
Vital Equipment/Area Guidelines Study: Vital Area Committee Report

Final Report

**U.S. Nuclear Regulatory
Commission**

Office of Nuclear Reactor Regulation



NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W.;
Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082,
Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Information Support Services, Distribution Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

Vital Equipment/Area Guidelines Study: Vital Area Committee Report

Final Report

Manuscript Completed: March 1986
Date Published: February 1988

Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555



ABSTRACT

A study was conducted by the staff to (1) re-evaluate the guidelines and bases used to determine what are the vital equipment and areas to be protected against radiological sabotage in nuclear power plants and (2) to recommend revised guidance. On the basis of this study, the staff has recommended a revised vital equipment/area protection philosophy: to protect as vital the reactor coolant pressure boundary and one train of equipment that would provide the capability to achieve and maintain hot shutdown. To implement this overall protection philosophy, the staff also has recommended new analysis assumptions or guidelines to identify the specific equipment and areas in each plant that require protection as "vital".

CONTENTS

| | <u>Page</u> |
|--|-------------|
| *ABSTRACT | iii |
| *FOREWORD | vii |
| EXECUTIVE SUMMARY | ix |
| *MEMORANDUM TRANSMITTING VITAL AREA COMMITTEE FINAL REPORT | xi |
| 1. INTRODUCTION | 1-1 |
| 2. OBJECTIVES | 2-1 |
| 3. BACKGROUND OF LICENSING PRACTICES FOR PHYSICAL PROTECTION OF POWER REACTORS AGAINST SABOTAGE | 3-1 |
| 4. BASIC STUDY PREMISES | 4-1 |
| 5. SCOPE AND METHODOLOGY | 5-1 |
| 6. STUDY RESULTS | 6-1 |
| 6.1 Proposed Vital Equipment/Area Protection Philosophy and Analysis Assumptions | 6-1 |
| 6.2 Impact on Licensed Plants | 6-17 |
| 7. RECOMMENDATION | 7-1 |
| APPENDICES | |
| A EDO Memorandum of May 1, 1985 Establishing the Vital Equipment/Area Guidelines Study | A-1 |
| B Review Guideline 17 and Regulatory Guide 1.29 | B-1 |
| C Action Plan Memorandum of July 1, 1985 | C-1 |
| D Summary of Briefings to Vital Area Committee | D-1 |
| E Current LANL Vital Equipment/Area Analysis Assumptions | E-1 |

*These sections were not included in VAC study transmitted by March 5, 1986 Memorandum, but are being added to that Memorandum in the present publication.

CONTENTS (Continued)

| | <u>Page</u> |
|--|-------------|
| APPENDICES (Continued) | |
| *F (1) Disposition of Comments Received on the Draft Vital Equipment/Area Guidelines Study and (2) Comments Received on the Draft VAC Report | F-1 |
| *G Implementation Considerations for Revised Vital Equipment/Area Guidelines | G-1 |
| *H Proposed Generic Letter of Transmittal for Final VAC Report | H-1 |

*Appendices F, G, and H were not included in VAC study transmitted by March 5, 1986 Memorandum, but were Enclosures 2, 3, and 4, respectively, to that Memorandum.

FOREWORD

On May 1, 1985, the Executive Director for Operations directed the staff to initiate a study to re-evaluate the existing guidelines and bases used to determine what are the vital equipment and areas to be protected against radiological sabotage in nuclear power plants and to recommend revised guidance as necessary. A Vital Area Committee was established to conduct the study. This report documents the study and its results.

Vital Area Committee

Frank J. Miraglia, Chairman
Director, Division of Pressurized Water
Reactor Licensing-B
Office of Nuclear Reactor Regulation

Robert F. Burnett, Member
Director, Division of Safeguards
Office of Nuclear Material Safety and Safeguards

Frank P. Gillespie, Member
Acting Director, Division of Accident Analysis
Office of Nuclear Regulatory Research

James G. Partlow, Member
Director, Division of Inspection Programs
Office of Inspection and Enforcement

EXECUTIVE SUMMARY

This report presents the results of a study (1) to re-evaluate the guidelines and bases used to determine what are the vital equipment and areas to be protected in nuclear power plants and (2) to recommend revised guidance. The study was established by the Executive Director for Operations (EDO) on May 1, 1985, to address questions that had been raised about the validity and consistency of past and current criteria for identifying equipment that must be protected against radiological sabotage, and to consider recent research on this subject.

The EDO designated two staff groups to carry out the study: a Vital Area Committee (VAC) and a Management Policy Review Group (MPRG). The VAC conducted the study, while the MPRG provided broad policy direction and guidance to the VAC and approved its study plans and products. The VAC was chaired by Frank J. Miraglia, NRR; its members included Robert F. Burnett, NMSS; James G. Partlow, IE; and Frank P. Gillespie, RES. The MPRG consisted of Victor Stello, DEDROGR; Harold R. Denton, NRR; and John G. Davis, NMSS.

On the basis of the study, the VAC has recommended a revised vital equipment/area protection philosophy: to protect as vital the reactor coolant pressure boundary and one train of equipment -- with its associated piping, water sources, power supplies, and instrumentation -- that provide the capability to achieve and maintain hot shutdown. To implement this overall protection philosophy, the VAC also has recommended revised analysis assumptions or guidelines, to be applied on a case-by-case basis, to identify the specific equipment and areas in each plant that require protection as "vital". These analysis assumptions are as follows:

- (1) For purposes of protection against radiological sabotage, the primary coolant pressure boundary consists of the reactor vessel and reactor coolant piping up to and including a single, protected, normally closed isolation valve or protected valve capable of closure in interfacing systems.
- (2) Any transient or event that causes significant core damage will result in an attendant 10 CFR 100 release.
- (3) One train of equipment (with the associated piping, water sources, power supplies, controls, and instrumentation) that provides the capability to perform the functions (reactivity control, decay heat removal, and process monitoring) that are necessary to achieve and maintain hot shutdown for a minimum of 8 hours from the time of reactor trip should be protected as vital. In addition, the major components of the reactor coolant makeup system and associated support equipment necessary to achieve this goal should be protected as vital.

- (4) The control room and any remote locations from which vital equipment can be controlled or disabled (such as remote shutdown panels, motor control centers, circuit breakers, or local control stations) should be protected as vital areas.
- (5) Only the power mode of reactor operation and hot standby (for PWRs) need be considered as long as all equipment designated as vital for power operation is maintained as vital in other modes.
- (6) Off-site power is unavailable.
- (7) Random failures do not occur simultaneously with an act of radiological sabotage. However, the saboteur can take advantage of the unavailability of equipment during maintenance. Thus, whenever any components or systems normally protected as vital are inoperable for any period of time, appropriate compensatory measures (such as stationing guards at alternate locations) must be taken to ensure that the capability to reach hot shutdown is maintained.
- (8) Breaks in multiple main steam lines that cannot be isolated lead to 10 CFR 100 releases.
- (9) Cable runs in trays and conduit need not be protected as vital unless cables necessary for safe shutdown capability are individually identifiable and the identification is reasonably accessible. However, cable terminals or junctions and areas such as cable spreading rooms, through which large numbers of cables pass, must be protected.
- (10) Saboteurs may use explosives in amounts that they can carry.
- (11) No credit is given for equipment not located in vital areas.
- (12) Following the start of a refueling outage, the spent fuel pool should be protected as vital long enough to ensure that sabotage to the pool cannot result in a 10 CFR 100 release.
- (13) The backup supporting power supply of the Central Alarm Station (CAS) is essential for continuous operation of CAS in the event of loss of normal power.

The VAC believes that the application of the recommended protection philosophy, with its implementing analysis assumptions, will contribute to the overall program designed to provide a high degree of assurance against radiological sabotage.

MEMORANDUM TRANSMITTING VITAL AREA COMMITTEE FINAL REPORT

On March 5, 1986, the Chairman of the Vital Area Committee (VAC) sent a memorandum (see next page) notifying the recipients that the VAC had completed its study effort and was enclosing its final report. That report, its appendices A through E, and background material (appendices F, G, and H) that accompanied the issuance of March 5, 1986, are now being issued as NUREG-1178.

The March 5th memorandum cites two references:

- (1) Memorandum from William J. Dircks, "Vital Equipment/Area Guidelines Study," dated May 1, 1985, and
- (2) Memorandum from Frank J. Miraglia, "Vital Equipment/Area Guidelines Study Action Plan," dated July 1, 1985.

These are reproduced here as appendices A and C, respectively.

The March 5th memorandum also refers to "Enclosure 1" (the text of this report and appendices A through E), "Enclosure 2" (Appendix F), and "Enclosure 3" (Appendix G). Appendix H contains the proposed generic letter of transmittal for the final VAC report; this was designated as Enclosure 4 to the March 5th memorandum.



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

March 5, 1986

MEMORANDUM FOR: Victor Stello, Jr.
Acting Executive Director
for Operations

Harold R. Denton, Director
Office of Nuclear Reactor Regulation

John G. Davis, Director
Office of Nuclear Material Safety
and Safeguards

FROM: Frank J. Miraglia, Chairman
Vital Area Committee

SUBJECT: VITAL AREA COMMITTEE FINAL REPORT

References: (1) Memorandum from William J. Dircks, "Vital Equipment/
Area Guidelines Study," dated May 1, 1985
(2) Memorandum from Frank J. Miraglia, "Vital Equipment/
Area Guidelines Study Action Plan, dated July 1, 1985

In accordance with references (1) and (2), the Vital Area Committee (VAC) has completed its study effort. The Committee's final report is provided for your review and action as Enclosure 1.

The VAC has considered all the comments received from the cognizant Headquarters Offices and the Regions on the draft report. Enclosure 2 provides those comments and discusses the Committee's disposition of them.

Enclosure 3 discusses the Committee's considerations and recommendations concerning implementation of the revised vital equipment/area guidelines. Finally, Enclosure 4 is a proposed generic letter for transmitting the VAC report to industry.

If you agree with the contents of the report and the supporting documents provided herein, we recommend that you consider providing Enclosures 1 and 2 to the cognizant Headquarters Offices and the Regions for their information prior to issuing the report publicly.

We are available to meet with the MPRG to discuss the report or the other enclosures to this memorandum.


Frank J. Miraglia, Chairman
Vital Area Committee

Enclosures:
As stated

cc: R. Burnett
J. Partlow
F. Gillespie

1. INTRODUCTION

Definitions of vital equipment/areas have been evolving since 1978. The topic has been addressed in several studies done by the staff of the Nuclear Regulatory Commission (NRC), as well as in NRC-sponsored research programs. These studies and recent staff evaluations of physical security plans have raised questions about the validity and consistency of the assumptions and criteria being used to determine vital equipment and areas. For this reason, on May 1, 1985, the Executive Director for Operations (EDO) established a committee (1) to re-evaluate the guidelines and bases used to determine the equipment and areas to be protected as vital and (2) to develop and recommend revised assumptions and guidance.

The EDO designated two staff groups to carry out the study: A Vital Area Committee (VAC) and a Management Policy Review Group (MPRG). The VAC was given responsibility for actual conduct of the study, while the MPRG was to provide broad policy direction and guidance to the VAC and to approve the study plans and products. The VAC was chaired by Frank J. Miraglia, NRR; its members included Robert F. Burnett, NMSS; James G. Partlow, IE; and Frank P. Gillespie, RES. The MPRG was composed of Victor Stello, DEDROGR; Harold R. Denton, NRR; and John G. Davis, NMSS. A copy of the EDO memorandum establishing the study is included as Appendix A to this report.

Section 2 below gives the objectives of the study. Section 3 traces the evolution of vital equipment-related regulations, guidance, and practice. Section 4 gives the justification for the assumptions used by the VAC in evaluating the specific vital equipment assumptions, Section 5 discusses the scope and methodology of the study, and the study results are detailed in Section 6. Recommendations are given in Section 7. The appendices provide additional background material.

2. OBJECTIVES

The objectives of the study were (1) to perform a structured evaluation of existing and proposed vital equipment/area assumptions, criteria, and guidance and (2) to develop a comprehensive and consistent set of recommended assumptions for determining equipment and areas to be designated as vital in nuclear power plants. Both the assumptions and the rationale supporting them were evaluated individually and collectively for completeness and technical adequacy.

Based on this evaluation, the principal objective of the Vital Area Committee was to develop and recommend revised assumptions and guidance, with rationale and justification for the revisions. The assumptions and guidance were to satisfy the following criteria:

- (1) Consider all conditions of normal operation, anticipated operational occurrences, transients, and accidents of the types presently considered in the design-basis analysis of nuclear power plants; consider outage conditions and activities to the extent that loss of operational functions and capabilities during outages impacts vital equipment and areas.
- (2) Be readily and uniformly applicable by safety/safeguards analysts in identifying vital equipment and areas on a case-by-case basis.
- (3) Have the concurrence of all cognizant NRC Offices.

3. BACKGROUND OF LICENSING PRACTICES FOR PHYSICAL PROTECTION OF POWER REACTORS AGAINST SABOTAGE

Sabotage protection for power reactors was first addressed in a February 1967 Commission Order directing Florida Power and Light Company to address industrial sabotage protection at the Turkey Point plant. In October 1971, the Commission published guidance for licensees in Safety Guide 17, "Protection of Nuclear Power Plants Against Industrial Sabotage."

This initial security program was significantly upgraded in March 1977, with the publication of 10 CFR 73.55, which applied to approximately 50 operating reactors and about 25 applications for operating licenses. In 1977-78, in addition to the several Regulatory Guides already in existence, the NRC staff developed 23 review guidelines (Branch Technical Positions) and 3 NUREG reports for use as guidance for power reactor applicants/licensees and as acceptance criteria by reviewers. One such document, NUREG-0416, was a workbook that gave step-by-step procedures for licensees/applicants to show how they proposed to meet each regulatory requirement. At the conclusion of each NRC staff review, the reviewer prepared a Security Plan Evaluation Report. All approved plans covered all the functional requirements of 10 CFR 73.55(b) through (h). However, implementation of the functional requirements varied.

Review Guideline 17, "Definition of Vital Areas," published in January 1978, stated that essentially all safety-related equipment must be considered vital, and that the systems listed in Regulatory Guide 1.29, "Seismic Design Classification," should be considered vital. Applicants/licensees had to provide a sound technical basis for any deviation from this list. Review Guideline 17 also suggested that vital areas be separated into two categories: Type I (successful sabotage could be accomplished by sabotage activities within single area) and Type II (successful sabotage could be accomplished only by acts of sabotage in multiple areas, such as damage to various items of accident mitigation equipment). Because there was no regulatory basis for requiring an additional level of protection for Type I areas, no practical use was made of this distinction. A copy of Review Guideline 17 and Regulatory Guide 1.29 are included as Appendix B to this report.

In 1978, NRC contracted with the Los Alamos National Laboratory (LANL) to provide a site-specific vital equipment/area analysis for each reactor. This analysis was to be used by the NRC staff to validate the vital area identification provided by licensees in their approved plans. During the initial implementation phase of 10 CFR 73.55, eight separate teams reviewed licensees' vital area identification and security plans. As a

result of some uncertainty as to what constituted vital equipment, review results varied, and the staff recognized that the initial review findings might require revision. This possible need for revision was documented in the staff's safety evaluation reports and, in some cases, in license conditions, by the following statement or an equivalent: "The identification of vital areas and measures to control access to these areas, as described in the plan, may be subject to amendments in the future."

By the end of 1979, the staff had physical security plans for all operating power reactors, and, to a great extent, these plans had been implemented. However, at many sites, licensees were using compensatory measures for parts of the system that had not been installed or that were not functioning properly.

The compliance of licensees of operating plants with Review Guideline 17 can be summarized as follows:

- (1) Review Guideline 17 calls for all safety-related equipment to be protected as vital.
- (2) The first units of any plants licensed since 1980 satisfy this guidance.
- (3) About two-thirds of the physical security plans approved by the NRC staff probably do not completely satisfy Review Guideline 17 but meet it to varying degrees.

During its review of Duke Power Company's proposed vital area program for the Catawba plant, the staff used LANL's modeling assumptions as a technical basis for evaluating the adequacy of protecting the plant's standby shutdown facility, which was an alternative to protecting certain other safety-related equipment. The staff had previously approved this standby shutdown facility protection strategy for the McGuire and Oconee plants. This strategy calls for a hardened facility with separate ac and dc power, reactor controls, and cabling. It relies on the normal auxiliary feedwater system for emergency heat removal and a charging pump for primary water make-up. In the course of this review, a number of questions surfaced concerning LANL's modeling assumptions. To address these concerns, the VAC was established to review the vital area identification process in general, and the modeling assumptions specifically.

