire risk assessments for several DOE weapons lab facilities for the purpose of evaluating the cost/benefit impact of various fire protection system design changes

WENS has been a leader in risk-informed regulation since the mid-1980s when WENS, under the auspices of the Combustion Engineering Owners Group (CEOG), prepared and submitted a topical report justifying an increase in the surveillance test interval for selected Plant Protection System components based on risk-benefit arguments. Since 1993, WENS has been working with the CEOG and the NRC in developing risk-informed bases for reducing technical specification requirements such as allowed outage times and end states. In these activities, WENS and the CEOG pioneered the use of Joint Application Reports to demonstrate the risk/benefits of a proposed risk-informed change over a spectrum of plants from the CE fleet. As part of the work related to the risk-informed applications, WENS has been performing cross-comparisons of the CEOG member PRAs at increasing levels of depth and has been developing PRA standards and position papers for the CEOG members. WENS has worked with the other Owners Groups to develop a PRA Certification/Peer Review Process and is currently in the process of implementing this process for the CEOG plants.

WENS has also helped develop methodology for Risk-Informed In-service Testing (RI-IST). WENS provided one of the two white papers demonstrating the applicability of the ASME's risk-informed IST methodology for the OMN-3 and the OMN-CV code cases.

Additionally, WENS worked with EPRI and DE&S to develop the EPRI approach to a Risk-Informed In-Service Inspection (RIISI) program for piping systems that is the subject of two new ASME code cases, as alternatives to the current ASME Section XI approach.

Appendix A
Project Participants

WENS is currently involved in the ASME process to develop an ASME standard on Risk Assessment for Nuclear Power Plant Applications and WENS has been providing support to NEI's Risk-Based Applications Task Force (RBATF).

Sandia National Laboratories

Current activities at Sandia stem from its broad-based safety research for the NRC, DOE, and other organizations in the areas of probabilistic risk assessment. The following paragraphs provide a summary of the many relevant technical areas in which Sandia is currently involved or has recently been involved. Besides applications to commercial nuclear energy plants, Sandia is involved in a number of PRA activities in defense and other industries.

Level 1 PRA – Sandia has been involved in the development of systems analysis technology, including methods for internal and external events and all modes of operation. Methods for modeling hardware failure, human reliability, common cause failures, and other aspects affecting core damage frequency have been developed. Cost-benefit studies have been performed to resolve issues affecting service water systems, control circuits, and decay heat removal systems.

Current projects include:

- Technical support for the development of consensus PRA standards by the American Society of Mechanical Engineering.
- Development of Risk-Informed In-service Inspection Methodology.
- Technical support for modification of key parts of 10CFR50.
- Identification and Resolution of Issues Associated with Low Power and Shutdown Operation.
- Development of a new human reliability analysis methods.

Level 2 PRA – Sandia developed the NUREG-1150 Level 2 PRA methods that currently represent the state of the art. These methods have been applied to a number of plants and can account for a wide range of plant systems responses, accident progression scenarios, structural responses, and fission product behavior. A number of software tools have been developed to assist in these analyses. Sandia is currently working with INEEL to develop simplified approaches for future analyses of accident precursors.

Level 3 PRA – Sandia has developed the MACCS code, which is currently the most commonly used code for offsite consequence analysis. MACCS can calculate a wide range of consequence measures, including health effects and economic consequences. Sandia has provided technical expertise to support a joint multi-year NRC/European Commission effort to systematically develop credible and traceable uncertainty

distributions for input variables to accident consequence codes that can be used to support risk-informed regulatory decisions. Methods for integrating the three levels of PRA have also been developed and applied to numerous plants to estimate overall risk and to examine the importance of particular contributing factors. Integrated uncertainty analysis techniques have also been developed

Fire – Sandia is currently working on projects that will make improvements in fire risk assessment. Examples include: (1) developing new analysis tools, (2) developing models to predict smoke damage to electrical equipment that occur during and immediately after a fire, and (3) the collection and characterization of experimental data relevant to fire research.

Nuclear Weapons – Sandia has been involved in research on critical issues regarding the safety of accelerator production of tritium and commercial light water reactor options to produce tritium for the weapons complex in the next century. As part of its science-based stockpile stewardship initiative, Sandia is increasing its analytical capability to evaluate the risks of inadvertent nuclear detonation and of plutonium dispersal. As part of these activities, Sandia has developed the ARRAMIS PRA software package and is developing advanced object oriented software tools.

Other PRA Programs – Sandia has had or currently has major PRA programs in the areas of transportation of nuclear and other hazardous cargoes, commercial aircraft, nuclear power, chemical weapons disposal, telecommunications, and electric power grid reliability.

Idaho National Engineering & Environmental Laboratory

Currently, INEEL is working closely with the U.S. NRC on a number of risk-informed performance-monitoring activities. These efforts include a new multi-year program to develop a set of risk-informed performance indicators to replace those developed in 1986 and presently in use. An essential part of the NRC's new risk-informed monitoring effort is having a set of performance indicators that are risk-informed and reflect safety performance of the plants at a high level, while allowing for NRC action to respond to performance problems before undue risk to the public occurs.

INEEL is also developing the NRC's reliability database. The Reliability and Availability Database System (RADS) will extract data from various sources, and allow manipulation and analysis of the data to support NRC risk-informed regulatory activities. The Equipment Performance Information Exchange (EPIX), the new Institute of Nuclear Power Operations (INPO) database (replacing the Nuclear Plant Reliability Data System [NPRDS]), will be primary source for RADS data. Also included will be data from NPRDS (archived data), Licensee Event Reports (LERs), Monthly Operating Reports (MORs), and INPO's Safety System Performance Indicator (SSPI) program.

For the past four years (and continuing), INEEL staff has been collecting and analyzing specific safety system reliability data under an NRC program aimed at tracking system reliability performance for selected systems at U.S. commercial nuclear power plants. These system reliability studies have focused on emergency diesel generators (all U.S.

LWRs), high pressure core spray (BWR), high pressure coolant injection (BWR), reactor core isolation cooling (BWR), isolation condenser (BWR), auxiliary feedwater (PWR), high pressure safety injection (PWR), reactor protection systems (PWR and BWR), and potential core-damage accident sequence initiating events. The raw-data is collected primarily from LERs, but also includes information from MORs and NPRDS. Each system is studied on an industry-wide scale, plant-specific basis, and from a year-to-year perspective.

The Accident Sequence Precursor (ASP) program is a NRC sponsored effort with the objective of producing standardized plant-risk analysis models for every LWR in the U.S. These models are used by the NRC on a routine basis for evaluating the safety significance of operational events (i.e. precursors) occurring in the nuclear power industry. Using risk models that are standardized across the entire industry facilitates risk evaluations among plants (i.e. differences in results are not caused by different modeling approaches or assumptions). INEEL has developed these models and is in the process of improving and expanding them to include external event capabilities and Level-2/3 modeling (i.e., containment performance and radiological health consequences).

The System Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE) is a set of four computer programs developed at INEEL under the sponsorship of the NRC. These programs were developed to create and analyze PRAs. Development began in the mid-1980's with version 1.0 of the Integrated Reliability and Risk Analysis System (IRRAS, one of the programs comprised by SAPHIRE). Current refinements underway include the capability to integrate Level-2/3 models with the Level-1 PRA models (i.e., core damage frequency modeling). In addition, SAPHIRE includes the capability of including external event analyses (including seismic).

Duke Engineering & Services

DE&S has worked with EPRI to develop an EPRI approach to a risk-informed inservice inspection (RI ISI) program for piping systems that is the subject of two new ASME code cases as alternatives to the current ASME Section XI ISI approach. In this approach, an inservice inspection program is optimized based on the risk assessment of pipe ruptures in each system that is subjected to the evaluation. Risk is defined as a combination of the potential for pipe rupture and the consequences of such a rupture. Pipe rupture potential is related to the degradation mechanism pipe is exposed to. Rupture consequences are related to the conditional probability of a serious accident given the occurrence of a rupture.

The new RI ISI program reduces the number of inspections, cost of implementation, and workers exposure, while maintaining or reducing the total risk associated with pipe ruptures. This is accomplished by redirecting the inspections to the highest risk locations.

Two new ASME code cases based on the EPRI RI ISI methodology are:

1. Code Case N578, which applies to ASME Class 1, 2, 3, and NNS piping, and

2. Code Case N560, which applies to Class 1 piping.

One of the Code Case N578 pilot plant applications, Arkansas Nuclear One (ANO) Unit 2, was approved by the NRC in December of '98. Two pilot plants, ANO Unit 1 and Vermont Yankee applied Code Case N560. Vermont Yankee received approval in November of '98. ANO Unit 1 is currently in the review process.

Massachusetts Institute of Technology

Professors of MIT have published numerous papers in the areas of technological risk and reliability assessment and management. Their current research areas include risk-informed and performance-based regulation, risk management involving multiple stakeholders, the influence of organizational factors on safety, and software dependability.

Professor Apostolakis is a member of the statutory Advisory Committee on Reactor Safeguards (ACRS) of the US Nuclear Regulatory Commission. As the chairman of the ACRS Reliability and Probabilistic Risk Assessment Subcommittee, he worked very closely with the NRC staff in formulating the structure of the pioneering Regulatory Guide 1.174, "An Approach for Using PRA in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis." His support was instrumental in getting the risk-informed Graded Quality Assurance plan submitted by the South Texas Project approved by the Commission. He is currently actively involved in the revision of the Senior Management Meeting process and the development of a human reliability program plan for the NRC (he also chairs the Human Factors Subcommittee). He is also the Editor-in-Chief of the International Journal *Reliability Engineering and System Safety*, and a member of the editorial board of the journal *Process Safety and Environmental Protection (Transactions of the Institution of Chemical Engineers).*

MIT organized the first two International Conferences on Probabilistic Safety Assessment and Management (PSAM) in Beverly Hills (1991) and San Diego (1994). The PSAM conferences are held biennially and are the major international meetings on the use of probabilistic methods to assess and manage the risks from major technological systems and processes, such as chemical and petroleum facilities, nuclear plants, defense systems, and waste repositories.

North Carolina State University

Professors of NCSU's Civil Engineering Department are developing mechanistic models for evaluating accurate behavior of structural systems in nuclear power plants. They are also developing a better understanding of the component failure modes. Information on mechanistic behavior and failure modes is an essential input needed in the risk assessment studies. The objective is to develop technologies that give realistic behavior, are simpler and eliminate much of the uncertainty associated with structural behavior in the presently used methods. Therefore, the new methods will enhance reliability, reduce excessive conservatism, and reduce construction and operating costs. Some of the developments are either completed or at an advanced stage, while work on others has just

started. Technology related to one the products, CREST program, is being studied by the USNRC. Following is a list of project topics on which NCSU researchers are either currently working or have worked on recently.

Coupled Piping-Building Systems: The computer program CREST is used to accurately evaluate seismic forces in piping systems which may be up to an order of magnitude lower than those calculated using conventional techniques. CREST requires information on modal properties of uncoupled building and piping systems and performs a coupled piping-building system analysis.

B_2 Index Values: Tables for numerous stainless steel elbow sizes and schedules are evaluated using the ASME Code allowed nonlinear finite element analyses. Guidelines are provided for using a nonlinear analysis to calculate the index values for other sizes, schedules and materials.

Material Model for Ratcheting in Piping Components: A computer program, RATCHET, with a new cyclic plasticity model has been developed at the Center and validated against experimental results. The program works with ANSYS and evaluates realistic ratcheting phenomena in piping components.

Unanchored Objects: Charts and tables have been developed to determine if an object would rock or slide, probability of overturning or safe acceleration level for a given probability, and mean plus one standard deviation sliding distances. Computer programs ROCK and SLIDE predict rocking and sliding behavior of unanchored objects such as scaffolding when subjected to earthquake ground motion. In the future, shake table testing will be conducted to validate the analytical model.

Electrical Cabinets and Control Panels: A computer program, INCABS, has been developed to evaluate cabinet dynamic properties and realistic in cabinet spectra with limited information on significant structural members without a finite element model. The computer program implements a Ritz vector approach, developed at NC State and validated against the test data.

Fatigue Failure of Piping Weld Connections: Comparison of various sets of fatigue test data in literature, reasons for variation in the fatigue strength from different tests, examination of data in the context of ASME mean fatigue curves, and evaluation of stress intensification factors and plastic intensification factors K_e for welded components in piping systems.

Egan & Associates

Egan & Associates has recently been involved in a number of issues related to the licensing of new facilities, risk assessment in the regulatory context, and performance-based regulation. The firm is a longstanding member of NEI's ALWR Regulatory Working Group.

The firm was lead counsel in the NRC design certification of WENS's System 80+ ALWR, and worked extensively with NEI, DOE, and NRC on innumerable issues associated with Part 52, the future of nuclear power, and the licensing of advanced plants. One issue extensively dealt with was PRA generally, and the plant-specific PRA in particular.

One member of the firm, Mr. Malsch, served for over fifteen years as Deputy General Counsel and Acting General Counsel of the NRC. During that time, he was responsible for review of all adjudicatory licensing decisions of the Atomic Safety and Licensing Boards and Appeal Boards, for all adjudicatory licensing decisions of the Commission itself, including the Commission's decisions authorizing operation for Shoreham, Seabrook, Diablo Canyon, and Three-Mile Island Unit 1 (restart), and for the legal review of all NRC regulations.

While at NRC, Mr. Malsch originated the design certification concept in 10 CFR Part 52, was responsible for the development of the design certification and combined licensing rules in 10 CFR Part 52, and served as NRC's lead attorney in the initial design certification reviews for the WENS and GE standard designs.

Mr. Malsch served as lead NRC attorney in the development and promulgation of the NRC safety goals for nuclear power reactors, and in the use of the safety goals in implementing the backfit rule (10 CFR § 50.109).

Mr. Malsch originated the legal and regulatory concepts which formed the basis for the backfit rule, and which allowed the commission to distinguish between measures which are necessary for safety (adequate protection) and measures which are discretionary additions to safety.

Prior to leaving the NRC in 1997, Mr. Malsch served as a member of NRC internal task forces on use of quantitative safety goals, use of probabilistic risk assessment and risk-informed regulation, and was extensively involved in all NRC licensing and hearing process reforms, including amendments to the Atomic Energy Act and reforms of 10 CFR Parts 2 and 50. He also participated extensively in NRC reviews of the use of expert elicitation, especially its application in seismic design reviews and high-level waste repository performance assessment.

Appendix B

Publications and Reports

Appendix B
Publications and Reports

The publications and reports issued during the first phase of the project for Risk Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants, and included in this appendix, are:

- "Reliability Databases and Reports," Idaho National Engineering and Environment Laboratory, July 24, 2000.
- "Probabilistic Safety Assessment and the Regulatory Process: Analysis of Necessary Changes," Egan & Associates, July 12, 2000.
- "A Framework for Risk-Based Regulation and Design for New Nuclear Power Plants," Sandia National Laboratory and Massachusetts Institute of Technology, July, 2000.
- "A Framework for Regulatory Requirements and Industry Standards for New Nuclear Power Plants," paper presented at the PSAM5 Conference, Fall 2000.
- "Nuclear Energy Research Initiative - An Overview of the Cooperative Program for the Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants," paper presented at the Korea Atomic Industrial Forum Conference, April, 2000.

Reliability Databases and Reports

Appendix B
Reliability Databases and Reports (Draft)

CONTENTS

Appendix B
Reliability Databases and Reports (Draft)

Acronyms

ALWR	Advanced Light Water Reactor
ASEP	Accident Sequence Evaluation Program
CANDU	Canada Deuterium-Uranium
CCF	Common Cause Failure
CCPS	Center for Chemical Process Safety
CFR	Code of Federal Regulations
D-in-D&D	Defense-in-Depth and Diversity
EPIX	Equipment Performance and Equipment Exchange
GIDEP	Government-Industry Data Exchange Program
HEP	Human Error Probability
I&C	Instrumentation and Control
INPO	Institute of Nuclear Power Operations
IPE	Individual Plant Examination
LER	Licensee Event Report
NERI	Nuclear Energy Research Initiative
NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission
NUCLARR	Nuclear Computerized Library for Assessing Reactor Reliability
OREDA	Offshore Reliability Data
PLC	Programmable Logic Controller
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
RAC	Reliability Analysis Center
RADS	Reliability and Availability Data System

SCSS	Sequence Coding and Search System
SSC	System, Component, Or Structure
SSPI	Safety System Performance Indicator

Terminology

Commercial-grade SSCs —SSCs that were not designed and manufactured under a quality assurance program complying with Title 10 CFR Part 50, Appendix B.

COTS– Commercial-of-the-shelf item

Dependent failure—Two events are statistically dependent if the $Prob(A \cap B) = Prob(A)\ Prob(B|A) = Prob(B)\ Prob(A|B) \neq Prob(A)\ Prob(B)$.

Independent failure—Two or more events are statistically independent if $Prob(A \cap B) = Prob(A)\ Prob(B)$.

Maintenance unavailability—Probability that a system is out of service for maintenance at any instant in time.

Nuclear grade SSCs —SSCs that meet the criteria specified in Title 10 CFR Part 50, Appendix B.

Operating experience—A term used to represent the industry operating experience (demands, failures, and faults). It is also referred to as operational data, operating data or industry experience.

PLC—programmable logic controller.

PRA/IPE—A term used to represent the data sources (PRAs, IPEs, and NUREG reports) that describe plant-specific system modeling and risk assessment, rather than a simple focus on operating data.

Reliability—The probability of a component or system to perform a required function under stated conditions for a stated period of time. Typically computed as one minus the unreliability.

Unreliability—Probability that the system will not fulfill its required mission under stated design conditions.

Appendix B
Reliability Databases and Reports (Draft)

Introduction

Risk-informed analysis is becoming a part of the regulation process of the licensing of U.S. commercial nuclear power plants. In order to minimize the cost of new nuclear power plants, risk-informed analysis is being applied to the design stage in an attempt to simplify new designs. The use of risk-informed analysis in the design stage may eliminate the deterministic standards and regulatory requirements that do not significantly contribute to reliability and safety. A research project entitled "Risk Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants", funded by the U.S. Department of Energy Nuclear Energy Research Initiative (NERI), addresses this topic. The project will use probabilistic risk assessment (PRA) tools to evaluate all of the regulatory requirements and industry standards from a cost-benefit (risk impact) approach in order to simplify future designs. The risk-informed assessment process requires an equipment reliability database that is defensible. Although there are significant equipment reliability and performance data available from existing nuclear power plants to support the risk-informed assessment of future designs, data to support new equipment technologies need to be identified. Where risk-informed assessment data are not currently available, methods and programs need to be developed. This report provides an annotated list of potential sources of reliability data to support the risk-informed design assessment.

Data Requirements for PRA

The risk-informed design assessment will identify systems, structures, and components (SSCs) that can be simplified in order to reduce costs associated with new power plant designs. The proposed simpler SSCs will require evaluation of the SSCs reliability and risk impact. The reliability and availability parameters required in the PRA models are defined in the following equation for component total unavailability.

For standby component unavailability

$$Q_{Total} = q_d + \tfrac{1}{2} \lambda_s T_{test} + q_{planned} + q_{unplanned}$$

where: Q_{Total} = component total unavailability

q_d = component failure probability on demand (due to demand-related stresses)

$\tfrac{1}{2} \lambda_s T_{test}$ = component failure rate from standby or environmental stresses

T_{test} = component test interval

$q_{planned}$ = component unavailability due to planned maintenance

$q_{unplanned}$ = component unavailability due to unplanned maintenance (i.e., repair).

For operating components (e.g., pumps, motors, diesel generators, control valves, etc.) the mission reliability needs to be accounted for in the component unavailability equation

$$Q(T_{mission}) = 1 - \exp(-\lambda_{run} T_{mission})$$

where: λ_{run} = component failure rate while in operation

$T_{mission}$ = time the component operates to mitigate an accident.

For PRA modeling of redundant components, the common cause failure probability (q_{ccf}) needs to be factored into the unavailability equation.

The data sources described below are reviewed for their applicability to the component unavailability equations defined above.

Sources of Data

This report is an annotated bibliography of nuclear, non-nuclear, and foreign data sources that are currently available or under development. The sources of data include computerized databases, databases that are supplemented with reports, and reports that include data that may or may not be computerized.

Nuclear Reactor

Reliability and Availability Data System (RADS)

The U.S. Nuclear Regulatory Commission (NRC) initiated rulemaking requiring licensees to submit reliability and availability data to the NRC for most risk-significant SSCs. In response, the nuclear industry proposed a voluntary alternative to the rule. The proposed alternative is based on the Equipment Performance and Information Exchange (EPIX) system which provides component failure and demand data for a broad scope of systems and the Safety System Performance Indicator (SSPI) system which provides train unavailability data within its scope. [The EPIX system is intended to replace the Nuclear Plant Reliability Data System (NPRDS).]

To support NRC in risk-informed decision making, NRC is developing a database comprised of data from the SSPI system and the EPIX system. The NRC data system is called Reliability and Availability Data System (RADS). In addition to these data, the RADS database will contain other data (e.g., LERS) available to NRC. Other inputs to the database will be from UNITINFO (general plant information, e.g., reactor type, low and low power license dates, defueling dates, etc.), OUTINFO (outage dates), MORP1 (critical hours obtained from the monthly operating reports), and MORP2 (monthly outage information) databases maintained by the INEEL

RADS will be a source of plant-specific and generic component reliability data and train or component availability data. These data are intended for use in probabilistic risk assessment and risk-informed applications. RADS will contain key components in the risk-significant systems as defined by each utility in implementing the Maintenance Rule. It is estimated that there will be approximately 1000 key components per unit. For each key component, the demand failure probability, standby failure rates, operating failure rate, unplanned unavailability, planned unavailability, total unavailability, and concurrent train unavailability resulting from unplanned maintenance will be estimated. Software will provide both point estimates and confidence bounds, tests of homogeneity, trending analysis, Bayesain estimation capabilities, as well as identification of common cause failures.

By default, each parameter of possible interest will be estimated in a classical way, with a point estimate and confidence limits. They also will be estimated in a Bayesian way, with the Jeffreys noninformative prior as the default prior distribution. If the data set includes multiple plants or systems, the program will examine possible heterogeneity, and will try to perform an empirical Bayes analysis, yielding plant-specific or system-specific estimates.

At the user's request, the software will identify all multiple events involving hardware in the selected data set at a single plant, discovered within a user-specified time span. These groups of candidate common-cause events will be available for the user to browse, to save to a file, or to print.

The database will preserve the security of the proprietary data (EPIX and SSPI) per NRC/INPO agreement. NRC authorization is required for access to the database. Users will access RADS (residing on NRC servers) from a PC. An operating version of the RADS software and database is scheduled to become available in May 2000.

In a study (Lofgren 1997) evaluating the viability of SSPI and EPIX systems to support NRC's risk-informed analyses, it was concluded that most of the PRA risk parameters needed to implement risk-informed regulation can be estimated from the data residing in the SSPI and EPIX databases.

NPRDS

The Nuclear Plant Reliability Data System (NPRDS) is a computerized database of engineering, operational, and failure data on systems and components installed in U.S. nuclear plants. (The EPIX system described below will replace NPRDS.) INPO has been responsible for this database since 1982. The NPRDS acquires data through a voluntary approach. Further, the degree of reliance on the statistical data generated from NPRDS data is dependent on the consistency and completeness of reporting by individual contributors.

NPRDS data is available to INPO members, participant organizations, USNRC, and certain other industry organizations through on-line searches of the database. Since NPRDS is being phased out by the EPIX system and the data is proprietary, the availability of these data is limited for future applications.

EPIX

Equipment Performance and Information Exchange (EPIX) system is maintained by the Institute of Nuclear Power Operations (INPO). EPIX was designed for the industry. EPIX provides information about components in the risk-significant systems as defined in the Maintenance Rule. The Maintenance Rule, 10 CFR 50.65, "Requirements for monitoring the effectiveness of maintenance at nuclear power plants," is a risk-informed, performance-based rule that requires licensees of commercial nuclear power plants to monitor the effectiveness of maintenance of certain SSCs that are within the scope of the rule.

The scope of the information collected in the EPIX database includes all equipment within the scope of the Maintenance Rule. Data from this system includes unplanned equipment unavailability, failure rates, and numbers of repetitive maintenance-preventable functional failures.

This is a database of root cause information on failures and on equipment failures that cause power reductions. The database provides failure rate and reliability information for a limited number of important plant components. EPIX is an infant system (utilities began submitting data in 1997). Data is reported on a component level in order to calculate failures per demand and failures per operating (run) hour. EPIX has the capability to link a component to its functions, system, and train and collects the consequences of the component failure for all three.

EPIX data is available to INPO members, participant organizations, USNRC, and certain other industry organizations through on-line searches of the database.

Findings of an evaluation (Lofgren, 1997) of the EPIX system data with respect for supporting NRC's application to risk and reliability data state that EPIX data provides sufficient information to estimate demand failure probabilities for all components of interest.

SSPI

The Safety System Performance Indicator (SSPI) system is a joint project of INPO and World Association of Nuclear Operators (WANO). It is maintained by INPO. SSPI gives information about trains in the risk-significant systems as defined in the Maintenance Rule. It contains train level failure, outage time (both planned and unplanned), and demand information for four systems (High Pressure Injection, Decay Heat Removal, Residual Heat Removal, and Emergency ac Power). Components and trains within these systems are referred to as SSPI-scope components and trains.

Lofgren concludes SSPI data provides sufficient information to estimate unavailability at the train level for systems within its scope. No system level information outside SSPI scope is provided. Lofgren further states that SSPI data does not provide sufficient information to estimate demand failure probabilities for all components, especially valves. Other technical issues reported by Lofgren include estimation of planned outage unavailability for risk-significant, non-SSPI components and estimation of operating failure rates for normally standby, rotating equipment.

SCSS

Sequence Coding and Search System (SCSS) is a system for storing, retrieving, and analyzing commercial nuclear plant operating experience data as described in Licensee Event Reports (LERs). LERs are submitted to the Nuclear Regulatory Commission (NRC) by Licensees in response to reporting requirements as defined in the Code of Federal Regulations for events occurring at our nation's commercial nuclear power plants. LERs are then analyzed and coded by staff of the Nuclear Operations Analysis Center (NOAC) at the Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee. The coded LERs are entered into the SCSS database and made available for subsequent studies and analysis.

The SCSS Web site provides easy to use, on-line access to information stored in the SCSS database and facilitates the exchange of information associated with LERs. The SCSS Web site and SCSS database are maintained and operated by the NOAC and sponsored by the NRC's Office of Nuclear Regulatory Research (RES). The SCSS database is NRC's official database for LERs.

The SCSS database currently stores over 43,000 LERs submitted since 1980. In addition to the full text of an LER, the SCSS database stores two primary types of LER information as follows: 1) LER Header information and 2) LER Coded Event information. NOAC analysts reduce LER descriptive text to coded, searchable, time-ordered sequences of Coded Events which are stored in the SCSS database. SCSS provides a tool for retrieval of LER information based on a flexible search engine that can even identify specific time-ordered event sequences. Information provided by SCSS is used to report and identify conditions related to safety including actuations of safety equipment, degraded conditions in systems important to safety, and violations of plant technical specifications.

In addition to the LER Header information, events described in an LER are analyzed, coded, and linked in an event-tree format to create a time-ordered sequence of Coded Events. This time-ordered sequence of Coded Events is stored in the SCSS database in a manner that allows retrieval of LERs containing two (or more) specific events where the events occurred in a specific order. LER Coded Event information being stored in the SCSS database include:

Personnel Activity Events: Type of activity being performed (testing, maintenance, etc.), type of personnel involved (licensed, non-licensed, contractor, etc.), cause and effect of personnel error

Equipment Failure Events (Components, Trains/Channels, Systems): Type and number affected, cause and failure mode, effect of failures on plant systems and unit, component vendor and model data (if given in the LER) .

Nuclear industry organizations and the general public can obtain information from the SCSS on a cost recovery basis by contacting the Oak Ridge National Laboratory.

Although the SCSS is a good source of raw failure information related to safety systems, care should be exercised when using this data. A safety system, and any occurrences in which the safety system was not fully operable, as defined by plant technical specifications, are required by 10 CFR 50.73 to be reported in LERs. However, because some safety system consists of redundant trains, not all train level inoperabilities are captured in the LER data. Specifically, a plant is not required to report a single train inoperability unless the malfunction resulted in a train outage time in excess of technical specification allowable outage times, or resulted in a unit shutdown required by technical specifications. Otherwise, any occurrences where a train was not fully operable would not be reported. For example, no LER would be required to be submitted if, during the performance of a surveillance test, a pump failed to start but the redundant train(s) were operable and the cause of the failure to start was corrected with operability restored prior to expiration of the technical specification limiting condition for operation. This reportability requirement effectively removes any surveillance test data from being considered for the unreliability estimate except for those safety systems that do not have redundancies. However, for ESF actuations, all component failures that occurred as part of the ESF actuation are reportable by LER as required by 10 CFR 50.73(b)(2)(ii). Further, all ESF actuations are reportable as required by 10 CFR 50.73(a)(2)(iv).

NUCLARR

The Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) was developed for the USNRC, to collect human reliability and hardware failure data for risk analysis in the late1980's. NUCLARR is a data repository, with automated functions for retrieval and output by the individual user. This IBM-compatible databank, on a set of floppy diskettes, includes data files and a menu-driven system for data location, review, sorting, and retrieving. It has over 100 help screens to assist the user in navigating through the menu-driven software program. NUCLARR contains 1,400 records of hardware failure and 1,100 human error probability (HEP) records. Volume 5 of NUCLARR (NUREG/CR-4639) is a hard copy of the data and related information residing on the software Version 3.5 of the NUCLARR database.

The hardware data primarily consists of actual catastrophic failures. That is, the equipment failure required repair, replacement, or adjustment to return it to service. Equipment being unavailable as a result of human error is included in the HEP portion of the NUCLARR system. Equipment failures resulting from support system failures or improper inputs are not included in

the failure rate since they are generally modeled separately in PRAs. For operating equipment, failures had to occur during equipment operation and not, for example, during a pre-operational test.

The NUCLARR data are primarily from the public domain with some proprietary information specially coded to maintain source anonymity. The sources of data include data from probabilistic risk assessment reports (PRAs), human reliability analyses (HRAs), and plant operating experience. The time frame for these published sources of data is 1980 through 1992. The equipment taxonomies and data structures for NUCLARR were designed for PRA techniques that were in use at the time the database was developed.

The HEP and hardware data, respectively, involve the following data categories:

HEP Data: Job Title (e.g., Equipment Operator), Human Action (e.g., Monitor), Equipment Involved, Type of Error (Omission, Commission), Recovery (considered or not considered in calculating the HEP), Performance Shaping Factors, Origin of Data, HEP (Mean/Median), Upper and Lower Bounds, Statement of Error, Conditions, and Additional Information

Hardware Failure Data: Component and Design (e.g., motor operated valve), Normal State (e.g., normally standby), Failure Mode, Component Applications, Originating Facilities, Systems Involved, Failure Rate (mean/median; hourly/per demand), Upper and Lower Bounds, Statement of Conditions and Additional Information

NUCLARR also provides statistics for aggregated data sets. Volume 5 (Reece et.al 1994) includes the results of aggregated data sets from like components or human action and equipment combinations. NUCLARR stores demand-based and hourly failure rates. Other data needed for estimating PRA parameters are not available. Failure rates are treated as random variables that are log-normally distributed.

The NUCLARR system is documented in the 5-volume series NUREG/CR-4639. A Quick Reference User's Guide is also available to give guidance on the current version of the software in a condensed and easy-to-use format. There was a NUCLARR Users Group but has been disbanded when program funding was terminated in 1994.

D. I. Gertman et al., "Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)," U.S. Nuclear Regulatory Commission, NUREG/CR-4639, June 1989.

European Industry Reliability Data Bank: EIReDA 1998

Third edition of a reliability data bank of nuclear power plants operated by Electricte de France from 1978 to 1995. Comprised of estimates of reliability parameters, failure rate, failure probability for 133 components (e.g., pumps, tanks, valves, motors, sensors, etc.). Bayesian estimates: prior based on operational experience form 1978 to 1987 and updated on data collected from 34 power plants (1988-1993). Estimates are compared to data compiled from other sources (other power plants, modern petrochemical and processing plants). Engineering and operational characteristics and the maintenance to which components are submitted, a description of the sample from which the estimates were calculated, a color photograph and a general drawing and the boundaries of each component are given. Hardcopy and PC versions are available. The data bank is a joint publication of the European Commission and Electricite de France.

ISBN 2-9509092-0-5, pp. 350.

Retail Price: $765 US

T-Book 3rd Edition- Reliability Data of Components in Nordic Nuclear Power Plants

The book provides reliability data for unavailability calculations that are done for components defined in probabilistic safety assessments. The failure data is based on failure reports stored in a central database ATV (jointly owned reliability data system) and Licensee Event Reports delivered to the Swedish Nuclear Power Inspectorate (SKI). The data is comprised only of critical failures, i.e., failures that prevented the component from functioning or lead to repair. The data in the T-book includes data up to operating year 1987 (108 reactor years comprised of eleven BWRs and three PWRs).

Reliability data are presented for pumps, valves, rod drivers/control rods, instruments, and electrical components. Figures of the physical boundaries of the components are provided. The pump component is divided into three main categories: centrifugal, reciprocating and screw. Further subdivisions of the classifications are provided [e.g., turbine-driven, operational mode (operating, intermittent, and standby), horizontal/vertical, etc.]. The valve component is classified by function (e.g., isolation, control, check, etc.). Further subdivisions of the valve by type (ball, gate, seat) are provided. Instruments are classified by the parameter being measured and with regard to type of device (sensors/switches, transmitters, etc.). Electrical components are broken down by type (breakers, batteries, inverters, diesel generators, etc.) and by actual voltage level.

Failure rates (mean and uncertainties) and mean active repair times are tabulated for the various component classifications and for various component failure modes.

ISBN 91-7186-294-3; approximate cost $800.

NRC Studies

System reliability studies conducted by the U.S. Nuclear Regulatory Commission are intended to support several risk-informed regulatory activities. This includes providing information about relevant operating experience that can be used to enhance plant inspections of risk-important systems and information used to support staff technical reviews of proposed license amendments, including risk-informed applications. In the future, this work will be used in the development of risk-based performance indicators that will be based to a large extent on plant-specific system and equipment performance.

Findings and conclusions from the performance analysis of selected risk-important systems at 72 United States commercial reactors based on 1987–1997 operating experience are provided in various system specific reports. A report for each system describes the results of a risk-based analysis and engineering analysis of the system. The system reports provide an industry-wide perspective on their reliability, and how both industry (generic) and plant-specific performance compares with reliability estimates derived from data in PRAs and individual plant examinations (IPEs). These reports also provide an indication of how performance varies between plants and the measurable magnitude of that variation. The dominant system failure contributors are identified along with information on important failure modes and causes. All relevant operating experience on common cause failures that have been identified has been compiled and generic common-cause failure parameters have been estimated. A tabulation of failures, demands, and estimated failure rates for key equipment and system segments are also included. The reports

provide a mechanism for identifying individual licensee event reports (LERs) that are the source of the tabulated failure, demand, and failure-rate estimates.

The U.S. Nuclear Regulatory Commission plans to periodically update the information contained in these reports when additional data become available.

Initiating Events

A report entitled "*Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995*", NUREG/CR-5750, provides information relevant to initiating events of unplanned reactor trips, either automatic or manual. The report was produced at the Idaho National Engineering and Environmental Laboratory for the U.S. Nuclear Regulatory Commission. Data from all unexpected reactor trips during power operations at commercial nuclear power plants from 1987 through 1995 are contained in the report. The results, findings, conclusions, and information contained in this study are intended to support several risk-informed regulatory activities. This includes providing information about relevant operating experience that can be used to enhance plant inspections of risk-important systems and events and information used to support staff technical reviews of proposed license amendments, including risk-informed applications. This work also will be used in the development of risk-based performance indicators that will be based to a large extent on plant-specific system and equipment performance.

The objectives of the study are: 1) provide revised, historical frequencies for the occurrence of initiating events in U.S. nuclear power plants; 2)compare these estimates based on operating experience to estimates used in probabilistic risk assessments (PRAs), individual plant examinations (IPEs), and other regulatory issues; and 3)review the operating data from an engineering perspective to determine trends and patterns of plant performance on a plant-type [i.e., pressurized water reactor (PWR) or boiling water reactor (BWR)], plant-specific, and industry-wide basis.

Each reactor trip event was reviewed and categorized according to the initial event and, additionally, was marked if certain other risk-significant events occurred, regardless of their position in the event sequence. The data were analyzed for time dependence, reactor-type dependence, and between-plant variance. Dependencies and trends are reported, along with the raw counts and the best estimate for the initiating event frequencies.

The analysis of certain rare or infrequent initiating event categories, such as loss-of-coolant accidents (LOCAs), are based on U.S. and worldwide experience and cover periods before 1987. Medium and large pipe break loss-of-coolant accidents (LOCAs) were updated in this study using worldwide experience due to extremely low frequency of these types of events. The medium and large pipe break analysis consisted of three steps. First, the frequency of leaks or through wall cracks in large and medium-pipe piping was estimated using the number of reactor years and through-wall crack events in primary pressure boundary piping from world-wide experience for PWRs and total U. S. experience for BWRs. Second, for BWRs, a conservative IGSCC improvement factor of 20 was applied to the leak frequency calculation. Third, a conservative conditional rupture probability (given a through-wall crack or leak) is estimated and factored into the rupture (LOCA) frequency estimate. An error factor of 10 (assuming a lognormal distribution) was used to capture the uncertainties.

The small pipe LOCA frequency for PWRs and BWRs was developed from total U. S. experience. The estimate from WASH-1400 was updated using total U. S. reactor experience in a simple Bayes update.

Results of engineering analyses of the operating experience are compared with probabilistic risk assessment/individual plant examinations (PRA/IPEs) and NUREG-1150.

The LERs used in the analyses are listed in the report. The NRC plans to periodically update the information in this report. (An update addendum to this report is in draft form and includes data through 1998.)

J. P. Poloski, et. al., *Rates of Initiating Events at U. S. Nuclear Power Plants: 1987-1995*, NUREG/CR-5750, U. S. Nuclear Regulatory Commission, March 1999.

J. P. Poloski, et. al., *Rates of Initiating Events at U. S. Nuclear Power Plants: Update 1987-1998*, NUREG/CR-5750, Addendum (DRAFT), U. S. Nuclear Regulatory Commission, March 2000.

Reliability Studies: Selected Risk-Important Safety Systems

The U.S. Nuclear Regulatory Commission has conducted studies to monitor and report upon the functional reliability of risk-important systems in commercial nuclear power plants. The objectives of these studies are to: 1) estimate unreliability based on operational data, and compare the results with the assumptions, models, and data used in PRA/IPEs; and 2) provide an engineering analysis of the factors affecting system unreliability and determine if trends and patterns are present in the system operational data. The system studies compare the estimates and associated assumptions as found in PRAs to actual operating experience.

The system evaluation measures system unreliability using operating experience. Simple fault tree models were built for each of the systems based on standard PRA techniques. The system models are comprised of system functional segments. The segments may include several individual components (both active and passive components in a series network). Failure modes defined for these segments are based on the failure modes observed in the operational experience. Generally, these included failure to start (FTS), failure to run (FTR), failure to operate (FTO), failure due to being out of service for maintenance (MOOS), and common cause failures (CCF) for redundant train systems. Failure recoveries are also applied to active failures if supported by the operational data. Further, the systems are grouped into system classes based on similarity in design. When the system designs lack redundancy and diversity (systems such as RCIC or HPCI) only a single design class was developed. For more complex system designs such as AFW or HPI, there are as many as eleven system design classes for evaluating reliability.

Further, to make risk-based comparisons to the relevant information provided in the PRAs, unreliability estimates are calculated using the data collected from the operating experience and data extracted from probabilistic risk assessments and individual plant examinations (PRA/IPEs). The estimates of system unreliability based on operating experience are derived from data from unplanned demands as reported in LERs. These unplanned demands include actual ESF actuations as well as spurious and inadvertent ESF actuations. The data from this source are considered the closest representation of the plant conditions found during accident conditions. Data from component malfunctions that resulted in a loss of safety function for single train systems (or at least one train of the system for redundant train system) were not utilized. Generally, data based on surveillance tests were not used in the estimation of system unreliability because failures of an individual train of redundant train systems during a surveillance test are not reportable in accordance with 10 CFR 50.73, the Licensee Event Report (LER) reporting rule; and therefore an accurate count of these failures can not be obtained.

The systems that have been evaluated and the results published are:

Auxiliary/Emergency Feedwater (AFW), NUREG/CR-5500, Vol. 1

Westinghouse Reactor Protection System (RPS), NUREG/CR-5500 Vol. 2

General Electric Reactor Protection System (RPS), NUREG/CR-5500, Vol. 3

High-Pressure Coolant Injection (HPCI), NUREG/CR-5500, Vol. 4

Emergency Diesel Generators (EDGs), NUREG/CR-5500, Vol. 5

Isolation Condenser (IC), NUREG/CR-5500, Vol. 6

Reactor Core Isolation Cooling (RCIC), NUREG/CR-5500 Vol. 7

High Pressure Core Spray (HPCS), NUREG/CR-5500, Vol. 8

High Pressure Safety Injection (HPI), NUREG/CR-5500, Vol. 9.

Combustion Engineering and Babcock & Wilcox Reactor Protection System study in progress tentatively to be published end of fiscal year 2000. Updates to several of these system studies are ongoing.

CCF Database Program

The U.S. Nuclear Regulatory Commission and the Idaho National Engineering and Environmental Laboratory have developed and maintains a common cause failure (CCF) database and analysis software package for U.S. commercial nuclear power plants. The CCF data collection and analysis system consists of CCF event identification methodology, event coding guidelines, the CCF database containing both CCF events and an estimate of independent failure counts and a software system to estimate CCF parameters.

Documentation of the CCF database and analysis software system is described in NUREG/CR-6286, "*Common-Cause Failure Database and Analysis System.*" This technical report is published as four volumes: "Overview," "Event Definition and Classification of Common-Cause Failure Events," "Data Collection and Coding Common-Cause Failure Events," and "Common-Cause Failure Database and Analysis Software Reference Manual."

The database contains CCF-related events that have occurred in U.S. commercial nuclear power plants from 1980 through 1995. The events were identified from failure reports in the Nuclear Plant Reliability Data System (NPRDS), which is a proprietary database maintained by the Institute of Nuclear Power Operations (INPO), and LERs obtained from the Sequence Coding and Search System (SCSS) database maintained by the Oak Ridge National Laboratory for the NRC. The current data collection effort has separated the data by system as well as by component type.

The software system stores CCF data and independent failure events and automates the CCF parameter estimation process. Two methods are used in the system: alpha factor and multiple Greek letter. These models are used extensively in the nuclear industry. Because the CCF database contains proprietary information from NPRDS, the database itself is proprietary.

Results derived from the database can be used and can be referenced. Because NPRDS data are proprietary, NRC by a separate letter provides the CCF database and the CCF analysis software, along with supporting technical documentation, to only nuclear power plant licensees who are members of INPO.

A report, "*Common-Cause Failure Parameter Estimations*," NUREG/CR-5497, contains CCF parameter estimates for the majority of the risk-important safety systems and components in commercial nuclear power plants. Individual summary reports of these systems are provided in NUREG/CR-5497. The summary reports are for the following systems and components:

DC Power- Batteries and Chargers,

DC Power Distribution Circuit Breakers,

4160 Volt Ac Power Distribution Circuit Breakers,

Reactor Trip Circuit Breakers,

Emergency Diesel Generators,

Containment Spray Heat Exchangers, Motor-Operated Valves

Residual Heat Removal Heat Exchangers and Motor-Operated Valves

BWR Isolation Condensers and Air-Operated Valves, Motor-Operated Valves

PWR Auxiliary Feedwater Pumps and Air-Operated Valves, Check Valves, Motor-Operated Valves

Emergency Service Water Pumps,

PWR High Pressure Safety Injection Pumps,

BWR Low Pressure Coolant Injection Pumps and Check Valves, Motor-Operated Valves

PWR Low Pressure Safety Injection Pumps and Check Valves, Motor-Operated Valves

BWR High Pressure Coolant Injection and Reactor Core Isolation Cooling Pumps and Air-Operated Valves, Check Valves,

BWR Standby Liquid Control Pumps,

BWR Suppression Pool Strainers,

PWR Containment Sump Strainers,

Emergency Service Water Strainers,

Main Steam Isolation Air-Operated Valves,

BWR Safety Valves

PWR Pressurizer Safety Valves, Power-Operated Relief Valves, PORV Motor-Operated Block Valves

PWR Steam Generator Safety Valves, Power-Operated Relief Valves

BWR Pressure Relief and ADS Valves.

Also included in the individual summary report are system descriptions and figures, component boundaries, failure event definitions, and a table of alpha factors.

Accident Sequence Evaluation Program (ASEP)

A. D. Swain, *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, U.S. Nuclear Regulatory Commission, NUREG/CR-4772, February 1987.

NUREG/CR-4550 Analysis of Core Damage Frequency: Internal Events Methodology

NUREG/CR-4550 was one of many documents that supported the NUREG-1150 "*Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (Final Summary Report)*". Volume 1 of NUREG/CR-4550 provides a generic list of component failure rate statistics for selected equipment in commercial nuclear power plants. Tables of generic component failure rates, failure probabilities, and test and maintenance unavailabilities are provided. Failure probabilities for each mode of component failure and for test and maintenance failures were developed from analysis of plant-specific and industry-wide data. Tables of initiating event frequencies, common cause factors and human error probabilities are also provided.

The failure parameters provided in NUREG/C-4550 specify a range of estimates collected from other sources. These sources of data are identified in the tables. Along with the range of estimates of a component failure mode are the estimates (mean) used in ASEP and the corresponding probability distribution parameters. The lognormal distribution was assumed for the ASEP parameters. Basis for the ASEP parameters is provided in the tables.

Ericson, D. M., Analysuis of Core Damage Frequency: Internal Events Methodology, U.S. Nuclear Regulatory Commission, NUREG/CR-4550, Rev. 1, January 1990.

Component Reliability Data for Use in Probabilistic Safety Assessment (IAEA-TECDOC-478)

This document presents generic reliability data for components usually considered in probabilistic safety assessments (PSA). The document was published in 1988 by the International Atomic Energy Agency. Twenty-one sources (publications, reports, etc.) of reliability data reviewed and component information was recorded in a database. The sources of data is comprised of both foreign and U.S operating experience. The data sources cover the time frame from late 1970 through mid 1980. Data sources include: Wash1400, Swedish Reliability Data Book, NUREG-2815, NUREG-2728, IEEE Standard 500, Shoreham PSA, NUREG/CR 4550, Sizewell B Preconstruction Report, Oconee PSA, Old PWR (extensive plant-specific operating experience extracted from plant operating records), Heavy Water Reactor assessment (operating experience from a comprehensive overview of pant operating records), Zion PSA, EPRI NP-2433, German Risk Study, In-Plant Reliability Data Base, other selected NUREGs (LER Summary reports of component failures). The records in the database (approximately 1000) were established directly from the information from the sources reviewed.

Component information available in the report is categorized by component type, operating mode (primarily for pumps), operating environment, failure mode, failure rate (mean or median, upper and lower bounds, error factors, repair time), and source of information. Not every component record contains all these reliability attributes. Either a failure rate or probability is stated for each component type.

"*Component Reliability Data For Use In Probabilistic Safety Assessment*", IAEA-TECDOC-478, ISSN 1011-4289, IAEA, Vienna, October 1988.

AP600 Probabilistic Risks Assessment (DE-AC03-90SF18495)

The failure data used in the AP600 analysis is primarily based on existing operating plant data. The components in the AP600 design are similar to and are assumed to operate under similar conditions as those in existing operating plants. The logic and instrumentation failure data for the AP600 microprocessor–based components is derived from Westinghouse data. No contribution due to random software failure is considered, as software failure falls solely under the common mode design failure. Common mode software failures of individual software implementations and common mode failure of all software implementations are modeled.

A log-normal distribution was assumed for all data used in the reliability analysis. The error factors were derived from NUREG/CR-4550, NUREG/CR2728 (Interim Reliability Evaluation Program Procedures Guide), and engineering assessment.

Westinghouse plant-specific data for the assumed scheduled and unscheduled maintenance of AP600 nonsafety-related system pumps are provided. Common cause failure parameters (Multiple Greek Letter) and probabilities, as well as human error probabilities (THERP-based), are presented.

Simplified Passive Advanced Light Water Reactor Plant Program, AP600 Probabilistic Risk Assessment, U.S. Department of Energy, San Francisco Operations Office, DE-AC03-90SF18495.

Advanced Light Water Reactor Utility Requirements Document

The Electric Power Research Institute (EPRI) developed a set of design requirements for advanced light water reactors. Volume III ALWR Passive Plant, Chapter 1 Appendix A contains the key assumptions and groundrules (KAG) for performing the probabilistic risk assessment (PRA) required by 10 CFR 52.47(a)(1)(v). As part of this document, a reliability database consisting of initiating event frequencies, component failure rates, and common-cause failure parameters are provided. The document is proprietary information and is available only under license from EPRI.

The KAG provides a set of recommended generic failure rates that were derived from available data sources.

ADVANCED LIGHT WATER REACTOR UTILITY REQUIREMENTS DOCUMENT, Volume III, ALWR Passive Plant, Chapter 1, Appendix A, PRA Key Assumptions and Groundrules, Electric Power Research Institute.

Non-nuclear/Commercial

Bellcore

"*Reliability Prediction Procedure for Electronic Equipment*", Technical Reference, TR-TSY-000332, Issue 6, Dec. 1997. Many commercial electronic product companies are now choosing to use the Bellcore handbook for their reliability predictions. Bellcore is Bell Communications Research (a spin-off of AT&T Bell Labs), and is the research arm of the Bell Operating Companies. Bellcore previously used MIL-HDBK-217 for their reliability predictions, but found that 217 gave pessimistic numbers for its commercial quality products. In 1985, Bellcore used 217 as a starting point and modified (simplified) the models to better reflect their field experience. The Bellcore reliability prediction procedure, which is applicable to commercial electronic products, was developed also at this time. The procedure provides recommended methods for predicting device (basic component) and unit (customer replaceable assembly of devices) hardware reliability. Three methods are outlined: Method I- Parts count (MIL-HDBK-217F procedure); Method II-Unit or device level statistical predictions based on combining Method I predictions with test data; Method III- Statistical predictions of in-service reliability based on field data collected. Base failure rates are provided with tables of factors (e.g., temperature, environmental, quality level, etc.) that can be applied to establish a failure rate for a specific application.

Bellcore document "Reliability Prediction Procedure for Electronic Equipment" (document number TR-332, Issue 6) ca be ordered from Bellcore Customer Service in New Jersey; Phone: (800) 521-2673 or (732) 699-5800; the cost is about $1000. Bellcore was purchased by Science Applications International Corp (SAIC) in late 1997 and is now called Telcordia Technologies.

MIL-HDBK 217F Reliability Prediction of Electronic Equipment

The most widely known and used reliability prediction handbook is MIL-HDBK-217, the Military Handbook for "Reliability Prediction of Electronic Equipment". MIL-HDBK-217 is published by the Department of Defense, based on work done by the Reliability Analysis Center and Rome Laboratory at Griffiss AFB, NY. The MIL-HDBK-217 handbook contains failure rate models for the various part types used in electronic systems, such as ICs, transistors, diodes, resistors, capacitors, relays, switches, connectors, etc. MIL-HDBK-217 provides models for printed circuit boards, lasers, SAWS magnetic bubble memories, and tubes. MIL-HDBK-217 is geared towards both military and commercial equipment.

MIL-HDBK-217 was the original standard for reliability. It was designed to provide reliability math models for nearly every conceivable type of electronic device. MIL-HDBK-217 is intended to provide a consistent and uniform database for making reliability predictions when no substantial reliability experience exists for a component. MIL-HDBK-217 is used by both commercial companies and the defense industry. It contains two basic methods of calculating component level failure rates, the "parts stress method" and the "parts count method." The parts count method requires only limited information such as component type, complexity and part quality to calculate a part failure rate. The parts count section of the handbook is derived by assigning model factors for more involved part stress method to slightly conservative estimates of what would typically be expected. All of the specific default values are provided in Appendix A of the handbook. The parts stress method requires significantly more information such as case or junction temperature and electrical operating and rated conditions to perform a failure rate calculation.

Because MIL-HDBK-217 was the original standard for reliability prediction analyses, it is known and accepted worldwide.

In MIL-HDBK-217, the quality levels that are used differ from one part type to another. Rather than having a simple classification of general quality levels, the quality levels for components in MIL-HDBK-217 are derived from specific data that is component dependent. Therefore, the quality levels for resistors are different than the quality levels for semiconductors. The quality levels for semiconductors are different than the quality levels for integrated circuits. The quality levels for each part type were designed specifically for that classification of component.

The most recent revision of MIL-HDBK-217 is Revision F Notice 2, which was released in February of 1995. You can get a copy of MIL-HDBK-217F-2 from any source that provides Mil Specs, Mil Standards, Mil Handbooks, etc. The Defense Printing Service, Philadelphia, PA, Phone: (215) 697-2179, Fax: (215) 697-1462 is one such source or National Technical Information Service (NTIS) [WEB access: www.NTIS.gov] is another. Cost is approximately $60.

Handbook of Reliability Prediction Procedures for Mechanical Equipment (NSWC-98/LE1)

This report was developed as part of a research project to develop a standardized method of evaluating new mechanical designs for reliability and maintainability (R&M). The design evaluation techniques program initiated by the Carderock Division of the Naval Surface Warfare Center includes a methodology for evaluating a design for R&M that considers the material properties, operating environment and critical failure modes at the component level. This report presents an approach for determining the R&M characteristics of mechanical equipment. An analysis of a design for R&M can identify critical failure modes and causes of unreliability and provide an effective tool for predicting equipment behavior and selecting appropriate logistics measures to assure satisfactory performance when the equipment is placed in its operating environment. The current edition of the Handbook has twenty chapters of guidance information with equations, engineering tables, and procedures for estimating the reliability of a mechanical design for the intended operating environment.

This is a relatively new standard, and currently the only one of its kind. The Handbook is constantly being updated. In the 94 edition, nineteen basic mechanical components have been identified for which reliability prediction equations have been developed. All mechanical equipment is composed of some combination of these nineteen components and a designer can utilize the equations to determine individual component reliability and then combine results in accordance with the system reliability diagram to determine total system reliability in its operating environment. The current edition (1998) contains additional chapters on gearboxes and transmission systems, sensors and transducers, and impacting devices. Information on the impact of shock, vibration, and corrosion on mechanical reliability have been included so that a complete set of procedures for predicting the reliability of mechanical component is available.

Copies of the Handbook are available from: Carderock Division NSWC, 9500 MacArthur Blvd, Code 291, ATTN: Tyrone Jones, West Bethesda, MD 20817-5700. The cost of the Handbook is $100. For additional information, call Mr. Tyrone Jones at (301) 227-4383 or Mr. James Chesley (301) 227-1709.

OREDA

Offshore Reliability Data (OREDA) organization is currently sponsored by ten major oil companies. The main purpose is to promote the use and exchange of reliability technology and data between the participating companies. The OREDA project has established a comprehensive data bank with reliability data for exploration and production equipment mainly from the North Sea and the Adriatic Sea regions. The data bank comprises data from a wide variety of installations, equipment types and operating conditions.

OREDA provides the data in generic form in Reliability Handbooks. The current Handbook edition was issued in 1998. OREDA has been collecting data since the beginning of the eighties. The data in the Handbook represent the North Sea (Norwegian and UK sector) and the Adriatic Sea. Data have been collected for altogether 7,629 equipment units. The data represent a total observation period of 22,373 years, and 11,154 failures have been recorded. The data are presented in approximately 250 data sheets for various functions, applications, capacities, fluids, size, etc. of the equipment. For each component identified, quantitative generic information consists of failure modes, failure rate, repair time, active repair time (time to analyze, repair and restore equipment to service), and supporting information (number of events, population, time in service). Qualitative information in the handbook includes the component description, offshore applications, environmental and operational conditions, failure causes and additional description of failure modes, and component boundary specifications.

The OREDA-97 handbook covers a wide range of components and systems:

Mechanical: Compressors, Gas turbines, pumps, heat exchangers, vessels

Electrical: Electric generators

Control and Safety Equipment: Control Logic Units, Fire and Gas Detectors, Process Sensors, Valves

Subsea Equipment: Control Systems, Well Completions

The Handbook information is classified into the following systems: Process Systems, Safety Systems, Electrical Systems, Utility Systems, Crane Systems, and Drilling Equipment.

The data are stored in a database, and specialized software has been developed to collect, retrieve and analyze the information. Only the OREDA member companies have access to these databases, or they can give temporary contractors working on their behalf. Generic data are published in the data Handbook. Project participants are: AGIP S.P.A./STIN, BP International Ltd., Norsk Hydro a.s., SIEP B.V., Saga Petroleum a.s., Statoil UBT DVVO, Total S.A., Elf Petroleum Norge A/S, Exxon Production Research Co., Phillips Petroleum Company.

Price of the handbook is $385. Postal address:

Det Norske Veritas
Veritasveien 1
P.O. Box 300
N-1322 Høvik
NORWAY
Attn: OREDA Manager

Reliability Data for Control and Safety Systems- 1998 Edition

Several standards such as the International Electrotechnical Committee standard IEC 61508; "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related (E/E/PE) Systems" are highlighting the use of reliability analysis to design and verify the performance of computer-based control and safety systems. The analysis, however, has suffered from the lack of relevant reliability data. The handbook "Reliability Data for Control and Safety Systems - 1998 Edition" is a unique source for this kind of data. Here, more than 10 years of field reliability data is shared with the entire engineering community.

The handbook contains summary tables of reliability parameter values, including parameter definitions, approach and data sources and a description of the component together with reliability parameter values. Components included are typical components found in process control and shutdown systems, including emergency shutdown systems and fire and gas detection systems:

Input devices, among others: Process transmitters, gas/smoke/heat detectors

Control logic, among others: ESD node/single PLC system, field bus coupler

Output devices, among others: Different shutdown valves, pilot and control valve, pressure relief valve.

The reliability data handbook is the result of research and development work conducted in the PDS Forum. The PDS Forum (Formerly CSSF-Control and Safety Systems Forum-- Industry forum within the area of "Dependability of computer-based control and safety systems") was initiated in 1995. The forum is a professional forum for exchange of experience between Norwegian vendors and users of control and safety systems. The primary focus is on safety and reliability aspects of such systems. The basis of this work is a co-operation between oil companies, control and safety system vendors, engineering companies and researchers. All parties involved have a special interest in reliability issues of computer-based control and safety systems. In 1998, the main activity of the PDS Forum was to update the so-called "PDS-recommended data". The handbook is prepared and published by SINTEF. For the last 10 years, SINTEF has had a major activity on theory, techniques and tools for the design, validation, operation and evaluation of computer-based control and safety systems in the process industry. The OREDA database serves as a key component of the data.

The participants in the 1998 PDS Forum are:

Oil Companies: Amoco Norway Oil Company, BP Norge, Elf Petroleum Norge, Norsk Hydro ASA, Phillips Petroleum Company Norway, Saga Petroleum, Shell, STATOIL

Control and Safety Systems Vendors: ABB Industri, Autronica, Bailey Norge, Boo Instrument AS, Honeywell, ICS Group, Kongsberg Simrad, Norfass (Yokogawa), SAAS ASA, Siemens

Engineering Companies and Consultants: Aker Engineering, Det Norske Veritas, Dovre Safetec AS, Kværner Oil and Gas A.S, NORSOC, Umoe Olje og Gass.

CCPS

The Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE) has developed and operated an equipment reliability database. The database can be used to determine process integrity, reliability and availability of equipment components, process units and plants and develop risk-based maintenance planning and continuous improvement of key equipment.

Participants have access to their own data and the generic data developed from the experience of all participants. A guidelines book on collecting quality data suitable for inclusion in the database and Windows © based software for data analysis. Project participants are: Air Products & Chemicals Inc., Amoco Corporation, ARCO, BP Oil International, Caltex Services, Celanese Limited, Chevron Research and Technology Corp., Dow, DuPont, Eastman Chemical Co., Exxon, Factory Mutual Res. Corp., Flour Daniel Inc., GE Plastics, The Hartford Steam Boiler Inspection and Insurance Co., Hercules Inc., ICI-UK Intevep S.A. (Venezuela), Mitsubishi Chemical Corp., Phillips Petroleum Co., Rohm and Haas Co., Shell, Syncrude Canada, Ltd., Texaco, Westinghouse Savannah River Operations.

The guidelines book, "Process Equipment Reliability Data" was published in 1989. The data presented are primarily based on nuclear power plant information and experience data with some non-nuclear data (petro-chemical) provided. The results are presented are generic. A CCPS generic failure rate database taxonomy as well as diagrams of equipment boundaries are provided.

GIDEP

GIDEP (Government-Industry Data Exchange Program) is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by making maximum use of existing information. The program provides a media to exchange technical information essential during research, design, development, production and operational phases of the life cycle of systems, facilities and equipment.

GIDEP is managed and funded by the U.S. Government. Among its participating organizations are: US Army, Navy, Air Force, Defense Logistics Agency, National Aeronautical and Space Administration, Department of Energy, Department of Labor, Department of Commerce, General Services Administration, Federal Aviation Administration, US Postal Service, National Institute of Standards and Technology, National Security Agency, as well as, the Canadian Department of Defence. There are also hundreds of industrial organizations producing parts, components and equipment for the government which participate in the program. As a result of the government's emphasis on high quality products and services, any activity providing products or services to the government, and uses or generates the types of data exchanged within GIDEP, may apply for membership. GIDEP does not accept classified or proprietary information.

Participants in GIDEP are provided electronic access to the six major types of data. The ENGINEERING DATA contains quality assessment, engineering test, evaluation and qualification test reports, nonstandard parts data, parts and materials specifications, manufacturing processes, process controls, solderability data and related engineering data on parts, components, materials and processes. This data includes significant amounts of energy and environmental information.

The FAILURE EXPERIENCE DATA contains objective failure information as a result of ALERTs, SAFE-ALERTs, Problem Advisories and Agency Action Notices which notify users of nonconforming parts, components, chemicals, processes, materials, safety and hazardous situations. This data also includes failure analysis and problem information submitted from laboratory analysis.

The METROLOGY DATA contains calibration procedures and technical manuals for test and inspection equipment. It also contains engineering information on calibration laboratories, calibration systems and measurement systems. National Institute for Standards and Technology contributes a significant portion of the engineering data related to measurement science.

The PRODUCT INFORMATION DATA contains notices on parts, components and materials which are being discontinued or the attributes have been changed by the manufacturer. This data includes Diminishing Manufacturing Sources and Material Shortages (DMSMS) Notices of product discontinuances which suppliers have forwarded to GIDEP. It also contains information on alternate sources, after market suppliers, Department of Defense focal points of contact and related information. Another significant type of data is the Product Change Notices, which are also distributed as a part of this data set.

The RELIABILITY AND MAINTAINABILITY (R&M) DATA contains failure rate, failure mode and replacement rate data on parts, components, and subsystems based upon field performance and demonstration tests of equipment, subsystems and systems. This also includes reports on theory, methods, techniques and procedures related to reliability and maintainability practices. The URGENT DATA REQUEST system permits participants having technical problems to rapidly query the GIDEP community to obtain information that resolves the problem.

This source of data was not reviewed for this report. The summary is what is described on the WEB site. To get GIDEP data an organization must be a member of GIDEP. The GIDEP summary is included as a possible source of data for commercial-off-the shelf equipment.

Savannah River Site Non-Reactor Component Generic Failure Rate Database

A component generic failure database report has been developed as part of an overall effort to improve safety analysis methods for Savannah River Site (SRS) nonreactor nuclear facilities. The database was developed to support quantification of system fault-tree models. Examples of components covered include instrumentation, electrical equipment, pumps, valves, tanks, and piping. The following are goals of the database development effort: 1) provide information on various failure modes for each component, where possible, (e.g., valve failure to open/close upon demand and spurious operation, rather than just valve failure; 2) base component failure rates on actual data (failure events) wherever possible; 3) use the most up-to-date and applicable data sources available; and 4) provide a basis and reference for each component failure rate so that the basis can be reviewed and evaluated.

Data sources used in the database include Department of Energy (DOE) nuclear facilities, chemical processing facilities, commercial nuclear power plants, military systems, and offshore oil drilling facilities. Data sources were identified from existing databases, from interviews with DOE safety analysts, and from past safety analyses. A comprehensive list of components and failure modes was generated by reviewing past SRS safety analyses, and existing data sources, and consulting with SRS and other DOE safety analysts. The resulting list of components and failure mode combinations includes over 500 entries. The sources were divided into those listing actual failure data and those listing only failure rate estimates. All sources are categorized as:

Category 1 - Sources with actual failure data obtained from a detailed review of failure events (to ensure applicability to the failure mode being considered) and a detailed review of component populations and exposure duration (or demands). Twenty-one sources were identified, most dealing with commercial nuclear power plants or DOE reactors. A major source of commercial nuclear power plant information was the Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR).

Category 2 - Sources with actual failure data, but which have an added uncertainty in the data compared with Category 1 sources. This uncertainty can result from a less comprehensive search for actual failures, a more approximate method for determining component populations or exposure durations (or demands), or a less clear breakdown of failures into the failure modes of interest. Sixteen Category 2 sources were identified, covering nuclear power plants (NUCLARR has ten sources in this category), military systems (Rome Air Development Center), DOE nuclear facilities, offshore oil-drilling facilities (OREDA), and liquified natural gas plants.

Category 3 - Sources that list only failure rate estimates. Seven data sources were used for this category. These sources cover a variety of industries.

A goal of the effort was to base failure rate estimates on actual failure data (those contained in Category 1 and Category 2). Since the data quality was higher with Category 1, data aggregation was only performed within categories. If there are failure data from more than one source for a given component failure mode, aggregation routines combined the data to obtain a distribution of the failure rate. The aggregation routines are based primarily on those found in the NUCLARR software package. However, several modifications were made to cover special cases where a source listed a failure rate but no uncertainty estimate (i.e., Category 3 data), and where aggregation results indicated an error factor (95^{th} percentile/50^{th} percentile) greater than 30.

Estimates of component failure rate are presented in tabular form. The recommended results were based on the following aggregation preferences: first– Category 1, second–Category 2 (when Category 1 data did not exist), and last–Catgory 3 (when neither Category 1 or 2 data exists). Mean failure rates were rounded to 1, 3, or 5 times the appropriate power of 10. Also, error factors were rounded to 3, 5, 10 or 30. This rounding is reasonable for a generic database and reflects the precision of the results. Further, the component failure rates and respective failure modes were tabulated according to six system types: water, chemical process, compressed gas, HVAC/exhaust, electrical distribution, and instrumentation and control.

The following are some of the strengths of the resulting database:

- Extensive coverage of components and failure mode combinations (over 500).
- Wide range of sources used (commercial reactors, DOE facilities, chemical facilities, offshore oil drilling, military systems).
- Most failure-rate distributions based on actual data rather than estimates.
- Results for each aggregation for each data source are provided as well as the basis for each failure-rate distribution is provided; thereby the user can accept or modify the results.

Only failure rate and uncertainty estimates of either λ or q_d are provided. Repair times or equipment downtimes are not provided.

C.H. Blanton, E.V. Browne, and S.A. Eide, WSRC, Aiken, S.C., *Savannah River Site Generic Data Base Development (U)*, Westinghouse Savannah River Company, WSRC-TR-93-262, June 1993.

Savannah River Site Human Error Database for Non-Reactor Nuclear Facilities

A component generic failure database report has been developed as part of an overall effort to improve safety analysis methods for Savannah River Site (SRS) nonreactor nuclear facilities. The database was developed to support quantification of system fault-tree models. The report includes models and quantification results for 35 representative human errors. For 16 of the human errors, the recommended human error probabilities or rates are based solely on generic models developed from industry literature (no actual SRS data available). SRS-specific data were collected for the remaining 19 human errors. (The recommended SRS human error rates and probabilities were obtained using rounded generic model results as priors and the SRS specific models as the evidence in the Bayesian updates.) Of these 19 human errors, the final recommended values for two human errors were quantified using only SRS-specific actual data. The remaining 17 human errors quantified used both SPS-specific and generic models. For each human error rate, three different mean probabilities or rates are presented to cover a wide range of conditions and influencing factors.

The majority of the human errors presented are for pre-accident or initiators. Only six relate to post-accident conditions. Each human error rate or probability was to have a lognormal distribution characterized by a mean and an error factor. Each mean obtained from the generic model was rounded to 1, 3, or 5 times the appropriate power of ten. Many of the generic human error models were based on models, data, or estimates derived for applications at commercial nuclear power plants. The data and modeling generally uses THERP techniques as described in NUREG/CR-1278, "*Handbook of Human Reliability with Emphasis on Nuclear Power Plant Applications*".

The analysis for each human error rate or probability, as well as the basis for each human error model, are provided; thereby the user can accept or modify the results.

The document does not provide guidance for performing detailed human reliability analysis.

H. C. Benhardt, S.A. Eide, et.al, WSRC, Aiken, S.C., *Savannah River Site Human Error Data Base Development For Nonreactor Nuclear Facilities (U)*, Westinghouse Savannah River Company, WSRC-TR-93-581, February 1994.

Electronic Part Reliability Data (EPRD-97)

The purpose of this document is to provide empirical field failure rate data on electronic components. The component types for which data is presented in this document are capacitors, diodes, integrated circuits, opto-electronic devices, resistors, thryistors, transformers, and transistors.

The part types for which data is contained in this document is similar to those contained in existing reliability prediction methodologies, such as MIL-HDBK-217. MIL-HDBK-217 contains mathematical models that have been derived from empirical field failure rate data. The data contained in EPRD-97 is historically observed field failure rates. A majority of the data contained in EPRD-97 is comprised of commercial quality components. Therefore it can be used to predict reliability of non-military systems containing commercial quality components.

Appendix B
Reliability Databases and Reports (Draft)

The failure rate data contained in this document represents a cumulative compilation from the early 1970's through October 1996. RAC periodically purges data from the database in the event that newer data of higher quality is obtained. New field data is added periodically in an effort to keep the databases current. The goals of these data collection efforts are as follows:

1) To obtain data on relatively new part types and assemblies.

2) To collect as much data on as many different data sources, application environments, and quality levels as possible.

3) To identify as many characteristic details as possible, including both part and application parameters.

Data contained in this publication were collected from a wide variety of sources. RAC utilized the following generic sources of data for this publication:

· Published reports and papers

· Data collected from government-sponsored studies

· Data collected from military maintenance data collection systems

· Data collected from commercial warranty repair systems

· Data from commercial/industrial maintenance databases

· Data submitted directly to the RAC from military or commercial organizations that maintain failure databases.

RAC screens the data such that only high quality data is added to the database. In addition, only field failure rate data has been included.

EPRD-97, along with the RAC's document "*Nonelectronic Parts Reliability Data*" (NPRD-95), described in the next section, contains all (non-proprietary) component data that is in the RAC databases. These two documents are complementary and there is no duplication of data between them. Together they provide the capability of estimating the reliability of most component types used in electronic or mechanical systems.

The primary purpose of this document is to augment reliability prediction methodologies such as MIL-HDBK-217. MIL-HDBK-217 or other prediction methodologies do not contain failure rate models on every conceivable type of component and assembly. These reliability prediction models have been primarily applicable only for generic electronic components. EPRD-97 provides:

1) failure rate data on commercial quality components,

2) failure rates on state-of-the-art components, and

3) data on part types not addressed by MIL-HDBK-217 or other prediction methodologies models.

A hard copy of this document is available from IIT Research Institute/Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, Phone (888) 722-8737, FAX (315) 337-9932. Cost is $395.

Nonelectronic Part Reliability Data (NPRD-95)

The purpose of this document is to present summary failure rates by environmental and quality level on a wide variety of electrical, electromechanical, and mechanical parts/assemblies. This document contains data on more than 25,000 part types. The failure data is collected from both military and commercial applications. The generic sources of data for this publication are the same as those identified for EPRD-97.

The failure rate data contained in this document represent a cumulative compilation of data collected from the early 1970's through May 1994. However, data is periodically purged from the database in the event that newer data of higher quality is obtained or if data is on obsolete part types. New field data is added in an effort to keep the databases current. The goals of the data collection efforts are:

1) To obtain data on relatively new part types and assemblies for which there is a lack of field experience.

2) To collect as much data on as many different data sources, application environments and quality levels as possible.

3) To identify as many characteristic details as possible, including both part and application.

RAC states that additional steps have been taken to insure the quality of the data published in the document. Completeness of data, consistency of data, equipment population tracking, failure verification, availability of parts breakdown, and characterization of operational histories are all used to determine adequacy of data.

RAC states that in virtually all field failure data collected, time to failure was not available. Few DoD or commercial data tracking systems report elapsed time indicator (ETI) meter readings to allow time-to-failure compilations. Those that do report ETI readings lose accuracy following removal and replacement of failed items. To accurately monitor these times, each replaceable item would require its own individual time recording device. The data collection efforts typically track only the total number of item failures, part populations, and the number of system operating hours. The assumed underlying time-to-failure distribution for all failure rates presented in NPRD-95 is the exponential distribution. RAC further states that many of the part types for which data are presented typically do not follow the exponential failure law, but rather exhibit wearout characteristics, or an increasing failure rate in time. The failure rates are presented by generic component type, quality level, and environment.

A hard copy of this document is available from IIT Research Institute/Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, Phone (888) 722-8737, FAX (315) 337-9932. Cost is $195.

Failure Mode/Mechanism Distributions (FMD-97)

This document is the second in a series of Reliability Analysis Center (RAC) publications that provide Failure Mode and Mechanism Distributions on parts and assemblies. It updates

"Failure Mode/Mechanism Distributions, 1991" and provides a cumulative compendium of failure mode/mechanism data.

FMD-97 presents failure mode distributions on parts and assemblies to be used in support of reliability analyses. Data contained in this publication can be used to apportion a component's total failure rate by failure mode. This accomplished by multiplying the total failure rate by the percentage attributable to a specific failure mode. The failure mode distributions provide a baseline set of probabilities to be used in the reliability analyses.

The scope of this publication is electrical, electronic, mechanical, and electromechanical parts and assemblies on which the RAC has collected failure mode/mechanism data. The data contained in this publication was collected from a variety of sources. These sources, grouped by major categories, are:

(1) *Published information*; Literature searches were conducted that identified published sources presenting failure modes/failure mechanisms or failure mode distributions. Such sources are periodicals, technical reports, and data compendiums.

(2) *Maintenance data;* Several government-sponsored databases were used in support of FMD-97. In these databases, a repair technician will typically record information regarding the cause of failure at the time a maintenance action was performed. The primary disadvantage of this data type is that the failure mode/mechanism can not be confirmed. Data of this type was only included when a reasonable degree of credibility existed in the source.

(3) *Failure analysis reports*; RAC states that it continually collects and analyzes failure mode/mechanism data from failure analysis activities. The data in this category can be from failures in field operation or laboratory testing. The advantage of this kind of data is that it is usually of very high quality. A disadvantage is that much of the data is from laboratory testing, and therefore the stresses to which the part is exposed may not be consistent with the stresses seen by the part in field use operation. Additionally, some of the data contained in this document is from Destructive Physical Analysis (DPA) in which the part may not have functionally failed, but rather, an anomaly was discovered.