4. BASIC STUDY PREMISES

The Vital Area Committee adopted three premises for its study:

- (1) To protect the health and safety of the public from acts of radiological sabotage, the NRC requires physical protection system for nuclear power plants. The design basis threat for radiological sabotage, defined in 10 CFR 73.1(a), based on an extensive study of known adversarial characteristics, provides the bases for the design of security systems that will provide an adequate and prudent level of security at nuclear facilities.
- (2) Conformance with the requirements of 10 CFR 73.55(b)-(h) provides high assurance of protection against the design basis threat, recognizing that the Commission is considering improved access control relevant to 10 CFR 73.55(d). 10 CFR 73.55 requires each licensee to have the capability of meeting the specific detailed requirements of paragraphs (b) through (h). The Statement of Considerations for the rule states: "Compliance with the detailed requirements should essentially satisfy the general performance requirements stated in the rule in §73.55(a)" (42 FR 10838, February 24, 1977). Other Commission notices of public record issued in conjunction with other rulemaking proceedings essentially repeat this conclusion (42 FR 11201, February 28, 1979 and 44 FR 47759, August 15, 1979). Although the rule allows licensees and applicants to propose alternatives to paragraphs (b) through (h) that would be equivalent in meeting the performance objective, none have done so.
- (3) Successful radiological sabotage results in doses in excess of those defined in 10 CFR 100. The 10 CFR 100 criteria are intended to serve as a benchmark for the analysis of major events, that is, those events that pose a potential health hazard (a significant release of radioactivity as a result of a major accident or radiological sabotage). Equipment not designated and protected as vital is considered vulnerable to non-radiological sabotage. This study does not address non-radiological sabotage.

5. SCOPE AND METHODOLOGY

The study was carried out by the members of the Vital Area Committee (VAC) with supporting staff assistance from NRR, NMSS, RES, and IE. Throughout the study, the VAC met periodically with the Management Policy Review Group (MPRG) for guidance and approval.

The scope of the study included the following:

- (1) a review of all current regulations, guidance, definitions, assumptions, and criteria related to determining vital equipment and areas
- (2) a determination of the present status of the application of the items in (1) to various vintages of plants to establish what staff practice has been and is with respect to approving designated vital equipment and areas
- (3) identification of any deficiencies, ambiguities, inconsistencies, or other problems in the present regulatory approach
- (4) a review and evaluation of recent and current staff proposals, proposed rules, etc., as they relate to vital equipment and areas, such as
 - . protection of event-mitigating capabilities and their support facilities (e.g., water sources, pumps, switchgear, and cable runs)
 - . constraints on the vital island concept and compartmentalization requirements
 - . determination of an acceptable final state (hot or cold shutdown), the required duration of that state, reliance on outside assistance, and consideration of normal equipment repair capabilities
 - . provisions for compensating for vital equipment out of service for maintenance
 - . credit for plant-specific features and capabilities, such as feed-and-bleed
 - . relevant information, data, and recommendations from recent staff and contractor studies, as well as from operational experience relevant to vital equipment and areas
 - . methods used to protect critical equipment for other purposes, such as fire protection.

The VAC study and its results address light water reactors only. Other types of reactors will be considered on a case-specific basis, as appropriate. The VAC conducted the study in accordance with an action plan that had been approved by the MPRG. (A copy of the approved action plan is included as Appendix C to this report.) The VAC independently evaluated all relevant documentation. This review was augmented by 13 briefings by staff members and contractors on 16 study-related areas. (The briefings are summarized in Appendix D to this report.) The subjects of the briefings and organizations presenting them were as follows:

- . Current practices for vital equipment area reviews - NMSS
- . Vital equipment and vital area analyses - LANL
- . Vital area criteria for the Regulatory Effectiveness Review Program - NMSS
- . The Safeguards Insider Rules - NMSS
- . Vital Equipment Determination Research Study - RES/LANL
- . Current definitions and assumptions on vital areas - NRR
- . 10 CFR 50, Appendix R, Fire Protection - NRR
- . Generic Issue A-29, "Nuclear Power Plant Design for the Reduction of Vulnerability to Sabotage" - NRR
- . Vital area inspection program - IE
- . Vital area inspection program: implementation and critique of current assumptions and suggested changes - Regions I and II
- . USI A-45, "Shutdown Decay Heat Removal Requirements" - NRR
- . Precursor Studies of Risk Analysis of Several Known Safeguards Events - RES
- . Nuclear Power Plant Damage Control Measures - RES
- . Equipment Requiring Protection Under Various Condition Assumptions - NMSS
- . Selected Vital Equipment Assumptions - LANL
- . USI A-44, "Station Blackout" - NRR

6. STUDY RESULTS

6.1 Proposed Vital Equipment/Area Protection Philosophy and Analysis Assumptions

On the basis of its review and evaluation of relevant background information, data, and operational experience, the VAC developed an overall vital equipment/area protection philosophy or goal: to protect as vital the reactor coolant pressure boundary and one train of equipment --with the associated piping, water sources, power supplies, controls, and instrumentation -- that provide the capability to achieve and maintain hot shutdown.

Implementation of this philosophy would protect a set of safety-related components rather than protecting all safety-related components. It is derived from and is consistent with Appendix A to 10 CFR 100 and Appendix R to 10 CFR 50. Appendix A to 10 CFR 100 defines those structures, systems and components to be protected from the effects of earthquakes; the staff uses this to identify equipment to be protected in design basis events. Appendix R to 10 CFR 50 addresses fire protection. The proposed philosophy also builds on the existing defense-in-depth safeguards approach, which consists of a protected boundary, determining specific equipment and areas to be protected as vital, access authorization (minimizing the number of people with access to vital equipment), and an assumed shutdown capability.

In summary, protecting as vital the reactor coolant pressure boundary and one train of equipment (with associated piping, water sources, power supplies, and instrumentation) that provide the capability to achieve and maintain hot shutdown represents an approach to safeguards protection that is consistent both with the existing regulations for ensuring safety under design basis earthquake and fire conditions and with the current approach to safeguards protection. Application of this philosophy will contribute to the overall program designed to provide a high degree of assurance against radiological sabotage.

After developing this protection philosophy, the VAC re-examined, individually and collectively, 16 vital equipment/area assumptions currently used by LANL, and their bases. These assumptions provide the principal guidance used by safeguards analysts to identify equipment and areas that require protection against successful radiological sabotage. (The LANL assumptions are listed in Appendix E.)

This reexamination was based on the three premises defined in Section 4 above. In brief, they are

- (1) The design-basis threat of radiological sabotage is defined in 10 CFR 73.1(a).

- (2) Conformance with the requirements of 10 CFR 73.55(b)-(h) provides high assurance of protection against the design-basis threat.
- (3) Successful radiological sabotage results in doses in excess of those defined in 10 CFR 100.

After re-evaluating the current analysis assumptions, in light of the VAC protection philosophy and these three assumptions, the VAC developed the revised set of assumptions discussed below. Application of these assumptions might result in designation of vital equipment different from that recommended in NUREG-0992, "Report of the Committee to Review Safeguards Requirements at Power Reactors," dated May 1983, which was that several specific plant areas or equipment items be protected as independent vital islands.

6.1.1 Assumption 1

For protection against radiological sabotage, the primary coolant pressure boundary consists of the reactor vessel and reactor coolant piping up to and including a single, protected, normally-closed isolation valve or protected valve capable of closure in interfacing systems.

Rationale

Protection of the primary coolant pressure boundary, as defined, ensures that a saboteur cannot cause a loss-of-coolant accident (LOCA). Thus, this protection precludes the need to protect LOCA-mitigating equipment. Protection of a single valve is an adequate barrier for this purpose. Manual action to close a protected valve in an interfacing system is acceptable if that action can be taken in time to prevent an unrecoverable condition. Any valves upstream of a protected valve need not be protected if their failure will not result in a LOCA.

6.1.2 Assumption 2

Any transient or event that causes significant core damage will result in an attendant 10 CFR 100 release.

Rationale

This is a conservative approach that assumes that, except for a temporary loss of water and/or heat removal capability, the core must be kept covered with water and decay heat removal capability must be maintained to preclude core melt. If these conditions are not met, core melt is assumed. No credit is given for the protective or mitigating capabilities of the pressure vessel or the containment. Thus, core melting is assumed to result in doses in excess of those defined in 10 CFR 100.

6.1.3 Assumption 3

One train of equipment (with the associated piping, water sources, power supplies, controls, and instrumentation) that provides the capability to perform the functions (reactivity control, decay heat removal, and process monitoring) that are necessary to achieve and maintain hot shutdown for a minimum of 8 hours from the time of reactor trip should be protected as vital. In addition, the major components of the reactor coolant makeup system and associated support equipment necessary to achieve this goal should be protected as vital.

Rationale

Reactivity control is necessary to achieve and maintain subcritical reactivity conditions in the reactor. Decay heat removal is necessary to remove decay heat generated in the core during hot shutdown. Process monitoring is necessary to provide direct readings of the process variables needed to perform, control, and monitor the reactivity control and decay heat removal.

For those plants where an 8-hour hot shutdown capability without primary system makeup or alternate power sources cannot be demonstrated, the major components of those systems necessary to support reactivity control, decay heat removal, and process monitoring also must be protected as vital. For example, an alternate power source, such as a diesel generator, might be necessary to provide power for process monitoring instruments and for other equipment required for achieving and maintaining hot shutdown. Primary makeup water might be necessary to compensate for coolant leaked through the main reactor coolant pump seals and/or for operation of the power-operated relief valves.

Examples of equipment needed to perform these functions include, but are not limited to, the following:

| | |
|--|--|
| reactivity control | control rod scram components and systems (PWRs and BWRs) |
| decay heat removal | turbine-driven auxiliary feedwater pump, including control, water source (e.g., condensate storage tank), and main steam safety valves (PWRs) |
| | turbine-driven high pressure core injection (HPCI) pump, reactor core isolation cooling (RCIC) pump, isolation condenser, including auto start, control, and safety-relief valves (BWRs) |
| process monitoring | pressurizer pressure and level, steam generator pressure and level, reactor coolant hot and cold leg temperature (PWRs) |
| | reactor pressure and level, suppression pool temperature and level (BWRs) |
| reactor coolant makeup and reactor coolant pump seal cooling | charging pump, including water source and motor control center (PWRs) |
| support functions | diesel generator, including switchgear, cooling, startup, and controls (PWRs and BWRs) |
| | battery (PWRs and BWRs) |
| | service water pump and motor control center (PWRs and BWRs) |
| | component cooling water pump and motor control center (PWRs) |

6.1.4 Assumption 4

The control room and any remote locations from which vital equipment can be controlled or disabled (such as remote shutdown panels, motor control centers, circuit breakers, or local control stations) should be protected as vital areas.

Rationale

Because the equipment necessary to ensure hot shutdown following a sabotage-initiated transient can be controlled from either the control room or local areas, both must be protected as vital.

6.1.5 Assumption 5

Only the power mode of reactor operation and hot standby (for PWRs) need be considered as long as all equipment designated as vital for power operation is maintained as vital in other modes.

Rationale

Equipment identified as vital from an analysis of the power or hot standby modes of reactor operation also encompasses that necessary to protect against radiological sabotage in other modes. Therefore, plant-specific analyses of other modes are not necessary for vital equipment determination.

Consideration was given to a possible exception in the cold shutdown mode, since the cold shutdown decay heat removal (DHR) system, also referred to as the residual heat removal (RHR) system, is not required to be protected as vital for the power or hot standby modes. Because of the size of the decay heat removal (DHR) system piping (16-inch diameter) and the capacity of the residual heat removal (RHR) system pump (5500 gpm), the DHR system could drain the reactor vessel to hot leg level in less than 11 minutes in case of a DHR LOCA or uncontrolled containment spray. Without injection flow to the pressure vessel, the water level in the vessel would drop to the top of core from the hot leg level in about 15 minutes, and to the mid-point of the core in about 36 minutes. Therefore, the capability of isolating a damaged DHR system from the primary coolant pressure boundary during the cold-shutdown mode is required. This capability would be ensured by protecting the primary coolant pressure boundary, which includes the first isolation valve.

Additionally, normal procedures routinely require more than 6 hours to bring a PWR to cold shutdown after reactor scram. After reactor shutdown, decay heat rapidly decreases and is less than 0.5% at the end of 24 hours. Thus, after 24 hours of cold shutdown, less than 100 gpm of injected water is required to remove the remaining decay heat. This relatively small flow of water can be obtained from alternate water makeup sources - - such as the high-pressure injection system or the charging system, which already is protected. Thus, the time when significant fuel damage can be realistically caused is very limited.

Further support for this assumption is based on a recent NRC study that evaluated 130 total loss-of-DHR events in U.S. PWRs between 1976 and 1983. The durations of these events (before corrective actions were taken) ranged from less than 1 minute to 2½ hours. However, because of timely corrective actions taken by the operators, no serious damage resulted from any of these events.

6.1.6 Assumption 6

Off-site power is unavailable.

Rationale

Off-site power is transmitted by facilities outside the areas protected and controlled by the licensee. Therefore, the licensee cannot protect against the external assault defined in the design basis threat. This assumption is compatible with the basic premise that equipment not designated and protected as vital is vulnerable to damage and is not available.

6.1.7 Assumption 7

Random failures do not occur simultaneously with an act of radiological sabotage. However, the saboteur can take advantage of the unavailability of equipment during maintenance. Thus, whenever any components or systems normally protected as vital are inoperable for any period of time, appropriate compensatory measures (such as stationing guards at alternate locations) must be taken to ensure the capability to reach and maintain hot shutdown.

Rationale

The likelihood of a significant random equipment failure occurring simultaneously with a successful radiological sabotage act is very small, probably in the same order as the occurrence of an accident beyond the design basis. Although a saboteur might wait for such an event before initiating a sabotage act, this situation would require the saboteur to be in a continuous state of total readiness for indefinite periods, which seems unlikely. However, a planned maintenance outage is usually of significant duration and a saboteur can readily learn of the plans for such outages well in advance of their occurrence, allowing the saboteur time to implement successful radiological sabotage. Thus, radiological sabotage during unplanned equipment outages is less likely than during planned maintenance outages.

6.1.8 Assumption 8

Breaks in multiple main steam lines that cannot be isolated lead to 10 CFR 100 releases.

Rationale

The design-basis main steam line break is the unisolable double-ended rupture of a single main steam line upstream of the main steam line isolation valves. A licensee's analysis of this design-basis event must show that the main steam line break mitigating systems can prevent core damage resulting from both the positive reactivity increase caused by the overcooling transient and the loss of steam generator tube integrity. It is conservatively assumed that these mitigating systems cannot prevent core damage if a multiple main steam line break beyond the design basis were to occur. Therefore, three options are available to licensees: (1) protect all main steam lines, up to and including the main steam line isolation valves, as vital; (2) protect all main steam lines, as in (1) above, except the one covered by the design-basis main steam line break, and protect as vital the mitigating systems for that line; or (3) provide analyses demonstrating that sabotage-induced multiple steam line breaks are acceptable and protect as vital the required mitigating equipment and systems.

6.1.9 Assumption 9

Cable runs in trays and conduit need not be protected as vital unless cables necessary for safe shutdown capability are individually identifiable and the identification is reasonably accessible. However, cable terminals or junctions and areas such as cable spreading rooms, through which large numbers of cables pass, must be protected.

Rationale

Generally, it is not feasible for a saboteur to identify individual cables in cable trays. In some very few instances where individual cables in trays and conduits are tagged or labeled with coded identifications, such tags or labels are not readily accessible and significant effort would be required to trace the code to the actual cable identity. Thus, even in such cases, positive identification of specific individual cables is considered to be very difficult and unlikely. However, for facilities with such individually identified cables, justification will be required for not protecting the cables as vital.

Most licensees, however, have prepared documentation which identifies cable routings and locations. Therefore, a saboteur might not be able to identify a specific cable among many in a tray, but he could know that a certain cable is within a specific tray. Protecting all cable trays throughout their entire routings could be contrary to the objective of minimizing access to vital equipment, because designating large portions of the plant as vital greatly increases the number of personnel with access to vital areas. The approach that cable runs in trays and conduit need not be protected requires the acceptance of some degree of cable vulnerability. However, damage control can compensate for the loss of cable more readily than it can compensate for the loss of vital equipment served by these cables.