Because many different sources of data were used in the preparation of this document, the user of this data is encouraged to review the source descriptions. RAC states that a particular problem in deriving the failure distributions presented in FMD-97 was the manner in which several data sources were merged together to yield a single distribution. The previous version of this document, FMD-91, used a merging algorithm that weighted each data source equally. This algorithm consisted of converting the failure data to percentages, averaging the percentage associated with each mechanism, and adjusting (normalizing) the resultant percentage to ensure that the sum is equal to one hundred percent. One reason for accomplishing the data merge in this fashion for FMD-91 was that many of the data sources used at that time were provided to the RAC in percentage form, for which the specific number of failures associated with each failure mode/mechanism was not known. However, a disadvantage in using that method is that each data source is weighed equally and a source that contains many failures is weighed equally with one that contains very few failures. Virtually all of the new data that was collected to support this update to FMD-91 was provided in a form in which the quantities of failure were known. Where FMD-91 contained a significant amount of data in percentage form only (unknown failure quantities), less than 20% of the data inFMD-97 is percentage data only. For this reason, RAC used a data merging algorithm that weighs each data source in an amount proportional to the total number of reported failures in that data source.

A hard copy of this document is available from IIT Research Institute/Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, Phone (888) 722-8737, FAX (315) 337-9932. Cost is $100.

Reliability Analysis Center (RAC) Automated Databook (RAD)

The Reliability Analysis Center (RAC) Automated Databook (RAD) is intended to serve as a time efficient data search and retrieval tool for accessing information contained in RAC data publications NPRD-95, EPRD-97, and FMD-97.

The implementation of RAD closely follows the organization of the printed NPRD-95, EPRD-97, and FMD-97 giving access to the information through indexes. These indices allows the user to access information by specifying an Index Term, for NPRD-95, and EPRD-97, a Part or MIL Number, and for NPRD-95 and EPRD-97, a full National Stock Number (NSN), or NSN without the Federal Supply Class (FSC).

In addition to the indexed data retrieval, the RAD also allows the user to retrieve data through a Multi-Parameter Search Engine. This Search Engine provides extreme flexibility by allowing searches on full or partial part numbers for NPRD-95 and EPRD-97 data and narrowing a search to include only data from a specific manufacturer.

Additional search filters allow the user to specify specific environments and/or quality levels to limit search results in either the indexed data retrieval or the Multi-Parameter Search for NPRD-95 and EPRD-97 data.

A CD-ROM of the automated handbook is available from IIT Research Institute/Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, Phone (888) 722-8737, FAX (315) 337-9932. Cost is $500.

Digital I&C Systems Data

Nuclear power plants rely on instrumentation and control (I&C) systems for plant monitoring, control, and protection. Digital I&C systems have the potential for improved reliability and availability by the use of such capabilities as fault tolerance, self-testing, signal validation, and on-line diagnostics, compared to the analog systems currently in use at U.S. commercial nuclear power plants. Virtually all of the nuclear power plants in operation today have digital I&C components (National Research Council, 1997). Some were part of original designs (for example, diesel generator sequencers) using solid-state logic while other s involve plant retrofits ranging from relatively small scale replacements of components (recorders, meters and displays) to large scale microprocessor-based systems. The later includes reactor protection system retrofits at Haddam Neck, Sequoyah, Zion Unit 2, and Diablo Canyon; ATWS systems at Palo Verde Units 1,2; load sequencers at Turkey Point Units 3 and 4; and station blackout/electrical safeguards at Prairie Island Units 1 and 2. New, advanced nuclear power plant designs use digital I&C systems exclusively. There is world-wide application of digital I&C technology to nuclear power plants. In Canada (CANDU reactors), Japan (the ABWR located at Kashwazaki), Korea (CANDU designs at Wolsong 2/3/4 and the WENS System 80+ designs at Yonggwang 3/4), and Western Europe (Great Britain latest plant, Sizewell-B, France's Chooz-B plant). The Canadian CANDU plants generally have the most advanced digital I&C systems (Uhrig 1993). (The newest CANDU plant, Darlington, has almost 100% of it control systems and

over 70% of its plant protection systems being digital.) In the United States, the advanced reactor designs developed use all digital I&C systems.

Digital instrumentation and control (I&C) systems are vulnerable to common-mode failure caused by software error, which defeats the redundancy achieved by hardware architecture. A defense-in-depth and diversity (D-in-D&D) analysis of a digital computer-based reactor protection system, in which defense against common-mode failures was based upon an approach using a specified degree of system separation between echelons of defense was used in NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System." SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors," discusses common mode failures and other digital system design issues. As a result of the reviews of ALWR design certification applications that used digital protection systems, the USNRC documented its position with respect to common-mode failures in digital systems and defense-in-depth in SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs."

As a result of the reviews of ALWR design certification applications that used digital protection systems, the USNRC established acceptance guidelines for D-in-D&D assessments. The guidelines are described in Branch Technical Position HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (see NUREG-0800, Chapter7, Instrumentation and Controls).

1. The applicant/licensee should assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.

2. In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, should be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.

Siemens Power Corporation submitted a topical report describing a digital I&C system for reactor protection to USNRC for review and approval. On May 5, 2000, the USNRC concluded the topical report was acceptable for referencing in license applications subject to limitations in the safety evaluation (SE). The SE stated that although the reliability of the system was assessed with both probabilistic and deterministic reliability analyses, it does not use these analyses as the sole means for accepting the safety system. The analyses are only related to the hardware aspects of the system. Confirmatory testing of the system included the software.

Appendix B
Reliability Databases and Reports (Draft)

USNRC publications providing guidance on the use of digital I&C in nuclear power plants are:

NUREG/CR-6241 discusses graded acceptance processes for commercial off-the-shelf software used in reactor applications. The guidance in this NUREG will aid the reviewer in the evaluation of acceptance processes that are part of commercial dedications of PLC embedded, operating system, and programming tools software.

Branch Technical Position HICB-18, Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems.

EPRI report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," provides more detail on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors.

Hardware unavailability of digital I&C systems are estimated for various environmental stress factors and are compared to their existing analog counterpart in NUREG/CR-6579 (USNRC, 1998).

The National Research Council study identified six technical issues associated with the use of digital I&C technology in existing and advanced nuclear power plant designs. The six technical issues are: systems aspect of digital I&C technology; software quality assurance; common-mode software failure potential; quantitative safety and reliability assessment methods; human factors and human-machine interfaces; and dedication of commercial-of-the-shelf hardware and software. Of these six, common-mode software failure and the quantitative reliability assessment issues are relevant to the development of the reliability database to support risk trade-off studies of ALWR designs.

Probabilistic analysis, such as fault tree analysis, of physical failures in safety-critical systems is well understood, however, the analysis of design faults is not as straightforward. For example, software faults are considered design faults. The USNRC considers software design errors to be credible common-mode failures that must be assessed. Software reliability is generally difficult to measure, if at not impossible, since many of the factors which influence reliability are qualitative in nature. A methodology using Bayesian belief networks to combine both quantitative and qualitative reliability factors to assess software (COTS software included) failure probability is proposed by Dahll (2000). Additional reliability modeling techniques are provided in NUREG/CR-6101 (Lawrence 1993).

Operational and testing experience associated with digital I&C technology are necessary to assess the reliability and availability of the digital I&C systems. Generally, formal testing of large-scale commercial software is conducted to demonstrate the functionality of the software to meet its intended objectives. Testing is fine in systems that are not safety-critical. For software embedded in safety-critical systems, testing is not feasible since a large number of tests must be conducted in order to demonstrate a high reliability. To aid in the probabilistic assessment, failure rate databases of digital components and software are needed. The National Research study concluded that software failure probabilities should be included in PRAs rather than ignoring software failures. They stated that estimating software failure probabilities is similar to the techniques of estimating rare event probabilities. Bounded estimates of software failure probability can be obtained from valid random software testing and expert opinion. Some

operational failure data from nuclear power plant have been identified for the NERI project. These sources are:

Mitchell,C. M. and K. Williams, 1993. Failure experience of programmable logic controllers used in emergency shutdown systems, Reliability Engineering and System Safety, 39 (1993) 329-331.

Paula, H. M., 1993. Failure rates for programmable logic controllers, Reliability Engineering and System Safety, 39 (1993) 325-328.

Paula, H. M., M. W. Roberts, and R. E. Battle, 1993. Operational failure experience of fault-tolerant digital control systems, Reliability Engineering and System Safety, 39 (1993) 273-289.

Roca, L. R., 1996. Reliability analysis for Atucha II reactor protection system signals, Reliability Engineering and System Safety, 53 (1996) 155-183.

Khobare, S. K., et al., 1998. Reliability analysis of microcomputer circuit modules and computer based control systems important to safety of nuclear power plants, Reliability Engineering and System Safety, 59 (1998) 253-258.

Lee, E., 1994. *Computer-based Digital System Failures*, U.S. Nuclear Regulatory Commission, AEOD/T94-03, July 1994.

Probabilistic safety assessment (PSA) has become a standard analysis tool in the nuclear industry to support risk-based decision making by the utility as well as the regulators. Potential sources of digital I&C failure data exist in these PSAs. International nuclear power plants using digital I&C technology are:

Table 1. Selected international nuclear power plants using digital I&C systems for plant control and protection.

Plant Name	Reactor Type	Country	Comments
Pickering	PHWR	Canada	CANDU; Pickering NGS A Risk Assessment, Ontario Hydro, 1995
Darlington	PHWR	Canada	CANDU; Darlington Probabilistic Safety Evaluation, Ontario Hydro, 1987
Wolsong3/4	PHWR	Korea	CANDU; Probabilistic Safety Assessment Report, Wolsong NPP2/3/4, AECL 1995
Sizewell B	PWR	Great Britain	Westinghouse
Kori	PWR	Korea	Westinghouse
Ulchin 3/4	PWR	Korea	Westinghouse
Yonggwang 1/2	PWR	Korea	Westinghouse
Yonggwang 3/4	PWR	Korea	Westinghouse
Kashiwazaki 6/7	ABWR	Japan	Hitachi, Toshiba, and GE

The National Research Council study stated that the digital I&C systems for nuclear power plants have very similar technological characteristics to digital I&C systems for other safety-critical applications used in the chemical process and aerospace industries. The difference in applications is the need for very high levels of reliability under a wide range of conditions in the nuclear industry as compared to the others. Further they concluded that probabilistic analysis is essentially the same in theory for commercial-off-the shelf equipment. The only limitation in

application arises in determining what field experience is valid in assessing the failure probability. Testing and expert opinion may be necessary in order to perform bounding calculations.

References

Dahll, Gustav, 2000. Combining disparate sources of information in safety assessment of software based systems, Nuclear Engineering and Design, 195(2000) 307-319.

Lawrence J. D., 1993. Software Reliability and Safety in Nuclear Reactor Protection Systems, NUREG/CR-6101, UCRL-ID-114839, Lawrence Livermore National Laboratory, November 1993.

Lofgren, Ernest V., 1997. Letter Report submitted to William Galyean, INEEL, dated July 17, 1997, Evaluation of the Voluntary Approach for Meeting NRC's Needs for Reliability and Risk Data, SAIC.

National Research Council, 1997. Digital Instrumentation and Control Systems in Nuclear Power Plants, National Academy Press, Washington, D. C.

Ramani, S., Gokhale, S.S., and Trivedi, K.S., 2000. SREPT: software reliability estimation and prediction tool, Performance Evaluation, Vol.39, no.1-4, p.37-60.

Xie, M., Hong, G.Y., and Wohlin, C., 1999. Software reliability prediction incorporating information from a similar project, Journal of Systems and Software, Vol.49, No.1, p.43-8.

USNRC, 1991. SECY-91-292 "Digital Computer Systems for Advanced Light-Water Reactors", September 1991.

USNRC, 1993a. SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs", April 2, 1993.

USNRC, 1993b. Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs", July 15, 1993.

USNRC, 1998. "Digital I&C Systems in Nuclear Power Plants; Risk-Screening of Environmental Stressors and a Comparison of Hardware Unavailability With an Existing Analog System", NUREG/CR-6579, January 1998.

Appendix B
Probabilistic Safety Assessment and the Regulatory Process Analysis of Necessary Changes

1. Introduction

1.1 Study Context and Purpose

The "Risk Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants," referred to here as the "Risk Informed NPP Program," is part of the Department of Energy's NERI initiative. The Risk Informed NPP Program has as one of its general objectives the development of a scientific, risk informed approach for identifying and simplifying deterministic Nuclear Regulatory Commission ("NRC") regulatory requirements for nuclear power reactors that do not contribute significantly, or at all, to nuclear power plant safety or reliability. The Risk Informed NPP Program envisions a new substantive NRC regulatory framework which use quantitative risk criteria and probabilistic safety assessments ("PSAs") as the principal means for assuring safety. More specifically, the Program contemplates a system of standards that would define essential safety functions, and then set availability standards for those functions. The availability standards would relate back to the NRC's quantitative safety goals, which are presumed to provide adequate protection of the public health and safety. The current NRC framework, especially its use of deterministic concepts of defense in depth, would be retained only when uncertainties cannot be resolved using risk-based methods.

The dramatic restructuring of the NRC regulatory framework that is envisioned cannot be entirely successful without careful consideration of regulatory process issues, for the NRC's review and hearing process must match the demands that will be placed on them by the extensive use of PSAs. It is the purpose of this study to address some of these process issues.

1.2 Scope of Study

The focus of this report is on the licensing of nuclear power plants, including the issuance of construction permits and operating licenses under 10 CFR Part 50, and combined licenses under 10 CFR Part 52. The NRC review prior to operation after issuance of a combined license, and the NRC review associated with issuance of early site permits should not involve extensive use of PSAs, and will not be a focus of this paper. Nevertheless, to the extent these limited reviews involve the use of PSAs, this paper's suggestions will be useful here as well. Consideration of NRC hearings is especially timely because NRC is now considering whether the hearing process for nuclear power reactors should be changed.

NRC rule-making processes, including standard design certifications under 10 CR Part 52, will not be addressed here. The NRC Staff and other review processes that function outside of adjudicatory hearings will be addressed in a separate report, which will include consideration of NRC's standard design review processes. Design certification under 10 CFR Part 52 is accomplished by rule-making, which does not require any form of oral hearing with examination and cross-examination of witnesses, and so a study of design certification would focus on Staff review processes rather than hearing processes.

1.3 Description of NRC Review Processes

1.3.1 NRC Staff Reviews

The NRC Staff review process for applications for permits, licenses, and standard certified designs for nuclear power plants has not changed significantly over the last several decades. The review process is carried out under the overall direction of the Office of Nuclear Reactor Regulation ("NRR"), and involves use of NRR personnel, personnel from other NRC offices such as Nuclear Regulatory Research, and NRC

contractors. When an application is received, it is distributed among the various NRC and contractor personnel who are assigned to particular parts of the application according to their expertise. The NRC Staff review is conducted under the direct supervision of a Project Manager, who is responsible, among other things, for coordination and meeting schedule milestones. The Staff review culminates in the issuance of a Safety Evaluation Report ("SER"), which may be supplemented various times depending on the need to address issues left unresolved or newly arising. Section 182b of the Atomic Energy Act of 1954, as amended ("AEA"),[1] includes a statutory requirement for review of power reactor construction permit and operating license applications by the Advisory Committee on Reactor Safeguards ("ACRS"). The ACRS's review culminates in the issuance of the ACRS letter, which may also be supplemented as needed.

When the NRC was confronted with numerous nuclear power plant licensе applications in the early and mid 1970s, the basis structure of the Staff review process was much the same as it is today. However, in recent years the Commission itself has been much more involved in the review process. Essentially all significant regulatory policy and important safety decisions are presented to the Commission by Staff for their review and decision. This adds some delay because of the need for the preparation of the necessary Staff paper (a so-called SECY paper) with policy options and discussion. On the other hand, early Commission involvement adds certainty that the final review results will be satisfactory to the Commission, and may in the end avoid the delay that would be associated with a Commission decision late in the review process that required re-review by Staff.

Also, when NRC was reviewing numerous applications, the review tended to focus, as a practical matter, in a limited set of current safety issues under active Staff review for all plants and novel issued presented in the particular case, with the assumption, based on representations in the application, that other issues had been satisfactorily resolved in accordance with prior precedent, as reflected in the Standard Review Plan. Also, for a considerable time, certain issues were placed in a formal category of generic "unresolved safety issues." See § 210 of the Energy Reorganization Act of 1974, 42 U.S.C.§ 5850. A practice developed whereby these issues were not addressed in the review of individual applications, but instead addressed by various nuclear regulatory research initiatives, with the expectation that generic or plant specific backfits could be imposed after license issuance if research results proved this to be necessary. This practice had the practical effect of reducing the scope of issues for Staff review in individual cases.[2] In recent years, these generic safety issues were essentially all resolved.

When, several years ago, the Staff was presented with the first new nuclear power plant applications in some time, in the form of applications for design certification under 10 CFR Part 52, the Staff review process had to be restarted. There was no ongoing series of reviews with results that could be relied upon, and so no basis to focus on only a limited set of issues that were the current subject of Staff concern. Moreover, the results of the resolution of all of the "unresolved safety issues" needed to be applied,

The result of all these factors (increasing Commission involvement, need to restart the review process, and application of unresolved safety issues results), combined with the need to develop new

[1]The AEA is codified at 42 U.S.C.§ 2011 et seq. This paper will use the AEA section citations, rather than refer to the United States Code ("U.S.C.") section citations, because most practitioners in the field are more familiar with the AEA section numbers.

[2]The practice was modified as a result of various adjudicatory decisions which allowed licensing hearings to include consideration of generic unresolved safety issues provided that the issue was not (and was not scheduled to be) the subject of rule making and a showing was be made that the issue had a nexus to the application under consideration and the resolution offered in the application was unsatisfactory. E.g. Gulf States Utility Companies, 6 NRC 760 (NRC Appeal Board,1977).

regulatory principles for the generic review of final designs, was that the reviews for the first round of certified designs were, in comparison to Staff reviews in the 1970's, extremely intensive, and resource and time consuming. As noted, NRC review processes conducted outside of hearings will be the subject of a separate report.

1.3.2 NRC Licensing Hearings

The NRC hearing process for nuclear power plants also has not changed significantly in the last several decades, or indeed much at all since the 1960s. To be sure, the scope of licensing hearings has been limited substantially by the allowance for certified designs under 10 CFR Part 52, Subpart B, which carve out safety issues from adjudicatory hearings and resolve them by rulemaking, and the possibility of early site permits and combined construction and operating licenses under section 185b of AEA and 10 CFR Part 52, Subparts A and C, which resolve safety issues at the construction stage or earlier, leaving a narrower set of unresolved issues to be resolved at the next NRC approval stage. Also, the 1992 amendments to the AEA gave NRC discretion to decide the kind of hearing that would be held prior to operation in the case of combined licenses. But, at least since the 1960's, hearings on construction permits and operating licenses have been conducted under 10 CFR Part 2, Subpart G, or its equivalent, rules of practice which were designed by the Atomic Energy Commission (NRC's predecessor agency) to conform to the formal, "on-the-record" hearing requirements of the federal Administrative Procedure Act ("APA").[3] "On-the-record" hearings are also sometimes called "formal adjudications" or "formal hearings." When 10 CFR Part 52 added the concepts of early site permits and combined licenses in 1989, the traditional requirement for formal licensing hearings on nuclear power plant license applications was simply carried over to the new types of licenses. 10 CFR §§ 52.21,52.85.[4]

This practice of holding formal hearings has been controversial from almost the very beginning of the civilian nuclear power plant program in the 1950s and early 1960s. NRC is currently examining whether the practice is required, and if not, whether it should be modified.[5] This paper will not attempt to "re-plow" the ground reasonably well-plowed by the many previous examinations of whether formal hearings are required by the AEA. Instead, this paper will proceed on the premise that the legal issue is not resolved definitively,[6] and offer suggestions on how the hearing process might be improved assuming, for purposes of argument, that formal hearings are required.[7]

---

[3]5 U.S.C. §§ 551 et seq.

[4]Early site permits, another innovation under 10 CFR Part 52, are regarded as partial construction permits, and are therefore subject to formal hearings like construction permits. 10 CFR § 52.21. However, design certifications are considered rulemaking, and so no formal hearings are required. 10 CFR § 52.51(a); APA § 4. However, as a matter of discretion, NRC has provided for hearings on design certifications.10 CFR § 50.51(b).

[5]SECY-99-006, January 8, 1999.

[6]The APA itself never requires formal hearings: only the agency's enabling statute can do this by using language that triggers the APA formal hearing requirement. In the case of nuclear power plant licensing, this boils down to the question whether the "hearing" required by AEA § 189a triggers the APA formal hearing requirement. There is a long discussion of this issue a study by the NRC Office of General Counsel, SECY-99-006, January 8, 1999. See also Advanced Medical Systems, 31 NRC 271 (NRC Appeal Board,1990). In Union of Concerned Scientists v. NRC, 735 F.2d 1437,1444 n.12 (D.C.Cir.1984), cert.denied, 469 U.S. 1132 (1984), the U.S. Court of Appeals for the D.C. Circuit (to which all petitions for judicial review of final NRC licensing decisions may be brought) observed that "there is much to suggest that the Administrative Procedure Act's (APA) 'on the record' procedures...apply...." Later, in Union of Concerned Scientists v. NRC, 920 F.2d 50, 53 n 3 (D.C.Cir.1990), the same Court retreated somewhat by stating that "it is an open question whether section 189(a)--which mandates only that a 'hearing' be held and does not provide that the hearing be held 'on the record' --nonetheless requires the NRC to employ in a licensing hearing procedures designated by the [APA] for formal adjudications." In its brief before D.C. Circuit, sitting en banc, in Nuclear Information and Resource Service v. NRC, 969 F.2d 1169 (D.C.Cir.1992), NRC argued unequivocally for the first time, after over

2. Problems Associated with the NRC Hearing Process

2.1 The Problems in General

There has not been a careful analytical study of the NRC adjudicatory hearing process despite the many criticisms of it.[8] Thus any criticism of the process, and suggestions for improvement, must at this point be based on judgment and experience base on participation in the process and selected case studies.

A few notable hearing cases explain why the process is so controversial. The application by Metropolitan Edison Company, Jersey central Power & light Company, and Pennsylvania Electric Company for an operating license for the Three Mile Island Unit 2 nuclear power plant was contested by plant opponents who requested and were granted a formal hearing before an three member atomic safety and licensing board. All material safety issues were potentially open for litigation in a hearing. Fairly extensive and time consuming formal hearings were held on safety and environmental issues, which included testimony under oath and cross-examination of witnesses, and there was a 46 page initial decision. Metropolitan Edison Company et al, 6 NRC 1185 (1977). Yet despite the time and resources devoted to the formal hearing process, the case highlighted none of the safety problems that only a few years later were to cause the most serious accident in U.S. nuclear power plant history. With the exception of offsite emergency planning, none of the issues that were litigated in the hearing dealt with any of the design or human performance problems that were later determined to have caused the accident, and the hearing on intervenor's contention that offsite emergency planning was inadequate did not include any convincing evidence that intervenor's concerns were justified.[9]

Contested formal hearings on Long Island Lighting Company's application for an operating license for the Shoreham nuclear power plant spanned about a decade, and entailed several hundred days of hearings, testimony of over 200 witnesses, over 60,000 pages of transcript, and numerous initial and intermediate decisions, until NRC dismissed the intervenors from the proceeding in 1989. Long Island Lighting Company, 39 NRC 211 (1989). The plant never operated beyond low-power testing, and was later decommissioned.

---

40 years of briefing and argument in nuclear licensing cases, that no formal hearings on nuclear power plant licensing applications were required, but the Court resolved the case in NRC's favor without reaching the this hearing issue.

[7]If APA formal hearings are not required, then under the APA NRC nuclear power plant licensing constitutes informal adjudication. Only one section of the APA, 5 U.S.C.§ 555, addresses informal adjudications. This section provides for such things as the right to be represented by counsel when appearance before the agency is compelled, issuance and enforcement of agency subpoenas, and notice of a denial of any application, with a statement of reasons. 5 U.S.C.§ 555 says nothing about any hearing. However, section 189(a) of the AEA would still require some form of hearing in contested licensing cases, but the term "hearing" in section 189(a) can then be read to include only an opportunity to submit written comment. Siegel v. AEA, 400 F.2d 778 (D.C.Cir.1968).

[8]A reasonably complete discussion of problems posed by the NRC hearing process can be found in the transcript of a series of NRC-sponsored informal meetings of hearing process reforms, held in October, 1999, and attended by representatives on NRC Staff, nuclear industry, intervenor groups, and others. The transcript can be found on NRC's web site at nrc.gov.

[9]Intervenors were prescient in suggesting the inadequacy of offsite emergency planning, but were unable to convince the atomic safety and licensing board of the seriousness of their concern because their evidence was weak and not supported by Commonwealth of Pennsylvania officials. Intervenor presented no direct testimony and assumed the essentially impossible task of trying to support their case by cross-examination). The most seriously contested and litigated safety issue was the adequacy of the plant containment and other structures to withstand a commercial airplane crash.

These few cases illustrate why NRC's practice of holding formal NRC licensing hearings has been controversial. Such hearings often miss the mark widely in highlighting the important safety issues, and can easily consume enormous time, resources, and money. To be sure, significant issues are sometimes raised and resolved.[10] Also, NRC's rules in 10 CFR Part 2 on admitting issues (called "contentions") for the formal hearing are often (but not always) applied strictly, with the result that intervenors with little technical resources are unable to obtain a hearing on some issues of concern to them. But, the NRC's rules serve to screen out parties with little or no technical expertise, and thereby perhaps hasten the inevitable decision adverse to intervenors without all the time, resources, and expense of a full hearing.

In any event, the point is not that formal hearings have no safety benefit, but rather that the safety benefit that they do produce often comes at great delay and expense. Moreover, there seems to be no proportion between the time and resources required and the significance of the issues being litigated. There could be better ways to produce the same or a greater safety benefit at lower cost for all concerned.

2.2 Special Problems Posed by Use of Probabilistic Safety Assessments

The use of PSAs as the exclusive or principal means to demonstrate compliance with quantitative risk criteria, could pose special difficulties in a formal hearing process. This is illustrated by the NRC hearings on the Indian Point site that were held in the five years between 1980 and 1985. In response to a petition filed by the Union of Concerned Scientists, the NRC in 1980 directed the holding of a formal hearing on the safety risks posed by the Indian Point Units 2 and 3 plants, sited on the Hudson River about 24 miles north of the New York City line. The principal objectives of the hearing were to determine, using state of the art PSA, what safety risk was posed by continued operation of the two units, and whether, as the Union of Concerned Scientists and other plant opponents claimed, the two units posed a greater risk than other U.S. nuclear power plants.

This is the most complete NRC hearing on a full-scope PSA. Because of the need to resolve numerous scope and procedural issues, the actual hearings did not begin until June 1982. There were 55 days of hearings, with 20 parties participating and over 200 witnesses testifying, The hearing transcript totaled over 18,000 pages. Over 35 attorneys entered appearances for the various parties. The three member atomic safety and licensing board issued a 272 page recommended decision in October 1983, and the NRC Commission issued its own 60 page decision in May 1985. Consolidated Edison Company of New York and Power Authority of the State of New York, 18NRC811 (Atomic Safety and Licensing Board, 1983); 21NRC1043 (Commission, 1985).

As would be expected, substantial time and resources were devoted in the Indian Point hearing to PSA methodology issues, including treatment of uncertainties and use of Bayesian statistics, However, substantial time and resources were also devoted to issues of compliance with NRC deterministic requirements, including requirements dealing with emergency planning and pressurized thermal shock. This was because the ultimate issue in the case (the safety risk posed by the two units) not only required estimations of core-melt probability, containment performance, and offsite consequences, but subsumed issues of compliance with regulatory standards as well. Estimation of offsite consequences from

[10]See Florida Power & Light Company, 6 NRC 541,544 (Appeal Board, 1977) (Applicant prevailed in this construction permit application hearing, but NRC noted that "[i]ntervenors clearly assisted in the search for the truth. Their contribution should not pass unnoticed." No hearing in the history of the NRC has resulted in the final denial of a nuclear power plant license application. At most, contested formal hearings have sometimes led to additional disclosures of the details underlying applicant's or NRC Staff's conclusions, or in some cases conditions on operation or design changes.

postulated accidents in particular, proved to be especially controversial, since all aspects of compliance with NRC's emergency planning rules were placed in issue.

The Indian Point case illustrates how the use of PSAs can easily add additional issues for hearing. The potential issues for hearing litigation of a full scope so-called level 3 PSA, which includes estimates of core melt frequency, containment failure probability, and offsite effects, include essentially all of the safety issues addressed by NRC's safety rules in 10 CFR Part 50, as well as additional issues associated with PSA methodology, including statistical methodology, data base adequacy, completeness, and treatment of uncertainty.

Further, in a hearing focused on compliance with deterministic requirements, the requirements themselves cannot be challenged. 10 CFR § 2.758. Thus, for example, compliance with all of NRC's rules applicable to off-site emergency planning will be sufficient to establish that the emergency planning is acceptable. For a PSA compliance with deterministic requirements can still present a material issue, depending on the PSA methodology. For example, examination of each of the elements of proof for compliance with NRC emergency planning rules (e.g., evacuation time estimates) would be material in litigating a full scope PSA, since issues associated with compliance would be relevant to the calculation of actual health effects (for example, evacuation time estimates would be relevant in estimating the accident doses that would be received by persons being evacuated). But since the end result is not compliance with deterministic requirements but calculation of risk, the litigation would proceed as if the regulation were being challenged. Thus PSA hearings would present a larger potential scope of issues, and could become even more complex and time and resource consuming that the prior hearings focused on compliance with deterministic standards.

Finally, the use of PSAs may highlight important areas where expert judgment is required because there are no generally accepted scientific methods or data on which to base a decision. In contrast, most deterministic regulatory requirements are drafted with a view to compliance demonstrations that rely on available date and generally accepted scientific methods. This raises some special issues about how differences among experts are or should be resolved in NRC hearings. These special issues are discussed below under expert elicitation.

In sum, extensive use of PSAs could easily exacerbate the time and delay problems associated with the current process.

3. Methodology and Assumptions

3.1 Purpose of Hearings

At the outset one must ask what hearings on PSAs, or indeed any hearings in the nuclear power field, should accomplish. Obviously, the most important objective is to reach the correct decision, or the truth, in the individual case. But other subsidiary objectives are possibly relevant, including (1) educating the interested public about the issues, (2) assuring the interested public that NRC is responsive to safety concerns, thereby enhancing the credibility of the NRC decision process, (3) creating an open forum for exposure of debatable safety judgments, which would serve as an incentive for a cautious approach by NRC (especially NRC Staff participating in the hearing process) to safety issues, and (4) creating a full record for judicial review that would minimize the likelihood of judicial interference in licensing decisions.[11]

[11] Judicial review of NRC licensing decisions is provided by § 189(b) of the AEA.

This paper will focus on construction of alternative hearing processes that are fair and reach the correct result in each individual case, while at the same time minimizing the time and resources required to do this. It is proposed that only after several such processes are developed and put forth should the other factors (besides judicial review) be considered in choosing among them, or others. Of course no decision making process is perfect, but the premise of this paper is that any hearing process that creates a significantly greater danger of producing an incorrect result than the present formal hearing process will not be acceptable. As to judicial review, this paper makes the reasonable assumption that any process conducted in accord with the APA will be capable of producing an adequate record for judicial review.

3.2 Scope of Hearings

Another important premise is that the hearing process is not intended to be the tool for resolving all safety issues presented by an application, supplanting the role of the NRC Staff, ACRS, and Commission. It is possible to imagine that the hearing process could serve this function, and it may be that plant opponents in individual cases expect it to accomplish this result and are disappointed when it does not. However here is no reason to believe that such a process would produce better safety results overall than the current Staff and ACRS review process, and good reason to believe that such an approach would add much complication, delay, and confusion. Something approaching this has been tried in the case of power reactor construction permits, because of the requirement in AEA § 189(a) for a hearing even if no interested person requests one. In such cases AEC found it necessary to create a issue where none really existed, and require the presiding officer (usually an atomic safety and licensing board) to determine in each case, without conducting a de novo review, if the license application was sufficient and the Staff review of that application was adequate. 10 CFR § 2.104(b)(2)(i). However, this hearing process could never be effective as a quality check on Staff without creating a duplicate technical organization within the atomic safety and licensing board panel. Constraints on resources made this impossible. At most, atomic licensing board members could raise a few discrete issues of particular interest to them, a function which more properly belongs to outside persons with a personal stake in the licensing decision.[12]

3.3 Standing

Finally, NRC requires that intervenors show "standing" in order to be admitted as a party to a hearing, or to request a hearing. This requirement is based on § 189(a) of the AEA which grants the right to a hearing only to a "person whose interest may be affected." This requires that a potential intervenor demonstrate that (1) it will be injured, for example by being exposed to radiation from routine or accidental releases, (2) the injury is fairly traceable to the licensing action being challenged, (3) the harm is within the zone of interests protected by the laws applicable to the NRC review, such as the AEA, and (4) the harm will be redressed by some decision in the proceeding. Sacramento Municipal Utility District, 35 NRC 47 (Commission, 1992). This requirement is designed to assure that the intervenor has a sufficient stake in the licensing action to raise particular issues and pursue them vigorously. This paper will not analyze this requirement, as it does not seem to be affected by an increased use of PSAs.

4. Nature of the Issues

Before addressing the subject of NRC hearings, it is also essential to distinguish among the kinds of issues that can be raised in a hearing. In general, these fall into four categories (1) policy issues, such as

[12]See e.g., the atomic safety and licensing board's decision in the uncontested construction permit proceeding for the Donald C. Cook Plant, Indiana & Michigan Electric Company, 4AEC226 Atomic Safety and Licensing Board, (1968).

whether nuclear power should be allowed or, if it is permitted, what the standards for license issuance should be, (2) legal issues, such as how the AEA or the NRC regulations should be interpreted, (3) ordinary factual issues, such as what occurred, by whom was some action taken, or with what motive was some action taken, and (4) expert opinion factual issues, such as what is the availability of a certain reactor component.

4.1 Hearings on Policy and Legal Issues

Consistent with general administrative law principles, it is generally agreed that policy and legal issues are not suitable for resolution in formal hearings by testimony and cross-examination.[13] Put another way, hearings with testimony and cross-examination are required only required where there are genuine issues of material fact. This is an established principle of administrative law that borrows from the concept of summary judgment in civil judicial trials. See Gelhorn & Robinson, Summary Judgment in Administrative Adjudications, 84 Harv.Law Rev.612 (1971); 10 CFR § 2.749. While this principle is easily stated, it is sometimes difficult to apply because it requires a rigorous analysis of the issues presented in a particular case, and an identification of the standards or criteria that are, or should be, applied, and the assumptions that are proper to make. For example, it is easy to say that an individual licensing hearing is not the place to decide what the criteria should be for an adequate offsite emergency plan, but more difficult to see that the application of these criteria to admission of contentions and evidence requires a policy judgment whether off-site emergency planning requirements can ever disqualify a site absolutely. See Commonwealth of Massachusetts v. NRC 924 F.2d 311 (D.C. Cir. 1991), cert. denied, 5024.899 (19__).

Moreover certain policy issues are often phrased in a manner such that they wrongly appear to be expert opinion issues. For example, whether certain low doses of ionizing radiation have any adverse health effect is a matter for expert opinion, but what a "safe" level of radiation might be sounds like an expert opinion issue but is not because, unless a threshold for radiation health effects is assumed, the question cannot be answered without some policy or value judgment (usually called a science policy judgment) about acceptable levels of risk. There is hope, with scientific progress, that matters of expert opinion or judgment can be resolved definitively based on scientific advances; science policy issues can never be resolved scientifically because they are not really scientific questions.

Issues of law or policy can be resolved by a variety of informal processes, including opportunity for written comment or briefing papers, and informal meetings or hearings. In NRC practice, policy issues are usually resolved generically by informal rule-making, with opportunity for public written comment and, in important cases, informal hearings or meetings before NRC Staff or the Commission. Policy issues that arise in individual licensing cases, that have not been resolved by rule, are generally decided by the Commission after written briefing and perhaps an informal Commission meeting, but they must be clearly identified as such in order to avoid formal hearings. In NRC practice legal issues are resolved by the presiding officer and the Commission, after informal procedures which usually include oral argument and written briefs.

The NRC processes for addressing and resolving legal and policy issues are generally in accord with established administrative law principles, and do not present any problems when there is increased use of PSAs. PSAs will not generally present issues of material fact, like intent, motive, or reconstructing

[13]E.g., Alianza Federal de Mercedes v. FCC, 539 F.2d 732 (D.C.Cir.1976); Panhandle Producers v. Economic Regulatory Administration, 822 F.2d 1105 (D.C.Cir.1987).

past events and if the licensing framework is constructed carefully, hearings on PSAs will not present generic legal or policy issues. Rather, PSAs are expected to present issues of expert opinion.

5. The Formal Hearing Requirements of the Administrative Procedure Act

5.1 NRC Rules of Practice

NRC's rules of practice for the conduct of formal licensing hearings are set forth on 10 CFR Part 2, Subpart G. With some exceptions, these rules largely parallel the federal rules of civil procedure for civil trials before a district judge. The important exceptions include NRC's requirements in 10 CFR § 2,714 applicable to specification of issues in the initial pleadings, which are more stringent than the federal rules, NRC's allowance of written as opposed to oral testimony, 10 CFR § 2.743(b)(1), and the inapplicability of formal rules of evidence. 10 CFR § 2.743(c).. Thus NRC rules allow for discovery by admissions, interrogatories, depositions, and document production, 10 CFR § 2.740, issuance of subpoenas to compel testimony, 10 CFR § 2.720, testimony and cross-examination of witnesses,10 CFR § 2.743(a), motions for summary disposition (the equivalent of motions for summary judgment), 10 CFR § 2.749, and require a decision by the presiding officer[14] based only on the record. 10 CFR §§ 2.760, 2.780, 2.781.

5.2 Delays Associated with APA Requirements

Little of the delay and expense associated with formal NRC hearings can be traced directly to the need for compliance with APA requirements for the conduct of formal hearings. Much of the delay is associated with the practice of delaying the start of the hearing until the Staff evaluation documents (the SER and environmental impact statement) are filed. There is also time required to decide on the sufficiency and scope of issues to be heard under NRC's strict pleading rules in 10 CFR §2,714 (so-called contentions) and disputes over discovery, none of which are traceable to an APA requirement.[15] Delays are also associated with scheduling difficulties (which will occur no matter what degree of formality applies to the hearing), and the drafting of a decision (which also will be necessary no matter what degree of formality is applied).

5.2.1 Cross-examination

As illustrated by the Shoreham and Indian Point hearings, the actual conduct of the NRC hearing can also require substantial time and effort. However, NRC's practice in conducting oral hearings goes beyond what the APA requires. With the possible exception of the right to confront witnesses and conduct cross-examination, which will be discussed below, under the APA, construction permits, operating licenses, and combined licenses are initial licenses, and the APA allows evidence to be received in written form in such cases. APA 5 U.S.C.§ 556(d). NRC rules also provide for submission of evidence in written form. 10 CFR § 2.743(b). Thus the APA and NRC rules of practice will allow the conduct of a purely paper hearing in these NRC licensing cases, provided the parties will not be prejudiced. The only

[14]The presiding officer, in NRC practice, is usually a three member atomic licensing board composed of an attorney and two others with technical qualifications. However, the APA would also allow an administrative law judge or one or more members of the Commission to preside. APA 5.U.S.C.§ 556(a).

[15]The APA provides for issuance of subpoenas, but not specifically for pre-hearing depositions, and the Freedom of Information Act provides for production of agency documents, but not with specific respect to hearings. It has been held that due process does not require discovery. Kropat v. FAA, 162 F.3d 129 (D.C.Cir.1998).

prejudice that could result from a purely paper hearing would the denial of oral cross-examination. Under NRC practice, virtually all of the direct and rebuttal evidence is submitted to the presiding officer and the parties in written form before the beginning of the oral hearing, and the actual hearing is devoted almost entirely to oral cross-examination.

However, virtually all evidence in NRC nuclear plant licensing hearings will be expert testimony. While NRC has stated that the scope of cross-examination is within the discretion of the presiding officer, Public Service Company of Indiana, 7 NRC 313 (Appeal Board, 1978), NRC practice has been to allow cross-examination of experts, provided a cross-examination plan is submitted in advance to the presiding officer.

Thus, even assuming that a formal on the record adjudication is required under the APA, the need for oral hearings in an NRC licensing cases depends on whether intervenors have any right to conduct an oral cross-examination of opposing experts. However, the APA only requires such cross-examination as is "required for a fill and true disclosure of the facts," APA 5 U.S.C.§ 556(d). It is well established that the right to cross-examination in a formal APA hearing is not automatic, and the party asserting the right must establish that the right is necessary in the particular case. The D.C. circuit has held that the proper means to counter expert testimony is not cross-examination but direct and rebuttal testimony by opposing experts, and that before cross examination can be required by the APA it must be shown with great particularity why direct and rebuttal testimony of experts will not be sufficient. Cellular Mobile Systems of Pennsylvania v FCC, 782 F.2d 182,198-200 (D.C.Cir.1985).

The circumstances and Court's decision in the Cellular case are illustrative of the limited role for cross-examination of experts under the APA. In Cellular an applicant for a FCC cellular telephone license challenged the FCC's grant of the license to the competitor after a proceeding in which the comparative merits of both applications were considered. The FCC refused to allow Cellular to cross-examine several of the successful competitor's experts, including a Doctor Lehman who testified on market research matters. Cellular argued before the D.C. Circuit that, through cross-examination of Doctor Lehman, it would have corrected his mis-perceptions as to Cellular's modeling approach, criticized his claims as to the lack of relation between demand for pagers and demand for cellular, and demonstrated that multiple acceptable methods exist for forecasting demand, none of which are precise and all of which are speculative. The Court upheld the FCC's denial of cross-examination of Doctor Lehman, even in the face of this cross-examination plan, "for the simple reason that these are all issues that should properly have been addressed in direct and rebuttal submissions, not by cross-examination." Id at 200, note 41.

It has also been recognized that cross examination is most usually required only when there are disputes about motive, intent, credibility, or the factual details of a past event. E.g., Union Pacific Fuels, Inc. v. FERC, 129 F.2d 157, 164 (D.C.Cir.1997); Louisiana Ass'n of Indep. Producers and Royalty Owners v. FERC, 958 F.2d 1101,1113 (D.C.Cir.1992).[16] Such disputes are often found in NRC enforcement disputes but would virtually never arise in an NRC licensing hearing focused on PSA issues.

In sum, most of the delay in conducting NRC hearings cannot be traceable to any specific APA requirement applicable to formal hearings. The delay in completion of actual oral hearings once they

[16]The Louisiana Association case also holds that, where rebuttal testimony of experts is allowed, denial of cross-examination of experts does not deny due process, and the failure to disclose the full basis for the expert's opinion, as a result of disallowance of discovery and cross-examination, will go the weight to be accorded the expert's opinion. See also, The Gray Panthers et al v. Schweiker, 716F.2d 23(D.C.Cir. 1983).

begin can be associated with the current practice of allowing extensive cross-examination of experts, much of which can likely be eliminated even assuming the APA formal hearing requirements apply. Under the APA, the right to an oral hearing with examination and cross-examination of witnesses does not depend on the size or nature of the project, or even whether the case is simple or complex. Instead, it depends on the nature of the issues. A simple case involving the smallest NRC-licensed activity will require cross-examination if, for example, the outcome depends on resolution of a dispute over what occurred at some time in the past. A complex case involving a massive NRC-licensed nuclear power plant project can be resolved based on written submissions if there are only disputed issues of expert opinion, and the bases for the opposing opinions have been sufficiently disclosed so that effective rebuttal opinions can be prepared.

5.2.2 Special Treatment of Legislative Facts

There is a well-established legal principle that no formal hearing is required for the decision-maker to rely on so-called legislative facts. E.g., Concerned Citizens of Southern Ohio, Inc. v. Pine Creek Conservancy District, 429 U.S. 651,657 (1977); Association of National Advertisers, Inc. v. FTC, 627 F.2d 1151,1161 (D.C.Cir.1979). As Judge Friendly said in WBEN v. United States, 396 U.S. 601, 618 (2d Cir.), cert.denied, 393 U.S.914 (1968):

Adjudicatory hearings serve an important function when the agency bases its decision on the peculiar situation of individual parties who know more about this than anyone else. But when, as here, a new policy is based on the general characteristics of an industry, rational decision is not furthered by requiring the agency to lose itself in an excursion into detail that too often obscures fundamental issues rather than legislative facts are usually observations or predictions that have general applicability, while adjudicative facts, which are properly the subject of formal hearings, deal with particular parties and factual situations.

Based on this distinction, it may be possible to categorize industry-wide failure data, and statistical predictions about failure probability which depend on industry-wide data, as legislative facts not suitable for formal adjudicatory hearings. This approach is supported by the legislative history of the APA, which includes the observation that " where the subject matter and evidence are broadly economic or statistical in character and the parties or witnesses numerous, the direct and rebuttal evidence may be of such a nature that cross-examination adds nothing substantial to the record and unnecessarily prolong the hearing." H.R. Rep. No. 1980, 79th Cong. 2d Sess, printed in Administrative Procedure Act, Legislative History 1944, 1946, at pg. 271.

This distinction would certainly support the concept, discussed below, that certain generic aspects of PSAs (for example, certification or approval of certain industry-wide availability data) might be addressed in NRC rule-making and thereby removed from case-specific hearing litigation. Whether the concept could be extended to particular expert opinion PSA issues arising in an individual licensing case is more difficult to resolve definitively. On the one hand, expert opinions on matters applicable the nuclear industry as a whole, such as opinions about safety function availability based on industry-wide data, do appear to meet the definition of legislative facts. However, reliance on the concept of legislative fact may not itself serve to eliminate a hearing requirement when the legislative fact is material to the decision and sharply contested. Moreover, the application of industry-wide data to a plant specific PSA is not a legislative fact but an adjudicative one. In sum, the distinction between legislative facts and adjudicative facts will support rule-making that would narrow the scope of PSA hearings, but is not clearly useful otherwise.

5.2.3 Other APA Hearing Exceptions

The APA also contains an exception from the requirement of formal hearings in cases "in which decisions rest solely on inspections, tests, or elections." APA 5 U.S.C.§ 554(a)(3). The legislative history of this exception indicates that it was intended to apply where the most important element of the decision is the judgment of the person who did the test or inspection. Final Report of the Attorney General's Committee on Administrative Procedures at 37. This suggests that the original drafters of the APA may have recognized some limits on the usefulness of trial type procedures when the result depends on expert opinion, although then, as now, cross-examination of experts in civil trials before judges was the norm. However, case-law interpreting the exception greatly limits its application. The case-law holds that the exception does not apply where matters of subjective judgment are involved. E.g., Union of Concerned Scientists v. NRC, 735 F.2d 1437 (D.C.Cir.1984)(exception does not apply to evaluation of results of emergency planning exercises).

Still, it is clear that NRC practice in allowing cross-examination of experts is more generous than the law requires. NRC does not require, as a condition of cross-examination, a showing why direct and rebuttal written submissions are not sufficient for a full and true disclosure of the facts, and has not generally limited cross-examination to issues of motive, intent, credibility, or details of past events.

6. Possible Reforms

6.1 The Baseline-Paper Hearings

The suggestions for reform of the NRC formal hearing process which follow will presume that formal APA hearings are required. As noted above, there is uncertainty whether formal hearings are required by the AEA, and so this assumption is conservative. If the assumption proved to be wrong, then the result will only be that NRC will have more flexibility to fashion its hearing rules of procedure.

As explained above, the APA will allow for hearings in NRC construction permit, operating license, and combined license cases to consist entirely of written testimony of experts, provided there has been full disclosure of bases for the experts' opinions, and there are no issues relating to motive, intent, credibility, or past events. NRC could amend its rules to eliminate the need for oral hearings (essentially cross-examination) in such cases absent a specific demonstration why written expert rebuttal testimony cannot be prepared. NRC could further provide that if there has been a full prior disclosure of the expert's assumptions, methodology and factual predicates, cross examination will generally not be allowed unless there is a dispute over motive, intent, credibility, or past events.[17]

The NRC Staff acceptance process for applications, which addresses whether the application is sufficiently complete for initiation of Staff review, will need to be applied rigorously for this to work. However, even with a rigorous acceptance review process, it is likely that the license docket will still have gaps that would need to be filled for an intervenor's expert to prepare effective rebuttal. Thus, as soon as an intervenor is admitted as a party, the applicant should establish a data room with all of the materials referenced or relied upon in the application (PSA), and grant intervenor (and its experts) access.

[17]A general survey of NRC atomic safety and licensing board licensing decisions over the past quarter century would likely show that plant opponents are almost never successful in proving their case by cross-examination, without presenting their own expert testimony. Indeed, NRC devices such as summary disposition and pleading requirements for admissibility of issues for the hearing make it very difficult to proceed to hearing without the assistance of experts.

This change in NRC rules of practice would eliminate the need for most, if not all, oral hearings in initial licensing cases.[18] As noted, to be effective in eliminating oral hearings, there must be a sufficient prior disclosure of the bases of all expert testimony. Only with such prior disclosure can an expert's testimony be critiqued by an opposing expert, and effective rebuttal testimony prepared. If effective rebuttal testimony cannot be prepared, then there is a plausible basis to allow cross-examination, although ever in this circumstance it may be sufficient for the testimony to be discredited by the opposing expert for lack of basis.

Based on the above, one form of hearing could consist of the following. First, at some point during the Staff review, the intervenor would be required to file a list of issues it wishes to contest in reasonable specific detail. At the discretion of the Commission, intervenor could be required to file a more specific statement. The Staff and applicant would then be required to address each issue in a written submission which could if appropriate simply reference prior docketed materials. The application, as amended, and the Staff Safety Evaluation Report, as supplemented, along with the written submissions, would then be filed formally with the presiding officer, presumably a three member atomic safety and licensing board.[19] The filing would under the revised rules serve as an automatic motion for summary disposition of all contested safety issues. The burden would then shift to intervenor to present contrary expert opinion, or justify the need for cross-examination of Staff or applicant experts under the strict rules described above. Intervenor expert opinion would need to be supported by all material relied upon.

Absent the need for cross-examination, the hearing would be a paper hearing, consisting of the application and Staff Safety Evaluation Report materials, the written submissions on the contested issues by NRC Staff and applicant, the written expert testimony of intervenor, and written expert rebuttal testimony prepared by Staff and applicant. Cross-examination of intervenor's expert by Staff or applicant would be allowed, but only under the same strict rules that applied to intervenor cross-examination.

The presiding officer's decision would identify all of the genuine issues, grant summary disposition of those not put in proper controversy by expert opinion and (absent need for cross-examination) decide the controverted issues on the basis of the papers that have been filed. Before the decision on any properly controverted issues (opposing expert testimony), parties would be given the chance to present proposed findings, either in writing or by an informal oral argument, subject to questioning by the presiding officer.

Current NRC practice resembles this proposal somewhat. NRC's rules of practice currently require that a contention, to be admitted for litigation, include a statement of the alleged facts or expert opinion, together with references to specific sources and documents of which intervenor is aware and which intervenor intends to rely in support of the contention. The contention must have sufficient detail and support to show that there is a genuine dispute. 10 CFR § 2.714. In short, current NRC practice will not allow admission of an issue (or contention) for litigation, or even for discovery, without there being some support offered in support in the form of documentary evidence or expert opinion. See GPU Nuclear Inc., Jersey Central Power & Light Company, and Amergen Energy Company, LLC, __NRC__

[18]While the terminology is awkward, it is well established that a "hearing" can consist entirely of written submissions, with nothing oral to be actually heard. E.g., Siegel v. AEC, 400 F.2d 778 (D.C.Cir.1968).

[19]Use of a presiding officer other than a three-member atomic safety and licensing board, administrative law judge qualified under the APA, the Commission, or one or more Commission members, will present a legal issue of APA compliance if formal on-the-record hearings are required by the AEA. Section 556(b) of the APA provides that "there shall preside at the taking of evidence-(1) the agency;(2) one or more members of the body which comprises the agency; or (3) one or more administrative law judges appointed under section 3105 of this title."

(Commission, May 3, 2000). However, when NRC rejects a contention for lack of sufficient basis under the rule, it denies a hearing on that issue rather than holding one. The proposal discussed above for paper hearings would go the further step of holding a paper hearing on contentions which have been admitted for litigation because they have been supported with sufficient basis in expert opinion.[20]

6.2 Supplemental Hearing Procedures

On might, again with full regard for APA requirements, construct a public hearing process which attempts to adopt the processes followed within the scientific community for resolving PSA disputes and other expert opinion issues, to the extent practicable. At the outset three possibilities come to mind as possible models- scientific peer review, expert elicitation, and the NRC Staff review process itself.

6.2.1 Peer Review

Many scientific developments are subjected to a peer review process. This consists of a critical evaluation of the scientific work by peers with comparable expertise (subject matter experts) but who are independent of the work being reviewed. A common kind of peer review takes place in a pre-publication review of an article before publication in a scientific journal. Also, the National Academy of Sciences is often called upon to review scientific reports or issues and issue documented reports of its conclusions. In principle, the peer review process is sufficiently flexible to be tailored to fit the importance of the matter being reviewed.[21]

Typically, peer reviews address the quality of a proposed scientific approach to a problem, and entail the application of subject matter expertise to the proposal. The peers may comment on the validity of the assumptions, the appropriateness of and consistency in application of the methodology, the validity of the conclusions, and uncertainties. Peers could also comment on alternative approaches or explanations of the data being used, and the contributions of the proposal to advancement in the state-of-the-art. In peer reviews that have been structured with special care, because of the importance of the issue, there will be advance screening of subject matter experts for possible conflicts of interest, thorough documentation of the process, and structured interaction among several of the subject matter experts.[22]

---

[20]Elimination of the current requirements for filing of contention basis and for ruling on contention admissibility early in the application review process would give intervenors more time to obtain experts and prepare their case. Early contention filing would be unnecessary as a tool to limit discovery if discovery is otherwise limited or eliminated. On the other hand, postponing the identification of contested issues will prolong the period of uncertainty during which the need to hold a hearing (whether an oral or a paper hearing) will be undecided. Also if the application needs to include a specific evaluation of intervenor issues, and the Staff SER needs to address them as well, then the identification of intervenor's issues must be early enough in the process so that the SER schedule is not unduly affected. Delay will place a considerable pressure on the presiding officer, since once the Safety Evaluation Report is issued and filed with the presiding officer, the presiding officer's decision could be on the critical path for the ultimate NRC decision on the application. Timely decisions, off the critical path, should be feasible for paper hearings even with some delay in identification of the issues, but if there is no early requirement for filing of issues, there is a danger that the need for an oral hearing may not be decided until it is too late to avoid delay should an oral hearing be required.

[21]For a general discussion of DOE peer review processes, see Federal Research: DOE is Providing Independent Review of the Scientific Merit of its Research, GAO RCED-00-109.

[22]See DOE's rules on reviews of proposed grant and cooperative agreement projects in 10 CFR Part 600. The Department of Health and Human Services provides for peer reviews of activities of health care providers under the Peer Review Improvement Act. See, e.g.,42 U.S.C.§ 1320(c).

Appendix B
Probabilistic Safety Assessment and the Regulatory Process: Analysis of Necessary Changes

In the general sense, the NRC license application review process already includes several peer reviews- the review by NRC Staff and the review by the Advisory Committee on Reactor Safeguards. There is no apparent reason to add still another peer review to the process, but the question here is not about adding another review, but of restructuring an existing review process (the licensing hearing) so that it took advantage of processes found to work well in good peer reviews. In particular, assuming an interested person puts forward a reasonable specific issue of scientific opinion, can the hearing process incorporate useful lessons from the general field of peer reviews.

One difficulty with using peer review as a hearing model is that peer review may not be suitable in reaching a decision when there are two or more respectable points of view by legitimate experts. This is discussed further below. Also, there is no one model peer review to follow, But the essential elements of a good peer review appear to be (1) a decision by a person (or persons) with subject matter expertise who has not participated in the work being reviewed, and who has no financial or other personal stake in the review results, (2) a process that allows a full understanding of the work being reviewed, (3) a fair means to resolve differences of opinion, if more than one expert peer reviewer is involved, and (4) documentation of the processes and review results.

The paper hearing process outlined above would satisfy some but probably not all of these attributes. First, the presiding officer would not have participated in either the development of the application or the NRC Staff's review of it, and would have no financial stake in the review results. The results will be fully documented, given the APA requirement for a decision on the record. And the deliberations among three-member atomic safety and licensing board members, and a decision based on majority vote with opportunity for written dissent, would be a fair process.

However, it will probably be impracticable to have the presiding officer decision-maker be a subject matter expert for each expert opinion controverted issue, unless the NRC is willing to appoint licensing board members with subject matter expertise on a temporary case-by-case basis. Moreover, a purely paper-based decision process might place an undue constraint on the ability of the peer-reviewers (the presiding officer) to get a full understanding of the issues in controversy. There would likely need to be some form of process for face-to-face interaction between the testifying experts and the reviewers, although this could be at the discretion of the reviewers.

Also, the requirement of the APA that the decision be based only on the record could, unless carefully applied, place an undue constraint on the ability of the subject matter expert-decision-maker to consult expert sources for his or her review that are outside the record. Off-the-record consultation can raise serious issues, including dilution of the independence requirement when outside sources with a stake in the controversy are consulted and inability of the parties to address all opposing expert opinion. However, the subject matter expert needs to be able to apply his or her scientific expertise to bear, at least to the extent of applying generally accepted scientific principles and standard texts and reference materials.

This possible problem can be mitigated by judicious application of a long-standing NRC practice- the use of official notice. NRC's rules allow the decision-maker (or presiding officer) to take official notice, that is consider as part of the record for decision, "any technical or scientific fact within the knowledge of the Commission as an expert body." The NRC decision-maker can then apply those facts to the resolution of any controverted issue, provided only that the parties to the proceeding are advised whenever this is done and given an opportunity to controvert the use of the facts officially noticed by either appealing to the Commission or asking the presiding officer for reconsideration. 10 CFR § 2.743(i).

This will allow the expert decision-maker to use commonly used scientific texts, handbooks, treatises, and the like, but would not allow off-the-record consultation of other experts.

Finally, assuming that the decision of an atomic safety and licensing board is based on the evaluation of conflicting testimony by one or more board members with subject matter expertise, the use of this expertise can take the form of a simple exercise of expert judgment by the board. For example, in the Indian Point case discussed above, there was substantial evidence offered both in support of using Bayesian statistics and the proposition that states of belief of individuals can with confidence be converted into a realistic probability distribution. The presiding atomic safety and licensing board rejected this testimony, and chose instead to rely on other testimony using more (then) conventional methods. This appears to be simply the result of the board's expert judgment. See 18 NRC at 855-856. However, the basis for this judgment is not stated explicitly. The result of such a peer review type process is that the hearing outcome is dictated by the education, experience, and other personal qualities of the subject matter expert who happens to sit on the atomic safety and licensing board. This reduces the predictability of the process.[23]

6.2.2 Expert Elicitation

6.2.2.1 Role of Expert Elicitation

As indicated above, the focus here is on means to resolve issues of expert opinion. Experts can disagree for a variety of reasons. For example, different results can be reached because of incomplete analyses or internal inconsistencies. Also, experts often do not possess or actually use the same data. Sometimes experts do not have access, or for some reason do not actually use, the same data as other experts. Or, experts may differ as to the adequacy of weight to be given to particular data.

Apparently opposing experts sometimes have different answers because they are assuming different premises. For example, if the dispute is over whether low levels of ionizing radiation have adverse health effects, one expert may be addressing whether there is any evidence that there are no such effects, while another may be addressing whether there is any affirmative evidence that there are such affects. In effect, one expert has proceeded on the basis of a science policy judgment that effects should be presumed to occur absent evidence to the contrary, while the other has proceeded on the basis of the opposite premise. In the Seabrook operating license case, intervenors offered the opinion that offsite emergency plans were inadequate because the residual health effects following a postulated accident were too high, even assuming applicant's emergency plan functioned properly, while applicant and NRC Staff offered expert opinion that offsite emergency plans were adequate based on compliance with NRC emergency planning standards, and the implicit assumption that the actual magnitude of offsite health effects, after a postulated accident, were irrelevant.[24]

Experts may use the same data but use different analytical approaches. For example, in the Indian Point case noted above, PSA experts reached somewhat different results when one used what the atomic safety and licensing board referred to as "conventional statistical methods" and the other used Bayesian methodology.[25]

---

[23]It may be argued that the board's decision was based implicitly on its choice of what it saw as the "traditional" approach, but this is not explicit in the opinion.

[24]Commonwealth of Massachusetts v. NRC, supra.

[25]See Consolidated Edison Company of New York, 18 NRC 811, 849-856 (Atomic Safety and Licensing Board, 1983).

Various biases can affect the expert's opinions. In the nuclear field, where emotions rum high and experts can easily fall into a pro- and anti-nuclear camp, expert opinions may be influenced by the pressure to conform to general notions about how nuclear power is safe or unsafe. Or an expert's background and experience can influence the result. For example, imagine the different approaches that might be take by two experts about the likelihood of a tornado, one of whom just had his home destroyed by a tornado. Sometimes expert opinions are colored by different beliefs as to the degree of certainty required. An expert may believe that data are not sufficient to support a favorable safety conclusion because the expert believes that the consequences of a mistake will be a catastrophe, and as a result, a high degree of certainty is required.

Review of a contention and supporting testimony by an independent subject matter expert, as in a peer review, should be sufficient for decision if there are no factual issues and one expert's opinion can be disregarded because he or she has used an incorrect premise, addressed the wrong question, used incomplete or unreliable data, or relied on inconsistent assumptions or otherwise used faulty methodology or logic. Here subject matter experts should be able to reach consensus using normal techniques, since on careful analysis one opposing opinion is wrong or irrelevant.[26] But a more difficult situation is presented if the decision-maker is presented with conflicting expert opinion on the same issue, with both experts appearing to use the same assumptions and acceptable data, and neither expert is guilty of using faulty methodology or logic. An example of this is the conflict of expert opinion on the use of Bayesian statistics in the Indian Point hearing.

A possible resolution would be based on a comparison of the education, experience, and other expert qualifications of the experts, or an exploration of possible kinds of bias, with the result that the least biased expert with the better qualifications prevails, but this can be criticized as arbitrary given that both are legitimate experts, and both are using acceptable data and methodology. Moreover, this makes for a decision process based on subjective comparisons of expertise and bias.

Another possible approach would be adoption of that opinion that produces the more conservative (safer) result, especially if this result in consistent with current perception of the "usual way to approach the problem." A variant on this method would be to defer to the NRC Staff position. Indeed, since the NRC Staff is always a party, has an established track record of reasonably thorough expert reviews, has no financial interests at stake in the controversy, and can be presumed to have performed its review in accord with current Commission policies, such deference is natural. But this approach can penalize innovation and scientific advance, especially where the Staff position is an easily reached conservative one that sidesteps the difficult issues.

Ultimately, under the current process, the choice may be based upon the expert judgment of one or members of the atomic safety and licensing board, subject to Commission review. Assuming the expert opinions are all of essentially equal scientific validity, there is no scientific reason why the board's expert judgment should prevail over any other expert's judgment. But if a decision is necessary, the atomic safety and licensing board prevails simply because it has been delegated this decision function by the Commission, which is accountable ultimately to the citizens of the United States.

A significant difficulty with this process is that the decision-maker may have no assurance that the expert opinions that have been offered by the parties represent the full range of opinion on the issue.

---

[26]For example, in the recent case of Hydro Resources, 50 NRC 3 (Commission, 2000), the Commission rejected several concerns regarding the amount of water withdrawn from uranium producing wells.

In fact, the contrary is likely to be the case, since each party will likely have selected experts who would be expected to support their respective litigating positions. Expert elicitation offers a possible solution to this problem.

Expert elicitation is a formal, structured, and documented process whereby judgments of multiple experts are obtained. The process usually includes subject matter experts, as in peer reviews, normative experts, with expertise in statistics, decision analysis, probability encoding, and a generalist, who guides the elicitation.[27] Expert elicitation has been used by NRC on several occasions, most notably in NUREG-1150 and 10 CFR Part 100. 10 CFR § 100.23, which establishes seismic and geologic criteria for nuclear power plant siting, authorizes the use of a "probabilistic seismic hazard analysis" in establishing the safe shutdown earthquake ground motion, which represents the design basis for certain safety structures, systems, and components. The regulatory history for the rule indicates that NRC approved of certain probabilistic seismic hazard analyses which were based on expert elicitation. See 61 Fed.Reg. 65157, December 11, 1996.Thus it is clear that NRC has approved of the use of expert elicitation. NRC has even suggested guidelines for the proper conduct of expert elicitations,[28]

Expert elicitation provides a substantial advantage over the current hearing process, especially in assuring that the decision-maker has before it the full range of responsible expert opinion. However, many of the other elements of the expert elicitation process have almost exact parallels in a well conducted formal hearing process. Both processes include a very precise definition of the issue, a very clear definition of the permissible assumptions and underlying scientific data, a rigorous qualification of experts, an exploration of possible expert conflicts of interest and biases, and full documentation of the results.

Nevertheless, structuring the NRC hearing process based on expert elicitation techniques will be impracticable, if not impossible. It will not be possible, except perhaps in the most important cases, to use the full range of subject matter experts to testify about a contested issue, and to use the appropriate normative expert in decision-making, because doing so will be extremely expensive and time consuming,

A fundamental assumption of expert elicitation is that expert opinion can be regarded as another kind of scientific data that can be treated statistically. The use of multiple subject matter experts will capture the diversity, and hopefully the full range of expert opinion on a particular issue. However, to make this collection of judgments useful to a decision-maker, the judgments must be aggregated or combined in some fashion. For example, if the issue is the specification of a particular probability of an event occurring, each expert may have offered his or her own opinion as to the current uncertainty in the value, expressed as a probability distribution. Aggregation techniques have been developed to combine these various distributions into a single one for use in the PSA. Aggregation techniques include various statistical techniques such as averaging and weighted averaging. Unfortunately, there is no generally agreed upon way to do this.

The APA decision process, and the NRC decision process based upon it, generally assume that there is a single "right" answer to any given question, and that when experts offer conflicting opinions one is right and the other is wrong. Thus there is little (and likely no) precedent for a presiding officer (an atomic safety and licensing board) to aggregate the opinions of the various experts who have testified

[27]See Branch Technical Position on the Use of Expert Elicitation in the High Level Radioactive Waste Program, NUREG-1563, 1996.

[28]See note 27.

about a particular issue, or to assure that the experts testifying represent the full range of expert opinion. Indeed, since there is no consensus as to how expert opinions should be aggregated, that very aggregation method would, under normal evidentiary rules, itself be a matter for expert testimony and possible dispute.

In sum, expert elicitation techniques offer useful insights into how differences in expert judgment can be analyzed, but do not easily provide models for conducting licensing hearings. However, a properly conducted expert elicitation offers substantial advantages over a hearing process that includes the opposing opinions of a few experts, with no assurance that the range of respectable expert opinions are represented.

6.2.2.2 Expert Elicitation as Evidence

A properly conducted expert elicitation should have special evidentiary weight. NRC needs to address how expert elicitation results can be introduced as evidence and what weight they deserve. It is not clear whether the results of an elicitation can be sponsored into evidence by the generalist or normative expert. If not, how can the testimony of one or even a few of the subject matter experts represent the full range of opinion? Must every expert testify, or can the experts delegate a representative who can speak for all of them? Must the decision-maker accept the aggregation technique selected by the normative expert, or can the decision-maker use the expert judgments to apply a different aggregation methodology and reach a different decision? Perhaps the most serious question is how the results of an expert elicitation should be compared with the contrary testimony of a single intervenor expert. Treating the elicitation as no more weighty than the opinion of a single expert, to be contrasted with the opinions of one or a few others, would be contrary to the elicitation and aggregation concept, yet adding the testifying experts' opinion to the opinions already included in the elicitation, and then using the same aggregation technique, would be difficult, given the testifying experts' lack of participation in the process. And, if the atomic safety and licensing board's decision ultimately is based on the judgment of one or more experts on the licensing board, as in the Indian Point case, then the same questions can be raised about the role of this opinion.

If expert elicitation is to be used and the results offered as evidence in hearings, NRC should develop some evidentiary rules to facilitate this. Among other things, the rules should identify how the evidence should be introduced and the weight that should be given to expert elicitation results. Also, assuming atomic safety and licensing boards will make decisions based on their own expertise, as in the Indian Point case, NRC will need to be sure that board members are conversant with the PSA state of the art, and are fully attuned to the Commission's expectations as to how the new licensing framework should function.

6.2.3 NRC Staff Reviews

The NRC Staff has decades of experience in addressing and resolving differences in expert opinion. This process can be examined to see if one or more aspects of it can be adopted for use in licensing hearings.

The Staff review process consists of expert review of the application (and materials referenced therein, as needed), followed by submission of several rounds of written questions to the applicant. The questions are typically the subject of a face-to-face meeting between applicant's and NRC Staff experts, in which Staff might clarify the basis for its concerns and applicant might offer preliminary responses. The meeting is followed up by a formal applicant submission of answers to the questions posed by Staff, typically in the form of an amendment or supplement to the application. Policy or legal issues are referred to the Office of General Counsel, senior NRC officials, or the Commission itself for resolution. The process has never been conducted without some direct interaction between Staff and applicant experts. This suggests that a purely paper hearing might be unsatisfactory.

A public hearing process based on the Staff review process above might consist of the following. Intervenor would be allowed to submit written questions to the applicant. A limit on the number of questions could be imposed, as is the case for the number of written interrogatories allowed under the rules of discovery in the federal district courts.[29] Staff would be allowed to request that the interrogatories be clarified, if necessary, or to disallow those that appear irrelevant. A face-to-face informal, transcribed meeting between applicant and intervenor would be held, if requested by any party, facilitated by an NRC Staff member with some appropriate training in meeting facilitation. At the meeting applicant could seek clarification of intervenor's questions, and would be expected to offer preliminary responses, with an intervenor or Staff having the opportunity to comment. NRC Staff could question either party. After the meeting, if any, formal answers to the interrogatories would be filed. Staff would have the discretion to require more specific or clarified written answers.

At the conclusion of the intervenor interrogatories phase, intervenor would be required to file a list of issues it wished to contest, along with its own expert evaluation with supporting information, as if it were filing a competing application for license denial or conditioning. At this point the process would be reversed, with applicant and NRC Staff allowed to pose a limited number of questions to intervenor's expert, and with the opportunity to have a meeting with intervenor's expert.

Intervenor's issues and expert report would be addressed in the Safety Evaluation Report and application, to the extent they have not already been addressed, and the process would proceed as in the paper hearing process described above, with the application, Safety Evaluation Report, and expert report serving as the basis for decision. An opportunity for an oral presentation before the presiding officer, in the form of oral argument based on the written submissions, could be afforded.

Policy and legal issues would be resolved by simple referral to the Commission or presiding officer, based on written submissions, with the presiding officer or Commission having the option to hold an informal hearing or meeting.

---

[29] E.g., Rule 26.2(b) of the Local Rules of Civil Procedure for the U.S. District Court for the District of Columbia, which presumptively limit each party to a complex case to no more than 25 discrete questions, however the interrogatories are numbered.

6.2.4 Use of Presumptions

NRC's regulations serve to carve out issues from hearings and resolve them in rule-making, which under APA 5 U.S.C.§ 553 and AEA § 189a does not require any oral hearing. Siegal v. AEC, 400 F.2d 778 (D.C.Cir.1968). Design certification under 10 CFR Part 52, Subpart B is an example of this legal device. Under 10 CFR § 52.63 issues resolved in the design certification rule making cannot be raised in individual licensing hearings except on very limited grounds. All substantive NRC rules have a similar effect under 10 CFR §2.758. Thus. for example, compliance with 10 CFR § 50.46, "Acceptance Criteria For Emergency Core Cooling Systems for Light Water Nuclear Power Reactors," will generally serve to demonstrate that a particular emergency core cooling system design will be sufficient to cool the core so as to prevent core damage after a loss-of-coolant accident, and no party in a hearing will be allowed to argue that compliance with the criteria will not assure this result. This is an example of NRC's use of a legal presumption: compliance with 10 CFR §50.46 creates the presumption that the design in question will cool the reactor core following a postulated loss-of-coolant accident.

In most cases the presumption is associated with a regulatory requirement. For example, compliance with 10 CFR § 50.46 is required. But it is possible to create presumptions that do not have any associated requirements. The classic example of this is NRC's rule specifying the environmental effects of the uranium fuel cycle for inclusion in environmental impact statements. This rule in 10 CFR § 51.51, which was upheld by the U.S. Supreme Court in Vermont Yankee Nuclear Power Corp. v NRDC, 435 U.S. 519 (1978), specifies the environmental effects of the uranium fuel cycle and creates the presumption that use of these specifications will satisfy the requirement of the National Environmental Policy Act of 1969)"NEPA"). But 10 CFR § 51.51 does not impose any requirements on applicants or licensees to adopt any measures to eliminate or reduce the environmental effects so specified. This is left for other rules and other agencies.

Presumptions without requirements, like 10 CFR § 51.51, have the advantage of eliminating unnecessary hearing litigation without reducing an applicant's flexibility to propose innovative designs or techniques that would otherwise run afoul of an NRC requirement. Presumptions like this should be sustained in the courts so long as there is a rational connection between the matter presumed and the facts giving rise to the presumption. Massachusetts v. United States, 856 F.2d 378,383 (1st Cir.1988). They could be used to streamline or eliminate hearing litigation over PSA's. For example:

- NRC could by rule certify or approve of component failure databases, or even particular component failure probabilities.

- NRC could, by rule, approve of certain PSA methodologies.

6.2.5 Qualification of Experts

Only experts in a particular field are qualified to offer expert testimony. NRC could enforce strict rules on qualification of experts. For example, NRC might require certain minimum educational or professional experience requirements in order for someone to offer expert opinion on PSA matters.

6.2.6 Discovery

As noted above, NRC's rules allowing discovery are generous beyond what the APA would require, even for formal hearings, and might be modified. Except as required by the Freedom of Information Act, document production could be eliminated. However, to assure fairness and eliminate

the need for later cross-examination at the hearing solely to learn the bases for the expert opinions supporting the PSA, documents used to support the PSA, and necessary for an expert review of the PSA, should be disclosed automatically.

Depositions could be subject to the same rules that apply to cross-examination or eliminated altogether. As needed, interrogatories could be limited in number.

6.2.7 The New Framework Itself

The new risk-informed regulatory framework will be an important factor in eliminating unnecessary hearing litigation. Most importantly, regulatory science policy judgments must be resolved in the framework in order for the hearing not to become bogged down in policy disputes that are not amenable to scientific proof in the ordinary sense. This will necessarily include specification of the critical risk criteria, such as the ultimate quantitative safety goals which, if met, would be presumed to provide adequate protection. Acceptable core damages frequency and containment failure probability should also be specified, either as requirements or as criteria which, if satisfied, are presumed to show compliance with the quantitative safety goal criteria themselves. In especially difficult areas, the rulemaking could relate PSAs to deterministic criteria, with the result that the review and licensing hearing could focus on the criteria and not the PSA.

Treatment of uncertainty will be an important aspect of the new framework. In NRC licensing proceedings, the applicant has the ultimate burden of persuasion. APA 5 U.S.C.§ 556(d); Director, Office of Workers Compensation Programs, Department of Labor v. Greenwich Collieries, 512 U.S. 267 (1994). This means that if, after all of the evidence has been received and considered, the agency ultimately concludes that neither plant opponents nor plant proponents have proved their case, the application must be denied. However the degree of proof needed is somewhat unclear. The general rule in administrative law cases is that applicant's position must be supported by at least a bare preponderance of the evidence. Steadman v. SEC, 450 U.S. 91 (1981). NRC has followed this same definition of burden in licensing cases. Pacific Gas & Electric Co.,19 NRC 571 (Appeal Board, 1984), Commission review declined, 20 NRC 285 (1984). But NRC has also sometimes enunciated a different formulation that probably reflects more accurately actual practice. In Virginia Electric & Power Co., 1 NRC 10 (Appeal Board, 1975), the Commission's Appeal Board, which under the rules then extant spoke for the Commission itself, indicated that the burden of persuasion should be influenced by the gravity of the matter in controversy.[30]

These legal definitions of burden of persuasion convey no certain message about how to treat uncertainty in doing reviewing PSAs, or even how a quantitative risk standard should be expressed. One cannot say, for example, that preponderance of the evidence necessarily means that, in determining compliance with a quantitative probability standard (say a 10 e-5/reactor year core damage frequency), the risk number that must be chosen from a probability distribution is the one that is exceeded by no more than 49% of the estimates. This is because the 51% confidence interval is as easily a part of the substantive standard itself as it is a definition of the degree of proof.