6.1.10 Assumption 10

Saboteurs may use explosives in amounts that they can carry.

Rationale

This assumption provides for consideration of protecting, as vital, massive pieces of equipment (reactor pressure vessel, water tanks) that could otherwise not be damaged by individuals using conventional tools and thereby would not warrant protection as vital equipment. Determination of which equipment needs to be designated vital is insensitive to the specific amount of explosives that individuals can carry (see Assumption 11). Implementation of the assumption to determine which equipment needs to be designated vital does not require the analyst to consider specifically how much explosives can be used by the adversary. The goal was to bound the problem by characterizing an amount that could be carried, consistent with the design basis threat, and not require a vehicle.

6.1.11 Assumption 11

No credit is given for equipment not located in vital areas.

Rationale

Because some single plant areas contain either a common element, the major elements of an essential system, or elements of multiple essential systems, and because a saboteur is assumed to have whatever knowledge is required, once a saboteur enters such an area, there are no impediments to the successful completion of the radiological sabotage action. Therefore, it is assumed that if a saboteur gets into a single area containing several pieces of equipment, the saboteur can disable or manipulate all of the equipment in that area.

6.1.12 Assumption 12

Following the start of a refueling outage, the spent fuel pool should be protected as vital long enough to ensure that sabotage to the pool cannot result in a 10 CFR 100 release.

. Rationale

Protection of the spent fuel pool for the specified period of time immediately following refueling precludes damage to the spent fuel that would result in unacceptable releases.

6.1.13 Assumption 13

The backup supporting power supply of the Central Alarm Station (CAS) is essential for continuous operation of CAS in the event of loss of normal power.

. Rationale

The CAS is designated a vital area by 10 CFR 73.55(e)(1). Its backup supporting power supply must be protected to assure continuous CAS operation (1) to provide timely indication of an unauthorized attempt to enter a vital area, (2) to detect unauthorized penetration of the protected area, and (3) to assure a means of communicating with the local law enforcement agencies.

6.2 Impact on Licensed Plants

Generally, implementation of the proposed vital equipment/a; a protection philosophy and analysis assumptions would have a greater impact on facilities licensed before 1980 than on those licensed since then. The VAC estimates that the licensees of about one-third of the operating U.S. nuclear power reactors would not have to protect any equipment beyond that now protected. Licensees of the other two-thirds of the U.S. operating reactors might be required to classify additional equipment as vital. This equipment would range from a few items in some plants to many in others.

7. RECOMMENDATION

The Vital Area Committee recommends that the proposed vital equipment/area protection philosophy and analysis assumptions presented in Section 5.1 of this report be adopted and implemented. However, satisfaction of ~~the~~ requirements and assumptions of Review Guideline 17, issued in January 1978, should continue to be acceptable as an alternative to this revised guidance. The Committee believes that these assumptions represent a comprehensive and consistent approach to determining equipment and areas to be designated as vital in nuclear power plants and that their application will contribute to the overall program designed to provide a high degree of assurance against radiological sabotage.

APPENDIX A

EDO MEMORANDUM OF MAY 1, 1985

ESTABLISHING THE VITAL EQUIPMENT/AREA GUIDELINES STUDY



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

MAY 01 1985

MEMORANDUM FOR: Victor Stello, Deputy Executive Director for
Regional Operations & Generic Requirements

Harold R. Denton, Director
Office of Nuclear Reactor Regulation

John G. Davis, Director
Office of Nuclear Material
Safety & Safeguards

Frank J. Miraglia, Deputy Director
Division of Licensing, HRR

Robert F. Burnett, Director
Division of Safeguards, NMSS

James G. Partlow, Director
Division of
Inspection Programs

Frank P. Gillespie, Director
Division of Risk Analysis & Operations, RES

FROM: William J. Dircks
Executive Director for Operations

SUBJECT: VITAL EQUIPMENT/AREA GUIDELINES STUDY

The vital area definition process has been evolving since 1978 and has been addressed in several studies. Recent evaluations of licensees' physical security plans and site visits have raised questions about the validity of some of the assumptions and criteria used in the current vital equipment/area determination process.

In view of the uncertainty involved with the vital equipment/area guidelines, a need exists to reevaluate the bases and guidelines used to determine the equipment and areas to be protected as vital. Therefore, I am establishing a study effort to respond to this need. The participants, responsibilities and milestones are outlined broadly in the enclosure, "Charter, Membership and Action Plan for Vital Equipment/Area Guidelines Study." This approach will ensure coordination and consistency and bring together expertise in both the safety and safeguards perspectives.

The study should be completed and a final report issued within about eight months.

(Signed) William J. Dircks

William J. Dircks
Executive Director for Operations

Enclosure:
As stated

cc: Thomas E. Murley,
Administrator, Region I

J. Nelson Grace,
Administrator, Region II

James G. Keppler,
Administrator, Region III

Robert D. Martin,
Administrator, Region IV

John B. Martin,
Administrator, Region V

ENCLOSURE

CHARTER, MEMBERSHIP AND ACTION PLAN FOR VITAL EQUIPMENT/AREA GUIDELINES STUDY

I. Objective

This study is intended to cover the entire spectrum of NRC safeguards rules, guidance, contractor data, etc., as they pertain to vital equipment/area rules, guidelines and assumptions. A consistent, logical approach to identifying vital equipment/areas for subsequent protection is to be developed.

Consideration shall be given to conditions of normal operation, including anticipated operational occurrences, and those transients and accidents of the types presently considered in the design basis analysis of the plant. Consideration shall also be given to outage activities to the extent that loss of operational functions and capabilities impact vital equipment and areas.

II. Background

The vital equipment/area guidelines currently in use have evolved as follows:

- o 10 CFR 7 .2 defines in general terms equipment and areas that must be protected as vital.
- o "Definition of Vital Areas," Revision-1, Review Guideline No. 17 January 23, 1978 addresses in general terms the structures, systems and components that should be protected as vital. It also classifies vital equipment/areas into two general categories -- Type I and Type II.
- o The LANL Vital Area Analysis Assumptions are utilized by LANL under a technical assistance program to independently identify vital equipment/areas at power reactors.
- o A Working Group to Improve Vital Area Determination Techniques report of August 12, 1982, concluded that the techniques in use, subject to recommended modification, provide a reasonable approach, from a safeguards perspective, to identifying vital areas and equipment. It was recommended that a research project be initiated to further refine and improve the program. The research project is not yet complete.
- o NUREG-0992, May 1983, prepared by the Committee to Review Safeguards Requirements at Power Reactors, endorsed the vital island concept and further identified selected items of equipment that should be independently protected as vital at all power reactors.

- o The Proposed Insider Rule, published for public comment on August 11, 1984 would provide for the grouping of vital areas into "vital islands" and require protection of vital equipment only to the extent necessary to interrupt sabotage paths.

III. Organization

Two groups are established to carry out the study: A Vital Area Committee and a Management Policy Review Group.

The Vital Area Committee is chaired by Frank J. Miraglia, NRR. Its other members are Robert F. Burnett, NMSS; James G. Partlow, IE; and Frank P. Gillespie, RES.

The Management Policy Review Group is composed of Victor Stello, DEDROGR; Harold R. Denton, NRR; and John G. Davis, NMSS.

IV. Responsibilities

A. Vital Area Committee

- o Recommend a proposed Action Plan with milestones and specific milestone schedules.
- o Reexamine all existing and proposed requirements, assumptions, guidelines and their base for determining vital equipment and areas; either validate or modify them appropriately.
- o Recommend a clear, consistent and comprehensive set of guidelines for determining vital equipment and areas.
- o Obtain and integrate necessary supporting expertise in the form of input to the study effort and comments on drafts, from the line organizations represented on the Committee, as well as from other Headquarters Offices, the Regions and contractors, as appropriate.
- o Interact directly with the Management Policy Review Group as necessary to obtain guidance, direction and concurrence.
- o Prepare draft reports with recommendations and supporting bases for Management Policy Review Group review and approval.

B. Management Policy Review Group

- o Approve the Action Plan, its milestones and schedules.
- o Meet periodically, as necessary and appropriate, with the Vital Area Committee to provide broad policy direction and guidance for the conduct of the study and to discuss the study status, plans, progress and problems.
- o Approve and issue the final report to the EDO.

V. Preliminary Action Plan

The following proposed Action Plan broadly delineates the major tasks and milestone schedule for accomplishing the specified effort. It will be further refined by the Vital Area Committee and approved by the Management Policy Review Group.

- (1) Initial meeting of the Vital Area Committee to formalize the approach, identify needed resources and develop the schedule.

Target Date: Week 0

- (2) Vital Area Committee and supporting staff meet in working sessions to develop preliminary recommendations with rationale and justification. Interacts with other Offices and staff and with the Management Policy Review Group as necessary and appropriate. Preliminary recommendations presented to the Management Policy Review Group.

Target Date: Week 17

- (3) Management Policy Review Group reviews preliminary findings and provides guidance/recommendations to the Vital Area Committee.

Target Date: Week 20

- (4) Vital Area Committee integrates recommendations into draft vital equipment/area guidelines report. Draft report completed.

Target Date: Week 25

- (5) Draft report circulated for comments and concurrence from all cognizant Offices. Comments/concurrence received.

Target Date: Week 30

- (6) Vital Area Committee prepares final report for Management Policy Review Group approval. Management Policy Review Group submits final report to the EDO.

Target Date: Week 36

APPENDIX B
REVIEW GUIDELINE 17 AND REGULATORY GUIDE 1.29



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

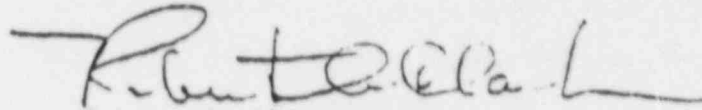
JAN 23 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch
Members, DOR

FROM: Robert A. Clark, Chief
Reactor Safeguards Licensing Branch, DOR

SUBJECT: DEFINITION OF VITAL AREAS, REVISION 1 -
REVIEW GUIDELINE NO. 17

Enclosed is Review Guideline Number 17, i.e., the
revised definition of vital areas.


Robert A. Clark, Chief
Reactor Safeguards Licensing
Branch, DOR

Enclosure:
As stated

DEFINITION OF
VITAL AREAS AND EQUIPMENT
Revision 1

A. Applicable Sections of 10 CFR 73

73.55 (c)(1):

"The licensee shall locate vital equipment only within a vital area, which in turn, shall be located within a protected area such that access to vital equipment requires passage through at least two physical barriers of sufficient strength to meet the performance requirements of paragraph (a) of this section. More than one vital area may be located within a single protected area."

73.2 (h):

"Vital area means any area which contains vital equipment within a structure, the walls, roof, and floor of which constitute physical barriers of construction at least as substantial as walls as described in paragraph (f)(2)."

73.2 (i):

"Vital equipment means any equipment, system, device, or material failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction or release are also considered to be vital."

B. Assumptions and Definitions

In the application of these regulations to a typical LWR plant, the following considerations and assumptions are made:

1. Paragraph 73.55 (c) requires vital equipment to be enclosed by two barriers. The combination of barriers, in conjunction with other components of the security system, must provide a sufficient delay to an intrusion to meet the performance requirements of 73.55 (a).
2. To "endanger the public health and safety by exposure to radiation" requires a significant off-site release of radioactivity. For LWR's the following sources of significant quantities of radioactivity should be considered:
 - a. The reactor core,
 - b. Spent fuel,
 - c. Radwaste systems, if the total radwaste inventory is greater than nxC , where:
 - n is the ratio of the applicable dose guideline of 10 CFR 100 to the dose computed for accidental releases in Chapter 15 of the FSAR, and
 - c is the release (curies) assumed in the accidental release calculation of the FSAR.
3. Vital Areas fall into two general categories:
 - a. Type I vital areas, i.e., those areas wherein successful sabotage can be accomplished by compromising or destroying

the vital systems^{1/} or components located within this area. (By definition, an area containing systems or components whose failure or destruction results in a direct release is a Type I vital area.)

b. Type II vital areas, i.e., those areas which contain systems or components whose failure or destruction would lead to successful sabotage only in conjunction with additional sabotage activity in at least one other, separate^{2/} vital area. (Safety related equipment designed to mitigate the consequences of failures of other systems usually falls into this category.)

4. When classifying vital equipment as Type I or II, the following assumptions apply:
- a) The concurrence of violent natural phenomena with a security contingency need not be considered.
 - b) Random (accidental) failure of equipment concurrent with a security contingency need not be considered. However, a security contingency during routine or planned outages of equipment, as permitted by the technical specifications, must be considered.

^{1/} "System" refers to all components, mechanical and electrical, including piping, cabling, power supply, and other support systems to carry out the design function provided by the system.

^{2/} For the purpose of this discussion, a vital area may be considered "separate" if it is separated from the area under consideration by a barrier or distance sufficient to delay the saboteur's access long enough to demonstrate interception and engagement by the security response force.

- c) Loss of off-site power must be assumed since it is impractical to protect transmission lines against sabotage.

C. Discussion

The definition of vital equipment, 73.2 (i), includes equipment whose failure would lead to a direct release, as well as equipment required to function for the protection of public health and safety following a postulated sabotage attack. This is analagous to the definition of safety-related equipment, which includes primary fission product barriers, as well as the systems required to mitigate the consequences of a breach of the barrier. Therefore, essentially all safety related equipment must be considered vital. In order to avoid duplication of safety analyses, the systems listed in Reg. Guide 1.29 should be considered vital.

It should be noted that a facility which provides sufficient delay time to permit interruption of the external threat of §(a)(1) at all vital area barriers, and for which adequate protection against the insider threat of §(a)(2) is provided for all vital areas would meet the requirements of 73.55 without the designation of any Type I Vital Areas. In practice, however, it is to the licensee's advantage to segregate vital areas into Type I and II, in order to take credit for the fact that a saboteur could not achieve successful sabotage in Type II vital areas without penetrating additional barriers.

D. Review Guidelines

1. All systems listed in Reg. Guide 1.29 as "Seismic Category I" are considered vital. (A sound technical basis must be provided by the licensee for any deviation from this list.)
2. Type I Vital Areas should be identified by the licensee, using the definitions and assumptions listed in B. If Type I Vital Areas are not identified by the licensee, the list provided in the Appendix may be used as guidance.
3. High assurance protection against the external and internal threat must be provided for all Type I Vital Areas. This requires a demonstration that any external Type I vital barriers provide sufficient delay to the external threat (§(a)(1)) to permit a timely engagement by the armed response force, and appropriately restricted access controls, controls of activity, or other methods of protection against the insider, to meet the internal threat (§(a)(2)). For Type II Vital Areas, a combination of multiple barriers, each of which meets the requirements of 73.2(f)(2) or its equivalent, and the associated individual access controls, provides high assurance protection against the external and internal threat.

Appendix

SAMPLE LIST OF TYPE I VITAL AREAS

1. Primary containment
2. Containment electrical and piping penetration areas
3. Control room
4. Cable spreading room
5. Primary shutdown system (if outside containment)
6. All areas associated with one complete decay heat removal system (including all necessary support systems, e.g., power supply, cooling, and lubricating systems.)
7. Battery rooms (including battery charger areas)

REGULATORY GUIDE

OFFICE OF STANDARDS DEVELOPMENT

REGULATORY GUIDE 1.20

SEISMIC DESIGN CLASSIFICATION

A. INTRODUCTION

General Design Criterion 2, "Design Bases for Protection Against Natural Phenomena," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Licensing of Production and Utilization Facilities," requires that nuclear power plant structures, systems, and components important to safety be designed to withstand the effects of earthquakes without loss of capability to perform their safety functions.

Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 establishes quality assurance requirements for the design, construction, and operation of nuclear power plant structures, systems, and components that prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. The pertinent requirements of Appendix B apply to all activities affecting the safety-related functions of those structures, systems, and components.

Appendix A, "Seismic and Geologic Site Criteria for Nuclear Power Plants," to 10 CFR Part 100, "Reactor Site Criteria," requires that all nuclear power plants be designed so that if the Safe Shutdown Earthquake (SSE) occurs, all structures, systems, and components important to safety remain functional. These plant features are those necessary to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent, or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guideline exposures of 10 CFR Part 100.