[30]NRC rules in 10 CFR § 50.57(a)(3) require "reasonable assurance" of not endangering safety, but this is probably intended to eliminate zero risk, or absolute assurance, as a substantive risk standard, as opposed to defining a standard of proof. E.g., Carstens v. NRC, 742 F.2d 1546, 1557 (D.C.Cir.1984); Nader v. Ray, 363 F.Supp 946, 954 (D.D.C.1973). Thus reasonable assurance is the amount of safety required to a meet the AEA standard of "adequate protection" in § 182.

Certain PSA uncertainty or burden of proof related issues are really science policy issues that cannot be resolved by scientific proof. They should be addressed in the regulatory framework itself. These include whether the risk standard should be expressed as a medium, mean, or some other number, and whether and how confidence intervals are to be treated. In areas where PSA are expected to be highly uncertain or impossible, for example estimating the likelihood of sabotage, the framework should provide for a licensing decision based on compliance with a deterministic standard. In certain other areas, where NRC has specifically rejected any quantitative risk goal, NRC would need to consider carefully whether to change its prior position. Emergency planning falls in this category, See Commonwealth of Massachusetts v. NRC, supra. In other areas where PSA results are possible but uncertain, uncertainty might be reduced by imposition of deterministic requirements for defense in depth measures.

7. Fairness and Due Process Considerations

All would probably agree that the hearing process must not only be effective in reaching the correct decision, and efficient in use of time and resources, but also be fair. Fairness has no precise definition, even in the legal sense of due process of law, because under established administrative law principles whether a hearing satisfies due process depends on a balance of various factors, including risk of an erroneous decision and the nature of the interests at stake.[31] Assuming the issues are all expert opinion issues, and the bases of the contrasting opinions have been fully disclosed, a paper hearing should satisfy due process requirements, even assuming that intervenors have a constitutionally protected interest.[32]

But the processes outlined above will probably not allow most potential intervenors to participate in the hearing process because most will not have access to the necessary experts to structure an effective presentation. On the one hand, this can be seen as entirely appropriate, since the hearing process is after scientific truth, and the search for scientific truth requires scientific expertise. On the other hand, the process can be criticized as too dependent on the views of experts, and insensitive to the lessons of common experience. Decomposition of the issues in dispute may be less than perfect, with the result that the outcome may in a subtle sense be critically dependent on resolution of a science policy, or pure policy issue, as to which non-expert opinion should be heard.

All this suggests that the processes discussed above need to be supplemented. A reasonable premise is that interested citizens and groups (stakeholders) will want to have the opportunity to influence the NRC licensing decision early in the review process when the agency will not be put on the defensive because of previous review conclusions, and when review schedules will not be disrupted. Another reasonable premise is that stakeholders will want access the highest levels of the NRC so that there is assurance that the persons with whom they communicate will have the fullest possible authority to respond.

Current NRC Staff practice of holding general informational meetings and allowing non-evidentiary limited appearances at an oral hearing before the presiding officer or Commission should be continued. But the considerations mentioned above suggest that the NRC Commission itself needs to be involved early in the process no matter what hearing format is chosen. There are many ways for this to be done, and what follows is illustrative.

---

[31]Mathews v. Eldridge, 424 U.S.319 (1976).

[32]They may not. See City of West Chicago v. NRC, 701 F.2d 630, 645 (7th Cir. 1983).

The Commission could solicit informal public comment, and hold an early informal Commission meeting, shortly after the application is filed. The specific purpose would be the identification of issues of special public concern.[33] Such issues, as specified by the Commission, would then be required to be addressed by the NRC Staff in its review and by applicant in a supplement to its application. Staff-applicant meetings on these particular issues would be held in the vicinity of the proposed site, and stakeholders would be allowed to attend and offer comment. After the Staff had completed its review, and before a decision on the license application, the same stakeholders would be given the opportunity to address the Commission informally. The process would be entirely informal, with no requirement that testimony be under oath or that only qualified experts be heard.

The relation between such an informal process and the hearing process options described above needs to be addressed. For controverted issues of opinion or fact, allowing both processes to be pursued in parallel on the same issues would give insufficient weight to the results of the more formal hearing process, with its strict requirement that matters of expert opinion can be addressed only by experts. Thus stakeholders would probably need to be advised that the hearing process is the appropriate means to raise issues of fact or expert opinion if they want to preserve the option of requesting judicial review of the NRC licensing decision.

8. Conclusion

The above analysis includes some suggestions how the NRC hearing process might be reformed, with a special focus on hearings on PSA issues. However, it has to be recognized that the NRC Staff review process will almost certainly result in a license application that is supported by very substantial and credible expert opinion. It will not be likely that applicant's or NRC Staff's experts will be found to have used faulty logic, clearly inadequate data, or improper assumptions. Accordingly, so long as NRC Staff supports its SER with expert opinion offered into evidence in hearings, the normal and expected result of any properly conducted hearing will be that the NRC Staff position will be chosen. Nuclear plant opponents who expect the hearing process to regularly produce results that are favorable to them are expecting too much, no matter how the hearing process is structured.

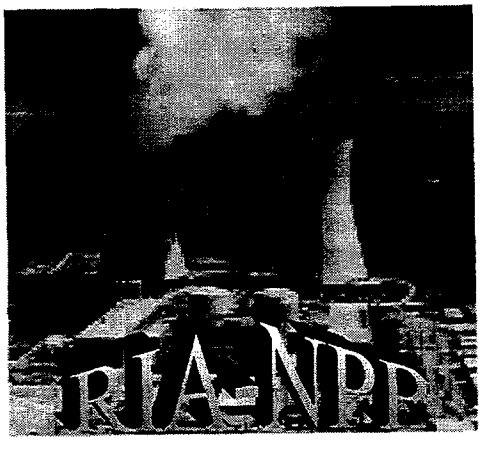
Indeed a hearing process that regularly produced decisions contrary to NRC Staff positions would mean that NRC Staff has lost essential expertise or failed to follow Commission policy, or that the presiding hearing officers have done so. In any case, something would be very wrong at the NRC. If concerned citizens are to play an effective role, it must be at the beginning of the process at the Commission level, where policy is established and NRC Staff attention and resources can be directed to issues of special concern.

[33] An interesting parallel is the informal scoping process that is required for environmental impact statements by the NRC regulations in 10 CFR §§ 51.26-51.29.

A Framework for Risk-Based Regulation and Design for New Nuclear Power Plants

Nuclear Energy Research Initiative

A FRAMEWORK FOR RISK-BASED REGULATION AND DESIGN FOR FUTURE NUCLEAR POWER PLANTS



RISK-G-004-2000
Version 1.0
March 22, 2000

Appendix B
A Framework for Risk-Based Regulation and Design for Future Nuclear Power Plants

Please provide comments on this document to:

Felicia A. Durán
Senior Member of Technical Staff
Sandia National Laboratories
Risk, Reliability, and Modeling
P.O. Box 5800, MS 0747
Albuquerque, New Mexico 87185-0747
PHONE: 505/844-4495
FAX: 505/844-1648
EMAIL: faduran@sandia.gov

Appendix B
A Framework for Risk-Based Regulation and Design for Future Nuclear Power Plants

Table of Contents

List of Figures

List of Tables

Appendix B
A Framework for Risk-Based Regulation and Design for Future Nuclear Power Plants

1.0 INTRODUCTION

The current set of regulatory requirements and industry standards for nuclear power plants is a collection of deterministic criteria, based largely on engineering judgement that has evolved over the last 40 years. A growing awareness within government and industry is that many of the current requirements and standards are not contributing significantly to safety and reliability and, therefore, have needlessly driven the costs of new nuclear plants into a range that will not be economically competitive in the deregulated U.S. power industry. Moreover, the overly prescriptive nature of these requirements and standards inhibits the introduction of new, more advanced technologies.

Probabilistic risk assessment (PRA) is an analytical technique that has been used for the past several decades for integrating diverse aspects of design and operation in order to assess the risks from a nuclear power plant and to develop an information base for analyzing plant-specific and generic issues. An assessment of the plant-specific risk provides both a measure of potential accident risks to the public and insights into the adequacy of plant design and operation. The state of the art of PRA is now sufficiently mature that we can apply PRA to identify systematically the regulatory requirements and industry standards that are needed to maintain the desired level of safety and reliability. The U.S. nuclear industry and the U.S. Nuclear Regulatory Commission (NRC) are already working together to apply risk-informed regulation to the regulation of existing plants.[34] The initial NRC/industry efforts are progressing to address primarily the operation and maintenance of existing nuclear plants. Of course, this effort is constrained by the fact that the operating plants have been licensed under the traditional deterministic regulatory system. What is needed beyond the current effort is the application of a more aggressive risk-informed approach to all regulatory requirements and industry standards, as well as to the regulatory process, focusing upon those issues that affect the design and licensing of new plants. The U.S. Department of Energy (DOE), through its Nuclear Energy Research Initiative (NERI), has funded this project to perform a risk-informed assessment of regulatory and design requirements for future nuclear power plants. As part of the work for this project, this paper presents the development of a framework and guidelines for risk-based regulation and design for new nuclear power plants.

Current regulations and standards are based, in large part, on the principles of defense in depth and safety margins. Defense in depth has evolved since the first research reactors were designed in the 1940s. The NRC Advisory Committee on Reactor Safeguards (ACRS)[35] and Sorensen et al.[36] discuss this evolution, identify two schools of thought on

---

[34] U.S. Nuclear Regulatory Commission, "Framework for Risk-Informing Regulations," Draft for Public Comment, Rev. 1.0, February 10, 2000, http://nrc-part50.sandia.gov/Document/framework_rev_ai_2.pdf

[35] Letter to Shirley Ann Jackson, Chairman, U. S. Nuclear Regulatory Commission, from D. A. Powers, Chairman, Advisory Committee on Reactor Safeguards, "The Role of Defense in Depth in a Risk-Informed Regulatory System," May 19, 1999.

the scope and nature of defense in depth, and recommend an approach for moving forward with risk-informed regulation. The two schools of thought (views) of defense in depth are labeled "structuralist" and "rationalist." The structuralist view asserts that defense in depth is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations. The regulations for defense in depth are derived by repeated application of the questions, "What if this barrier or safety feature fails?" or "What if our models are wrong?" In contrast, the rationalist view would base regulations on risk information, with defense in depth employed only where necessary to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression. As background for the development of the framework, a more detailed discussion of the structuralist and rationalist approaches to defense in depth for developing risk-based regulations is presented in Section 2. For new plants, the rationalist approach to defense in depth, employed within the context of PRA, is preferred to more effectively develop a body of regulations that eliminates requirements and standards that do not contribute significantly to safety and reliability. This approach also reduces the overly prescriptive nature of these requirements and standards so that the plants can be designed and operated more efficiently and the introduction of new, more advanced technologies is less inhibited.

The framework discussed herein will be developed using the top-down hierarchy illustrated in Figure 1. The goal of this effort is to provide a framework for developing and implementing risk-based regulations that ensure adequate protection to the health and safety of the public. An approach based on evaluating quantitative risk against established safety goals is proposed to achieve the goal. Strategies for using full-scope PRA for all operating modes will be developed. Guidance for tactics will be defined to support development of strategies. Section 3 provides an expanded representation and discussion of the development of the framework using the hierarchy in Figure 1. The goal, approach, and strategies are developed and examples of supporting tactics are provided. Some additional discussion of tactics and implementation of the framework to identify systematically the body of regulatory and design requirements necessary to maintain safety is provided in Section 4. By implementing such a framework, it is expected that the resulting body of requirements and standards would not only provide a regulatory environment that would maintain the goal of protection of public health and safety, but would also reduce the unnecessary burden imposed by the current regulations and standards.

The development of a framework for risk-based regulation and design discussed herein involves ideas that have been and continue to be controversial. Many of the issues that arise in the development of the framework have not and will not be resolved satisfactorily at this point. The DOE NERI team, however, will identify and begin the process of resolution for issues critical to the successful development of this framework.

---

[36] J. N. Sorensen, G. E. Apostolakis, T. S. Kress, and D. A. Powers, "On the Role of Defense in Depth in Risk-Informed Regulation," Presented at PSA '99, Washington, DC, American Nuclear Society, August 22-25, 1999.

2.0 STRUCTURALIST VS RATIONALIST APPROACHES TO DEFENSE IN DEPTH FOR RISK-BASED REGULATION

The term defense in depth is used to describe applications of multiple measures to prevent or mitigate accidents. The measures applied can be embodied in structures, systems, and components (SSCs) or in procedures (including emergency plans). Defense in depth can be applied at various levels. Redundant or diverse means may be used to accomplish a function, the classic example being the use of multiple barriers (fuel, cladding, reactor coolant pressure boundary, spray or scrubbing systems, and containment) to limit the release of core radionuclides. Alternatively, as discussed in this section, redundant or diverse functions may be used to accomplish the higher goal of protecting the public from nuclear power plant accidents. As stated above, the NRC ACRS has identified two schools of thought (views) on the scope and nature of defense in depth, and recommends an approach for moving forward with risk-informed regulation.

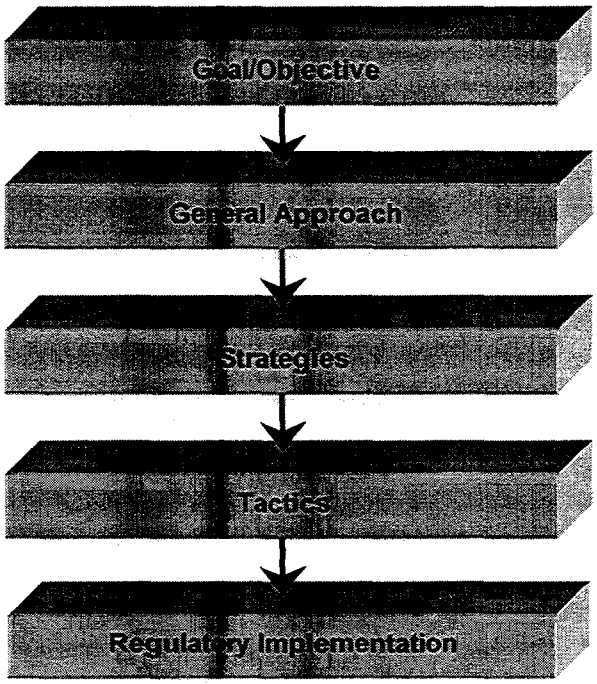


Figure 1. Hierarchy for framework development.

The structuralist view asserts that defense in depth is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations. The regulations for defense in depth are derived by repeated application of the questions, "What if this barrier or safety feature fails?" or "What if our models are wrong?" The results of that process are documented in the regulations themselves, specifically in Title 10 of the Code of Federal Regulations.

It is a characteristic of the structuralist view that balance must be preserved among four high-level lines of defense. The risks to public health and safety are dominated by accidents resulting in the release of fission products from the reactor core. The first line of defense, therefore, is to eliminate all initiators that could conceivably lead to core damage, but it is recognized that perfect initiator prevention is not possible. The frequency of such initiators, although significantly less than before TMI-2, is about one per reactor year. As a second line of defense, systems such as the emergency core cooling system (ECCS) are required to prevent core damage given postulated initiators. Further, although such systems are designed for a wide spectrum of initiators and compounding equipment failures, no prevention system is deemed to be perfect. As a third line of defense, barriers including containment and associated heat and fission product removal systems are required. These barriers would be effective in preventing large radionuclide releases for many severe accidents, but scenarios exist in which containment would be breached or bypassed. A fourth line of defense, offsite emergency preparedness, is therefore required. It is evident that the structuralist approach does not

utilize any criteria to determine how much defense in depth is sufficient. Consequently, many of the current regulatory requirements do not contribute to safety significantly and so cannot justify their cost.

In contrast, the rationalist view asserts that defense in depth is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression. This view is made practical by the ability to quantify risk and estimate uncertainty using PRA techniques. It should be pointed out that both the structuralist and the rationalist points of view are intended to deal with the uncertainties associated with reactor accidents. The difference is that the structuralist view does not deal with uncertainties in a quantitative manner while the rationalist view takes advantage of the fact that advances in PRA allow the quantitative estimation of some of these uncertainties.

The process envisioned by the rationalist is as follows: (1) Establish quantitative safety goals, such as the quantitative health objectives (QHOs), core damage frequency, and large release frequency, (2) design and analyze the plant using PRA methods to establish that the safety goals are met, and (3) evaluate the uncertainties in the analysis, including those due to model inadequacies, system performance and reliability, and lack of knowledge, and then determine what steps (i.e., defense-in-depth measures) should be taken to compensate for those uncertainties.

What distinguishes the rationalist view from the structuralist view is the degree to which the rationalist depends on establishing quantitative safety goals and performing formal probabilistic analyses, including analyses of uncertainties, as far as the analytical methodology permits. The exercise of engineering judgement, to determine the kind and extent of defense-in-depth measures, occurs after the capabilities of the analyses have been exhausted. The quantification of uncertainties provides a means for determining how much redundancy and diversity (i.e., defense in depth) is sufficient.

The structuralist and rationalist views are not necessarily in conflict. As stated above, both views can be construed as a means of dealing with uncertainty. The two schools differ in the process used to deal with uncertainty in reaching an acceptable level of safety. The structuralist approach has evolved from the early days of nuclear power with a process of accumulating DID features until a judgement was made that sufficient protection against uncertainty in performance had been achieved. With the development of PRA methods, the rationalist approach uses these tools to quantify uncertainty and to explicitly account for DID features in reducing uncertainties to acceptable levels. The main difference is that the structuralist accepts DID as a fundamental principle, while the rationalist would place DID in a subsidiary role. Additionally, the structuralist does not deal with uncertainties in a quantitative manner, while the rationalist takes advantage of the fact that advances in PRA allow the quantitative estimation of some of these uncertainties. However, neither incorporates any absolute means of determining when the degree of defense in depth achieved is sufficient.

In terms of developing a framework for risk-informed regulation, perhaps these two approaches to defense in depth can be represented by a spectrum, as illustrated in Figure 2. This figure also includes points with which to compare and contrast the framework for risk-informed regulation being developed by the NRC for current plants[1] against the framework for risk-based regulation and design for new plants being developed by the DOE NERI project.

The approach recommended by the ACRS for risk-informing 10 CFR 50 for current operating plants–and being developed by the NRC for current operating plants[1]–maintains a structuralist high-level defense-in-depth approach for initiator prevention, core-damage prevention, containment, and offsite emergency preparedness. At lower levels in the safety hierarchy, the ACRS recommends the rationalist model. This approach is consistent, for example, with the option provided in 10 CFR 50.46 to permit the use of best-estimate calculations with uncertainty analyses to demonstrate compliance with the ECCS acceptance criteria. In terms of the spectrum of approaches to defense in depth in Figure 2, this approach starts at the structuralist end of the spectrum and proceeds to take steps to the right to become more rationalist. It is expected that efforts for risk-informing regulations for existing plants will most likely address only certain selected regulations.

While the ACRS has recommended a structuralist high-level defense-in-depth approach for risk-informing current regulations, it has also been critical of the capricious use of defense-in-depth arguments to undermine the focus of risk-informed methods of regulation.[2,3] Considering the spectrum of approaches to defense in depth, a more aggressive rationalist approach to developing regulations for future plants would be more effective in eliminating requirements and standards that do not contribute to safety. A

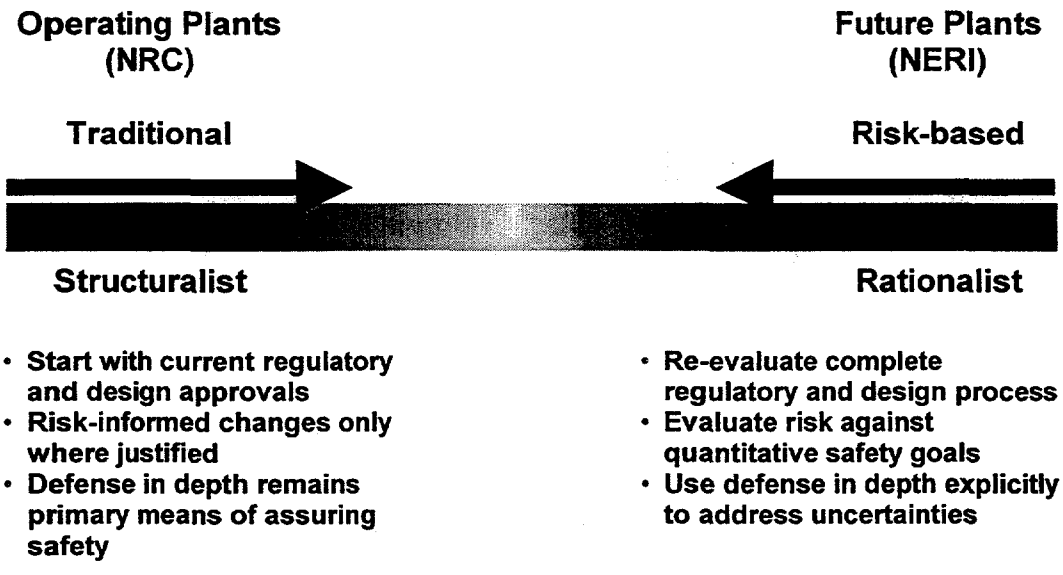


Figure 2. Spectrum of Approaches to Regulation

completely rationalist approach would determine risk estimates and compare them to established quantitative risk goals. Key to this alternative is the establishment of quantitative risk goals, such as the QHOs, core damage frequency, and large release frequency.

Additionally, the rationalist approach relies on the use of state of the art PRA technology to provide an integrated and systematic analysis of the plant that explicitly addresses sources of uncertainty. The state of the art of PRA is now sufficiently mature, and will continue to be developed for application to new plants, that these tools can be used effectively to identify systematically the regulatory requirements and industry standards that are needed to maintain the desired level of safety and reliability. Defense in depth is secondary in this approach and would be applied only where it is necessary to address uncertainties beyond the capabilities of PRA techniques or where it is truly justified for maintaining safety.

The strategies for applying defense in depth for a rationalist approach may be incorporated in a structuralist manner. For example, defense in depth may be manifested in safety goals and acceptance criteria, which are input to the design process. In choosing goals for core damage frequency and QHOs, for example, a judgement is made on the balance, or allocation of risk, between prevention and mitigation. In terms of the spectrum of approaches to defense in depth in Figure 2, this approach starts at the rationalist end of the spectrum and takes steps to the left as risk and uncertainty are evaluated explicitly to determine what defense-in-depth measures should be incorporated to maintain safety and reliability.

3.0 TOP-DOWN DEVELOPMENT OF THE FRAMEWORK

This section provides an expanded representation and discussion of the development of the regulatory framework using the hierarchy in Figure 1. An expanded representation of the framework is presented in Figure 3. For the purposes of making regulatory decisions, development of the framework is based on the concept that meeting the quantitative regulatory safety goals with high confidence fulfills the goal of protecting the public. High confidence is attained through explicit consideration of uncertainties, including modeling adequacy and equipment design and performance, in a full-scope, detailed PRA for all operating modes. For the purposes of developing the requirements for risk-based regulation, implementation of the framework is carried out by defining functional system characteristics, within the context of how PRA is performed, to determine what areas need to be regulated to assure safety. Implementation for design is achieved by specifying design configurations and using PRA to evaluate the design, then iterating with subsequent design changes. A rationalist approach to defense in depth will be employed only where necessary to address uncertainties. Thus, within this framework, PRA provides the basis for both developing and evaluating compliance with requirements for risk-based regulation and design.

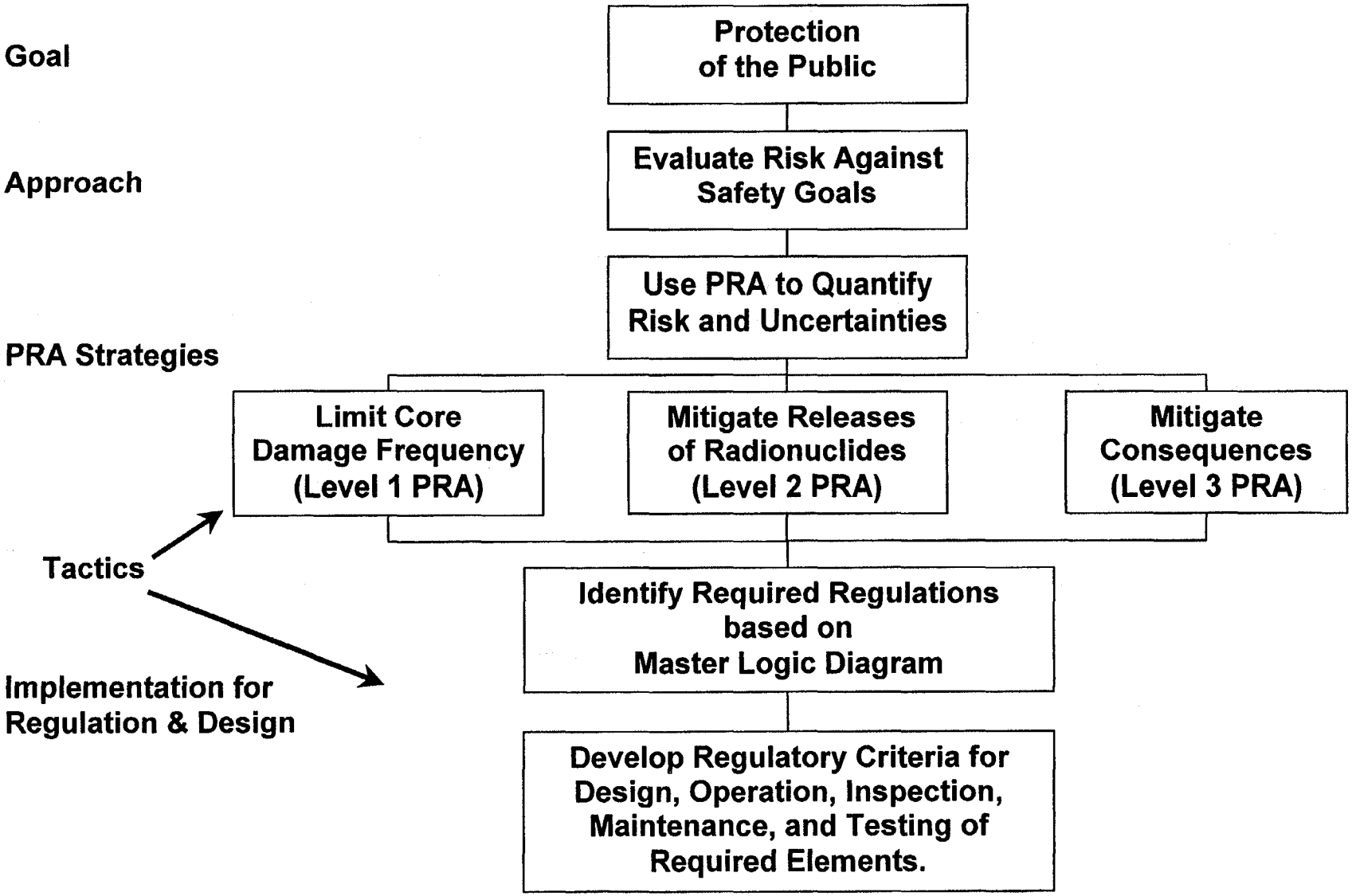


Figure 3. Framework for Risk-Based Regulation and Design

3.1 Goal: Protection of the Public

Section 182(a) of the Atomic Energy Act requires the NRC to ensure that nuclear power plant operation provides adequate protection to the health and safety of the public. In its rules and decisions the Commission refers to this requirement as either the "adequate protection" requirement or the "no undue risk" requirement. The interchangeable use of these two terms has been accepted in legal decisions.

The Commission has said on many occasions that compliance with the NRC regulations "should provide a level of safety sufficient for adequate protection of the public health and safety and common defense and security under the Atomic Energy Act."[37] Thus, adequate protection is presumptively assured by compliance with the NRC regulations and other license requirements. New information may reveal a significant unforeseen hazard, a substantially greater potential for a known hazard, or insufficient margins and backup capability.

The possibility of developing a generally applicable definition of adequate protection to guard against possible misuse of the term has been discussed extensively.[38] It is correct to say that adequate protection is not zero risk, that it is the same as no undue risk, that it has long-term and short-term aspects, and that it is that level of safety which the Atomic Energy Act requires. However, these statements do not eliminate the need for engineering judgement or provide a numerical standard or risk definition for application in determining what constitutes adequate protection. The NRC is actively pursuing quantitative measures of safety, and a more generally applicable definition of adequate protection may emerge from these efforts. In fact, the NRC has established safety goals for nuclear power plants, including QHOs that state the Commission's expectations with respect to how safe is safe enough. Although licensees of operating plants are not required to demonstrate that they meet the quantitative goals, comparisons of PRA and Individual Plant Examination (IPE) results to the goals are common. For these plants, it is not reasonable to expect that the NRC will make decisions wholly based on quantitative safety goals, that is, implement a completely risk-based rather than risk-informed approach. For future plants, however, the determination of adequate protection using increased reliance on comparisons of PRA results to quantitative risk measures should be considered.

Note that the NRC's safety goals are not quantitative measures of adequate protection. For example, the safety goal of 5×10^{-7} for individual acute fatality is considered to be lower than the limit of adequate protection. These limits have not been determined by the NRC yet. The ACRS has provided its views on the relationship between the concept of "adequate protection," as used in the NRC regulations, and the current NRC Safety Goals, from the standpoint of level of risk[39,40] for existing plants. Additionally, the ACRS has discussed the concept of a three-region

---

37 FR Doc. 88-12624, Statement of Considerations, Revisions to Backfit Rule, 10 CFR 50.109, July 6, 1988 American Nuclear Society, August 22-25, 1999.

38 Center for Strategic and International Studies, "The Regulatory Process for Nuclear Power Reactors. A Review," Washington, DC, August 1999.

39 Letter to Shirley Ann Jackson, Chairman, U. S. Nuclear Regulatory Commission, from R.L. Seale,

approach for risk-based regulation, that is, a goal and an upper limit. The three-region approach proposed by the ACRS would make explicit the distinction between the goal and the adequate protection values for each risk metric. The NERI framework development will use the goals since they are available. It should be emphasized that the NERI framework development is relatively independent of numerical values. When numerical values for adequate protection are promulgated, the framework would still be applicable with minor adaptation.

3.2 Approach: Evaluate Risk Against Safety Goals

The general approach for this regulatory framework is to evaluate risk against quantitative safety goals. Within this framework, regulatory decisions are made based on an evaluation of the results from a full-scope, detailed PRA for all operating modes against established quantitative safety goals. Developing the requirements for risk-based regulation and design to support this approach is achieved by defining functional system characteristics, within the context of how PRA is performed, to determine what areas need to be regulated for the purposes of assuring and maintaining the desired level of safety and reliability delineated by the established quantitative goals. Key to developing regulatory and design requirements within this framework is the establishment of quantitative risk goals, such as, for example, the QHOs, core damage frequency, and conditional probability of large release. For new plants, a detailed plant-specific PRA for all operating modes, along with an explicit treatment of uncertainties, would confirm that established quantitative safety goals are met.

As discussed above, existing quantitative goals will be used as a starting point for this framework development. Established QHOs and related subsidiary goals will be used to guide the development of risk-based regulation and design. The intent is to develop requirements in such a way that compliance will provide reasonable assurance of meeting specific quantitative goals and the goal of protection of the public.

To delineate quantitative goals, the PRA strategies of the framework must be expressed using quantifiable measures of risk. One method of assessing the level of protection against accidents at a given nuclear power plant is simply to compare PRA results to the QHOs for early-fatality and latent-cancer risks:

- the risk of an early fatality as a result of a plant accident should be less than 5×10^{-7}/year for members of the public located within 1 mile of the exclusion area boundary, and

---

Chairman, Advisory Committee on Reactor Safeguards, "Risk-Based Regulatory Acceptance Criteria for Plant-Specific Application of Safety Goals," April 11, 1997.

[40] Letter to Shirley Ann Jackson, Chairman, U. S. Nuclear Regulatory Commission, from R.L. Seale, Chairman, Advisory Committee on Reactor Safeguards, "Elevation of CDF to a Fundamental Safety Goal and Possible Revision of the Commission's Safety Goal Policy Statement," May 11, 1998.

- the risk of dying from cancer as a result of a plant accident should be less than $2x10^{-6}$/year for members of the public residing within 10 miles of the plant.

For new plants, QHOs and related subsidiary goals set forth in this section apply to mean risk measures quantified in full-scope PRAs. Unfortunately, the QHOs are difficult to apply for developing risk-based regulations. Simply replacing existing regulations with the QHOs would be a completely rationalist approach and would not consider limitations and uncertainties inherent in PRA. As such, it is appropriate to investigate allocation of risk by establishing subsidiary goals. The quantitative goals discussed here provide targets for the framework development. Compliance with regulation and design requirements developed by implementing the framework should provide a reasonable expectation that the quantitative goals will be met.

The QHOs are the highest-level quantitative goals. The QHOs were originally set as a measure of "safe enough," and in that sense they go beyond adequate protection. Given this position of the Commission, no risk arguments exist for setting quantitative goals more stringent than the QHOs.

While there is no basis for being more stringent than the QHOs, the limitations and uncertainties inherent in PRA, which tend to grow as postulated accidents proceed in time, influence the quantitative allocation among the three PRA strategies.

Because public risks are dominated by accidents that involve core damage and containment failure, subsidiary goals based on other risk measures associated with the calculations for Level 1, Level 2, and Level 3 PRAs are developed for the framework. The subsidiary goals are consistent with the QHOs. A summary of the proposed goals is provided below:

(1) For the strategy to limit core damage frequency (Level 1 PRA):

- the probability of core damage should be less than 10^{-4}

(2) For the strategy to mitigate releases of radionuclides (Level 2 PRA):

- the conditional probability of a large release (either early or late) should be less than 0.1

(3) For the strategy to mitigate consequences (Level 3 PRA):

- the conditional probability of an early fatality for an individual should be less than 0.1
- the conditional probability of a latent cancer for an individual should be less than 0.1

As discussed in Section 2, this approach relies on the use of state of the art PRA technology to provide an integrated and systematic analysis of the reactor system that explicitly addresses sources of uncertainty. The state of the art of PRA is now sufficiently mature that these tools can be used effectively to identify systematically the regulatory requirements and industry standards that are needed to maintain the desired level of safety and reliability. Within the current

capabilities of PRA techniques, sources of uncertainty will be quantified to gain as complete an understanding as possible about the range of risk and uncertainty before defense in depth is applied to address uncertainties.

> ***Issue:*** Because of the inherent limitations of PRA, meeting the safety goals alone might not necessarily provide assurance of adequate protection, and therefore, it may be desired to require some level of defense in depth, in the traditional sense, for the purposes of balance or as an acknowledgement that events not envisioned might occur. The NERI effort, however, proposes to begin with an extreme rationalist approach to defense in depth. As such, any decision to require defense-in-depth measures at this level of the framework would first require as complete an understanding as possible of the risk and uncertainties of the design and operation of a new plant. As the development of the framework progresses, sources of uncertainty will be explicitly identified and attempts will be made to quantify all these sources of uncertainty, including those which may not usually be quantified, so that a complete profile of range of the risk and uncertainty can be determined. It is proposed that results of a full-scope Level 3 PRA for an existing plant be reviewed for this exercise.

3.3 PRA Strategies

Within this framework, the strategies for both developing and evaluating compliance with requirements for risk-based regulation and design is to use PRA to quantify risk and uncertainties. These strategies are based on consideration of the risk information available from Level 1, Level 2, and Level 3 PRA analysis and include the following: (1) prevent core damage, (2) mitigate release of radionuclides, and (3) mitigate consequences.

The Level 1 PRA evaluates the potential of accident initiators and the system response to prevent core damage. The Level 1 PRA identifies accident initiators, accident sequences, and accident probabilities, and calculates core damage frequency and defines core damage states. The frequency estimate for core damage is compared to the corresponding goal. For protection of the public, the focus of a Level 1 PRA is to limit the frequency of accident initiators and limit the probability of core damage given accident initiation. Key uncertainties for a Level 1 PRA include information about system reliability and performance in response to an initiating event.

The Level 2 PRA encompasses the response to and mitigation of core damage, including containment of fission products. A Level 2 PRA takes the plant damage states defined in the Level 1 analysis and continues to evaluate accident progression, determine containment response, calculate release probabilities, and define source terms. The risk estimates here can be compared to risk goals for conditional probability of large release, both early and late. Key sources of uncertainty for a Level 2 PRA include understanding of the phenomenology of accident progression.

The Level 3 PRA encompasses the response to and mitigation of radionuclide releases, including emergency response. The Level 3 PRA takes the source terms defined in the Level 2 analysis

and continues to evaluate radionuclide transport, perform dose and health effects modeling, and calculate the resulting public risk, including early and latent cancer fatalities. These risk estimates can be directly compared to the quantitative health objectives or to subsidiary goals for conditional probability of early fatalities and latent cancer risks. Key sources of uncertainty for a Level 3 PRA include dose and health effects modeling.

> ***Issue:*** Current PRA techniques may be limited in their ability to address the needs of this framework at this time. It is expected that continued development of PRA technology will provide additional capability for PRA to be used for this framework. The NERI team will identify technology development needs as the framework development progresses.

3.4 Tactics

Various tactics are applied to support the PRA strategies and implementation. One set of tactics is necessary to support the PRA analysis and to identify design alternatives, including identifying required safety functions for each PRA strategy and the SSCs required to achieve the safety functions. This set of tactics ensures that requirements not significant to safety are not included for consideration. A second set of tactics will include the more traditional defense-in-depth measures that could be employed to either reduce uncertainties or add to safety. Defining this set of tactics involves first evaluating the types of tactics that could be employed and then taking a rationalist approach to determine which tactics it makes sense to apply. Table 1 provides a listing of tactics that could be applied in the implementation of the framework. As the framework implementation progresses, guidelines will be developed for determining how to apply tactics for risk-based regulation and design.