This guide describes an acceptable method of identifying and classifying those features of light-water-cooled

nuclear power plants that should be designed to withstand the effects of the SSE.

B. DISCUSSION

After reviewing a number of applications for construction permits and operating licenses for boiling and pressurized water nuclear power plants, the NRC staff has developed a seismic design classification system for identifying those plant features that should be designed to withstand the effects of the SSE. Those structures, systems, and components that should be designed to remain functional if the SSE occurs have been designated as Seismic Category I.

C. REGULATORY POSITION

1. The following structures, systems, and components of a nuclear power plant, including their foundations and supports, are designated as Seismic Category I and should be designed to withstand the effects of the SSE and remain functional. The pertinent quality assurance requirements of Appendix B to 10 CFR Part 50 should be applied to all activities affecting the safety-related functions of these structures, systems, and components.

a. The reactor coolant pressure boundary.

b. The reactor core and reactor vessel internals.

c. Systems¹ or portions of systems that are required for (1) emergency core cooling, (2) postaccident containment heat removal, or (3) postaccident

¹The system boundary includes those portions of the system required to accomplish the specified safety function and connected piping up to and including the first valve (including a safety or relief valve) that is either normally closed or capable of automatic closure when the safety function is required.

USNRC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public methods acceptable to the NRC staff at implementing specific parts of the Commission's requirements in delineated techniques used by the staff in evaluating specific problems or postulated accidents, or to provide guidance to applicants. Regulatory Guides are not substitutes for regulations and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings required to the issuance or continuance of a permit or license by the Commission.

Comments and suggestions for improvements in these guides are encouraged at all times and guides will be revised as appropriate to accommodate comments and to reflect new information or experience. However, comments on this guide if received within about two months after its issuance will be particularly useful in evaluating the need for an early revision.

Comments should be sent to the Secretary of the Commission, U.S. Nuclear Regulatory Commission, Washington, D.C. 20540, Attention: Document and Service Section.

The guides are issued in the following ten broad divisions:

- | | |
|-----------------------------------|------------------------|
| 1. Power Reactors | 6. Proliferation |
| 2. Research and Test Reactors | 7. Transportation |
| 3. Fuels and Materials Facilities | 8. Occupational Health |
| 4. Environmental and Siting | 9. Accident Review |
| 5. Materials and Plant Protection | 10. General |

Copies of published guides may be obtained by written request indicating the divisions desired to the U.S. Nuclear Regulatory Commission, Washington, D.C. 20540, Attention: Director, Office of Standards Development.

containment atmosphere cleanup (e.g., hydrogen removal system).

d. Systems¹ or portions of systems that are required for (1) reactor shutdown, (2) residual heat removal, or (3) cooling the spent fuel storage pool.

e. Those portions of the steam systems of boiling water reactors extending from the outermost containment isolation valve up to but not including the turbine stop valve, and connected piping of 2-1/2 inches or larger nominal pipe size up to and including the first valve that is either normally closed or capable of automatic closure during all modes of normal reactor operation. The turbine stop valve should be designed to withstand the SSE and maintain its integrity.

f. Those portions of the steam and feedwater systems of pressurized water reactors extending from and including the secondary side of steam generators up to and including the outermost containment isolation valves, and connected piping of 2-1/2 inches or larger nominal pipe size up to and including the first valve (including a safety or relief valve) that is either normally closed or capable of automatic closure during all modes of normal reactor operation.

g. Cooling water, component cooling, and auxiliary feedwater systems¹ or portions of these systems, including the intake structures, that are required for (1) emergency core cooling, (2) postaccident containment heat removal, (3) postaccident containment atmosphere cleanup, (4) residual heat removal from the reactor, or (5) cooling the spent fuel storage pool.

h. Cooling water and seal water systems¹ or portions of these systems that are required for functioning of reactor coolant system components important to safety, such as reactor coolant pumps.

i. Systems¹ or portions of systems that are required to supply fuel for emergency equipment.

j. All electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action.

k. Systems¹ or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.

l. The spent fuel storage pool structure, including the fuel racks.

m. The reactivity control systems, e.g., control rods, control rod drives, and boron injection system.

n. The control room, including its associated vital equipment, cooling systems for vital equipment, and life support systems, and any structures or equipment inside or outside of the control room whose failure could result in incapacitating injury to the occupants of the control room.²

o. Primary and secondary reactor containment.

p. Systems,³ other than radioactive waste management systems,³ not covered by items 1.a through 1.o above that contain or may contain radioactive material and whose postulated failure would result in conservatively calculated potential offsite doses (using meteorology as prescribed by Regulatory Guide 1.3, "Assumptions Used for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Boiling Water Reactors," and Regulatory Guide 1.4, "Assumptions Used for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Pressurized Water Reactors") that are more than 0.5 rem to the whole body or its equivalent to any part of the body.

q. The Class 1E electric systems, including the auxiliary systems for the onsite electric power supplies, that provide the emergency electric power needed for functioning of plant features included in items 1.a through 1.p above.

2. Those portions of structures, systems, or components whose continued function is not required but whose failure could reduce the functioning of any plant feature included in items 1.a through 1.q above to an unacceptable safety level should be designed and constructed so that the SSE would not cause such failure.

3. Seismic Category I design requirements should extend to the first seismic restraint beyond the defined boundaries. Those portions of structures, systems, or components that form interfaces between Seismic Category I and non-Seismic Category I features should be designed to Seismic Category I requirements.

4. The pertinent quality assurance requirements of Appendix B to 10 CFR Part 50 should be applied to all activities affecting the safety-related functions of those portions of structures, systems, and components covered under Regulatory Positions 2 and 3 above.

¹Lines indicate substantive changes from previous issue.

²Wherever practical, structures and equipment whose failure could possibly cause such injuries should be relocated or separated to the extent required to eliminate this possibility.

³Specific guidance on seismic requirements for radioactive waste management systems is under development.

¹See footnote 1, p. 1.29-1.

APPENDIX C

ACTION PLAN MEMORANDUM DATED JULY 1, 1985



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON D. C. 20555

July 1, 1985

MEMORANDUM FOR: Victor Stello, Deputy Executive Director
for Regional Operations and Generic Requirements

Harold R. Denton, Director
Office of Nuclear Reactor Regulation

John G. Davis, Director
Office of Nuclear Material Safety and Safeguards

FROM: Frank J. Miraglia, Chairman
Vital Area Committee

SUBJECT: VITAL EQUIPMENT/AREA GUIDELINES STUDY ACTION PLAN

- References:
1. Memorandum from William J. Dircks, "Vital Equipment/Area Guidelines Study," dated May 1, 1985.
 2. Memorandum from Frank J. Miraglia, "Vital Equipment/Area Guidelines Study Action Plan," dated May 21, 1985.
 3. Memorandum from Frank J. Miraglia, "Vital Equipment/Area Guidelines Study Revised Action Plan," dated June 17, 1985.

Based upon discussions at our meetings with the Management Policy Review Group on June 4 and June 25 and further consideration by the Vital Area Committee, we have modified and finalized the action plan to reflect your guidance and recommendations. We plan to proceed with the study in accordance with this action plan, which is enclosed, unless you direct us otherwise.

We will meet with you again in late July to review our progress and status.

A handwritten signature in black ink that reads "Frank J. Miraglia".

Frank J. Miraglia, Chairman
Vital Area Committee

Enclosure:
As stated

cc w/enclosure:
T. Murley, Administrator, Region I
J. Nelson Grace, Administrator, Region II
R. Burnett, Director, Division of
Safeguards, NMSS
J. Partlow, Director, Division of
Inspection Programs, IE
F. Gillespie, Director, Division of
Risk Analysis and Operations, RES

VITAL EQUIPMENT/AREA GUIDELINES STUDY
ACTION PLAN

Objectives of Study

Develop a comprehensive and consistent set of recommended assumptions, performance criteria and guidance, in a report to the EDO, for determining vital equipment/areas in nuclear power plants. The assumptions and guidance should:

1. Consider conditions of normal operation, including anticipated operational occurrences, and those transients and accidents of the types presently considered in the design basis analysis of nuclear power plants;
2. Consider outage activities to the extent that loss of operational functions and capabilities during outages impacts vital equipment;
3. Be readily applicable to identification of required vital equipment and areas on a case-by-case basis; and
4. Have review and concurrence of all cognizant offices.

Preliminary Basic Assumptions

The Vital Area Committee (VAC) has established the following basic assumptions at the inception of the study. These assumptions will be reexamined and changed, if necessary and with MPRG approval, as the study proceeds.

1. The design basis threat of radiological sabotage is as defined in 10 CFR 73.1(a).
2. Conformance with the requirements of 10 CFR 73.55(b)-(h) provides high assurance of protection against the design basis threat. This recognizes that the Commission is considering improved access control relevant to 10 CFR 73.55(d).
3. Successful radiological sabotage results in doses in excess of those defined on 10 CFR 100. The study will consider protection against radiological sabotage only and will not address non-radiological sabotage.

Scope of Study

The Vital Area Committee (VAC) will:

1. Review all regulations, guidance, definitions, assumptions and criteria currently in effect related to determination of vital equipment and areas;

2. Determine the present status of the application of the items in (1) above to various vintages of plants to establish what staff practice has been and is at present with respect to approving designated vital equipment and areas;
3. Identify any deficiencies, ambiguities, inconsistencies and other problems in the present regulatory approach;
4. Review and evaluate recent and current staff proposals, proposed rules, etc., as they relate to and impact vital equipment and areas. For example, this would include the following:
 - a. Protection of event mitigating capabilities and their support facilities; e.g., water sources, pumps, switchgear, cable runs;
 - b. Constraints on vital island concept and compartmentalization requirements;
 - c. Acceptable final state (hot vs. cold shutdown), required duration of that state, reliance on outside assistance, and consideration of normal equipment repair capabilities;
 - d. Provisions for compensating for vital equipment which is out of service for maintenance;
 - e. Credit for plant-specific features and capabilities such as feed-and-bleed;
 - f. Information, data and recommendations from recent staff and contractor studies as well as operational experience relevant to vital equipment and areas; and
 - g. Methods used to protect critical equipment for other purposes, such as fire protection.

Study Methodology

The following approach is planned for Vital Area Committee information and data acquisition and assessment:

1. Independent VAC review and evaluation of all relevant documentation; and
2. A series of briefings to the VAC by staff and NRC contractors, as outlined in Attachment 1 (note that these briefings have been completed).

Schedule

The attached figure (Attachment 2) shows the milestones and target dates for the first phase of the study which will produce preliminary recommendations to the Management Policy Review Group (MPRG). The balance of the study will involve obtaining necessary concurrences of the recommendations and preparing a report.

BRIEFING SCHEDULE FOR VITAL AREA COMMITTEESession 1 - May 21, 1985, 10:00 a.m. Room 2242 Air Rights

- ^ Current practices for pre-licensing vital area reviews - NMSS
- ^ LANL vital area analyses - LANL
- ^ Vital area criteria for RER reviews - NMSS
- ^ Summary of Insider Rule - NMSS

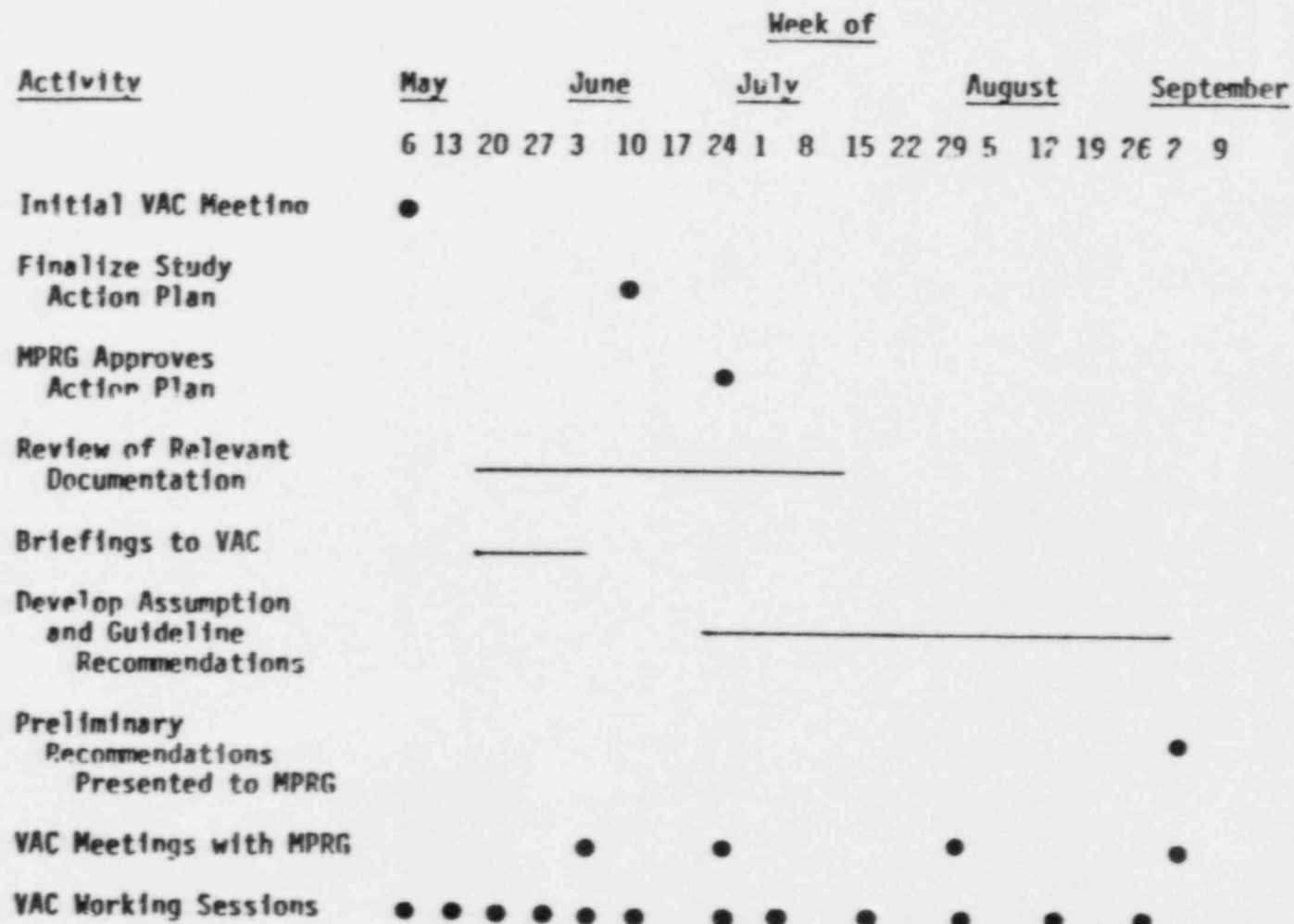
Session 2 - May 30, 1985, 9:00 a.m. Room P-422 Phillips

- ^ RES/LANL vital area study - LANL
- ^ Evaluation of current definitions and assumptions on vital areas - PPP/DSI
- ^ Appendix R, Fire Protection - NRR/DSI
- ^ Generic Issue A-29, "Nuclear Power Plant Design for the Reduction of Vulnerability to Sabotage - NRR/DSI
- ^ Vital area inspection program - IE
- ^ Vital area inspection program implementation and critique of current assumptions and suggested changes - Regions I & II

Session 3 - June 6, 1985, 9:00 a.m. Room P-422 Phillips

- ^ USI A-45, "Shutdown Decay Heat Removal Requirements" - NRR/DST
- ^ Review of "Precursor Studies of Risk Analysis of Several Known Safeguards Events" - RES
- ^ Review of "Nuclear Power Plant Damage Control Measures" - RES

Schedule For Initial Phase of Study



APPENDIX D

SUMMARY OF BRIEFINGS TO THE VITAL AREA COMMITTEE

In a series of 13 briefings delivered to the Vital Area Committee (VAC) between May 21 and September 12, 1985, NRC staff members and contractors from the Los Alamos National Laboratory (LANL) augmented the VAC review to determine what vital equipment and which vital areas in nuclear power plants required protection against radiological sabotage. Each of 11 briefings discussed an individual subject. Two of the briefings (Briefing 6 and 10) discussed 3 and 2 subjects, respectively. Each of the briefings is summarized below.