3.5 Implementation for Regulation and Design

Implementation for regulation is achieved by defining functional system characteristics to determine what areas need to be regulated for the purposes of assuring safety. Defining these characteristics will be accomplished by taking a top-down approach to identify the safety functions and SSCs that are required to maintain safety, and to identify the accident initiators and system response failures that could compromise safety. Once the appropriate SSCs required to achieve safety have been identified, then decisions on appropriate tactics, such as those in Table 1, can be made to develop regulatory requirements. The specification of these tactics will be based on a systematic evaluation of the areas that need to be regulated for the purposes of assuring safety and will also evolve from this process. For example, after identifying the safety functions required to maintain safety and reliability, or identifying the accidents that could compromise safety, decisions may be made to include in the regulations the tactics for, respectively, general Design Criteria and Standards and Design Basis Events. The specification of these tactics will be based on the identified safety functions and accidents. It is also possible within this framework that these features of current regulations might not necessarily be developed as part of this risk-based regulation and design.

Appendix B
A Framework for Risk-Based Regulation and Design for Future Nuclear Power Plants

Regulatory requirements for design, operation, inspection, maintenance and testing will be required. Implementation for design is achieved by specifying design configurations and using PRA to evaluate the design, then iterating with subsequent design changes. A rationalist approach to defense in depth will be used explicitly to address uncertainties. The PRA analyses can be used iteratively to identify the set of regulatory requirements and design features that are needed to achieve the desired level of safety for each of the three PRA strategies. More discussion on an approach for regulatory and design implementation is discussed in Section 4.

Table 1 Possible Tactics for Regulation and Design

DESIGN & ANALYSIS	PERSONNEL TRAINING & TESTING
Design Basis Events	Operator Training and Licensing
Acceptance Criteria and Safety Margin	Fitness for Duty Program
Design Criteria and Standards	Emergency Planning Drills
Single Failure Criteria	SPECIAL TREATMENT (Non-Scope)
Redundancy	Design Considerations
Diversity	Qualification
Separation Criteria	Change Control
Automation	Documentation
Multiple Fission-Product Barriers	Reporting
Safety Analysis Reports	Maintenance
PRAs, IPEs	Testing
Safety Goals	Surveillance
Provide Emergency Response Facilities	Quality Assurance
PLANNING, PROCEDURES	
Operating Procedures	
Technical Specifications	
Severe Accident Guidelines	
Maintenance Plans and Procedures	
Inspection Plans and Procedures	
Testing Plans and Procedures	
Emergency Plans	

4.0 IMPLEMENTATION GUIDANCE

One purpose for the development of this framework for risk-based regulation and design for new plants is to eliminate regulatory requirements that are not contributing to safety and reliability and are therefore causing unnecessary regulatory burden and cost to licensees. Of course, the reduction of requirements should not affect safety adversely. To ensure the development of only regulations that are required to assure safety, it is first necessary to determine what areas require regulation. One method is to develop a master logic diagram (MLD) that can be used to take a top-down approach to identify the safety functions, and SSCs that are required to maintain safety and to identify the accident initiators and system response failures that could compromise safety.[41,42] An example of such an MLD is provided in Figure 4. The top event is stated in terms of risk exceeding the safety goals. The gray-shaded events (excessive health effects, excessive offsite release, and excessive core damage) in the diagram correspond to Level 1, Level 2, and Level 3 PRA strategies, respectively, in Figure 3. The sixth level of the diagram defines the system functions that are required to assure safety. The next level down indicates that initiating events and failure of mitigating systems, containment, and emergency response will cause failure of the safety functions. The last level on the diagram indicates that internal initiators for all operating modes and external initiators will be considered for completeness. By further development of the diagram to specify initiating events and mitigation failures, it should be possible to determine the "regulatory risk space" for which regulatory and design requirements are needed. Additionally, because this approach identifies the functionality of specific systems and the SSCs needed to achieve the required functionality, the information generated by further development of this diagram will also be useful for the implementation of the framework for design.

---

41 G. E. Apostolakis, "Some Issues Related to Goal Allocation and Performance Criteria," Presented at the 8th International Conference on Structural Mechanics in Reactor Technology, Brussels, Belgium, August 19-23, 1985.

42 PRA Procedures Guide, NUREG/CR-2300, U.S. Nuclear Regulatory Commission, September 1981.

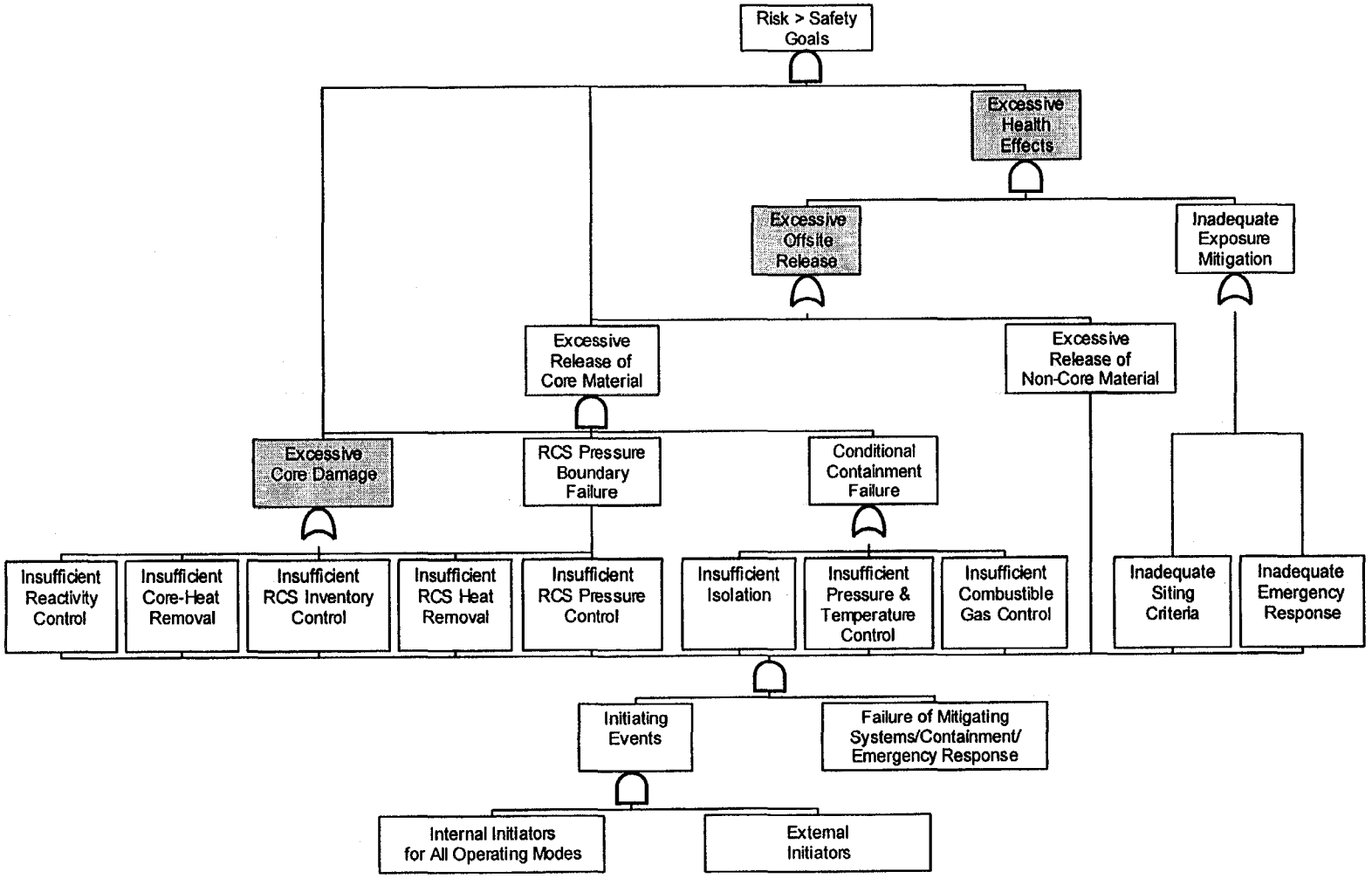


Figure 4: Example Master Logic Diagram for Framework Implementation

Development of the MLD will proceed to develop the bottom levels of the diagram for one or two system functions. For regulatory implementation of the framework, the SSCs required to maintain the selected system functions will be identified, and the initiating events and system response failures that could compromise this safety function will be identified. The result of this exercise will be the determination of areas that require regulation. Once these have been identified, the application of the tactics (Table 1) will be investigated to develop regulations for design, operation, inspection, maintenance and testing. The result of this will be the development of guidance for developing risk-based regulations.

For design implementation, it is proposed that the threats to each system function will first be identified, then success criteria for SSCs that support the system function will be determined. An initial design will be proposed with a preliminary determination of margin, reliability, and uncertainty. Then a PRA analysis will be conducted to determine risk estimates. A second iteration begins by modifying design features to adjust margin, reliability, and uncertainty. A second PRA analysis is then conducted and the differences in risk and design cost estimated. Based on the experience with this implementation, guidance for risk-based design can be developed.

5.0 SUMMARY

This report presents a framework for risk-based regulation and design for future nuclear power plants. This approach incorporates characteristics of structuralist and rationalist models for defense in depth. The differences, as presented here, are primarily a matter of which model is the starting point and the degree to which both models are applied. The top-down development of the framework takes an aggressive rationalist approach to evaluate risk estimates against established goals based on PRA analyses. Traditional defense-in-depth measures are employed only where necessary to address uncertainties in the analyses and only after the development of a complete an understanding as possible of the risk and uncertainty. Within this framework PRA, provides the basis for both developing and evaluating compliance with requirements for risk-based regulation and design. For the purposes of making regulatory decisions, development of the framework is based on the concept that meeting the quantitative regulatory safety goals with high confidence fulfills the goal of protecting the public. High confidence is attained through explicit consideration of uncertainties, including modeling adequacy and equipment design and performance, in a full-scope, detailed PRA for all operating modes. For the purposes of developing the requirements for risk-based regulation, implementation of the framework is carried out by defining functional system characteristics, within the context of how PRA is performed, to determine what areas need to be regulated to assure safety. Implementation for design is accomplished by specifying design configurations and using PRA to evaluate the design, then iterating with subsequent design changes.

This framework is more challenging to implement because the overall approach–keeping risk lower than established goals and requiring justification for adding defense in depth–is a significant change from the current regulatory philosophy. Additionally, although much of the

foundation for treatment of uncertainties exists, developing regulatory processes to accomplish this is another significant issue. Nonetheless, the rationalist approach is preferred for developing a body of requirements and standards for new plants that will provide a regulatory environment that ensures protection of the public, reduces the unnecessary burden imposed by the current regulations and standards without compromising safety, and thereby improves the market competitiveness of new plants.

6.0 REFERENCES

1 U.S. Nuclear Regulatory Commission, "Framework for Risk-Informing Regulations," Draft for Public Comment, Rev. 1.0, February 10, 2000, http://nrc-part50.sandia.gov/Document/framework_rev_ai_2.pdf

2 Letter to Shirley Ann Jackson, Chairman, U. S. Nuclear Regulatory Commission, from D. A. Powers, Chairman, Advisory Committee on Reactor Safeguards, "The Role of Defense in Depth in a Risk-Informed Regulatory System," May 19, 1999.

3 J. N. Sorensen, G. E. Apostolakis, T. S. Kress, and D. A. Powers, "On the Role of Defense in Depth in Risk-Informed Regulation," Presented at PSA '99, Washington, DC, American Nuclear Society, August 22-25, 1999.

4 FR Doc. 88-12624, Statement of Considerations, Revisions to Backfit Rule, 10 CFR 50.109, July 6, 1988 American Nuclear Society, August 22-25, 1999.

5 Center for Strategic and International Studies, "The Regulatory Process for Nuclear Power Reactors. A Review," Washington, DC, August 1999.

6 Letter to Shirley Ann Jackson, Chairman, U. S. Nuclear Regulatory Commission, from R.L. Seale, Chairman, Advisory Committee on Reactor Safeguards, "Risk-Based Regulatory Acceptance Criteria for Plant-Specific Application of Safety Goals," April 11, 1997.

7 Letter to Shirley Ann Jackson, Chairman, U. S. Nuclear Regulatory Commission, from R.L. Seale, Chairman, Advisory Committee on Reactor Safeguards, "Elevation of CDF to a Fundamental Safety Goal and Possible Revision of the Commission's Safety Goal Policy Statement," May 11, 1998.

8 G. E. Apostolakis, "Some Issues Related to Goal Allocation and Performance Criteria," Presented at the 8th International Conference on Structural Mechanics in Reactor Technology, Brussels, Belgium, August 19-23, 1985.

9 PRA Procedures Guide, NUREG/CR-2300, U.S. Nuclear Regulatory Commission, September 1981.

PSAM5 Conference Paper –

A Framework for Regulatory Requirements and Industry Standards for New Nuclear Power Plants

A Framework for Regulatory Requirements and Industry Standards for New Nuclear Power Plants*

Felicia A. Durán and Allen L. Camp
Sandia National Laboratories, P.O. Box 5800, MS 0747, Albuquerque, NM 87185-0747, United States
faduran@sandia.gov, alcamp@sandia.gov
George E. Apostolakis and Michael W. Golay
Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139-4307, United States
apostola@mit.edu, golay@mit.edu

Abstract

This paper summarizes the development of a framework for risk-based regulation and design for new nuclear power plants. Probabilistic risk assessment methods and a rationalist approach to defense in depth are used to develop a framework that can be applied to identify systematically the regulations and standards required to maintain the desired level of safety and reliability. By implementing such a framework, it is expected that the resulting body of requirements will provide a regulatory environment that will ensure protection of the public, will eliminate the burden of requirements that do not contribute significantly to safety, and thereby will improve the market competitiveness of new plants.

1. Introduction

Current regulatory requirements and industry standards for nuclear power plants (NPPs) are a collection of deterministic criteria, based largely on engineering judgement, that have evolved over the last 40 years. A growing awareness within government and industry is that many of the current requirements are not contributing significantly to safety and, therefore, have driven costs of new NPPs into a range that will not be economically competitive in a deregulated electric power industry.

The state of the art of probabilistic risk assessment (PRA) is sufficiently mature that we can apply PRA to identify systematically the requirements needed to maintain a desired level of safety. The U.S. nuclear industry and the U.S. Nuclear Regulatory Commission (NRC) are already working together to apply risk-informed regulation to the regulation of existing plants [1]. The NRC/industry efforts are progressing to address primarily the operation and maintenance of existing plants. Of course, this effort is constrained by the fact

* Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

that the operating plants have been licensed under the traditional regulatory system. What is needed beyond the current effort is a new approach to all regulations, focusing on the design and licensing of future plants. This paper summarizes the development of a framework for risk-based regulation and design for new NPPs.

2. Structuralist vs Rationalist Approach to Defense in Depth

Current regulations and standards are based, in large part, on the principles of defense in depth (DID) and safety margins, which have evolved since the first reactors were designed in the 1940s. The NRC Advisory Committee on Reactor Safeguards (ACRS) [2] and Sorensen et al. [3] discuss this evolution, identify two schools of thought on DID, labeled "structuralist" and "rationalist," and recommend an approach for risk-informed regulation.

The two schools differ in the process used to deal with uncertainty in reaching an acceptable level of safety. The structuralist approach has evolved from the early days of nuclear power with a process of accumulating DID features until a judgement was made that sufficient protection against uncertainty in performance had been achieved. With the development of PRA methods, the rationalist approach uses these tools to quantify uncertainty and to explicitly account for DID features in reducing uncertainties to acceptable levels. The main difference is that the structuralist accepts DID as a fundamental principle, while the rationalist would place DID in a subsidiary role. Additionally, the structuralist does not deal with uncertainties in a quantitative manner, while the rationalist takes advantage of the fact that advances in PRA allow the quantitative estimation of some of these uncertainties. For new plants, the rationalist approach to DID, employed within the context of PRA, is preferred to more effectively develop a body of regulations that eliminates requirements that do not contribute significantly to safety.

The rationalist relies on PRA methods to provide an integrated and systematic analysis of the plant that explicitly addresses sources of uncertainty. The process envisioned by the rationalist is: establish quantitative safety goals, such as health objectives, core damage frequency, and large release frequency; design and analyze the plant using PRA methods to establish that the safety goals are met; evaluate the uncertainties in the analysis, including those due to model inadequacies, system performance and reliability, and lack of knowledge; and determine what steps (i.e., DID, new design features) to take to address those uncertainties. The quantification of uncertainties in terms of probability distribution functions provides a means for determining how much redundancy and diversity (i.e., DID) is sufficient.

3. Development of the Framework

The framework we have proposed for risk-based regulation and design is illustrated in

Figure 1. A top-down hierarchy, indicated on the left side of Figure 1, is being used to define the goal, establish an overall approach, and develop and implement appropriate strategies and tactics. The framework is based on an application of PRA methods and reflects a rationalist approach to DID.

Regulations for NPPs are required to ensure adequate protection to the health and safety of the public. Accordingly, the *goal* of this effort is to provide a framework for developing and implementing risk-based regulations that meet this requirement. An *approach* based on evaluating risk against quantitative safety goals is proposed to achieve the stated goal. With respect to adequate protection, the NRC has established safety goals including Quantitative Health Objectives (QHOs) that state the Commission's expectations with respect to how safe is safe enough. Although the NRC's safety goals are not considered quantitative measures of adequate protection, for new plants, we will consider the determination of adequate protection using increased reliance on comparisons of PRA results to quantitative risk measures. The safety goals we are using for the framework, indicated in the gray boxes in Figure 1, have been adapted from the NRC's goals.

The *strategies* for developing and evaluating compliance with requirements for risk-based regulation and design are based on the use PRA to quantify risk and uncertainties. High confidence is achieved through explicit consideration of uncertainties, including modeling adequacy and equipment design and performance. These strategies include consideration of the risk information available from Level 1, Level 2, and Level 3 PRA analyses. Level 1 PRA evaluates the potential for accident initiators and the system response to prevent core damage. An estimate of core damage frequency is compared to the corresponding goal. Level 2 PRA encompasses the response to and mitigation of core damage, including containment of fission products. Risk estimates here can be compared to goals for conditional probability of large release, both early and late. Level 3 PRA encompasses the response to and mitigation of radionuclide releases, including emergency response. These risk estimates can be directly compared to the QHOs or to subsidiary goals for conditional probability of early fatalities and latent cancer risks.

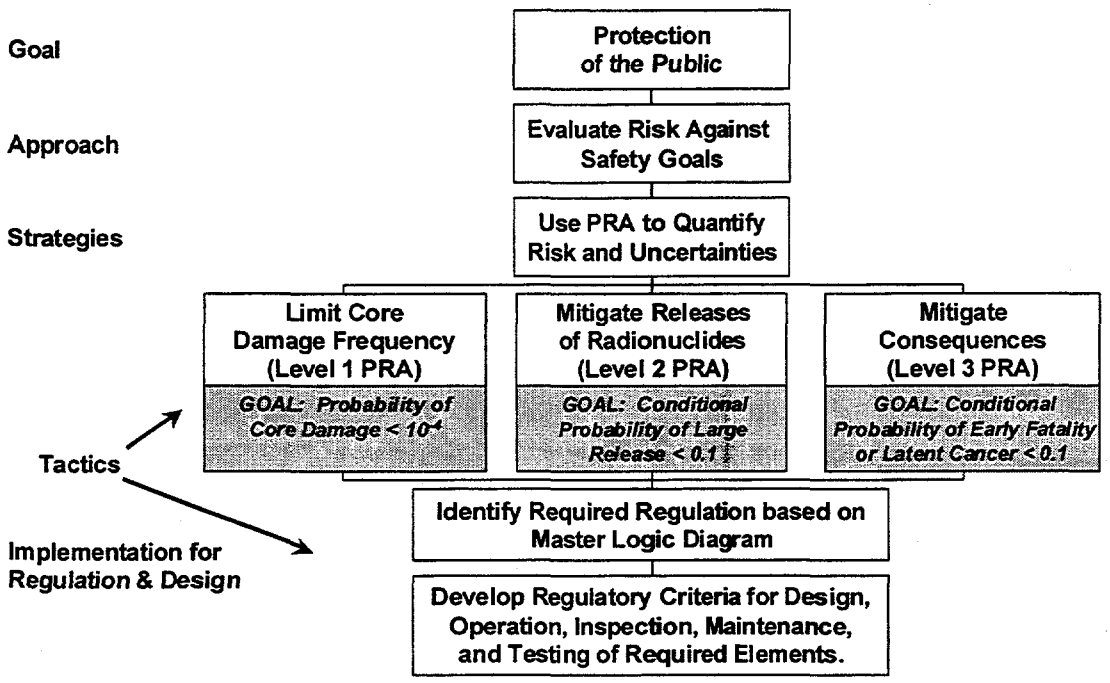


Figure 1. Framework for Risk-Based Regulation and Design

To develop risk-based regulations, *implementation* of the framework is achieved by defining functional system characteristics, within the context of how PRA is performed, to determine what areas need to be regulated to assure safety. Implementation for design is achieved by specifying design configurations and using PRA to evaluate the design, then iterating with subsequent design changes. A master logic diagram (MLD), illustrated in Figure 2, is used to take a top-down approach to identify the safety functions, and systems, structures, and components (SSCs) that are required to maintain safety and to identify the accident initiators and system response failures that could compromise safety [4]. The top event is stated in terms of risk exceeding the safety goals. The gray shaded events correspond to the Level 1, Level 2, and Level 3 PRA strategies, respectively, in Figure 1. The sixth level of the MLD defines the system functions that are required to assure safety. The next level down indicates that initiating events and failure of mitigating systems, containment, and emergency response can compromise safety functions. The last level of the MLD indicates that internal initiators for all operating modes and external initiators will be considered for completeness. Further development of the MLD will determine the "regulatory risk space" for which regulatory and design requirements are needed.

Various *tactics* (e.g., design criteria, procedures, redundancy, emergency response, etc.) are applied to support the PRA strategies and implementation. Once the SSCs required to achieve safety have been identified, then decisions on appropriate tactics for regulation and design can be made. The specification of these tactics will be based on a systematic

evaluation of the areas that need to be regulated for the purposes of assuring safety and will also evolve from this process.

4. Summary

We have presented a framework for risk-based regulation and design for new NPPs. PRA methods and a rationalist approach to DID are used to develop the framework. For new plants, a detailed plant-specific PRA for all operating modes, along with an explicit treatment of uncertainties, would confirm that established quantitative safety goals are met. Within the current capabilities of PRA methods, sources of uncertainty will be quantified to gain as complete an understanding as possible about the range of risk and uncertainty before DID is applied to address uncertainties. Within this framework, PRA provides the basis for both developing and evaluating compliance with requirements for risk-based regulation and design.

5. References

1. U.S. Nuclear Regulatory Commission, Framework for Risk-Informing Regulations, Draft for Public Comment, Rev. 1.0, February 10, 2000, http://nrc-part50.sandia.gov/Document/framework_(4_21_2000).pdf
2. Letter to Shirley Ann Jackson, Chairman, U.S. Nuclear Regulatory Commission, from D.A. Powers, Chairman, Advisory Committee on Reactor Safeguards, Subject: The Role of Defense in Depth in a Risk-Informed Regulatory System, May 19, 1999
3. Sorensen, J.N., Apostolakis, G.E., Kress, T.S., and Powers D.A., On the Role of Defense in Depth in Risk-Informed Regulation. Proceedings of The International Topical Meeting on Probabilistic Safety Assessment, Washington, DC, pp. 408-413, 1999
4. Apostolakis, G.E., Some Issues Related to Goal Allocation and Performance Criteria. Proceedings of the 8th International Conference on Structural Mechanics in Reactor Technology, Brussels, Belgium, Paper M2 4/3, 1985

Acknowledgement: This work was performed as part of the U.S. Department of Energy's (DOE's) Nuclear Energy Research Initiative (NERI).

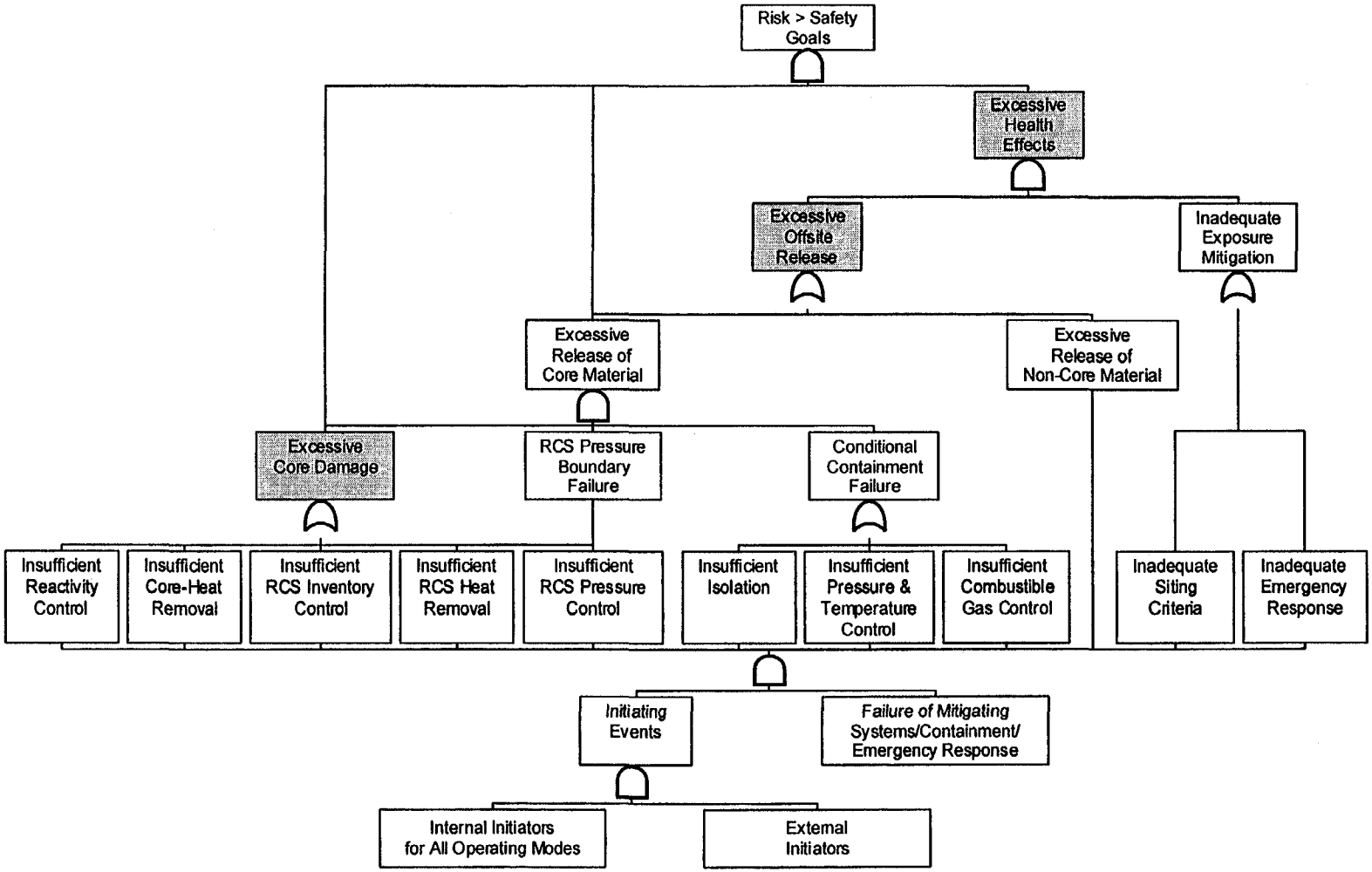


Figure 2 Example Master Logic Diagram for Framework Implementation

Appendix B

Nuclear Energy Research Initiative

An Overview of the Cooperative Program for the Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants

Appendix B
An Overview of the Cooperative Program for the Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants

Nuclear Energy Research Initiative

An Overview of the Cooperative Program for the Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants

Stanley E. Ritterbusch
Westinghouse Electric Company, Nuclear Systems
2000 Day Hill Road
Windsor, Connecticut, 06095 USA

ABSTRACT

EPRI studies have shown that nuclear plant capital costs will have to decrease by about 35% to 40% to be competitive with fossil-generated electricity in the United States. Also, the "first concrete" to fuel load construction schedule will have to be decreased to less than 40 months. Therefore, the U. S. Department of Energy (DOE) initiated the Nuclear Energy Research Initiative (NERI) and WENS proposed a cooperative program with Sandia National Laboratory (SNL) and Duke Engineering & Services (DE&S) to begin an innovative research effort to drastically cut the cost of new nuclear power plant construction for the U. S. de-regulated market place. This program was approved by the DOE through three separate but coordinated "cooperative agreements." They are the "Risk-Informed Assessment of Regulatory and Design Requirement s for Future Nuclear Power Plants" (Risk-Informed NPP), the "Smart Nuclear Power Plant Program" (Smart-NPP), and the "Design, Procure, Construct, Install and Test" (DPCIT) Program. DOE funded the three cooperative agreements at a level of $2.6 million for the first year of the program. Funding for the complete program is currently at a level $6.9 million, however, WENS and all partners anticipate that the scope of the NERI program will be increased as a result of the overall importance of NERI to the U. S. Government.

The Risk-Informed NPP program, which is aimed at revising costly regulatory and design requirements without reducing overall plant safety, has two basic tasks: "Development of Risk-Informed Methods" and "Strengthening the Reliability Database." The overall objective of the first task is to develop a scientific, risk-informed approach for identifying and simplifying deterministic industry standards, regulatory requirements, and safety systems that do not significantly contribute to nuclear power plant reliability and safety. The second basic task is to develop a means for strengthening the reliability database, along with the data collection and evaluation methods, that will be needed to evaluate the safety and reliability of future nuclear power plant designs.

Appendix B
An Overview of the Cooperative Program for the Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants

At the end of the Smart-NPP, DPCIT, and Risk-Informed NPP programs it is expected that methods will have been sufficiently developed and demonstrated to define a more extensive program that will address large-scale development and implementation – leading to the required 35% to 40% reduction in nuclear plant cost for the U. S. de-regulated market and a much shorter construction schedule. The new design and regulatory process is envisioned to use risk-based information to the extent practical and to use "defense-in-depth" only when necessary to address uncertainties in PSA models and equipment performance.

In the following sections, the Smart-NPP and DPCIT programs are briefly summarized and the Risk-Informed NPP program is described in more detail.

SMART NUCLEAR POWER PLANT PROGRAM

The goal of this program is to design, develop, and evaluate the methods for implementing smart equipment and predictive maintenance technology. In this program, "smart" equipment means components and systems that are instrumented and monitored to detect incipient failures in order to improve their reliability. The resulting smart equipment methods will be combined with a more risk-informed regulatory approach to allow plant designers to simplify designs without compromising overall reliability and safety. This concept will allow designers to address reliability at the component and system level while reducing dependence on costly practices such as redundancy and diversity of safety systems.

This program began with a system evaluation and prioritization study that identified and prioritized nuclear plant equipment which would most likely benefit from the addition of "smart" features (e.g., sensors, data processing, and man-machine interface devices). A criteria list was developed and BWR and PWR equipment lists were generated and prioritized. An optimum equipment health-monitoring system is being developed for a selected component (i.e., a normally operating horizontal centrifugal pump). The smart equipment methodology will include a "virtual machine" capability to simulate equipment behavior in order to evaluate the overall benefits to system performance from designing in smart features.

Methodologies also will be developed for consolidating and presenting the data obtained from "smart" equipment to ensure that the health of the "smart" plant is readily understandable. A strategy will be developed for providing smart equipment information to plant operators, maintenance personnel, and plant management that integrates with existing Man-Machine Interface (MMI) methods. A survey has been conducted to determine how smart equipment information is presented to users in other industrial applications; results are now being evaluated and applicable characteristics will be adopted for this project. This task includes the development of a detailed description of how to apply smart features to a variety of equipment types. This task will also help in the development of the design methodology needed to allow communication and integration among the smart components, control room systems, and plant operators.

The final task in this program will be to expand the concept of smart equipment to system and plant levels. Achievement of this level of integration represents a formidable challenge. To be

able to perform this level of integration, it will first be necessary to develop techniques to combine equipment health information from individual machines into plant health information. While it is obviously beneficial to perform health monitoring on individual pieces of equipment, the ultimate goal is to develop methodologies to combine health-monitoring information into a plant-wide system.

DESIGN, PROCURE, CONSTRUCT, INSTALL AND TEST PROGRAM

Reduction of the complete design-testing cycle for new nuclear plants is the goal of this project. The key objectives of this project are (1) leveraging Information Technology, (2) determining the impact on schedule reduction of long lead time items and possible remedies, (3) incorporation of insights from manufacturing, (4) linking 3D Computer Assisted Design (CAD) to Project Management tools, (5) applying conceptual ideas such as modularity, (6) examining potential the critical path and determining how to eliminate interfaces that cause substantial rework, (7) adopting an electronic commerce business model in which suppliers and the design/manufacturing organization are not just linked, but work is handed off to be performed in parallel paths, and (8) determining the applicability of finite element analysis to identify potential improvements in nuclear containment structures that would allow significant reductions in capital cost and schedule.

This program will achieve its goals by producing a balance between integrating information technology in the design methods and tools, designs for constructability, and collaborative work practices made possible through current advances in the business of linking vendors and design/build organizations together in a mutual project. This development approach expects to break new ground in challenging the questions of why/how work is performed. In order to create that challenge, the DPCIT cycle will be adopted as the point of reference in the investigations. In the final analysis, any proposed improvements must point towards meaningful reductions in the length of time and total cost of the DPCIT cycle. This method of accounting forces all costs and time to be rolled up for impact on the project, thus avoiding the problems of sub-optimization of individual components at the expense of the overall goal. The merger of the potential improvements in the DPCIT cycle will be expressed in a series of models to describe how the improvements can be implemented for the next generation plant. The proposed models are:

The Product (or Plant) Model represents the physical design. The primary objects in the model are the plant "parts" and "assemblies" of parts. This is essentially the same model used in most Product Data Management (PDM) Systems. Each part or assembly has a set of associated attributes that describe the part. One of the key attributes is cost of the part. A roll up through the Model allows determination of equipment costs. The Product model is visualized with a 3D CAD application that is linked to the model.

The Productivity (or Schedule) Model represents the time line over the period of interest. In the case of this study that is from contract award to commercial operation, but it could be extended through out the life of the plant. The primary objects in this model are activities that are conducted to execute the DPCIT cycle. Again each activity has a set of associated attributes that

describe the activity (e.g. start, finish, precursors). Since resource unit costs and duration will be included in the model, an output of activity cost and schedule can be obtained directly from the model The productivity model is visualized through scheduling tools such as Gant and PERT and can be automated using commercial tools like Primavera or MS project.

The Process Model represents the method and practices that are used to accomplish the activities of DPCIT cycle that used. The primary objects of the model are processes that have attributes such as input data and out put data. The Process model can be constructed and visualized using several management analyses tools and techniques (e.g., matrix reordering).

Given the need to break new ground and adopt new methods, this program has chosen a process that has been proven for high technology development projects. The process elements are (1) the Knowledge Acquisition Phase which includes extracting lessons learned from prior US nuclear construction and borrowing the best practices from other industries, (2) the Collaboration On Model Characteristics Phase in which the various insights from the Knowledge Acquisition Phase are reviewed to determine which of them would meet the project goals and could be practically implemented, and (3) the Production of Prototype Models Phase which addresses the development of the revised processes for new plant design, procure, construct, install, and test that can deliver on the promise of substantially reduced cycle time.

RISK-INFORMED DESIGN AND REGULATORY PROCESS

Risk assessments have always been a consideration in the design and regulation of nuclear power plants. Emphasis on diversity and redundancy in safety systems was adopted in the design and regulation of nuclear power plants to ensure that the health and safety of the public was protected. Qualitative risk judgments are reflected in safety analysis methods. Events judged to be more frequent have more conservative analysis methods and more stringent acceptance criterion. For example, no fuel failures are allowed for a Loss of Offsite Power event, but some fuel failures are allowed for the less frequent Control Rod Ejection event. Safety analyses also include the most limiting "single failure" of the mitigation systems and margin is frequently added throughout the design and analysis process to resolve uncertainty related to equipment performance or the analysis method itself.

The process of adding conservatism to resolve such uncertainties has been called "defense-in-depth" and this principle has been developed and refined over the past three decades. Defense-in-depth has never been quantitatively defined and, therefore, it has been used in a subjective or qualitative manner (i.e., engineering judgement) to maintain confidence in plant safety. This approach has resulted in not only improved design features and increased plant safety, but also plant designs that are no longer economically competitive with fossil-generated electrical power.

The ability to perform probabilistic safety assessments (PSAs) has been developed and implemented over the past three decades through efforts such as the Reactor Safety Study (WASH-1400), "Severe Accident Risks: A Study of Five U. S. Nuclear Power Plants" (NUREG-1150), and the PSAs performed for ALWR Design Certifications such as System 80+ and AP-

600. The PSA methods that were developed have enabled plant designers to assign a probability to a specific event sequence and estimate the likelihood of severe core damage. In some cases, PSAs have also been used to determine which features should or should not be included in a plant design for the purposes of severe accident protection. Application of these methods has enabled both the plant designer and the regulator to develop confidence that the normal design process results in adequate margin to prevent severe accidents and mitigate them should they occur.