1. Current Practices for Vital Equipment/Area Reviews

D. Kasun (NMSS), May 21, 1985

This briefing gave the history of the review of vital equipment as defined in 10 CFR 73.2(i) and Review Guideline 17, which require that essentially all safety-related equipment be considered vital. Some of the early plans protected only Type I equipment and areas (those where a single successful act of sabotage could lead directly to a 10 CFR 100 release). Other plans did not identify LOCA-mitigation or emergency power as vital. Many plans did not specify onsite water sources as vital. Because of such variability in application of the guidance, NRC contracted with LANL in 1978 to perform a vital area program review.

From 1980 to 1983, NRC required applicants to follow Review Guideline 17, essentially without deviation, except that during this period, the staff accepted vital equipment designations approved prior to 1980 on first units for subsequent units at multi-unit sites.

Since June 1983, all plans for plants being licensed have been in full compliance with Review Guideline 17, which means that essentially all safety-related equipment is protected as vital. The SER is used to identify safety-related systems and components and applicants' plans are required to demonstrate that this equipment is located in vital areas.

Other relevant current practices require that barriers to vital areas be solid and substantial, and completely enclose the vital equipment. Seismic Category I reinforced concrete water tanks inside protected areas are accepted as is. Accessible openings are not permitted.

Devitalization of certain areas is permitted when the reactor is in the cold shutdown condition. However, the control room, containment, alarm stations, and emergency power, water, and RHR equipment necessary to maintain the reactor in a safe shutdown condition are not devitalized. The spent fuel pools are normally classified as vital areas.

2. Vital Equipment/Area Protection History and Assumptions

R. Haarman (LANL), May 21, 1985

The development of the Los Alamos National Laboratory (LANL) vital area program and its implementation were outlined. The SETS Code, developed by Sandia National Laboratory, and the generic fault trees were described. Both were developed for use in the vital area analysis program.

The LANL vital area analysis involves a preliminary detailed review of the FSAR. The site is then visited by a Los Alamos team for further specific review. The field data are reduced into computer input and used to tailor the generic fault tree to the site-specific data. A computer analysis is then conducted using the SETS and fault tree techniques to define the minimum equipment required to be protected as vital. After a review and check for accuracy and consistency, the results are submitted to the staff.

3. Vital Area Criteria for the RER Program

B. Mendelsohn (NMSS), May 21, 1985

The objectives of the Regulatory Effectiveness Review (RER) program were outlined. They are to: (1) validate the LANL vital area analysis, (2) assess implemented security system effectiveness, (3) assess contingency response capabilities, (4) assess safety/safeguards interfaces, (5) identify potential generic safeguards issues, and (6) validate the regulatory base.

The process of the RER involves a preliminary analysis of site data, followed by an onsite review and a documentation of the results. The post-review phase involves identification of needed changes to LANL finalization of draft vital area definitions, review by NRR and transmittal of the findings to the licensee for consideration and appropriate action.

Program concerns were identified with respect to the regulatory basis, i.e., the ambiguity of the 10 CFR 73.2 definition of vital equipment and the implementation of the minimum protection set under the current rule. The use of RER reports by licensees as bases for 10 CFR 50.54 security plan changes and the possibility of diminished security effectiveness if too much equipment is designated as vital equipment were also identified as program concerns. Suggestions for changes to the LANL vital area modeling assumptions were also made.

4. The Safeguards Insider Rules

P. Dwyer (NMSS), May 21, 1985

The components, access authorizations, pat-down search, and miscellaneous amendments of the current Safeguards Insider Rulemaking package were presented and discussed. The "vital island" concept also was discussed.

Some of the stated advantages of the vital island concept include: reduced obstacles to emergency access/egress and protection of co-located vital equipment using existing common barriers.

As a result of public comment and other considerations regarding the Safeguards Insider Rules, the following actions have been planned or taken: (1) the NUMARC proposal for an industry-regulated access authorization program is being considered by the Commission as an alternative to the rulemaking and (2) the vital island concept was deleted from the Miscellaneous Amendments pending completion of the vital equipment/area study and the recommendations of the Vital Area Committee.

5. The Vital Equipment Determination Research Study

P. Pan and A. Neuls (LANL), May 30, 1985

The categorization and status of the following 12 research topics were discussed.

- (1) Identifying individual safety-related cables
- (2) Disabling complete cable trays
- (3) Disabling systems needed during shutdown or refueling conditions
- (4) Disabling sensor systems, instrumentation and non-safety-related control systems
- (5) Treating spatially extended systems and components (i.e., piping, electrical distribution, and heating, ventilation, and air conditioning (HVAC) systems)
- (6) Scenarios involving air systems
- (7) Disabling electrical equipment by grounding or lifting of grounds
- (8) Relating best-estimate analyses of plant responses to systems failures to the corresponding Final Safety Analysis Report (FSAR) analyses
- (9) Effective inclusion of random events, such as anticipated transients, in fault-tree methodologies
- (10) Possible system failures after which stable hot shutdown cannot be maintained indefinitely
- (11) Considering the use of non-safety-related equipment, unanalyzed procedures, or operator ingenuity to recover from system failures
- (12) Reactor protection system vulnerability

Of these 12 research topics, LANL considers only the first one resolved. The LANL analysis of the cable identification assumption analysis included reviews of plant documentation and interviews of plant, construction, and vendor personnel at several operating plants. The results show that, with very few exceptions, the individual cables cannot be identified in cable trays, and that the issue of cable identification has no impact on current fault tree modeling of assumptions.

LANL is still reviewing the remaining eleven vital area topics.

6. (a) Current Definitions and Assumptions on Vital Areas
(b) 10 CFR 50, Appendix R, Fire Protection
(c) Generic Issue A-29, "Nuclear Power Plant Design for the Reduction of Vulnerability to Sabotage"

J. Wermiel and A. Singh (NRR), May 30, 1985

The discussion included an approach to identifying vital equipment which protects the reactor coolant pressure boundary and one train of equipment needed for achieving hot shutdown, assuming loss of offsite power. This approach was explained in the context of the 10 CFR 50, Appendix R, post-fire safe shutdown requirements, wherein hot shutdown is to be achieved independent of postulated fire damage in any plant area.

Additional considerations were discussed pertaining to vital areas, including: (1) Alternate or remote shutdown panels should always be considered as vital equipment since shutdown capability independent of the control room must be available and (2) when a vital component is inoperable for maintenance for longer than a few hours, a backup component should be available and temporarily protected as vital in order to maintain one train for shutdown at all times.

Generic Issue A-29, which is evaluating various system designs, plant layouts and safeguards alternatives for effects on reducing vulnerability to sabotage in new and old plants was also discussed.

7. The Vital Area Inspection Program

L. Bush (IE), May 30, 1985

The inspection procedures for identifying vital equipment/areas are primarily based upon the commitments contained in the licensees' security plans. The inspectors verify through onsite inspections that the equipment and areas designated as vital are afforded the level of protection required by the approved security plans and the regulations.

IE is in the process of developing a training program for regional inspection staff personnel in the methodologies used in the identifying vital systems, equipment, and areas requiring protection.

8. The Vital Area Inspection Program: Implementation and Critique of Current Assumptions and Suggested Changes

T. Martin and G. Smith (RI); K. Barr (RII), May 30, 1985

The various approaches to protecting vital equipment/areas taken by licensees in Regions I and II were discussed. The number of areas in nuclear power plants designated as vital ranges between 3 and 22. Enveloping areas with some compartmentalization are generally used. It was suggested that consideration be given to protecting only certain key vital areas in conjunction with use of the "two-man" rule.

Concerns were discussed about lack of consistency in identifying vital equipment/ areas at recently licensed plants. On a generic basis, Region II agreed with the vital island concept contained in the proposed Safeguards Insider Rules package. This approach, along with a more stringent access authorization program, would go a long way toward resolving the Region II concerns.

9. USI A-45, "Shutdown Decay Heat Removal Requirements"

A. Marchese (NRR), June 6, 1985

The specific objectives of this unresolved safety issue (USI) resolution program, which were outlined, include: (1) determination of the safety adequacy of decay heat removal in existing nuclear power plants for achieving both hot shutdown and cold shutdown; (2) evaluation of the feasibility of alternative methods for improving decay heat removal, including diverse alternatives dedicated to decay heat removal; (3) assessing the value and impact of the most promising alternative methods; and (4) developing a plan for implementing new licensing requirements for decay heat removal, including developing a comprehensive and consistent set of decay heat removal requirements.

Some general findings have revealed that co-locating redundant safety equipment and support systems in relatively large open compartments provides a variety of opportunities for adverse insider activities.

Some sabotage countermeasures were discussed, ranging from procedure changes and equipment modifications to independent decay heat removal systems. A summary of European experience provides evidence that, in the long run, it is more economical to construct an independent dedicated system than to make piecemeal changes throughout the plant.

10. (a) Precursor Studies of Risk Analysis of Several Known Safeguards Events

(b) Nuclear Power Plant Damage Control Measures

P. Ting (RES), June 6, 1985

Eleven safeguards events selected by NMSS were discussed from an accident sequence precursor standpoint to provide an estimate of the contribution of these deliberate acts to the susceptibility of operating power reactors to severe core damage.

All 11 events, as reported, were considered benign from the standpoint of potential severe core damage. Information concerning intent of the person causing each event is unknown, and hence the likelihood of additional deliberate acts as a part of each event cannot be estimated.

The main objectives of damage control measures for sabotage mitigation are: (1) to restore or maintain a functional capability and (2) to extend time available to restore a capability lost as a result of sabotage. Some of the damage control measures considered included using existing systems in normal or alternate modes of operation, i.e., required equipment in-place and system-level design changes. Conventional damage control measures were not considered.

Some examples of types of systems-level design changes considered for PWRs and BWRs include:

| <u>System</u> | <u>Modification</u> |
|--|--|
| High-pressure coolant injection (BWRs) | Modify for suppression pool feed-and-bleed cooling |
| Safety injection system (PWRs) | Cross-connect to substitute for AFW system |

Some conclusions drawn from the review of the research projects indicate that:

- (1) Damage control is not a stand-alone safeguards measure for sabotage mitigation but can be an effective part of an integrated safeguards system.
- (2) Many design features to facilitate damage control are not included in current plants.
- (3) Systems used for damage control must be protected as vital.

11. Equipment Requiring Protection Under Various Condition Assumptions

J. Wermiel (NRR); B. Mendelsohn and D. Kasun (NMSS), August 1, 1985

In support of the Vital Area Committee's evaluation of the current vital equipment/area analysis assumptions, supplementary briefings by NRR and NMSS staff were made in a number of areas related to system response to sabotage.

NRR identified the equipment in one train needed for hot and cold shutdown. For cold shutdown, only certain RHR-related equipment is needed beyond that required for hot shutdown. It was also noted that there is no difference between equipment needed to maintain hot shutdown for 24 hours and that required to maintain shutdown for 8 hours except for additional water supply.

NRR commented on the effects of total loss of all ac (station blackout) and dc power on the ability to achieve and maintain safe shutdown. The major impacts would be: inability to monitor plant status (loss of dc power), and inability to provide reactor coolant pump seal cooling and primary makeup (loss of ac power).

NRR stated that because of 10 CFR 50, Appendix R, fire protection requirements, licensees have catalogued and documented power, control, and instrumentation cable runs so that those associated with vital equipment are more readily identifiable than was the case before the Appendix R requirements existed.

Finally, NRR indicated agreement with the assumption that a loss of offsite power is the bounding transient with respect to challenge of safety systems in a PWR.

NMSS identified specific pieces of equipment requiring protection as vital in recently licensed PWRs and BWRs. These include auxiliary shutdown panels, even though they might not be safety-related, and vital water sources, including distribution systems.

NMSS also discussed the implications of station blackout to a 10 CFR 100 release following a sabotage event and reaffirmed that a source of 125-volt dc control power and 120-volt ac instrument power are assumed necessary for safe shutdown in the RER vital area validation program.

12. Selected Vital Equipment Assumptions

P. Pan and D. Cameron (LANL), August 8, 1985

LANL representatives cognizant of vital equipment-related technical assistance efforts sponsored by both NMSS and RES briefed and participated in discussions with the VAC on the rationale for implementing several of the currently used analysis assumptions. The following points were made regarding the assumptions discussed (see Appendix E).

- (1) Assumption on core melt - LANL's modeling assumes that the core must be kept covered with water and decay heat removal capability must be maintained to preclude core melt and an attendant 10 CFR 100 release.
- (2) Assumption on identification of cables in cable trays - LANL reiterated its earlier position that, on the basis of LANL studies, plant visits, and discussions with utility personnel, it is normally not possible to identify individual cables in cable trays. However, in satisfying 10 CFR 50 Appendix R requirements, licensees have prepared documentation that identifies cable routings and locations. Therefore, although a saboteur might not be able to identify a specific cable among many in a tray, the saboteur could know that a certain cable is found in a specific tray. It was noted that destroying or disabling of power, control, or instrumentation cables to vital components is unacceptable and, if such cables are determined to be vulnerable, they would have to be protected. It was also noted that by indiscriminately destroying an entire cable tray, the saboteur might also be eliminating cables necessary to the success of the act of sabotage.
- (3) The VAC-proposed draft assumption on disabling valves and other equipment - This is essentially covered by the assumption which states that if a saboteur gets into a single area, he or she can disable all equipment in that area. By making a few minor changes to the latter assumption, this one can be deleted. A related point was made concerning diversionary flow. That is, if a pipe that comes off a vital pipe line is destroyed and if a pipe that is destroyed is of significant size relative to the main pipe, essentially the main pipe has been destroyed.

- (4) Assumption on operating modes - Although in most cases, vital equipment identified for sabotage acts during full-power operation would include as a subset vital equipment needed for other modes, such as shutdown or refueling, this needs to be verified on a case-by-case basis to be sure. Also, it was noted that some licensees may devitalize certain components and systems during cold shutdown and refueling so that compensatory measures might be needed.
- (5) The VAC-proposed draft assumption on check valves - It was noted that all check valves should be considered invulnerable to sabotage from remote locations because: (a) check valves (except motor-operated) cannot be manipulated and, therefore, can be considered an integral part of the pipe, and (b) it is easier for a saboteur to achieve his/her purpose by destroying the pipe.

13. USI A-44, Station Blackout

A. Rubin (NRR), September 12, 1985

The Committee was briefed on the status of the Station Blackout USI, which involves loss of all offsite and onsite ac power, because of its relevance to identification of equipment and systems required to achieve and maintain hot shutdown.

The proposed technical resolution to this USI would require plants to cope with a loss of all ac power either for 4 or 8 hours, depending on the reliability of their power grid and their onsite emergency power supply. The critical items are the coolant pump seals, and licensees would be required to demonstrate that leak rates through the seals during the blackout period remain low enough to preclude core uncovering.

On the basis of this briefing, the Committee concluded that the results of these USI analyses, demonstrating self-sufficiency for at least 4 hours in the absence of any ac power, are relevant to the identification of equipment required to be protected as vital.

APPENDIX E
CURRENT LANL VITAL EQUIPMENT/AREA ANALYSIS ASSUMPTIONS

Current assumptions made by analysts at the Los Alamos National Laboratory about sabotage involving vital equipment and vital areas in a nuclear power plant include:

1. A 10 CFR Part 100 release is the successful sabotage criterion.
2. A significant core melt will probably lead to a breach of the reactor vessel and containment and subsequently will result in a 10 CFR 100 release, based on three modes of failure (see WASH-1400):
 - . steam explosion
 - . containment overpressure
 - . China syndrome
3. The use of explosives is included in the analysis. All types of explosives, including shaped charges, are assumed to be available to the saboteur, and the staff assumes the saboteur has the necessary skills to use them. The amount of explosives is assumed to be what can be carried on an individual's back.
4. The licensee cannot take credit for availability of offsite power. This assumption is based on the fact that offsite power is transmitted by facilities outside the protected area and hence, is completely vulnerable to outside assault. Note that there are scenarios in which it is to the saboteur's advantage to maintain offsite power and, in all these cases, the automatic scram features are included. Therefore, it is the NRC staff position that protecting these features as Type I Vital is adequate protection.
5. If the saboteur gains access to those areas where the reactor protection system (rod scram equipment) can be disabled, a fuel melt incident will occur. This assumption infers an initiating event that requires a plant scram. The vast number of areas where these initiating events can be caused has motivated the NRC to adopt the position that protection of the rod scram as Type I Vital obviates the need to protect those areas where the events can be initiated.
6. If a saboteur gets into a single area containing several pieces of equipment, he can disable all of the equipment in that area.
7. The saboteur is assumed to be knowledgeable of all scenarios, which infers that staff analysis is extremely conservative. However, there are some details of the plant that are not practical to determine or are too difficult to verify in the field, as the routing of cables in cable trays and conduit. It is usually difficult for maintenance personnel to identify cable runs. However, identification of terminal boxes and junction points is a practical task, hence cable junctions are identified in the analysis. Furthermore, there are scenarios for which the saboteur needs power to perform sabotage successfully, so the indiscriminate cutting of cables (hence the protection of all cable trays) would not be to the saboteur's advantage.

8. The code does not go into detail on exactly how the saboteur disables equipment; the code assumes the saboteur has sufficient knowledge of motors, pumps, motor control centers, etc. to disable the system.
9. The analysis is performed assuming the reactor is in the operating mode, and other conditions (such as shutdown and refueling) are subsets of the operating mode.
10. Check valves located inside the containment are considered "safe" from sabotage caused by a saboteur located outside the containment.
11. The saboteur cannot take credit for random failures or the concurrence of violent natural phenomena with sabotage; however, it is reasonable to assume the saboteur can take advantage of equipment unavailable on planned outages. Therefore, Technical Specification requirements for operation with minimum equipment are considered.
12. The licensee need only consider maintaining the plant at hot shutdown conditions. Primary system leaks are considered on a plant-specific basis.
13. Obviously, in many of the assumptions, certain judgments must be made regarding damage control measures that can be taken by the licensee on a site-specific basis; however, the NRC staff's guidance has been very conservative and does not usually permit the licensee damage control credit.
14. An important assumption made in determination of area boundaries is that for flexibility of analysis only, the staff considers any area that has four walls, a ceiling and a floor to be an area. Where motor control centers or electrical racks could be separately protected, they are also considered as areas.
15. Loss of all ac power (station blackout), plus loss of dc power for instruments and critical equipment, will lead to fuel melt (NMSS staff position).
16. A bounding transient (PWR) is considered to be loss of offsite power. This has been assumed to be the most significant transient in that it disables the reactor coolant pumps and shuts off feedwater to the steam generators. A comparison of transients in a plant probabilistic risk analysis showed that the equipment required to protect against this transient includes all, or nearly all, of the equipment demands of other transients. This places almost total reliance on mitigation systems (auxiliary feedwater) to remove the decay heat. On a generic basis, however, this transient places no demands on primary loop inventory control. A research group has been reviewing the needs for primary inventory control to protect against radiological sabotage.

APPENDIX F*

DISPOSITION OF COMMENTS RECEIVED ON THE DRAFT VITAL
EQUIPMENT/AREA GUIDELINES STUDY AND COMMENTS
RECEIVED ON THE DRAFT VAC REPORT

*Designated "Enclosure 2" in March 5, 1986 memorandum transmitting Vital Area Committee Final Report.

Disposition of Comments Received on the
Draft Vital Equipment/Area Guidelines Study

The draft VAC report was transmitted on October 21, 1985, with a request for comments to:

Director, Office of Nuclear Reactor Regulation (NRR)
Director, Office of Nuclear Materials Safety & Safeguards (NMSS)
Director, Office of Inspection & Enforcement (IE)
Director, Office of Nuclear Regulatory Research (RES)
Administrator, Region I (RI)
Administrator, Region II (RII)
Administrator, Region III (RIII)
Administrator, Region IV (RIV)
Administrator, Region V (RV)

In response to that request, comments were received from each addressee.

The original comments are attached as an appendix to this summary discussion of their disposition. The Vital Area Committee carefully considered each comment and the disposition of each comment is discussed below. Each comment was accommodated by modifying the report appropriately or a reason given for not doing so. The comments are referenced by the assumption number in the draft report, use of the abbreviations indicated above and the pages/items in the Appendix to this summary.

Assumption 1

Comment: Suggested that a definitive statement be made that the containment building, or drywell in a BWR, be vital. Also suggested that there may be a conflict between this assumption and assumption #11, which allows the saboteur multiple actions on all vital equipment in a single area. (RII, Page 2)

Response: We agree that, as a practical matter, protection of components of the primary coolant pressure boundary as vital would be accomplished by licensees protecting containments (drywells in the case of BWRs) as vital areas. Since this is a logical result of the assumption, a change in the assumption is not considered necessary.

There is no conflict with assumption #11 in that sabotage in a vital area is assumed to be precluded.

Comment: Stated that the steam generator tube walls are not considered a part of the primary system boundary and, therefore, should be explicitly included for protection as vital since steam generator tube ruptures may be indirectly caused by malfunctions in non-safety related systems. (RES, Page 12)

Response: The entire steam generator, including the tubes, are part of the primary system pressure boundary and protected as vital.

Assumption 2

Comment: Questioned whether the threshold of successful radiological sabotage should be lowered to meet 10 CFR Part 50.72 or 10 CFR Part 20.403 criteria instead of 10 CFR Part 100. (RIV, Page 8, Item 3)

Response: The 10 CFR Part 100 release threshold is conservative and appropriate, particularly since it is the same offsite dose threshold utilized in other accident evaluations.

Comment: Questioned whether the rationale that no credit for protective or mitigating capabilities of the pressure vessel and/or containment is appropriate, and whether they should be given the same credit as they receive in design basis accidents. (RIV, Page 9, Item 4a.)

Response: The standard for acceptable protection is prevention of a 10 CFR Part 100 release. Credit is given for anything within vital areas providing such protection, including the reactor vessel.

Assumption 3

Comment: Recommended that certain equipment be considered for addition to the typical list of equipment requiring protection. Also proposed that the words "continuously operable" be added to the assumption, or require two redundant trains of vital equipment since vital equipment in some plants (e.g., auxiliary feedwater pumps) may not be required to be operable by technical specifications. Further noted lack of an 8-hour diesel fuel oil capacity, which is a concern if the diesel is required to be vital. (RII, Pages 2 & 3)

Response: No additions have been made to the list of equipment in the assumption as it only provides examples of necessary equipment and is not all-inclusive. Assumption #7 covers the concern over the words "continuously operable" by requiring vitalization of a backup when any vital component is inoperable. The need for protection of an 8-hour capacity of diesel fuel oil will be resolved on a case-by-case basis depending on the reliance placed on the diesel.

Comment: Stated that some portions of decay heat removal systems may not be safety-related and thus not maintained operable. Also questioned reliance on a single train of vital equipment. (RIII, Page 5, Item 3)

Response: The decay heat removal systems to be utilized for sabotage protection are covered by the tech specs; therefore, their operability status is known and the systems are suitably maintained. Also refer to the response to the previous comment.

Comment: Pointed out the need for additional flexibility to implement changes in the vital areas required by this assumption based on differences in plants. (RIV, Page 9, Item 4b.)

Response: The assumptions will be applied on a case-by-case basis; therefore flexibility is provided.

Comment: Suggested that this assumption be made clearer and more definitive, and cited examples of concerns regarding implementation. (NMSS, Pages 14 & 15)

Response: More definitive guidance which addresses the specifics in the points raised here will be developed by the staff as part of the implementation plan for applying the revised vital equipment assumptions. The vital equipment selected by the licensees will be reviewed against this guidance on a case-by-case basis to confirm that it satisfies the assumptions.

Assumption 4

Comment: Questioned why the control room and associated cable spreading rooms were not identified as vital. Suggested that the one vital operable train for removing decay heat be capable of operation from the control room and not rely on local operation in normally unmanned remote vital areas. Cited an example. (RII, Page 3, Item 4)

Response: Assumptions #4 and #9 have been reworded to address the first part of this comment. As part of the decay heat removal capability for mitigation of a sabotage-induced transient, each licensee must address the means provided for starting and controlling required pumps. In the example cited, the licensee must demonstrate that a feasible and protected means of starting the turbine-driven auxiliary feedwater (AFW) pump is provided and can be accomplished in accordance with the revised assumptions. This might mean that the automatic start capability of the turbine-driven AFW pump will require protection as vital. This issue will be addressed on a case-by-case basis.

Comment: Suggested that some examples of locations from which vital equipment could be controlled or disabled be added to the assumption. (RV, Page 10)

Response: Assumption #4 has been reworded to address this comment.

Comment: Suggested that the word "disabled" may be more correct than "controlled" in the assumption. (NMSS, Page 15)

Response: Assumption #4 has been reworded to address this comment.

Assumption 5

Comments: Stated that assumptions #5 and #7 appear to contradict each other with regard to operating mode and equipment unavailability and that assumption #5 does not take into account multiple maintenance outages on vital equipment or unique valve alignment. (RII, Page 5, Items 1 & 4) Suggested that conditions other than the power mode be considered since sabotage during such conditions can cause a DBA or 10 CFR Part 100 release. Stated that much greater flow rates are required after shutdown than indicated in the rationale. Stated that rationale is misleading in that, under certain conditions, significant core damage can occur a long time after shutdown. (RIV, Page 9, Item 5) Suggested that assumption include "hot standby". (RES, Page 12)

Response: Revised wording of the rationale responds to the above comments.

Assumption 7

Comments: Stated that, based on experience, concurrent random failures should be considered with a sabotage event. (RII, Page 4) Recommended that redundant trains be protected as vital in order to avoid reliance on appropriate compensatory measures when vital equipment is unavailable. (RIII, Page 5, Item 5) Requested that the terms "appropriate compensatory measures," "radiological sabotage" and "single failure criteria" be further defined. (RIV, Page 9, Item 6) Questioned the assumption as not considering undetected failures and noted that not all Class IX accidents are of low likelihood. (RES, Page 12)

Response: These comments questioned the advisability of allowing for the protection of single train, given that 100% reliability of the protected train, if called upon in a casualty situation, cannot be assured. The Committee's view is that the recommended approach is consistent with NRC policy concerning the operability of important equipment. For example, fire protection requirements are predicated upon the assumption that any one train of equipment needed for safe shutdown will be available following a postulated fire. Similarly, Limiting Conditions for Operation (LCOs) allow continued operation for varying periods of time even though normally available redundant equipment is temporarily not available. While it is acknowledged that absolute reliability of the single protected train cannot be assured, the recommended approach is consistent with established policy. This matter was discussed with the Management Policy Review Group during a status meeting prior to completion of the Committee Report.

Suitable flexibility in required protection for one train should be permitted on a case-by-case basis. In practice, some plants may find it easier to protect redundant trains. However, it should be up to the individual plant to determine how protection for a secondary train will be achieved when the primary vital equipment is unavailable.

Assumption 9

Comments: Recommended that the cable spreading room be protected as a separate vital area. (RIII, Page 6, Item 6) Stated that the assumption may not be valid since IEEE Standards recommend cable identification. (RES, Page 12)

Response: Assumption #9 has been reworded to address these comments.

Assumption 10

Comment: Recommended that a design basis amount of explosives be specified. (RES, Page 12)

Response: Determination of which equipment needs to be designated vital is insensitive to the specific amount of explosives that individuals can carry in light of Assumption 11, which states that no credit is given for any equipment not located in vital areas. Implementation of the assumption to determine which equipment needs to be designated vital does not require the analyst to consider specifically how much explosives can be used by the adversary.

The goal was to bound the problem by characterizing an amount that could be carried, consistent with the design basis threat, without requiring a vehicle.

Assumption 12

Comment: Requested that a more specific definition of a 10 CFR Part 100 threat from the spent fuel pool be provided based on storage of other highly radioactive components/equipment in the pool. (RIII, Page 5, Item 2)

Response: Other than spent fuel, the VAC can identify no other components/equipment stored in the spent fuel pool which, when damaged, would cause a 10 CFR Part 100 release as defined for radiological sabotage.

Comment: Noted that safeguards staff might not be able to determine how long the spent fuel pool must be protected as vital. (RV, Page 10)

Response: The determination of required duration can be calculated on a case-by-case basis by the appropriate plant staff.

Comment: Recommended that the assumption be clarified by adding "following the start of a refueling outage" and by noting in the rationale that average environmental conditions can be assumed for the offsite dose calculations. (NMSS, Page 15)

Response: The assumption has been reworded as suggested. The Committee considered the suggested change in the rationale to involve an unnecessary level of detail.

General Comments

Comment: Recommended that the protection philosophy mention the need for protection of certain portions of the electrical power supplies and control and instrumentation for the one train of vital equipment. (RI, Page 1)

Response: The proposed addition was made to the vital equipment/area protection philosophy and analysis assumptions.

Comment: Suggested that additional flexibility may be required for implementing the protection philosophy. (RIV, Page 8, Item 1a) Suggested an additional section that addresses HTGR facilities. (RIV, Page 8, Item 1b.)

Response: Part a. The report provides for any implementation flexibility that might be required; no changes are necessary.

Part b. The report has been revised to state that HTGR facilities will be treated separately and that this report considers LWRs only.

Comment: Suggested a clarification with regard to protection of one or both trains, particularly if the status of one train is unknown. (RIV, Page 8, Item 2a.) Requested a better definition of a vital area. (Item 2c.) Requested that the revised report be provided for comments again. (Item 2 d.) Requested a better definition of "a set of important safety-related components". (Item 2e.)

Response: Item 2a. Assumption #3 does state that one train of equipment will be protected as vital. Assumption #7 has been reworded to address compensatory measures to assure that one train is always available as necessary.

Item 2c. This is defined in 10 CFR 73.2(1)(h).

Item 2d. The VAC has solicited, received and addressed comments on its draft report in accordance with the EDO's directive of May 1, 1985. Any further review of the report would be at the discretion of the EDO.

Item 2e. For clarification, additional safety-related components have been added to the assumptions as appropriate.

Comment: Certain assumptions result in vulnerabilities comparable to those in the design basis envelope, and therefore, lead to Class IX events. (RES, Page 11)

Response: Assumption #7 has been reworded to address this comment.

Comment: Requested that the report indicate whether or not credit could be given for feed-and-bleed in site-specific cases. (NMSS, Page 15)

Response: The implementation plan to be developed by the staff will indicate that credit can be taken for any means of decay heat removal (including feed-and-bleed) for mitigation of a sabotage-induced transient provided that (1) all necessary equipment for that means is protected as vital, and (2) an acceptable analysis demonstrating the adequacy of the proposed method in accordance with the revised assumptions is provided. This issue will be reviewed on a case-by-case basis.

Comment: Stated that further measures are needed to assure the equivalence of redundant protected trains. (IE, Page 17)

Response: Assumption #7 has been reworded to address this comment. The response to the comments on Assumption #7 also applies to this comment.

APPENDIX TO APPENDIX F



UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION I
631 PARK AVENUE
KING OF PRUSSIA, PENNSYLVANIA 19406
NOV 19 1985

MEMORANDUM FOR: Frank J. Miraglia, Chairman
Vital Area Committee

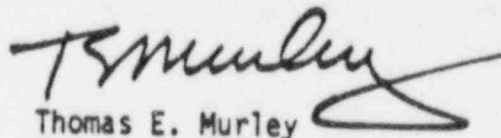
FROM: Thomas E. Murley
Regional Administrator, RI

SUBJECT: VITAL EQUIPMENT/AREA GUIDELINES STUDY -
VITAL AREA COMMITTEE DRAFT REPORT

Your memorandum of October 21, 1985, requested review of the subject report. We have completed our review and offer the following comments for your consideration.

We believe that the three premises which formed the basis for the protection philosophy are sound and that the objective of the study to develop a consistent, logical approach to identify vital equipment/areas for subsequent protection has been achieved. Further, the revised set of analysis assumptions appear to be well founded and support the vital equipment/area protection philosophy which is espoused. We note, however, that the statement of the philosophy fails to mention the need for protecting as vital, certain portions of electrical power supplies and control and instrumentation for the one train of equipment that will provide the capability to achieve and maintain hot shutdown. Finally, with regard to the conclusion concerning the impact of implementation on licensed plants, it is our view that these guidelines would be welcomed by licensees, since it should provide most licensees with the option of reducing the current number of vital areas.

Thank you for the opportunity to review the draft report. We found that it treated the issues very well and we support the Committee's efforts.