These PSA methods also enable the designer to quantify the large and sometimes excessive degree of conservatism in the normal design process. For example, safety systems are engineered to provide a very high level of confidence that a large degree of fuel melting will not occur and that a coolable core geometry will be maintained even if a large double-ended pipe bread occurs (i.e., the design basis LOCA). Even though safety systems are designed to prevent significant fuel melting, it must also be assumed (per the defense-in-depth principle) that a significant degree of fuel melting occurs and corresponding mitigation systems must be designed to limit offsite doses at the site boundary to less than 3 Sv to the thyroid or 0.25 Sv Total Effective Dose Equivalent (TEDE). For the System 80+ design, the design basis LOCA resulted in a 2-hour thyroid dose at the site boundary of 1.72 Sv and a TEDE dose of only 0.07 Sv. When a severe LOCA was analyzed using more realistic PSA-based, but still conservative, methods the 24-hour thyroid dose at the site boundary was only 0.03 Sv and the 24-hour TEDE dose for the weighted average of all core damage events was only 0.005 Sv. These results show that there is approximately a factor of 50 conservatism in the design basis methods.

While the PSA has provided valuable insight to plant safety analysis and confidence in overall plant safety, these insights, lessons learned, and analysis capabilities have not been completely fed back into the design and regulatory process. Therefore, the heart of the Risk-Informed NPP program is the development of methods by which PSAs can be used to remove excessive conservatisms, simplify plant designs, lower their cost, and (at the same time) maintain a high level of safety.

The Risk-Informed NPP program has two basic tasks, as shown in Figure 1: "Development of Risk-Informed Methodologies" and "Strengthening the Reliability Database." The objectives of the first task are to (1) develop a scientific, risk-informed approach for identifying and simplifying (modifying or eliminating) deterministic industry standards and regulatory requirements that do not significantly contribute to nuclear power plant reliability and safety and (2) develop an approach for simplifying nuclear plant designs themselves using the new risk-informed industry standards and regulatory criteria.

The second basic task of this project is the development of methods to strengthen the reliability database that will be needed to demonstrate the safety and reliability of future nuclear power plant designs. To perform a more risk-informed assessment of future designs, plant designers will need to demonstrate that their new plant designs satisfy probabilistic safety goals. This will require good, defensible equipment reliability data. While the nuclear industry has a significant amount of data on the reliability and performance of the equipment used in today's nuclear plants, there are still gaps to be filled. For example, there is limited data on the reliability

and performance of the new, advanced "smart" equipment that may be introduced in new nuclear plant designs. The result of this task will be a clear understanding of new data needs and requirements for obtaining those data.

RISK-INFORMED PROJECT ACTIVITIES

One of the first activities of this project was the specification of overall project principles and objectives in a Regulatory Framework Document. After many discussions and early draft documents, the first major draft of the Regulatory Document was completed in March 2000. The major principles are summarized below.

- This project will retain the basic regulatory concepts of adequate protection of the health and safety of the public, safety margin, and defense-in-depth. However, these concepts will be applied using the most current risk-based models and scientific technology. Further, this project will remain consistent with the current ongoing NRC risk-informed program for operating reactors.

- We will do what is technically correct and justifiable, not necessarily what is easy. This principle applies to both design activities and the establishment of regulatory criteria.

- The resulting design and regulatory process must retain basic prevention and mitigation strategies so that the regulators and the public are convinced that the new approach is conservative. Therefore, the new process will follow the current objectives of preventing core damage, mitigating radioactivity releases should core damage occur, and preparing an emergency evacuation plan. The methods and criteria used to achieve these objectives, however, will be based on risk-informed evaluations (e.g., less restrictive containment design methods and a smaller emergency evacuation zone).

- This project will review the complete design and regulatory process and identify all factors that have a significant impact on plant cost. This will result in a method for complete re-design of a nuclear power plant starting from the basic function of power production. Only the minimum set of safety equipment needed to meet safety criteria using risk-based methods will be added to the design. To the maximum extent possible, all major design methods, assumptions, uncertainties, and acceptance criteria will be identified and retained only if justified according to risk-based models.

- The emphasis on use of risk-based models will require that probabilistic design and safety criteria be established. While these criteria have not yet been selected, it is expected that they will address issues such as core damage frequency, containment reliability, and offsite radiological releases. It will not be easy to establish firm probabilistic criteria because in the past PSA models and assumptions have only been used to perform an overall general assessment of plant performance and safety. Nonetheless, such criteria and the supporting PSA methods need to be established if this project is to be successful.

- Once PSA methods and acceptance criteria have been established, they will be used to the greatest extent practical to resolve the uncertainties and safety margins in the design process. These uncertainties and margins exist due to uncertainty in equipment performance, uncertainty about analysis methods, and conservatism added by the designer and regulator (engineering judgment).

- The current approach to defense-in-depth will be used only when the uncertainties cannot be resolved using risk-based methods. This, in effect, means that the application of risk-based methods is the primary means for assuring plant safety and that defense-in-depth is subsidiary to these risk-based methods. This is a very significant change from the current design and regulatory process wherein defense-in-depth is the primary means for assuring safety and risk-informed changes are made only when justified.

- Along with a new design and regulatory process, it is envisioned that a new set of regulations will have to be developed. These new regulations would not replace the current regulations – which must remain in place for currently operating plants. Rather, it is expected that a new set of regulations will be developed specifically for future plants. While defense-in-depth would be subsidiary to risk-based methods, the probabilistic criteria and supporting PSA methods would be elevated to a more firm level than in the current regulations.

This new design and regulatory process is compared to the current NRC risk-informed process in Figure 2.

The execution of the new design process for a sample problem has been initiated. While problems will have to be solved and changes will have to be made to the design process itself as this sample problem is completed, a few of the issues which are expected to be addressed are listed below.

- Identification of a new set of design basis accidents using PSA methods.

- Reduction of the size of the double-ended pipe break used for design of safety systems and the containment. That is, Leak-Before-Break technology will be used to justify elimination of the large double-ended pipe break from the design basis.

- Technical consistency of assumptions, methods, and criteria to the extent practical given the state of knowledge available. For example, the design includes safety systems to maintain a coolable core geometry during a LOCA (i.e., significant fuel damage must be prevented). Nonetheless, safety grade mitigation systems are designed to mitigate a severely damaged core. While some mitigation capability is certainly reasonable, it may not be necessary to include the same extent of redundancy in safety equipment as in current designs – perhaps two (vs. four) trains of mitigation equipment are adequate given the low probability of the specific event being analyzed.

- Use of the "single failure criterion" in the design of safety systems only when justified based on weaknesses in the PSA model or other design considerations.

- Use of safety grade classification for equipment specifications only when justified. Equipment that has very high, demonstrable reliability (e.g., "smart" equipment) would not need to be safety grade.

- Use of normally operating "smart" equipment to perform safety functions. This is a deviation from the current practice where normal and safety equipment functions are separated to the extent practical.

- Inclusion of passive components to increase reliability to the extent scientifically justified.

- Integrated analyses methods (e.g., integrated structure-piping models) to eliminate unnecessary margin from the design.

It is believed that only with changes such as those described above, and many others of a similar nature, can a significant amount of equipment be removed from the plant design while still maintaining the same level of safety.

SUMMARY

It is clear that the U. S. Government and the DOE in particular are creating major new research and development projects through the NERI program. It is expected that these new projects will be carried out over the next decade and that DOE plans to ensure that new nuclear power plant construction remains competitive in the U. S. deregulated market. WENS will support this NERI objective through (1) timely completion of the three cooperative agreements comprising the coalition and (2) support of future NERI research and development projects to ensure that major reductions in plant capital costs, construction schedules, operating costs are achieved.

The first major draft of a Regulatory Framework Document for a new design and regulatory process has been developed. The major features of the new process are:

- A completely new design and regulatory process, including

- Evaluation and possible revision all major assumptions, criteria, and safety margins, affecting the cost of a nuclear power plant,

- Retention of the basic prevention and mitigation concept,

- Use of PSA risk-based methods to resolve all uncertainties and margins to the maximum extent possible, and

- Use of defense-in-depth only when uncertainties cannot be resolved with risk-based methods.

When future research and development are completed, implementation of the new design and regulatory process will result in a significantly simplified nuclear plant design with the same level of safety as today's designs. The efforts of the WENS coalition will be coordinated with the U. S. NRC and with other industry programs. The DOE would welcome international participation in NERI projects and, therefore, WENS hopes that a partnership can be formed with Korean organizations to (1) incorporate experience from the KSNP and KNGR programs into NERI and (2) improve those same programs using NERI results.

The development of a completely new, risk-informed design and regulatory process – including the results from the Smart Equipment and DPCIT projects – is the only way capital costs for a new plant can be decreased by 35% to 40% and the construction schedule shortened to less than 40 months. These reductions are necessary to ensure that new nuclear power plants will be competitive in the U. S. deregulated market.

Appendix B
An Overview of the Cooperative Program for the Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants

1. U.S. Nuclear Regulatory Commission, "Framework for Risk-Informing Regulations," Draft for Public Comment, Rev. 1.0, February 10, 2000,
2. http://nrc-part50.sandia.gov/Document/framework_rev_ai_2.pdf
3. Letter to Shirley Ann Jackson, Chairman, U. S. Nuclear Regulatory Commission, from D. A. Powers, Chairman, Advisory Committee on Reactor Safeguards, "The Role of Defense in Depth in a Risk-Informed Regulatory System," May 19, 1999.
4. J. N. Sorensen, G. E. Apostolakis, T. S. Kress, and D. A. Powers, "On the Role of Defense in Depth in Risk-Informed Regulation," Presented at PSA '99, Washington, DC, American Nuclear Society, August 22-25, 1999.
5. FR Doc. 88-12624, Statement of Considerations, Revisions to Backfit Rule, 10 CFR 50.109, July 6, 1988 American Nuclear Society, August 22-25, 1999.
6. Center for Strategic and International Studies, "The Regulatory Process for Nuclear Power Reactors. A Review," Washington, DC, August 1999.
7. Letter to Shirley Ann Jackson, Chairman, U. S. Nuclear Regulatory Commission, from R.L. Seale, Chairman, Advisory Committee on Reactor Safeguards, "Risk-Based Regulatory Acceptance Criteria for Plant-Specific Application of Safety Goals," April 11, 1997.
8. Letter to Shirley Ann Jackson, Chairman, U. S. Nuclear Regulatory Commission, from R.L. Seale, Chairman, Advisory Committee on Reactor Safeguards, "Elevation of CDF to a Fundamental Safety Goal and Possible Revision of the Commission's Safety Goal Policy Statement," May 11, 1998.
9. G. E. Apostolakis, "Some Issues Related to Goal Allocation and Performance Criteria," Presented at the 8th International Conference on Structural Mechanics in Reactor Technology, Brussels, Belgium, August 19-23, 1985.
10. PRA Procedures Guide, NUREG/CR-2300, U.S. Nuclear Regulatory Commission, September 1981.

Appendix B
An Overview of the Cooperative Program for the Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants

Figure 1: Task Schedule for the Risk-Informed NPP Program

ID	Task Name
17	**Development of Risk-Informed Methodologies**
18	1.1 - Identify all Applicable Regulatory Requirements
19	1.2 - Identify SSCs and Costs for Typical Plant
20	1.3 - Develop Methodology to Risk-Inform Regulations
21	1.4 - Develop Methodology to Simplify SSCs
22	1.5 - Identify High Priority Requirements and SSCs
23	1.6 - Apply Methodologies to Sample SSC
24	1.7 - Evaluate Regulatory Process
25	1.8 - Coordinate Activities with Industry & NRC
26	
27	**Strengthening the Reliability Database**
28	2.1 - Identify Current Data Sources
29	2.2 - Identify Weaknesses in Current sources
30	2.3 - Develop Programs to Correct Weaknesses

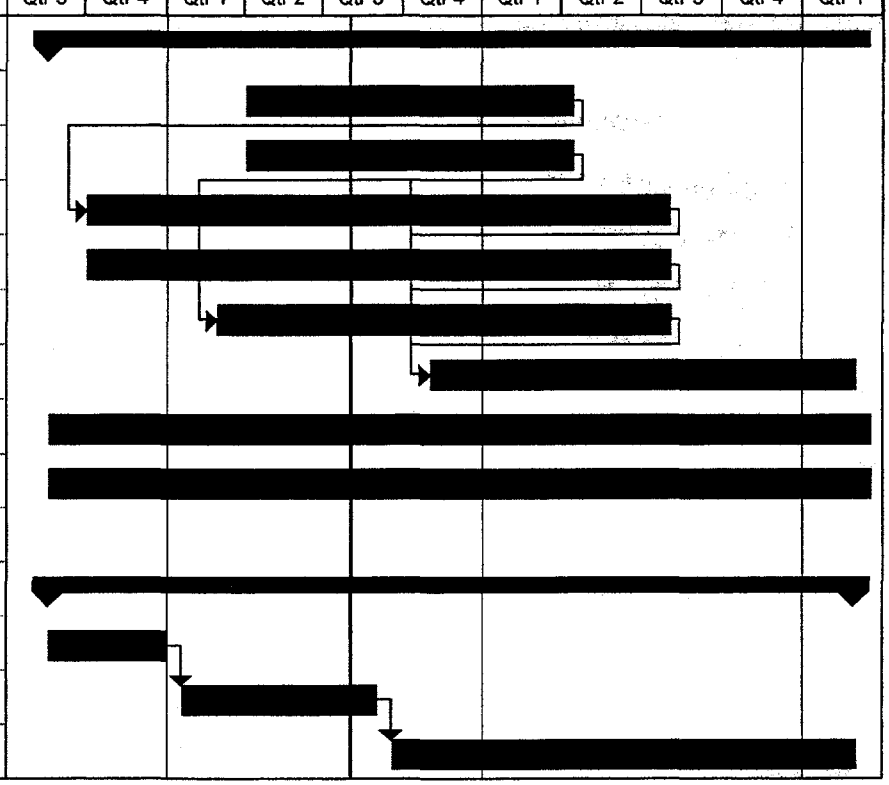
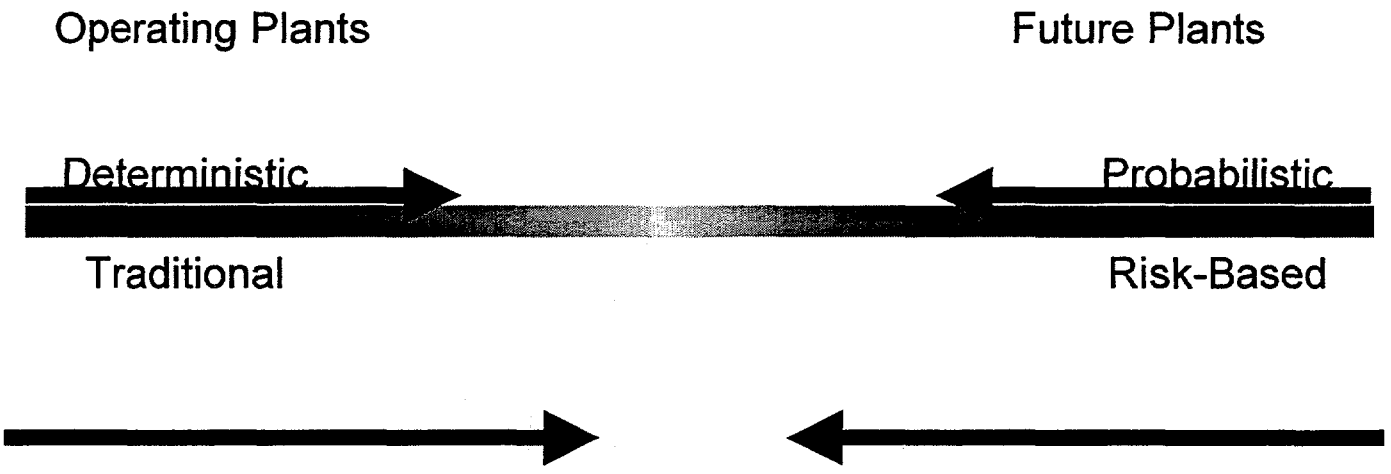


Figure 2: Comparison of NRC and NERI Risk-Informed Processes



Appendix C

Key Presentations and Meetings

Appendix C
Key Presentations and Meetings

In support of the project for Risk Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants, Westinghouse sponsored or participated in the following meetings and made corresponding presentations.

- NRC Workshop on Risk-Informed Regulation, Rockville, MD, September 15, 1999.
- Overview Meeting With Korea Power Engineering Company, September, 1999.
- Risk-Informed Project Kickoff Meeting, Windsor, CT, October 7-8, 1999.
- Risk-Informed Project Meeting, Rockville, MD, November 30-December 1, 1999.
- Status Meeting with Korea Power Engineering Company, December 9, 1999.
- NEI Risk-Informed Working Group Meeting, Washington, DC, February 15, 2000.
- NRC Risk-Informed Workshop, Rockville, MD, February 24-25, 2000.
- Status Meeting with Korea Electric Power Company and Korea Power Engineering Company, February 28 – 29, 2000.
- Risk-Informed Project Review Meeting, Windsor, CT, March 9-10, 2000.
- NRC Research Management Information Meeting, Adjunct to the Regulatory Information Conference, March 28, 2000.
- IAEA Consultancy Working Group on Water Cooled Reactor Technology Meeting, Vienna, Austria, April, 2000.
- DOE Annual Project Review Meeting, Albuquerque, NM, July 18, 2000.

The significant aspects of the above meetings and presentations, as related to this project's technical interactions with other organizations, are summarized below.

NRC Workshops: WENS represented this project at two NRC workshops on risk-informing the current regulations for current plants (September 1999 and February 2000). The purpose of the presentation at the first workshop was to introduce our project, state its purpose of developing new methods for design and regulation of future plants, and state the importance of coordinating our project with other industry and NRC initiatives. NRC supported the desire to coordinate related programs.

At the second workshop, our draft regulatory framework document was summarized, with emphasis on differences (not conflicts) with the current NRC program for operating reactors. NRC Research personnel encouraged our project to think "boldly" in terms of challenging current regulatory assumptions even though future review and approval of NRC staff might be difficult.

NRC Research Management Meeting: At the Regulatory Information Conference in March 2000, WENS met with representatives of NRC Research to summarize the status

of our project. Again, we were encouraged to proceed as planned and it was agreed that at some undetermined future time (possibly during Phase 2 of this project) a briefing should be provided to the Commissioners.

NEI Risk-Informed Working Group: WENS attended two meetings of this working group. This project's plans were summarized and the intent to closely coordinate activities with the ongoing NRC effort was summarized. Other NEI working group members supported this project and its approach.

IAEA Consultancy Group: WENS represented this project at two meetings of this working group. The purpose was to draft a report on optimizing water-cooled reactor technology. This draft was accomplished and it is consistent with and supportive of DOE's NERI program, specifically including this Risk-Informed Assessment project and its two related NERI projects for "Smart" Equipment and Improved Design and Construction methods. Another meeting is scheduled for December 2000 to further coordinate these projects.

Korean Organizations: WENS made three status presentations to Korea Electric Power Company and Korea Power Engineering Company. An invitation was made to participate in our NERI projects at no cost to DOE, and as long as Korean detailed information and labor were contributed to our projects. This cooperation is being coordinated via DOE management and may be initiated in Phase 2.

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

Acronyms & Abbreviations

Regulatory Documents	
bul	Nuclear Regulatory Commission (NRC) Bulletin
cfr	Code of Federal Regulations
cir	NRC Circular
drg	Draft Regulatory Guide
glt	NRC Generic Letter
inm-....	NRC Inspection Manual with Chapter Reference
inm-toc	NRC Inspection Manual Table of Contents
not	NRC Information Notice
nureg	Formal NRC Staff Publication
pol	NRC Policy Statement
reg	NRC Regulatory Guide
srp	Standard Review Plan (NUREG-0800)
sts	Standard Technical Specifications
sts4-ge...	Standard Technical Specifications for the General Electric Model 4 w/ paragraph reference
sts6-ge...	Standard Technical Specifications for the General Electric Model 6 w/ paragraph reference
stsb&w...	Standard Technical Specifications for Babcock & Wilcox w/ paragraph reference
stsce...	Standard Technical Specifications for Combustion Engineering w/ paragraph reference
stswst...	Standard Technical Specifications for Westinghouse Electric w/ paragraph reference

Other Abreviations & Acronyms	
ACI	American Concrete Institute
ACS	American Chemical Society
AEC	Atomic Energy Commission
AICHE	American Institute of Chemical Engineers
AISC	American Institute of Steel Construction
ANS	American Nuclear Society
ANSI	American National Standards Institute
APHA	American Public Heath Association

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

Acronyms & Abbreviations (continued)

API	American Petroleum Institute
ASA	Acoustical Society of America
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASNT	American Society for Nondestructive Testing
ASQC	American Society for Quality Control
ATC	Applied Technology Council
ASTM	American Society for Testing and Materials
AWS	American Welding Society
AWWA	American Water Works Association
CMAA	Crane Manufacturers Association of America
DEMA	Diesel Engine Manufacturers Association
DOE	US Department of Energy
DOT	US Department of Transportation
EPA	US Environmental Protection Agency
ERDA	US Energy Research and Development Administration
FFPR	Federal Specification
FM	Factory Mutual
FWPCA	Federal Water Pollution Control Act
GS of A	Geological Society of America
HEI	Heat Exchanger Institute
HHS	US Department of Health and Human Services
HPS	Health Physics Society
HPSSC	Health Physics Society Standards Committee
ICEA	Insulated Cable Engineers Association
ICRP	International Commission on Radiological Protection
ICRU	International Commission on Radiological Units and Measurements
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISA	Instrument Society of America
ISO	International Standards Organization
MIL	Military Standard
MSS	Manufacturers Standards Society
NACE	National Association of Corrosion Engineers
NBS	National Bureau of Standards
NCMA	National Concrete and Masonry Association

Acronyms & Abbreviations (continued)

NCRP	National Council on Radiation Protection
NEA	Nuclear Energy Agency
NEMA	National Electrical Manufacturers Association
NETA	National Electrical Testing Association
NFPA	National Fire Protection Association
NIOSH	National Institute for Occupational Health and Safety
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
N/S	in the "Standard Version" column indicates that no version date was specified in the citation
NRA	National Rifle Association
NSF	National Science Foundation
OSHA	Occupational Safety and Health Administration
UL	Underwriters Laboratory
USGS	United States Geological Survey

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

Codes & Standards Cited in NRC Regulatory Documentation

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
10cfr100	NBS	NBS Handbook 69	1959	Maximum Permissible Body Burdens and Maximum Permissible Concentrations of Radionuclides in Air and in Water for Occupational Exposure
10cfr2 App. C	ASME	ASME Code	N/S	ASME Boiler and Pressure Vessel Code
10cfr2, App. C	DOT	DOT 7A	N/S	Authorized Type A Packages
10cfr2, App. C	EPA	40 CFR 190	N/S	Environmental Radiation Protection Standards for Nuclear Power Operations
10cfr20	NBS	NBS	N/S	National Voluntary Laboratory Accreditation Program (NVLAP)
10cfr20	DOT	10 CFR 73.421-424	N/S	Physical Protection of Plants and Materials
10cfr20	NIOSH	30 CFR 11	N/S	National Institute for Occupational Safety and Health
10cfr20	DOT	49 CFR 173.403 (m) and (w)	N/S	Shippers - General Requirements for Shipments and Packages
10cfr20	EPA	38 FR 24936	1973	Memorandum of Understanding between the Environmental Protection Agency and the Atomic Energy Commission
10cfr20 Subparts A-O	NIST	NIST	N/S	National Voluntary Laboratory Accreditation Program (NVLAP)

Thursday, July 27, 2000

NUREG/CR-5973 Database Query Results

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
10cfr20 Subparts A-O Requirements for Shipments and Packages	DOT	49 CFR 173.403 (m) and (w)	N/S	Shippers - General
10cfr20 Subparts A-O Requirements for Shipments and Packages	DOT	49 CFR 173.421-424	N/S	Shippers - General
10cfr34 Nondestructive Testing	ASNT	ASNT-IRRSP	N/S	American Society for
10cfr34 Specifications for Design and Test of Apparatus	ANSI	ANSI N432	1980	Gamma Radiography -
10cfr34 Specifications for Design and Test of Apparatus	NBS	NBS Handbook 136	1982	Gamma Radiography -
10cfr36 Requirements for Reinforced Concrete	ACI	ACI 318	1989	Building Code
10cfr40 Protection Standards for Uranium and Thorium Mill Tailings	EPA	40 CFR 192, Subparts D and E	N/S	Health and Environmental
10cfr50 App. E Development of State and Local Government Radiological Plans in Support of Light-Water Nuclear Power Plants	EPA	EPA-520/1-78-016	1978	Planning Basis for the Emergency Response
10cfr50 App. G Vessel Code	ASME	ASME B&PV Code Addenda	1972	ASME Boiler and Pressure
10cfr50 App. G Inspection of Nuclear Power Plant Components	ASME	ASME Section XI	N/S	Rules for Inservice
10cfr50 App. G Surveillance Tests for Light-Water Cooled Nuclear Power Reactor Vessels	ASTM	ASTM E185	1979	Practice for Conducting

Thursday, July 27, 2000

NUREG/CR-5973 Database Query Results

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
10cfr50 App. G Surveillance Tests for Light-Water Cooled Nuclear Power	ASTM	ASTM E185	1982	Practice for Conducting Reactor Vessels
10cfr50 App. G Ductile Failure	ASME	ASME Sec. III, Appendix G	N/S	Protection Against Non-
10cfr50 App. H Surveillance Tests for Light-Water Cooled Nuclear Power	ASTM	ASTM E185	1979	Practice for Conducting Reactor Vessels
10cfr50 App. H Inspection of Nuclear Power Plant Components	ASME	ASME Section XI	N/S	Rules for Inservice
10cfr50 App. H Surveillance Tests for Light-Water Cooled Nuclear Power	ASTM	ASTM E185	1982	Practice for Conducting Reactor Vessels
10cfr50 App. H Nuclear Power Plant Components	ASME	ASME Section III	N/S	Rules for Construction of
10cfr50 App. H Surveillance Tests for Light-Water Cooled Nuclear Power	ASTM	ASTM E185	1973	Practice for Conducting Reactor Vessels
10cfr50 App. J Leakage Testing Requirements	ANSI	ANSI N45.4	1972	Containment System
10cfr50 App. J Leakage Testing Requirements	ANS	ANS 56.8	1987	Containment System
10cfr50 App. K Single Component, Two-Phase Mixture	ASME	Journal of Heat Transfer	1965	Maximum Flow Rate of a
10cfr50 App. K Flux in a Bundle Cooled by Pressurized Water	ASME	ASME	1969	Correlation of Critical Heat

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
10cfr50 App. K	ASME	Transactions of ASME, 695 - 702	1948	Prediction of Pressure Drop During Forced Circulation Boiling of Water
10cfr50 App. K	ANS	ANS 5.1	1971	Decay Heat Power in Light Water Reactors
10cfr50 App. R	IEEE	IEEE 384	1974	Standard Criteria for Independence of Class 1E Equipment and Circuits
10cfr50 App. R	IEEE	IEEE 384	1974	Standard Criteria for Independence of Class 1E Equipment and Circuits
10cfr50.33	EPA	EPA-520/1-78-016	1978	Planning Basis for the Development of State and Local Government Radiological Emergency Response Plans in Support of Light-Water Nuclear Power Plants
10cfr50.34	ASME	ASME Sec. III, NE-3220	1980	Stress Intensity and Buckling Stress Values for Other Than Bolts
10cfr50.34	ASME	ASME Sec. III, Division 2	1980	Code for Concrete Reactor Vessels and Containments
10cfr50.34	ASME	ASME Sec. III, CC-3720	1980	Liner
10cfr50.44	ASME	ASME Sec. III, CC-3720	1980	Liner
10cfr50.44	ASME	ASME Sec. III, NE-3220	1980	Stress Intensity and Buckling Stress Values for Other Than Bolts
10cfr50.44	ASME	ASME Sec. III, Division 2	N/S	Code for Concrete Reactor Vessels and Containments

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
10cfr50.47	EPA	EPA	N/S	Emergency Worker and Life Saving Activity Protective Action Guides
10cfr50.49	IEEE	IEEE 323	1974	Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
10cfr50.54	EPA	EPA-520/1-78-016	1978	Planning Basis for the Development of State and Local Government Radiological Emergency Response Plans in Support of Light-Water Nuclear Power Plants
10cfr50.55a	ASME	ASME B&PV Code	1980	ASME Boiler and Pressure Vessel Code
10cfr50.55a	ASME	ASME B&PV Code Addenda	N/S	ASME Boiler and Pressure Vessel Code
10cfr50.55a	ASME	ASME B&PV Code	1972	ASME Boiler and Pressure Vessel Code
10cfr50.55a	ASME	ASME B&PV Code	1989	ASME Boiler and Pressure Vessel Code
10cfr50.55a	ASME	ASME B&PV Code	1977	ASME Boiler and Pressure Vessel Code
10cfr50.55a	ASME	ASME Sec. XI, Subsec. IWV	1989	Inservice Testing of Valves in Light-Water Reactor Power Plants
10cfr50.55a	ASME	ASME OM Part 4	1988	Examination and Performance Testing of Nuclear Power Plant Dynamic Restraints (Snubbers)
10cfr50.55a	ASME	ASME Sec. XI, Table IWB-2600	1974	Not found

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
10cfr50.55a	ASME	ASME Sec. XI, Tables IWB-2500 and IWB-2500-1	1975	Examination Categories
10cfr50.55a Examination	ASME	ASME Sec. XI, IWC-1220	1975	Components Exempt from
10cfr50.55a	ASME	ASME Sec. XI, Table IWC-2520	1974	Not found
10cfr50.55a Inspection of Nuclear Power Plant Components	ASME	ASME Section XI	1973	Rules for Inservice
10cfr50.55a	ASME	ASME Sec. XI, Table IWC-2520 or IWC-2520-1	1975	Not found
10cfr50.55a Inspection of Nuclear Power Plant Components	ASME	ASME Section XI	1983	Rules for Inservice
10cfr50.55a	ASME	ASME Sec. XI, IWC-2411	1975	Inspection Program A
10cfr50.55a Systems for Nuclear Power Generating Stations	IEEE	IEEE 279	1971	Standard Criteria for Safety
10cfr50.55a	ASME	ASME Sec. XI, IWA-2430(d)	1989	Inspection Intervals
10cfr50.55a in Light-Water Reactor Power Plants	ASME	ASME OM Part 10	1988	Inservice Testing of Valves
10cfr50.55a Components to Which They are Applicable	ASME	ASME Sec. III, NCA-1140	N/S	Nature of These Rules and

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
10cfr50.55a Nuclear Power Plant Components	ASME	ASME Sec. III, Division 1	1989	Rules for Construction of
10cfr50.55a in Light-Water Reactor Power Plants	ASME	ASME OM Part 6	1988	Inservice Testing of Pumps
10cfr50.55a Nuclear Power Plant Components	ASME	ASME Sec. III, Division 1	1980	Rules for Construction of
10cfr50.55a Inspection of Nuclear Power Plant Components	ASME	ASME Section XI	1974	Rules for Inservice
10cfr50.55a Inspection of Nuclear Power Plant Components	ASME	ASME Sec. XI, Div. 1	1989	Rules for Inservice
10cfr50.55a	ASME	ASME Sec. XI, Table IWB-2500-1	1989	Examination Categories
10cfr50.55a Inspection of Nuclear Power Plant Components	ASME	ASME Sec. XI, Div. 1	1980	Rules for Inservice
10cfr50.55a Specifications	ASME	ASME Sec. XI, Table IWA-1600-1	1988	Referenced Standards and
10cfr50.55a Specifications	ASME	ASME Sec. XI, Table IWA-1600-1	1989	Referenced Standards and
10cfr50.55a	ASME	ASME Sec. XI, IWB-2000	N/S	Examination and Inspection
10cfr50.55a Acceptance Criteria for Austenitic Piping	ASME	ASME Sec. XI, IWB-3640	1984	Evaluation Procedures and

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
10cfr50.55a Specifications	ASME	ASME Sec. XI, Table IWA-1600-1	1987	Referenced Standards and
10cfr50.61	ASME	ASME Sec. III, NB-2331	N/S	Material for Vessels
10cfr50.73 Unique Identification in Power Plants and Related Facilities	IEEE	IEEE 803	1983	Recommended Practice for - Principles and Definitions
10cfr51 Understanding Regarding Implementation of Certain NRC and Policy Statement on Implementation of Section 511 of the Control Act (FWPCA)	EPA	40 FR 60115	1975	Second Memorandum of EPA Responsibilities and Federal Water Pollution
10cfr51 Control Act	FWPCA	FWPCA	N/S	Federal Water Pollution
10cfr61 Hazardous Waste	EPA	40 CFR 261	N/S	Identification and Listing of
10cfr71 Requirements for Shipments and Packaging	DOT	49 CFR 173	N/S	Shippers General
10cfr71 Regulations	DOT	49 CFR 170-189	N/S	Hazardous Materials
10cfr73 Operations	DOE	DOE Order 5632.1	N/S	Protection Program
10cfr73 Book	NRA	NRA	1976	High Power Rifle Rules
10cfr73 Special Nuclear Material and Vital Equipment	DOE	DOE Order 5632.2	N/S	Physical Protection of

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
10cfr73 Index	NRA	NRA	N/S	NRA Target Manufacturers
10cfr73 Material on Shipping Papers	DOT	49 CFR 172.202	N/S	Description of Hazardous
10cfr73 Security Alarm Systems	Fed Spe	Federal Specification W-A-00450 B	N/S	Components for Interior
10cfr73 Security Alarm Systems	Fed Spe	Federal Specification W-A-450B	N/S	Components for Interior
10cfr73 Audiometers	ANSI	ANSI S3.6	1973	Specifications for
10cfr73 Basic Interface Requirements	ANSI	ANSI MH5.1	1971	Cargo Container Chassis -
10cfr73 - Specification and Testing: General Cargo Containers for	ISO	ISO 1496	1978	Series 1 Freight Containers General Purposes
10cfr73 Reference Zero for the Calibration of Pure-tone Air Conduction	ISO	ISO 389	1975	Acoustics Standard Audiometers
44 FR 61123 Development of State and Local Government Radiological Plans in Support of Light Water Nuclear Power Plants	EPA	EPA-520/1-78-016	1978	Planning Basis for the Emergency Response
45 FR 2893 Development of State and Local Government Radiological Plans in Support of Light Water Nuclear Power Plants	EPA	EPA-520/1-78-016	1978	Planning Basis for the Emergency Response
49 FR 12335 Certain Hazardous Material Incidents and Detailed Hazardous	DOT	49 CFR 171.15	N/S	Immediate Notice of Material Incident Reports

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
49 FR 12335	DOT	49 CFR 178	N/S	Shipping Container Specifications
55 FR 27522	EPA	40 CFR 261	N/S	Identification and Listing of Hazardous Waste
55 FR 27522	DOT	49 CFR 173	N/S	Shippers General Requirements for Shipments and Packaging
bul71-03	ASME	ASME Section I	N/S	Power Boilers
bul74-03	ASME	ASME Sec. XI, Table IS-251	N/S	Not found
bul75-01	ASME	ASME Sec. XI, Appendix I	1974	Ultrasonic Examinations
bul76-01	ASME	ASME Section XI	1974	Rules for Inservice Inspection of Nuclear Power Plant Components
bul77-05	IEEE	IEEE 323	1974	Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
bul77-08	NFPA	NFPA 101	N/S	Code for Safety to Life Team Fire in Buildings and Structures
bul78-11	ASME	ASME B&PV Code	N/S	ASME Boiler and Pressure Vessel Code
bul79-01A	NEMA	NEMA 4	N/S	National Electric Code

Appendix D

Codes and Standards Cited in NRC Regulatory Documentation

(Sample of NUREG/CR-5973, Rev. 2 Converted Database)

DOCUMENT	*CODE*	*STANDARD*	*Standard Version*	*STANDARD TITLE*
bul79-01B	NEMA	NEMA	N/S	National Electric Code
bul79-01B	IEEE	IEEE 323	1971	Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
bul79-01B	IEEE	IEEE 323	1974	Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
bul79-01b Sup 2	IEEE	IEEE 650	N/S	Standard for Qualification of Class 1E Static Battery Chargers and Inverters for Nuclear Power Generating Stations
bul79-01b.s01	IEEE	IEEE 323	1974	Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
bul79-01b.s02	IEEE	IEEE 323	1974	Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
bul79-01b.s02	IEEE	IEEE 323	1971	Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
bul79-02.r02	ACI	ACI 349	1976	Code Requirements for Nuclear Safety Related Concrete Structures
bul79-03	ASME	ASME Section III	N/S	Rules for Construction of Nuclear Power Plant Components
bul79-03a	ASME	ASME Section III	N/S	Rules for Construction of Nuclear Power Plant Components
bul79-13.r02	ASME	ASME Sec. III, Table NC-5111-1	N/S	Thickness, Penetrameter Designations, and Essential Holes

Appendix E

List of Structures, Systems, and Components for a Typical Plant

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Reactor Coolant System				
Reactor Vessel	1	I	RC	1
Steam Generators (primary/secondary)	1/2 [1]*	I	RC	1
Pressurizer	1	I	RC	1
Reactor Coolant Pumps [2,3,9]*	1	I	RC	1
Piping within Reactor Coolant Pressure	1/2 [4]	I	RC	1
Boundary [5]	[6]	[6]	RC	1
Control Element Drive Mechanisms	3	I	RC	1
Core Support Structures and				
Internals Structures [7]	2	I	RC	1
Fuel Assemblies [8]	3	I	RC	1
Control Element Assemblies [8]	NNS	II [10]	RC	2
Closure Head Lift Rig	1/3 [12]	I	RC	1
Heated Junction Thermocouple Probe				
	1	I	RC	1
Assembly	3	I	RC	1
HJTC Pressure Housing	NNS	NS	RC	3
ICI Cable Tray Support Frame	1	I	RC	1
ICI Holding Frame	1	I	RC	1
ICI Guide Tubes	1	I	RC	1
ICI Guide Tube Supports	1	I	RC	1
ICI Seal Housing	1/2	I	RC	1
ICI Seal Table	1/2	I	RC	1
Piping [27]				
Valves [27]				
In-containment Water Storage System				
IRWST	3	I	RC	1
Holdup Volume Tank	3	I	RC	1
Pressure Relief Dampers	3	I	RC	1
Cavity Flooding System				
Piping	2	I	RC	1
Valves	2	I	RC	1
Safety Depressurization System				
Valves	1/2	I	RC	1
Piping	1/2/NNS	I/NS	RC	1/3
Spargers	2	I	RC	1
Safety Injection System				

* Refer to Notes at end of table.