Thomas E. Murley
Regional Administrator

cc:
V. Stello, EDO
R. Burnett, SG
F. Gillespie, DRAO
J. Partlow, DQASIP
H. Denton, NRR
J. Davis, NMSS
J. Taylor, IE
R. Minogue, RES
Regional Administrators, RII, RIII
RIV, RV



UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION II
101 MARIETTA STREET, N.W.
ATLANTA, GEORGIA 30323

NOV 20 1985

MEMORANDUM FOR: Frank J. Miraglia, Chairman
Vital Area Committee

FROM: J. Philip Stohr, Director
Division of Radiation Safety
and Safeguards

SUBJECT: VITAL EQUIPMENT/AREA GUIDELINES STUDY
VITAL AREA COMMITTEE DRAFT REPORT
(REFERENCE: FRANK J. MIRAGLIA MEMORANDUM,
DATED OCTOBER 21, 1985)

The Region II staff has reviewed the reference memorandum in its entirety, while putting special emphasis on Section VI.A as requested. The following staff comments are provided as they relate to the proposed vital equipment/area protection philosophy and analysis assumptions:

1. Executive Summary

We concur with the philosophy of the Vital Area Committee (VAC) to protect as vital the reactor coolant pressure boundary and one train of equipment with associated piping and water sources that provide the capability to achieve and maintain hot shutdown, which would be provided on a case-by-case for each plant.

2. Assumption 1

This appears to require, as a practical matter, that the containment building, or drywell in a BWR, be vital, which appears necessary. We suggest that a definitive statement be made to that effect. Additionally, there seems to be a conflict between this assumption and assumption #11 which allows the saboteur multi-actions on all vital equipment in a single area. Assumption #1, on the other hand, protects a single piece of equipment and, contrary to the attributes of the design threat (use of explosives, para-military training, etc.) precludes the "insider" from causing a LOCA.

3. Assumption 3

We concur with the assumption and rationale. However, under the typical list of equipment the following additions should be considered:

- (1) Reactivity control - Boration capability, including control and boration source.
- (2) Decay heat removal - Power operated relief valves (Steam generator/PWR).
Suppression pool cooling (RHR suppression pool cooling mode/BWR).

CONTACT:
K. P. Barr
FTS 242-5612

NOV 20 1985

- (3) Process instrumentation - Source range flux instrumentation. Level instrumentation for all tanks used.
- (4) Reactor coolant makeup (PWR) - Charging pumps or high pressure injection pumps (pressurizer power operated relief valves may be required to reduce pressure to allow use of high pressure injection pumps).
- (5) Reactor coolant system pressure control - Charging pumps or pressurizer heaters (PWR). Safety relief valves or depressurization system valves (BWR).
- (6) Support functions - Diesel generator (PWR and BWR), fuel supply and tank.

Additionally, with respect to assumption #3, Region II proposes the words continuously operable be used or else require two redundant trains. Some of the equipment considered vital and used to hold in hot shutdown is not required by Technical Specifications to be operable at all times during full power operation. An example is auxiliary feed pumps. If only one of three installed auxiliary feed pumps becomes inoperable, typically power operation may continue. If that pump is the designated vital pump, sabotage protection is gone. One could put out special action statements on vital equipment but a better solution is to simply require one train to be continuously operable. The licensee would then probably make all redundant equipment in the opposite train vital. In any case we must ensure that at least a single operable train is available.

One problem that many plants have is they do not have an 8-hour capacity of diesel fuel-oil in the day tank in a vital area. This should be clearly required under support functions.

4. Assumption 4

Why not include control room and associated cable spreading rooms? Some licensees have the control room only vital but a single act of sabotage in the cable spread area can render the main control room blind and useless. Therefore, the cable spread rooms must be vital also. Possibly, this is covered under assumption 10, but we should be more specific.

As a related comment, the one vital operable train for removing decay heat should be capable of operation from the control room without an individual present in the normally unmanned remote vital area. As an example, some licensees now take credit for local manual operation of a turbine driven auxiliary feed pump. However, in the midst of a serious security intrusion, it is not clear that a member of the plant staff can get to the pump to operate it locally. Therefore, the equipment should be operable from the control room.

NOV 20 1985

5. Assumption 7

We cannot ignore previous experience that random failures do occur simultaneously with the reliance upon safety related equipment. The recent random failures of under voltage reactor trip assemblies at D. C. Cook highlight the random failures during operational emergencies. We believe that the same random failure possibility exists whether or not a sabotage event occurs.

While the above comments have been the result of Safeguards, Reactor Projects and Reactor Safety personnel, Ken Barr of my Safeguards staff is the Region II point of contact for this effort.


Philip Stohr



UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION III
799 ROOSEVELT ROAD
GLEN ELLYN, ILLINOIS 60137

NOV 15 1985

MEMORANDUM FOR: Frank J. Miraglia, Chairman, Vital Area Committee

FROM: Jack A. Hind, Director, Division of Radiation Safety
and Safeguards, Region III

SUBJECT: VITAL EQUIPMENT/AREA GUIDELINES STUDY - VITAL
AREA COMMITTEE DRAFT REPORT

As requested in your October 21, 1985 memorandum, we have reviewed the document on the above subject and have the following comments:

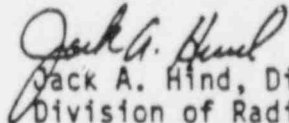
1. Page iii & iv - Assumptions 5 and 7 - These two assumptions appear to contradict each other. Assumption 5 states that only the power mode of operation should be considered while assumption 7 indicates that the unavailability of equipment may be exploited by the adversary.
2. Page iv - Assumption 12 - Many facilities store other highly radioactive components/equipment in the spent fuel pool which continuously poses a 10 CFR Part 100 threat to the public health and safety. A more specific definition of what constitutes a 10 CFR Part 100 threat from the spent fuel pool should be included as part of the report.
3. Page 17 - Assumption 3 - Some portions of the decay heat removal systems may not be safety-related equipment. The dependence on nonsafety-related equipment, which may not be adequately maintained, as the single train to maintain hot shutdown appears to provide a lesser degree of protection than if both trains were protected as vital.
4. Page 19 - Assumption 5 - The rationale, although logical, does not take into account multiple maintenance outages on vital equipment and/or unique valve alignments during maintenance/refueling outages that could be exploited to cause the reactor to drain in other than operation modes.
5. Page 21 - Assumption 7 - What will be "appropriate compensatory measures" to assure continuity of the hot shutdown capability? The description of compensatory measures used, on this assumption, appears to logically indicate that when the "primary train" is disconnected or taken out of service the "secondary train" then becomes "vital." We believe that this "floating" vital area concept could lead to an unacceptable level of risk.

NOV 15 1985

of system failure. Consequently, we recommend that the "secondary" system should continue to be protected as vital.

6. Page 23 - Assumption 9 - The cable spreading room presents a sabotage threat because "all" cables are located in this room and a "single" action could remove the entire control capability from the control room without the need to enter the control room at all. This room should be protected as a separate vital area.

Should you or your staff desire to discuss these comments, please contact D. A. Kers at FTS 388-5766 or J. R. Creed at FTS 388-5643.


Jack A. Hind, Director
Division of Radiation Safety
and Safeguards

cc: H. R. Denton, NRR
J. G. Davis, NMSS
J. M. Taylor, IE
R. B. Minogue, RES
T. E. Murley, RI
J. N. Grace, RII
R. D. Martin, RIV
J. B. Martin, RV



UNITED STATES
NUCLEAR REGULATORY COMMISSION

REGION IV
611 RYAN PLAZA DRIVE, SUITE 1000
ARLINGTON, TEXAS 76011

NOV 25 1985

MEMORANDUM FOR: Frank J. Miraglia, Chairman Vital Area Committee
FROM: Robert D. Martin, Regional Administrator, RIV
SUBJECT: VITAL EQUIPMENT/AREA GUIDELINES STUDY - VITAL AREA
COMMITTEE DRAFT REPORT

This is in response to your subject memorandum dated October 21, 1985. Members of my staff have reviewed the Draft Report and their comments are attached for your consideration.

We appreciate the opportunity to comment on this important matter. Should you have any questions regarding our comments, please contact either Doyle Hunnicutt, FTS 728-8137, or Larry Yandell, FTS 728-8108.

Robert D. Martin
Regional Administrator

cc:
H. R. Denton, NBR
J. G. Davis, NMSS
J. M. Taylor, IE
R. B. Minoque, RES
K. E. Murley, RI
J. N. Grace, RII
J. G. Keppler, RIII
J. B. Martin, RV

ATTACHMENT

COMMENTS ON VITAL EQUIPMENT/AREA GUIDELINES STUDY
VITAL AREA COMMITTEE DRAFT REPORT

1. Section VI. Study Results, entire section - General Comments
 - a. Additional flexibility may be required to implement changes that may occur or that may have significant impact on some utilities or one category of power plants (examples: NSSS for BWR vs. NSSS for B&W PWR).
 - b. This draft appears to address only light water cooled nuclear power plants. Should there be an additional section or paragraph that would address HTGR facilities? Should there be provisions for custom reviews of certain plants or plants under certain circumstances (examples: very poor performance histories, accidents and/or incidents that could easily have affected the health and safety of the public, and/or problems identified by the licensee or NRC)?
2. Section VI. Study Results, page 12.
 - a. Should clarify whether both trains or, as a minimum, one train must be available. Specify how to assure one train is available, if the other train status is unknown or not verified.
 - b. The assumptions and the rationale for these assumptions appear to be comprehensive and logically presented.
 - c. An improved definition of what constitutes a "vital area" is needed.
 - d. The revised edition of this draft should be presented for comments at the earliest date possible. It is assumed that the draft report will receive the standard publication and time limits as similar publications (NRC Commission, utilities, general public and other interested parties).
 - e. The philosophy of a set of important safety-related components should be more precisely defined.
3. Section VI. Study Results, page 14.
 - a. Should the threshold of successful radiological sabotage be lowered to meet 10 CFR Part 50.72 or 10 CFR Part 20.403, instead of 10 CFR Part 100?

Attachment (Continued)

4. Section VI. Study Results, page 16

a. Is the rationale that no credit for protective or mitigating capabilities of the pressure vessel and/or containment considered appropriate? Should this rationale permit same allowance as DBA or other acceptable standard?

b. Assumption 3 - same comment as 1.a. above.

5. Section VI. Study Results, page 19.

a. Other plant conditions can cause DBA and/or 10 CFR Part 100. The "vital areas" study should incorporate other postulated conditions.

b. The time period when large (several thousand gallons of water per minute) are required is not included as a significant item. The second paragraph of the RATIONALS could mislead some public reviewers with the indication that only a small quantity (less than 100 gpm) of water is required after about 24 hours shutdown time.

c. The statement at the end of the second paragraph, "There is a very limited time span during which any significant damage can be caused" is not appropriate and is very misleading. Significant damage can be caused for a long time (greater than a month) under specified conditions.

6. Section VI. Study Results, Page 21

a. The term "appropriate compensatory measures are required" should be further defined.

b. The rationale does not address fully the sabotage issue. The term "successful radiological sabotage" should be defined. A "successful radiological sabotage" could easily be panic caused by a small (Less than limits stated in 10 CFR Part 20) release with media and rumor inputs to the general public.

c. The rationale of "single failure criteria" should be further defined and covered in this document.



UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION V

1450 MARIA LANE, SUITE 210
WALNUT CREEK, CALIFORNIA 94596

NOV 8 1985

MEMORANDUM FOR: Frank Miraglia, Chairman, Vital Area Committee

FROM: D. F. Kirsch, Deputy Director
Division of Reactor Safety and Projects

SUBJECT: VITAL EQUIPMENT/AREA GUIDELINES -
VITAL AREA COMMITTEE DRAFT REPORT

The subject draft report, forwarded to Region V under cover memo, dated October 21, 1985, has been reviewed. Overall we find the study better than most we have read. It appears that the committee has developed a comprehensive and consistent set of recommended assumptions. If the intent is for the safeguards staff to use the proposed vital equipment/area protection philosophy and analysis assumptions without reactor safety staff holding their hands, then the following comments are in order:

Assumption 4:

Some examples would be helpful, e.g., remote shutdown panel, MCC, circuit breakers and local control stations.

Assumption 12:

It is clear to the reactor staff how to determine "long enough", but the safeguards staff have no idea of how to make that determination.

Should you have any questions, contact T. Young or D. Schuster at FTS 463-3853 or 463-3780 respectively.

Robert J. Pate Sr.

D. F. Kirsch, Deputy Director
Division of Reactor Safety and Projects

cc:
D. Schuster



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

NOV 8 1985

MEMORANDUM FOR: Robert B. Minogue, Director
Office of Nuclear Regulatory Research

FROM: Demetrios L. Basdekas
Electrical Engineering, Instrumentation & Control Branch
Division of Engineering Technology, RES

SUBJECT: VITAL EQUIPMENT/AREA GUIDELINES STUDY DRAFT
REPORT (RES-85-1933)

Bill Morris asked me to review the subject draft report and provide you with my comments with focus on Section VI.A "Proposed Vital Equipment/Area Protection Philosophy and Analysis Assumptions." I have reviewed the report and my comments are:

There are some good, prudent conservatisms contained in several proposed assumptions and they reflect the understandable concern about the issue of sabotage. A few assumptions, however, leave potential "windows of vulnerability" which, by and large, correspond to the imperfections of the design basis envelope, that may be responsible for Class IX events.

My primary concern on the issue of sabotage has been related to (1) an insider with knowledge of how the plant works and access to relevant engineering drawings and records and (2) the accessibility and design/operational characteristics of "control systems not required for safety", which nonetheless may have important safety implications considering the fact that, as a rule, have no redundancy or diversity and other desirable characteristics associated with safety grade systems. As an example, our review of the Oconee-1 control systems* has determined that certain failures in the Integrated Control System (ICS) "hand power" circuitry result in a core melt unless the operator correctly diagnoses the problem and takes corrective actions within 30 minutes. Considering the fact that the attention of the operator during such a sequence would be heavily taxed by a number of distractions, the chances of recovery may not be acceptable. If a knowledgeable "insider" further degrades the information available in the control room, he may be successful in a sabotage attempt. I do not know if the ICS "hand power" circuitry is located within a vital area or not. If it is, then the concern is taken care of by the proposed assumptions; if it is not, then it appears that we may have a safeguards problem in plants with such a design. This is just one example I wanted to use as an illustration of the problem. We should not assume that it is the only one.

* NUREG/CR-4047, Section 3.2.3.1 "Loss of ICS Hand Power."

Additional comments on specific proposed assumptions follow:

● Assumption 1

The steam generator tube walls are not considered to be part of the primary system boundary. This should be reconsidered in view of the fact that steam generator tube ruptures may be indirectly caused by malfunctions in not safety related systems.

● Assumption 5

It may be prudent to consider including "hot standby."

● Assumption 7

There may be a weakness in this assumption in that it does not consider undetected failures. Furthermore, the statement contained in the first sentence under "Rationale" p. 21 is not universally true. Not all Class IX accidents are necessarily of low likelihood.

● Assumption 9

This assumption is based in part, on the conclusion that "it is not possible to identify individual cables in cable trays." My understanding of our own identification requirements along with recommended industry practice, as recently codified in IEEE Stds 804/1983 and 603/1984 would indicate that this conclusion may not be correct, particularly for newer plants.

● Assumption 10

It is stated as part of this assumption that "The amount of explosives is assumed to be what adversaries can carry." This is too vague and a "design basis amount" could be specified.

I am well aware of the technical and policy related complexities of this issue and I believe that the Vital Area Committee performed a gallant attempt to address them. There is some room for important details to be addressed and I wish I had more time to delve into them with focus on the safeguards implications of control systems because of their obvious potential to affect the safety vector of the plant.

Finally, in reiterating my initial part of my discussion, Criterion 1 of Section II, Objectives, p.3, embodies the primary weakness of some of the proposed assumptions; namely, that it restricts their scope to "the design basis analysis of nuclear power plants." And we know that the design basis envelope has been repeatedly shown to have significant "windows of vulnerability."

One of my long standing recommendations has been to examine the sabotage aspects of control systems design, installation and maintenance. I hope sometime soon our resource availability will allow us to do that.

If I can help any further, let me know.