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Safety Injection Pumps	2	I	RB	1
Safety Injection Tanks	2	I	RC	1
Piping [24,27]	1/2	I	RB/RC	1
Valves [27]	1/2	I	RB/RC	1
Shutdown Cooling System				
Shutdown Cooling Heat Exchangers	2/3 [1]	I	RB	1
Shutdown Cooling Pumps	2	I	RB	1
Shutdown Cooling Mini-Flow Heat Exchanger	2/3 [1]	I	RB	1
Piping [27]	1/2/3	I	RB/RC	1
Valves [27]	1/2/3	I	RB/RC	1
Containment Spray System				
Containment Spray Pumps	2	I	RB	1
Containment Spray Heat Exchangers	2/3 [1]	I	RB	1
Containment Spray Mini-Flow Heat Exchanger	2/3 [1]	I	RB	1
Spray Nozzles	2	I	RC	1
Piping [27]	2/3	I	RB/RC	1
Valves [27]	2	I	RB/RC	1
Chemical and Volume Control System (CVCS)				
Regenerative Heat Exchanger	2	I	RC	1
Letdown Heat Exchanger	2/NNS [1,34]	I	RC	1
Seal Injection Heat Exchanger	NNS [34]	I	NA	2
Purification Ion Exchangers	NNS [34]	I	NA	2
Deborating Ion Exchanger	NNS [34]	I	NA	2
Volume Control Tank	NNS [34]	I	NA	2
Chemical Addition Package	NNS	NS	NA	3
Boric Acid Batching Tank	NNS	NS	NA	3
Charging Pumps	NNS [34]	I	NA	2
Dedicated Seal Injection Pump	NNS [34]	I	NA	2
Dedicated Seal Injection Pump Suction Stabilizer/Pulsation Dampener	NNS [34]	I	NA	2
Boric Acid Makeup Pumps	NNS [34]	I	NA	2
Reactor Makeup Water Pumps	NNS	NS	NA	3
Boric Acid Concentrator	NNS	NS	NA	2
Pre-holdup Ion Exchanger	NNS [34]	I	NA	2
Charging Pump Mini-flow Heat Exchanger	NNS [34]	I	NA	2
Boric Acid Condensate Ion Exchanger	NNS	NS	NA	2
Reactor Drain Pumps	NNS [34]	I	NA	2
Holdup Pumps	NNS	NS	NA	3

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
CVCS (Cont'd.)				
Reactor Drain Tank	NNS	NS	RC	2
Holdup Tank	NNS	NS	YA	2
Equipment Drain Tank	NNS [34]	I	NA	2
Reactor Makeup Water Tank	NNS	NS	YA	2
Gas Stripper	NNS [34]	I	NA	2
Purification Filters	NNS [34]	I	NA	2
Reactor Drain Filter	NNS [34]	I	NA	2
Seal Injection Filters	NNS [34]	I	NA	2
Reactor Makeup Water Filter	NNS	NS	NA	2
Boric Acid Filter	NNS [34]	I	NA	2
Letdown Strainer	NNS [34]	I	NA	2
Pre-holdup Strainer	NNS [34]	I	NA	2
Boric Acid Condensate IX Strainer	NNS	NS	NA	3
Ion Exchanger Drain Header Strainer	NNS	NS	NA	3
Boric Acid Batching Strainer	NNS	NS	NA	3
Chemical Addition Strainer	NNS	NS	NA	3
Boric Acid Storage Tank [33]	NNS [34]	I	YA	2
Boric Acid Batching Eductor	NNS	NS	NA	2
Letdown Orifices	2	I	RC	1
Piping [27]	1/2/3/NNS [35]	I/NS	RC/NA/YA	1/2
Valves [27]	1/2/3/NNS [35]	I/NS	RC/NA/YA	1/2
Emergency Feedwater System				
Cavitating Venturi	2	I	RC	1
Motor-Driven Emergency Feedwater Pumps	3	I	RB	1
Steam-Driven Emergency Feedwater Pumps	3	I	RB	1
Emergency Feedwater Pump Turbines	3	I	RB	1
Emergency Feedwater Storage Tanks	3	I	NA	1
Piping [27]	2/3	I	NA/RB/RC	1
Valves [27]	2/3	I	NA/RB/RC	1
Fuel Handling System				
Refueling Machine	NNS	II	RC	2
Fuel Transfer System	NNS	II	RC/NA	2
1. Transfer Carriage	NNS	II	RC/NA	2
2. Upending Machine	NNS	II	RC/NA	2
3. Hydraulic Power Unit	NNS	II	RC/NA	2
Fuel Transfer Tube, Valve, Stand	NNS	II	RC/NA	2
CEA Change Platform	NNS	II	RC	2
Fuel Handling System (Cont'd.)				
Long and Short Fuel Handling Tools	NNS	NS	RC/NA	3
Upper Guide Structure Lifting Rig	NNS	II [11]	RC	2

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Core Barrel Lifting Rig	NNS	II [11]	RC	2
Spent Fuel Handling Machine	NNS	II	NA	2
New Fuel Elevator	NNS	II	NA	2
Underwater Television	NNS	NS	RC/NA	3
Refueling Pool Seal	NNS	NS	RC	2
In-Core Instrumentation and CEA Cutter	NNS	NS	RC	3
Extension Shaft Uncoupling Tool	NNS	NS	RC	3
Fuel Transfer Tube Quick Closure	2	I	RC	2
CEA Handling Tools	NNS	NS	RC	3
ICI Insertion and Removal Tools	NNS	NS	RC	3
Spent Fuel Racks	3	I	NA	1
New Fuel Racks	3	I	NA	1
Condensate and Feedwater System				
Condensate Pumps	NNS	NS	TB	2
Feedwater Pumps	NNS	NS	TB	2
Feedwater Pump Controllers	NNS	NS	TB	2
Feedwater Booster Pumps	NNS	NS	TB	2
Startup Feedwater Pump	NNS	NS	TB	2
Low Pressure Feedwater Heaters	NNS	NS	TB	2
High Pressure Feedwater Heaters	NNS	NS	TB	2
Deaerator	NNS	NS	TB	2
Piping (13)	2/NNS	I/NS	TB/NA/RC/MS	1/2/3
Valves (13)	2/NNS	I/NS	TB/NA/RC/MS	1/2/3
Main Condenser System				
Main Condenser	NNS	NS	TB	2
Condensate Storage System				
Condensate Storage Tanks	NNS	NS	YA	2
Condensate Storage Tank Recycle Pumps	NNS	NS	SB	2
Piping	NNS	NS	YA/SB/TB	2/3
Valves	NNS	NS	YA/SB/TB	2/3
Condensate Cleanup System				
Piping	NNS	NS	TB	2/3
Polishers/Demineralizers	NNS	NS	TB	2
Resin Traps	NNS	NS	TB	2
Valves	NNS	NS	TB	2/3
Main Condenser Evacuation System				
Vacuum Pumps	NNS	NS	TB	2
Piping	NNS	NS	TB	2/3
Valves	NNS	NS	TB	2/3

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Demineralized Water MakeupSystem (DWMS)				
Demineralizer Makeup Water Pumps				
Demineralizers	NNS	NS	SB	3
Vacuum Degasifier	NNS	NS	SB	3
Demineralized Water Storage Tank	NNS	NS	SB	3
Vacuum Pumps	NNS	NS	YA	3
Demineralizer Recycle Pump	NNS	NS	SB	3
Vacuum Degasifier Transfer Pumps	NNS	NS	SB	3
Demineralized Water Transfer Pumps	NNS	NS	SB	3
Regenerant Waste Neutralization Tank	NNS	NS	SB	3
	NNS	NS	SB	3
DWMS (Cont'd.)				
Piping [27]	2/NNS	I/NS	All	1/3
Valves [27]	2/NNS	I/NS	All	1/3
Extraction Steam System				
Piping	NNS	NS	TB	2
Valves	NNS	NS	TB	2
Heater Vents				
Piping	NNS	NS	TB	2
Valves	NNS	NS	TB	2
Turbine Generator System				
Turbine Generator				
High Pressure Turbine	NNS	NS	TB	2
Low Pressure Turbines	NNS	NS	TB	2
Generator	NNS	NS	TB	2
Moisture Separators	NNS	NS	TB	2
Steam Reheaters	NNS	NS	TB	2
Stop Valves	NNS	NS	TB	2
Control Valves	NNS	NS	TB	2
Reheat Stop Valves	NNS	NS	TB	2
Intercept Valves	NNS	NS	TB	2
Valves, other	NNS	NS	TB	2/3
Piping	NNS	NS	TB	2/3
Turbine Bypass System				
Turbine Bypass Valves	NNS	NS	TB	2
Valves, other	NNS	NS	TB	2
Piping	NNS	NS	TB	2
Turbine Gland Sealing System				
Gland Seal Condenser	NNS	NS	TB	2
Gland Seal Regulator	NNS	NS	TB	2
Piping	NNS	NS	TB	2

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Turbine Gland Sealing System (Cont'd)				
Valves	NNS	NS	TB	2
Turbine Lube Oil System				
Pumps	NNS	NS	TB	2
Oil Tank	NNS	NS	TB	2
Oil Turbine	NNS	NS	TB	2
Oil Coolers	NNS	NS	TB	2
Oil Filters	NNS	NS	TB	2
Piping	NNS	NS	TB	2/3
Valves	NNS	NS	TB	2/3
Turbine Control System				
EHC Pumps	NNS	NS	TB	2
EHC Coolers	NNS	NS	TB	2
EHC Sumps	NNS	NS	TB	2
Turbine Control System (Cont'd.)				
Piping	NNS	NS	TB	2
Valves	NNS	NS	TB	2
Turbine Generator Cooling System				
Hydrogen Coolers	NNS	NS	TB	2
Piping	NNS	NS	TB	2
Valves	NNS	NS	TB	2
Liquid Waste Management System				
Waste Collection Tanks	NNS	NS	RW	2
Waste Sample Tanks	NNS	NS	RW	2
Process Pumps	NNS	NS	RW	2
Process Demineralizers	NNS	NS	RW	2
Process Filters	NNS	NS	RW	2
Piping [27]	2/NNS	I/NS	TB/NA/RW RC/RB	1/2
Valves [27]	2/NNS	I/NS	TB/NA/RW RC/RB	1/2
Gaseous Waste Management System				
Gas Coolers/Condenser	NNS	NS	NA	2
Guard/Charcoal Beds	NNS	NS	NA	2
Piping [27]	2/NNS	I/NS	NA/RC	1/2
Valves [27]	2/NNS	I/NS	NA/RC	1/2
Solid Waste Management System				
Spent Resin Transfer Pumps	NNS	NS	NA/RW	2
Spent Resin Tanks	NNS	NS	NA/RW	2
HIC Fill/Dewatering Head	NNS	NS	RW	2

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Resin Forwarding Pumps	NNS	NS	RW	2
Dry Solids Compactor	NNS	NS	RW	2
Piping	NNS	NS	NA/RW	2
Valves	NNS	NS	NA/RW	2
Heater Drain System				
Reheater Drain Tanks	NNS	NS	TB	2
Moisture Separator Drain Tanks	NNS	NS	TB	2
Heater Drain Tank	NNS	NS	TB	2
Heater Drain Pumps	NNS	NS	TB	2
Piping	NNS	NS	TB	2/3
Valves	NNS	NS	TB	2/3
Process and Effluent Radiation Monitoring System (PERMS)				
Gaseous Process and Effluent Monitors	NNS			
Unit Vent	NNS	NS	NA	2
Waste Gas	NNS	NS	RW	2
Unit Vent Post-Accident	NNS	NS	NA	2
Containment Purge Exhaust	NNS	NS	NA	2
Condenser Air Ejector		NS	TB	2
Liquid Process and Effluent Monitors				
Component Cooling Water				
Liquid Waste Discharge	NNS	NS	NA	2
Plant Discharge Line	NNS	NS	RW	2
Station Service Water	NNS	NS	RW	2
Reactor Coolant Gross Activity	NNS	NS	CX	2
Turbine Building Drains	NNS	NS	NA	2
Steam Generator Blowdown	NNS	NS	TB	2
	NNS	NS	TB	2
Airborne Radiation Monitors				
Containment Atmosphere	3	I	NA	1
Nuclear Annex	NNS	NS	NA	2
Radwaste Building	NNS	NS	RW	2
Fuel Building	NNS	NS	NA	2
Ventilation Systems Multisampler	NNS	NS	NA	2
Control Room Intake (A&B)	3	I	NA	1
Reactor Building Annulus	NNS	NS	NA	2
Subsphere Ventilation	NNS	NS	NA	2
Area Radiation Monitors	NNS	NS	RC/NA/RW	2
Special Purpose Area Monitors				
Main Steam Line	NNS	NS	NA	2

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Purification Filter	NNS	NS	NA	2
Containment Area High Radiation	3	I	RC	1
Primary Coolant	3	I	RC	1
Containment Isolation System				
Piping	2	I	RC/RB	1
Valves	2	I	RC/RB	1
Component Cooling Water System [14]				
Heat Exchangers				
Pumps	3	I	CX	1
Surge Tanks	3	I	NA	1
Sump Pumps	3	I	NA	1
Chemical Addition Tank	NNS	NS	NA	3
Heat Exchanger Building Sump Pumps	NNS	NS	NA	3
Piping [27]	NNS	NS	CX	3
	2/3/NNS	I/NS	CX/YA/NA RB/RC	1/2/3
Valves	2/3/NNS	I/NS	CX/YA/NA RB/RC	1/2/3
Spent Fuel Pool Cooling System				
Pumps	3	I	NA	1
Exchangers	3	I	NA	1
Piping	3/NNS	I/NS	NA	1/3
Valves	3/NNS	I/NS	NA	1/3
Pool Purification System				
Pumps	NNS	NS	NA	2
Strainers	NNS	NS	NA	3
Demineralizers	NNS	NS	NA	2
Filters	NNS	NS	NA	2
Skimmer	NNS	NS	NA	3
Piping [27]	2/3/NNS	I/NS	NA/RC	1/2
Valves [27]	2/3/NNS	I/NS	NA/RC	1/2
Primary Sampling System				
Pump	NNS	NS	NA	2
Heat Exchangers	NNS	NS	NA	2
Sample Vessels	NNS	NS	NA	2
Piping [27]	2/3/NNS	I/NS	NA/RC	1/2
Valves [27]	2/3/NNS	I/NS	NA/RC	1/2
Sink	NNS	NS	NA	3
Boronometer	NNS	NS	NA	2
Process Radiation Monitor	NNS	NS	NA	2

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Secondary Chemistry Control Sampling System				
Heat Exchangers	NNS	NS	NA	2/3
Strainers	NNS	NS	NA	2/3
Monitors	NNS	NS	NA	2/3
Piping [27]	2/NNS	I/NS	NA/RC	1/3
Valves [27]	2/NNS	I/NS	NA/RC	1/3
Station Service Water System				
Pumps	3	I	SP	1
Strainers	3	I	SP	1
Sump Pumps	NNS	NS	SP	3
Traveling Screens	3	I	YA	1
Piping	3/NNS	I/NS	SP/CX	1/3
Valves	3/NNS	I/NS	SP/CX	1/3
Turbine Building Service Water System				
Piping				
Valves	NNS	NS	YA	2/3
Pumps	NNS	NS	YA	2/3
Strainers	NNS	NS	YA	2
	NNS	NS	YA	2
Turbine Building Cooling Water System				
Piping	NNS	NS	TB/YA	2/3
Valves	NNS	NS	TB/YA	2/3
Heat Exchangers	NNS	NS	YA	2/3
Pumps	NNS	NS	TB	2/3
Surge Tank	NNS	NS	TB	2/3
Chemical Addition Tank	NNS	NS	TB	3
Essential Chilled Water System				
Refrigeration Units	3	I	NA	1
Pumps	3	I	NA	1
Compression Tanks	3	I	NA	1
Chemical Addition Tanks	NNS	NS	NA	3
Essential/Normal Heat Exchangers	3/NNS [1]	I	NA	1/2
Piping [27]	2/3/NNS	I/NS	NA/RC/RB	1/2/3
Valves [27]	2/3/NNS	I/NS	NA/RC/RB	1/2/3
Strainers	3/NNS	I/NS	NA	1/3
Normal Chilled Water System [15]				
Refrigeration Units	NNS	NS	NA	2
Pumps	NNS	NS	NA	2
Compression Tanks	NNS	NS	NA	3
Air Separators	NNS	NS	NA	3
Chemical Addition Tanks	NNS	NS	NA	3

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Piping [27]	2/NNS	I/NS	NA/RC	1/3
Valves [27]	2/NNS	I/NS	NA/RC	1/3
Strainers	NNS	NS	NA	3
Condenser Circulating Water System				
Pumps	NNS	NS	YA	2
Cooling Towers (mechanical portion)	NNS	NS	YA	2
Piping	NNS	NS	YA/TB	2/3
Valves	NNS	NS	YA/TB	2/3
Strainers	NNS	NS	YA/TB	2
Traveling Screens	NNS	NS	YA	2
Instrument Air System				
Air Compressors	NNS	NS	NA	2
Piping [27]	2/NNS	I/NS	All	1/3
Valves [27]	2/NNS	I/NS	All	1/3
Air Receivers	NNS	NS	NA	3
Desiccant Air Dryers/Filters	NNS	NS	NA	2
Station Air System				
Air Compressors	NNS	NS	SB	3
Air Dryers/Filters	NNS	NS	SB	3
Air Receivers	NNS	NS	SB	3
Piping [27]	2/NNS	I/NS	All	1/3
Valves [27]	2/NNS	I/NS	All	1/3
Breathing Air System				
Air Compressors	NNS	NS	SB	3
Piping [27]	2/NNS	I/NS	All	1/3
Valves [27]	2/NNS	I/NS	All	1/3
Air Receivers	NNS	NS	SB	3
Air Dryer/Filters	NNS	NS	SB	3
Compressed Gas Systems				
High Pressure Gas Cylinders	NNS	NS	YA	3
Pressure Regulators	NNS	NS	YA	3
Leak Detection Systems	NNS	NS	All	3
Liquid Nitrogen Evaporators	NNS	NS	YA	3
Piping [26, 27]	2/NNS	I/NS	All	1/3
Valves [27]	2/NNS	I/NS	All	1/3
Fire Protection System				
Jockey Pump	NNS	NS	FP	2
Backup Storage Tank	NNS	I	NA	1
Fire Pumps	NNS	NS	FP	2
Backup Fire Pump	NNS	I	NA	1
Storage Tanks	NNS	NS	FB	2

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Water Spray Systems (Deluge and Sprinkler) Piping, Valves [16, 27]	2/NNS	I/II/NS	TB/NA/RC/RB/ DG/SB	1/2
Hose Systems/Standpipes [16, 27]	2/NNS	I/NS	All	1/2
Portable Fire Extinguishers [16]	NNS	NS	All	2
Exterior Distribution System				
Piping	NNS	NS	YA	2
Valves	NNS	NS	YA	2
Strainers	NNS	NS	YA	2
Alternate AC Source/Combustion Turbine-Generator	NNS	NS	YA	2
DG Engine Fuel Oil System [17]				
Fuel Oil Storage Tanks	3	I	DF	1
Recirculation Pumps	NNS	NS	DF	3
Booster Pumps	3	I	DG	1
Fuel Oil Day Tanks	3	I	DG	1
DG Engine Fuel Oil System [17]				
Fuel Oil Transfer Pumps	3	I	DG	1
Strainers	3/NNS	I/NS	DG/YA	1/3
Filters	3/NNS	I/NS	DG	1/3
Piping	3/NNS	I/NS	DG/DF/YA	1/3
Valves	3/NNS	I/NS	DG/DF	1/3
DG Engine Cooling Water System				
Circulation Pumps	3	I	DG	1
Keep Warm Pumps	3	I	DG	1
Jacket Water Coolers	3	I	DG	1
Jacket Water Standpipes	3	I	DG	1
Chemical Pot Feeders	3	I	DG	1
Piping	3	I	DG	1
Valves	3	I	DG	1
DG Engine Starting Air System [18]				
Compressors	NNS	NS	DG	2
Aftercoolers	NNS	NS	DG	3
Moisture Separators	NNS	NS	DG	3
Filter/Dryer Units	NNS	NS	DG	3
Air Receivers	3	I	DG	1
Strainers	3/NNS	I/NS	DG	1/3
Traps	NNS	NS	DG	3
Filters	3/NNS	I/NS	DG	1/3
Piping	3/NNS	I/NS	DG	1/3
Valves	3/NNS	I/NS	DG	1/3
DG Engine Lube Oil System [19]				

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Lube Oil Sump Tanks	3	I	DG	1
Lube Oil Coolers	3	I	DG	1
Oil Transfer Pumps	NNS	NS	DG/YA	3
Prelube Oil Pumps	3	I	DG	1
Clean and Used Lube Oil Storage Tanks	NNS	NS	YA	3
Filters	3	I	DG	1
Strainers	3/NNS	I/NS	DG	1/3
Piping	3/NNS	I/NS	DG/YA	1/3
Valves	3/NNS	I/NS	DG/YA	1/3
DG Engine Air Intake and Exhaust System				
Turbochargers	3	I	DG	1
Aftercoolers	3	I	DG	1
Silencers and Air Filters	3	I	DG	1
Piping	3	I	DG	1
Equipment and Floor Drainage System				
Reactor Building Subsphere Sump Pumps	3	I	RB	1
Other Sump Pumps				
Piping [27]	NNS	NS		3
Valves [27]	2/3/NNS	I/NS	All	1/3
	2/3/NNS	I/NS	All	1/3
Diesel Generator Building Sump Pump System				
Sump Pumps	3	I	DG	1
Piping	3/NNS	I/NS	DG/NA/RW	1/3
Valves	3/NNS	I/NS	DG/NA/RW	1/3
Control Complex Ventilation System				
Main Control Room Air Conditioning System				
Air Conditioning Units w/Filters	3	I	NA	1
Fans, Ductwork [31]	3/NNS	I/II	NA	1/2
Water-cooling Coils	3	I	NA	1
Heating Coils	3	I	NA	1
Dampers	3	I	NA	1
Technical Support Center Air Conditioning System				
Air Conditioning Units w/Filters	NNS	II	NA	2
Fans, Ductwork	NNS	II	NA	2
Dampers	NNS	II	NA	2

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Computer Room Air Conditioning System				
Air Conditioning Units w/Filters	NNS	II	NA	2
Fans, Ductwork	NNS	II	NA	2
Dampers	NNS	II	NA	2
Essential Electrical Rooms and Vital Instrumentation and Equipment Rooms (inc. Battery Rooms)				
Air Conditioning Units w/Filters	3	I	NA	1
Fans, Ductwork	3	I	NA	1
Dampers	3	I	NA	1
Balance of Building Air Conditioning System				
Filters	NNS	NS	NA	3
Water Cooling Coils	NNS	NS	NA	3
Fans, Ductwork	NNS	NS	NA	3
Dampers	NNS	NS	NA	3
Fuel Building Ventilation System				
Cooling Coil	NNS	NS	NA	3
Heating Coil, Supply	NNS	NS	NA	3
Air Handling Unit w/Filter	NNS	II	NA	2
Ductwork, Supply	NNS	II	NA	2
Exhaust System Filter Train	3	I	NA	1
Exhaust System Fans	3	I	NA	1
Exhaust System Dampers	3	I	NA	1
Ductwork, Exhaust	3	I	NA	1
Dampers, Supply	NNS	II	NA	2
Nuclear Annex Ventilation System [20]				
Supply Units				
Ductwork, Supply	NNS	II	NA	2
Cooling Coils	NNS	II	NA	2
Particulate Exhaust Filter Units	NNS	II	NA	3
Fans, Ductwork	NNS	II	NA	2
Dampers	NNS	II	NA	2
	NNS	II	NA	2
Radwaste Building Ventilation System				
Supply Air Handling Units				
Cooling Coils	NNS	NS	RW	2
Exhaust Filter Units	NNS	NS	RW	3
Fans	NNS	NS	RW	2

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Ductwork	NNS	NS	RW	2
Dampers	NNS	NS	RW/NA	2
	NNS	NS	RW	2
Reactor Building Subsphere Ventilation System				
Individual Cooling Units	3/NNS	I/II	RB	1/2
Exhaust Fans	3	I	NA	1
Cooling Coils and Heating Coils	3	I	NA	1
Exhaust System Filter Train	3	I	NA	1
Ductwork, Exhaust	3	I	NA/RB	1
Supply Fans	NNS	II	NA	2
Supply Air Handling Units	NNS	II	NA	2
Ductwork, Supply	NNS	II	NA/RB	2
Dampers, Exhaust	3	I	NA	1
Dampers, Supply	NNS	II	NA	2
Diesel Building Ventilation System				
Space Heater	3	I	DG	1
Emergency/Normal Fans	3/NNS	I/II	DG	1/2
Ductwork	3/NNS	I/II	DG	1/2
Dampers	3/NNS	I/II	DG	1/2
Filter, Normal Supply	NNS	NS	DG	2
Annulus Ventilation System				
Filter Trains	3	I	NA	1
Fans	3	I	NA	1
Dampers	3	I	NA	1
Ductwork	3	I	NA/RB	1
Containment Purge Ventilation System				
Water Cooling Coil				
Heating Coil	NNS	NS	NA	3
Supply and Exhaust Fans	NNS	NS	NA	3
Valves [27]	NNS	II	NA	2
Filter Trains	2/NNS	I/II	NA/RC	1/2
Ductwork [27, 30]	NNS [28]	II	NA	2
	2/NNS	I/II	NA/RC	1/2
Containment Cooling and Ventilation System				
Containment Cooling Subsystem	NNS	II	RC	2
Control Element Drive Mechanism Cooling Subsystem	NNS	II	RC	2
Containment Air Cleanup System	NNS	II	RC	2
Cavity Cooling Subsystem	NNS	II	RC	2
Ductwork	NNS	II	RC	2

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Dampers	NNS	II	RC	2
Turbine Building Ventilation System				
Fans	NNS	NS	TB	3
Dampers	NNS	NS	TB	3
Exhausters	NNS	NS	TB	3
Ductwork	NNS	NS	TB	3
Station Service Water Pump Structure Ventilation System				
Fans	3	I	SP	1
Dampers	3	I	SP	1
Ductwork	3	I	SP	1
Component Cooling Water Heat Exchanger Structure(s) Ventilation Systems				
Fans	NNS	II	CX	3
Dampers	NNS	II	CX	3
Space Heaters	NNS	II	CX	3
Ductwork	NNS	II	CX	3
Instrumentation and Control Systems (Cont'd.)				
Reactor Protective System (RPS) That portion of the PPS which generates signals that actuate reactor trip	3	I	NA/RC	1
Engineered Safety Features Actuation System (ESF) That portion of the PPS which generates signals that actuate engineered safety features	3	I	NA/RC	1
Safe Shutdown Systems The safe shutdown systems include those systems required to secure and maintain the reactor in a safe shutdown condition	3	I	DG/NA/CX SP/MS/ RB/RC	1
All other systems required for safety	3	I	NA/DG/CX SP/MS/ RB/RC	1
Equipment required to comply with 10CFR50.62	NNS	2	NA/RC	2
Equipment specified in Section 3.3.1.4 of ANSI/ANS-51.1	NNS	NS	All	2/3

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Control systems not required for safety	NNS	NS	All	2/3
Control Room Panels (safety-related)	3	I	NA	1
Control Room Panels (other)	NNS	II	NA	1
Instrument Valves and Piping Downstream of Safety Class 2 or 3 Root Valves (For Safety-Related Instruments)				
Piping, tubing, and fittings	2/3	I	All	1
Instrument valves	NNS	NS	All	3
Electric Systems				
Class 1E AC Equipment (includes associated transformers, protective relays, instrumentation and control devices:				
4.16 kV Buses	3	I	NA	1
480V Load Centers	3	I	NA	1
480V Motor Control Centers	3	I	NA/CX/DG/SP	
Class 1E DC Equipment:				
125V Station Batteries and Racks	3	I	NA	1
Electric Systems (Cont'd.)				
Battery Chargers	3	I	NA	1
125V Switchgear and Distribution Panels	3	I	NA	1
120V Vital AC System Equipment Inverters	3	I	NA	1
120V Distribution Panels	3	I	NA	1
Electrical Cables for Class 1E Systems				
125V DC Cables (including cable splices, connectors, and terminal blocks)	3	I	NA	1
5 kV Power Cables (including cable splices, connectors, and terminal blocks)	3	I	NA/DG/CX/ SP	1
600V Power Cables (including cable splices, connectors, and terminal blocks)	3	I	NA/DG/CX/ SP/MS/ RB/RC	
Control and Instrumentation Cables (including cable splices, connectors, and terminal blocks)	3	I	DG/CX/NA SP/MS/RB	1
Conduit and cable trays and their supports containing Class 1E cables and those whose failure	3	I	DG/CX/NA/ SP/MS/RB	1

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
during a seismic event may damage other safety-related items			RC	
Miscellaneous Class 1E Electrical Systems				
Containment building electrical penetration assemblies	3	I	RC	1
Non-Class 1E Electrical Systems	NNS	II/NS	All	2/3
Instrumentation and Display Systems not required for safety [32]	NNS	NS	All	2/3
Reactor Building Structure				
Containment Shield Building				
Steel Containment Vessel	3	I	RB	1
Internal Structure	2	I	RB	1
Equipment Hatch	3	I	RC	1
Personnel Airlocks	2	I	RC	1
Subsphere (Including Containment Support Dish)	2	I	RC	1
	3	I	RB	1
Nuclear Annex Structure				
Control Area	3	I	NA	1
EFW Tank/Main Steam Valve House Area	3	I	NA	1
Emergency Diesel Generator Areas	3	I	NA	1
CVCS/Maintenance Area	3	I	NA	1
Fuel Handling Area	3	II	NA	1
Other Structures				
Unit Vent	NNS	II	NA/RB	2
Turbine Building	NNS	II	TB	2
Radwaste Building [28]	NNS	I	RW	2
Station Service Water Pump/Intake Structure	3	I	SP	1
Component Cooling Water Heat Exchanger Structures and Pipe Tunnels	3	I	CX/YD	1
Diesel Fuel Storage Structure	3	I	DF	1
Station Services Building/Auxiliary Boiler Structure	NNS	NS	SB	3
Administration Building	NNS	NS	ADB	3
Warehouse	NNS	NS	WH	3
Fire Pump House	NNS	NS	FP	3
Alternate AC Source/Combustion Turbine-Generator Structure and Fuel	NNS	NS	YA	2

Appendix E
List of Systems, Structures and Components for a Typical Plant

Component Identification	Safety Class	Seismic Category	Location[25]*	Quality Class[29]*
Tank				
Dikes				
Dike (Holdup, Boric Acid Storage and Reactor Makeup Water Tanks) [28]	NNS	II	YA	2
Dike (Condensate Storage Tank) [28]	NNS	II	YA	2
Cranes				
Polar Crane	NNS	II	RC	2
Cask Handling Hoist	NNS	II	NA	2
New Fuel Handling Hoist	NNS	II	NA	2
Component Supports [23]	1/2/3/NNS	I/NS	All	1/2/3

Notes:

[1] Two safety classes are used for heat exchangers to distinguish primary and secondary sides where they are different.

[2] Loss of cooling water and/or seal water service to the reactor coolant pumps (RCPs) may require stopping the pumps. However, the continuous operation of the pumps is not required during or following an SSE. The auxiliaries are therefore not necessarily Safety Class 3 or Seismic Category I. Provision for cooling water to the pump bearing oil cooler and pump motor air cooler will not comply with the requirements of Regulatory Guide 1.29 (see Section 5.4.1.3).

[3] Only those structural portions of the RCPs which are necessary to assure the integrity of the reactor coolant pressure boundary are Safety Class 1.

[4] Safety class of piping within the reactor coolant pressure boundary (as defined in 10 CFR 50) is selected in accordance with the ANSI/ANS 51.1 criteria identified in Section 3.2.2. For purposes of CESSAR, Safety Class 1, 2, 3, and NNS of ANSI/ANS 51.1 are equivalent to Quality Groups A, B, C, and D of Regulatory Guide 1.26.

[5] Flow restricting orifices are provided in the nozzles for RCS sampling lines, pressurizer level and pressure instruments, RCP differential pressure instrument lines, SIS pressure instrument lines, RCP seal pressure instrument lines, the charging line differential pressure instrument line, and the SIS hot leg injection pressure instrument lines, to limit flow in the event of a break downstream of the nozzle. The orifice size, 7/32-inch diameter and 1-inch long, precludes exceeding fuel design limits while utilizing minimum makeup rates. This permits an orderly shutdown in the event of a downstream break in accordance with General Design Criterion 33 (see Section 3.1.29). A reduction may, therefore, be made in the safety classification of lines downstream of the orifice.

[6] The pressure boundary housing for this component is a reactor vessel appurtenance and is Safety Class 1 and Seismic Category I, as described in Section 3.9.4.3.

[7] Core support structures and internals structures are designed to the criteria described in Section 3.9.5.4.

[8] CEA and fuel assemblies are designed to the criteria described in Section 4.2.

[9] Reactor coolant pump auxiliary components required for lubrication and cooling of pump seals and thrust bearings are not subject to the quality assurance requirements of 10CFR50, Appendix B.

[10] Except Lifting Frame Assembly, which is NS.

[11] During normal plant operation only.

[12] Safety Class 1 for pressure boundary; Safety Class 3 for electrical portion of system.

[13] The piping, valves, and associated supports/restraints of the Main Feedwater System from (and including) the Main Feedwater Isolation Valves to the steam generator feed nozzles are Safety Class 2, Seismic Category I, and Quality Class 1; the remainder is Safety Class NNS.

[14] Non-safety Cooling Headers are Safety Class NNS, Seismic Category II, Quality Class 2.

[15] The Normal Chilled Water System serves no safety function. Portions of the system, which are located in non-safety related areas, are classed as non-seismic.

[16] Portions of the Fire Protection System piping, valves, and extinguishers which are not in safety-related areas of the plant are designed as non-seismic.

[17] Fuel Oil Recirculation System and storage tank fill line strainer are Safety Class NNS.

[18] The Starting Air System is Safety Class NNS from the starting air compressor through the desiccant drying towers, and Safety Class 3 from the starting air receiver tank inlet check valve to the engine connections.

[19] The Clean and Used Oil Transfer System is Safety Class NNS.

[20] Mechanical Equipment Room cooling components are Safety Class 3, Seismic Category I, and Quality Class 1.

[21] The piping, valves, and associated supports/restraints of the Main Steam System from each steam generator to (and including) the Main Steam Isolation Valves are Safety Class 2, Seismic Category I, and Quality Class 1; the remainder is Safety Class NNS.

[22] Piping is Safety Class 2 from the Steam Generators through the Containment Isolation Valves.

[23] Component supports are designed to the criteria described in Section 3.9.3.4.

[24] Safety Injection drain and vent piping is Safety Class NNS, Seismic Category NS and Quality Class 3.

[25] Locations:

CX	=	Component Cooling Water Heat Exchanger Structure
DG	=	Emergency Diesel Generator Area
FP	=	Fire Pump House
MS	=	Main Steam Valve House Area
RW	=	Radwaste Building
RB	=	Reactor Building
RC	=	Steel Containment

SP	=	Station Service Water Pump Structure
SB	=	Station Services Building
TB	=	Turbine Building
NA	=	Nuclear Annex
YA	=	Yard
SI	=	Station Service Water Intake Structure
DF	=	Diesel Fuel Storage Structures
ALL	=	Throughout Plant

[26] Hydrogen lines in safety-related areas are either designed to Seismic Category I requirements, or sleeved with the outer pipe vented to the outside, or equipped with excess flow check valves so that in case of a line break, the hydrogen concentration in the affected area will not exceed 2%.

[27] Containment isolation valves and containment penetration piping are Safety Class 2, Seismic Category I, and Quality Class 1.

[28] The foundations/dikes enclosures of these structures are designed such that if a Safe Shutdown Earthquake (SSE) occurs, the majority of the liquid inventory expected to be in the building/tank will be contained. It is assumed that the concrete would develop cracks and some liquid would be released. This event is bounded by the analysis in Section 15.7.3.

[29] The QA program provides a graded approach to the assurance of quality of work performed by and for WENS by the use of quality class designations to describe the various levels of controls as follows:

1) QC-1 is the highest level quality class and embodies all necessary controls for items and/or services which are required to meet 10 CFR 50 Appendix B requirements.

2) QC-2 is an intermediate level quality class which is used for items or services which require a moderate level of control of activities affecting quality, but which are neither Nuclear Safety-Related nor required to meet the requirements of 10 CFR 50 Appendix B. Circumstances appropriate for QC-2 designation include non-standard, complex items, or those which must perform reliably, in a harsh environment or with less than normal operator attention or maintenance.

3) QC-3 is the quality class which applies to all items or services which are not assigned to another quality class. Quality requirements may be specified in quality plans, procurement documents and/or special procedures if deemed necessary.

[30] The containment low and high purge exhaust ductwork up to the HEPA filters is Seismic Category I.

[31] Smoke fan is Safety Class NNS, Seismic Category II, and Quality Class 2.

[32] The ALMS is Quality Class 2. The ALMS pressurizer safety valve discharge sensors and signal processing equipment are Seismic Category I. All of the remaining NIMS components are qualified to remain operable following seismic events which do not require plant shutdown.

33] The boric acid storage tank is classified Seismic Category I but is not designed for tornado wind and wind pressures or tornado generated missiles because it is not required for safe shutdown or accident mitigation.

[34] These CVCS components will be constructed in accordance with ASME Boiler and Pressure Vessel

Code, Section III, Class 3.

[35] Some CVCS piping and valves designated Safety Class NNS will be constructed in accordance with ASME Boiler and Pressure Vessel Code Section III, Class 3, as shown on Figure 9.3.4-1. Piping and valves in this category are Seismic Category I, and Quality Class 2.