Demetrios L. Basdekas
Demetrios L. Basdekas
Electrical Engineering Instrumentation
and Control Branch
Division of Engineering Technology, RES



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

NOV 25 1985

MEMORANDUM FOR: Frank J. Miraglia, Chairman
Vital Area Committee

FROM: Robert F. Burnett, Director
Division of Safeguards, NMSS

SUBJECT: VITAL AREA COMMITTEE DRAFT REPORT

The following comments from my technical staff are submitted in response to your memorandum of October 21, 1985:

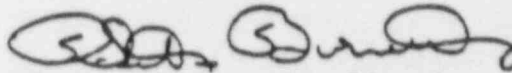
- ° It would be helpful if the Committee could make Assumption 3 clearer and more definitive, either in the assumption itself or in its supporting rationale. The rationale for Assumptions 3 and 4 in the October 1, 1985, memorandum from the Vital Area Committee (VAC) to the Management Policy Review Group (MPRG) anticipated that licensees' analyses and demonstrations in response to the Station Blackout (USI A-44) proposal would be available to aid in determination of what additional major components and associated support functions were necessary. Also, the VAC had discussed reasons why extensive service water piping would not need to be vital, but the draft rationale lacks guidance on this. It is suggested that some default positions be developed, and added to either the rationale or the assumptions, to provide guidance on the need for Reactor Coolant Pump (RCP) seal cooling and for support functions such as Heating, Ventilation and Air Conditioning (HVAC), service water piping, diesel generator fuel supplies, and DC battery duration. Whether conservative Final Safety Analysis Report (FSAR) analyses or best-estimate analyses are preferred for vital area decisions should also be addressed. The following are some examples the Committee may wish to consider:
 - ° Absent licensee analyses, restoration of RCP seal cooling within four hours of reactor trip will be assumed to be necessary to achieve the goal of Assumption 3.
 - ° Absent best-estimate analyses to the contrary, HVAC systems need not be protected as vital.

NOV 25 1985

- Absent analyses to the contrary, diesel generator cooling will be assumed essential for diesel generator operation.
- Pages 9 and 10 state that the study scope included credit for plant-specific features such as feed-and-bleed. It would be helpful if the report indicated whether or not credit could be given for feed-and-bleed in site-specific cases where the licensee has submitted an acceptable analysis that shows that it can be used to safely mitigate sabotage-induced transients.
- The period of time that the fuel pool needs to be vital and the degree of conservatism to be used in calculation of that time period could be clarified by changing Assumption 12 to read "following the start of a refueling outage" and by noting in the rationale that, in keeping with Assumption 7, average environmental conditions can be assumed for these calculations. (It is not likely for sabotage to be timed to coincide with extreme environmental conditions.)
- In the list of equipment in the Assumption 3 rationale, "auto start" and "condensate storage tank" (CST) should be deleted. Manual start can be acceptable and the CST is not always a vital water source.
- In Assumption 4, the use of the word "disabled" may be more correct than "controlled." If the location can be used to prevent licensee control of the equipment, that location need not be protected as vital. In some plants it would suffice to protect the location of the switch that transfers control from the control room to the remote shutdown panel. (The control room will, of course, be vital either way the assumption is written.)
- We recognize that the staff will have to develop an additional layer of guidance and acceptance criteria to implement the assumptions. Accordingly, they would appreciate any suggestions the Committee might have concerning their preliminary ideas as reflected in the following:
 - The VAC intended "reactivity control function" in Assumption 3 to equate only to reactor trip and to not mandate inclusion of other reactivity controls (such as safety injection through boron injection tanks).

NOV 25 1985

- In Assumption 9. "areas through which large numbers of cables pass" means only areas that are cable vaults or cable spreading areas for safety-related cables and does not require other areas in which redundant trains of safety-related cables may be located to necessarily be vital.
- Recommendation 1.c of the Safety/Safeguards Committee Report, NUREG-0992, is superceded by the new assumptions.
- Assumption 5 does not mean all vital equipment can be devitalized during cold shutdown.
- Other than as necessary to protect the primary coolant pressure boundary and one train of equipment for hot shutdown, no equipment within containments must be protected as vital (for example, equipment within the secondary containments for BWR's).



Robert F. Burnett, Director
Division of Safeguards, NMSS



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

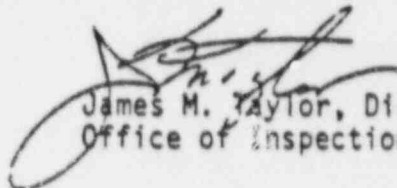
DEC 05 1985

MEMORANDUM FOR: Frank J. Miraglia, Chairman
Vital Area Committee

FROM: James M. Taylor, Director
Office of Inspection and Enforcement

SUBJECT: VITAL EQUIPMENT/AREA GUIDELINES STUDY-VITAL
AREA COMMITTEE DRAFT REPORT

This is in response to your memorandum of October 21, 1985 which requested comments/concurrence on the subject draft report. We have reviewed the draft report and agree with the overall philosophy to protect as vital the reactor coolant pressure boundary and one train of equipment to assure achieving and maintaining hot shutdown. However, in view of our experience with the performance of safety systems when called upon in a casualty situation, we believe that further measures are needed to assure the equivalence of redundant protected trains. This is particularly important since one of the assumptions upon which this philosophy is based is that random failures are assumed not to occur simultaneously with an act of radiological sabotage.


James M. Taylor, Director
Office of Inspection and Enforcement

Contact: R. Singh, IE
(x24149)

cc: V. Stello, EDO
H. R. Denton, NRR
J. G. Davis, NMSS
R. B. Minogue, RES
T. E. Murley, RI
J. N. Grace, RII
J. G. Keppler, RIII
R. D. Martin, RIV
J. B. Martin, RV
R. F. Burnett, NMSS
F. P. Gillespie, RES
J. G. Partlow, IE

APPENDIX G*

IMPLEMENTATION CONSIDERATIONS FOR REVISED VITAL
EQUIPMENT/AREA GUIDELINES

*Designated "Enclosure 3" in March 5, 1986 memorandum transmitting Vital Area
Committee Final Report.

Implementation Considerations For Revised Vital Equipment/Area Guidelines

The Committee considered various methods for implementing its findings, including rulemaking, Safety Evaluation Report (SER) staff positions, and follow-up staff reviews. The Committee's conclusions and recommendations with respect to these options are discussed below:

A. Rulemaking

No change in the rules is necessary to implement the assumptions because the definition of vital equipment now contained in 10 CFR 73.2(i) is broad enough to include the equipment that may be designated as vital under the Committee's assumptions. The very broad terms of the definition allow essentially any safety-related equipment or systems to be designated as vital. The Committee's assumptions fall within the scope of the current definition and protection of vital equipment based upon them would satisfy the standards of 10 CFR 73.55 and be acceptable.

B. SER Staff Positions

In the initial implementation of 10 CFR 73.55, applicants' and licensees' designations of vital equipment and vital areas were accepted in order to assure that functional security systems were in place promptly at operating reactors. However, the licensees and applicants were advised that the NRC staff intended to conduct a subsequent evaluation and analysis of those designations. Almost without exception, the SERs prepared in conjunction with initial security plan reviews contain language designed to place the licensee or applicant on notice that staff acceptance of the initial vital equipment and vital area designations was conditional. In the interim between the initial security plan reviews and the independent staff vital equipment and vital area evaluations for individual power plants, Review Guideline 17 (issued in January 1978) has been relied upon by the staff for approving security plans. Review Guideline 17 reflects a prudently conservative approach to security plan review warranted by the absence of more precise guidance. At the same time that Review Guideline 17 was being used as staff guidance for security plan reviews, Los Alamos National Laboratory (LANL) was tasked to conduct vital area studies which related directly to longer-range implementation strategy and are consistent with the staff's original position and intentions as expressed in the SERs.

C. Follow-Up Staff Confirmatory Reviews

As stated above, the NRC staff, through statements contained in the SERs, had advised licensees that it would conduct follow-up confirmatory vital area analyses at future dates. With contractor assistance from LANL, NRC compiled sabotage fault tree analyses to provide a technical basis for identifying the vital equipment (and areas) in each operating plant. What remains to be done is final verification of vital equipment locations and safeguards actually in place to determine what revisions, if any, are needed in each licensee's protection plans. This can be done effectively and efficiently in conjunction with the ongoing Regulatory Effectiveness Review (RER) Program. These reviews are currently scheduled at the rate

of 18 reactor units per year through early 1991. The schedule could be structured to assure that plants whose initial vital area analyses occurred early in the implementation phase of 10 CFR 73.55 are considered early in the RER follow-up confirmations.

The Committee considered the possibility of establishing a special staff capability in the Division of Safeguards to conduct vital area confirmatory reviews on an accelerated schedule. Experience has shown that three trained technical staff personnel, plus supervision and secretarial support, are required to perform 18 vital area validation reviews per year. This is the present capability. Any appreciable acceleration of the schedule would require a sizeable increase in staff. In view of this, and the fact that plants whose physical security plans were approved after 1979 generally satisfy the revised assumptions, the Committee does not believe that an accelerated schedule is necessary or advisable.

D. Implementation Recommendations

The following actions are recommended to implement the revised analysis assumptions:

1. Issue a Generic Letter to notify all power reactor licensees that the NRC has finalized its vital area assumptions. The Generic Letter will also point out that confirmatory analyses of licensee designations of vital areas, using the revised assumptions, will be accomplished through the Regulatory Effectiveness Review (RER) Program.
2. Continue the original plan to perform follow-up vital area analyses as stated in the SERs. These analyses will be done in conjunction with the ongoing RER program; each RER report will contain a vital area designation chapter for this purpose.
3. Provide licensees with the RER analyses, as they are completed, and request that proposed changes be made or that justification be submitted for not instituting changes required to conform with the revised assumptions. For reactor units where RERs have already been conducted (approximately 20), the staff will revise the vital area chapters of the RER reports where necessary, consistent with the final approved vital area assumptions and forward them to the licensees for their review and response as soon as practicable. Additional site visits by LANL should not be required to revise the RER reports, although in some instances, brief visits by staff may be advisable.
4. If backfit is appropriate at this stage, it will be treated in accordance with the backfit rule on a case-by-case basis. It is recognized that resulting backfits would be spread over an extended period. It cannot be stated at this time how many backfit actions would be required.

F. Follow-On Actions

A second level of licensing acceptance and review criteria will be developed to implement the recommendations of the Vital Area Committee Report. These criteria will be formulated by the NMSS staff and coordinated through appropriate management levels of NRR. NMSS will also revise and coordinate with NRR Section 13.6 of the Standard Review Plan (NUREG-0800) to incorporate by reference the new review criteria.

APPENDIX H*

PROPOSED GENERIC LETTER OF TRANSMITTAL FOR FINAL VAC REPORT

*Designated "Enclosure 4" in March 5, 1986 memorandum transmitting Vital Area Committee Final Report.

Generic Letter of Transmittal for VAC Report

TO: ALL POWER REACTOR APPLICANTS AND LICENSEES

SUBJECT: VITAL EQUIPMENT/AREA ANALYSIS GUIDELINES
(Generic Letter No. 86-)

Publication of 10 CFR 73.55 by the Commission in March of 1977 significantly upgraded the protection level of power reactors against radiological sabotage. By late 1979, physical security plans reflecting these regulations had been reviewed, approved and largely implemented for all power reactors operating at that time. However, because its position and guidance on vital equipment and area definitions were still evolving, the staff recognized that subsequent confirmation of its initial findings in this regard would be necessary and that changes might be required as a result of such confirmation. This recognition has been reflected in the staff's Safety Evaluation Reports to date by either the following or a similar statement: "The identification of vital areas and measures to control access to these areas, as described in the plan, may be subject to amendments in the future."

The staff has now formalized its guidance on the bases and analysis assumptions to be used in determining the equipment and areas which must be protected as vital in nuclear power plants. This guidance is identified and discussed in NUREG-1178, "Vital Equipment/Area Guidelines Study-Vital Area Committee Report," dated March, 1986. A copy of this report is enclosed for your information. We plan to use these guidelines in our confirmatory analysis of your currently-implemented vital equipment/area protection program. However, satisfaction of the requirements and assumptions of Review Guideline 17, issued in January, 1978 as an alternative to these guidelines, will continue to be acceptable. The results of our confirmatory analysis will be provided to you through the ongoing Regulatory Effectiveness Review (RER) Program. If your facility is among those which have already had an RER, you will be receiving the results of our confirmatory analysis as soon as practicable.

We believe that most of the nuclear power plants reviewed and licensed since January 1980, as well as some licensed earlier, will be found to satisfy the revised analysis assumption guidelines. Such licensees and applicants may, at their option, retain their current vital equipment and area designations or take advantage of the flexibility provided by the refined analysis assumptions. In the interim, we recommend that you review your vital equipment/area program with respect to the finalized guidance.

This letter is for information only and does not require any response. Should you have any questions concerning this matter, please contact Donald J. Kasun, Office of Nuclear Material Safety and Safeguards (301-427-4771).

Sincerely,

Victor Stello, Jr.
Acting Executive Director
for Operations

Enclosure:
As stated

| | | | | | | |
|--|--|--|--|-----------|----------|------|
| NRC FORM 335 (2-84) NRCM 1102, 3201, 3202 | U.S. NUCLEAR REGULATORY COMMISSION | 1. REPORT NUMBER (Assigned by TIDC, add Vol. No., if any) | | | | |
| BIBLIOGRAPHIC DATA SHEET | | NUREG-1178 | | | | |
| SEE INSTRUCTIONS ON THE REVERSE | | 3. LEAVE BLANK | | | | |
| 2. TITLE AND SUBTITLE | | 4. DATE REPORT COMPLETED | | | | |
| Vital Equipment/Area Guidelines Study: Vital Area Committee Report Final Report | | <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">MONTH</td> <td style="width: 50%; text-align: center;">YEAR</td> </tr> <tr> <td style="text-align: center;">March</td> <td style="text-align: center;">1986</td> </tr> </table> | MONTH | YEAR | March | 1986 |
| MONTH | YEAR | | | | | |
| March | 1986 | | | | | |
| 5. AUTHOR(S) | | 6. DATE REPORT ISSUED | | | | |
| | | <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">MONTH</td> <td style="width: 50%; text-align: center;">YEAR</td> </tr> <tr> <td style="text-align: center;">February</td> <td style="text-align: center;">1988</td> </tr> </table> | MONTH | YEAR | February | 1988 |
| MONTH | YEAR | | | | | |
| February | 1988 | | | | | |
| 7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) | | 8. PROJECT/TASK/WORK UNIT NUMBER | | | | |
| Office of Nuclear Reactor Regulation U.S. Nuclear Regulatory Commission Washington, DC 20555 | | 9. FIN OR GRANT NUMBER | | | | |
| 10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) | | 11a. TYPE OF REPORT | | | | |
| Same as 7a above. | | Technical | | | | |
| 12. SUPPLEMENTARY NOTES | | b. PERIOD COVERED (Inclusive dates) | | | | |
| 13. ABSTRACT (200 words or less) | | | | | | |
| <p>A study was conducted by the staff to (1) re-evaluate the guidelines and bases used to determine what are the vital equipment and areas to be protected against radiological sabotage in nuclear power plants and (2) to recommend revised guidance. On the basis of this study, the staff has recommended a revised vital equipment/area protection philosophy: to protect as vital the reactor coolant pressure boundary and one train of equipment that would provide the capability to achieve and maintain hot shutdown. To implement this overall protection philosophy, the staff also has recommended new analysis assumptions or guidelines to identify the specific equipment and areas in each plant that require protection as "vital."</p> | | | | | | |
| 14. DOCUMENT ANALYSIS -- a. KEYWORDS/DESCRIPTORS | | 15. AVAILABILITY STATEMENT | | | | |
| <table style="width: 100%;"> <tr> <td style="width: 50%;"> Nuclear Power Plants Sabotage Vital Areas Vital Area Barriers </td> <td style="width: 50%;"> Physical Security Physical Modifications Vital Equipment </td> </tr> </table> | | Nuclear Power Plants Sabotage Vital Areas Vital Area Barriers | Physical Security Physical Modifications Vital Equipment | Unlimited | | |
| Nuclear Power Plants Sabotage Vital Areas Vital Area Barriers | Physical Security Physical Modifications Vital Equipment | | | | | |
| b. IDENTIFIERS/OPEN ENDED TERMS | | 16. SECURITY CLASSIFICATION | | | | |
| | | <i>(This page)</i> <u>Unclassified</u> <i>(This report)</i> <u>Unclassified</u> | | | | |
| 17. NUMBER OF PAGES | | 18. PRICE | | | | |
| | | | | | | |

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300

SPECIAL FOURTH-CLASS RATE
POSTAGE & FEES PAID
USNRC
PERMIT No. G-67

120555078877 1 1AN1RS11S
US NRC-OARM-ADM
DIV OF PUB SVCS
POLICY & PUB MGT BR-PDR NUREG
W-537
WASHINGTON DC 20555