DETAILED RESPONSES RECEIVED FROM SD

7812270390

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

DEC 4 1978

MEMORANDUM FOR: Harold R. Denton, Director, NRR

FROM: Robert B. Minogue, Director, SD

SUBJECT: REVIEW OF REGULATORY ACTIONS AND STAFF POSITIONS WHICH RELY ON WASH-1400

We have surveyed the OSD staff to identify those regulatory actions or staff positions that have used or referred to the risk assessment models and results of WASH-1400 since its issuance in August 1974. The results of that survey are listed in Enclosure 1 by Division and Branch in OSD to facilitate review. In our assignment of categories to these actions we have taken the "licensing process" to be synonymous with the regulatory process. We have also taken "value of accident risk" as synonymous with value of accident consequence.

In addition to the items described in Enclosure 1 we have received a detailed analysis of the use of WASH-1400 in NRR actions from one of our employees who was formerly in NRR, E. Marinos. His analysis is provided as Enclosure 2 for your use.

Copies of the documents referred to in Enclosure 1 are also attached as requested.

Robert B. Minogue

Robert B. Minogue, Director
Office of Standards Development

Enclosures: As stated

Staff Review of the Extent to Which Licensing and Other Regulatory Actions or Staff Positions Have Relied on the Risk Assessment Results and Models of WASH-1400

1. SHSS

(a) (Category 1) Safeguards Standards Branch used WASH-1400 to provide an estimate of the consequences of sabotage. However, R. Jones states that the decisions to implement Reactor Sabotage regulations were based not on the WASH-1400 results but rather on the knowledge that sabotage could cause releases that would be harmful to the public. WASH-1400 is referenced in:

(1) "Safety and Security of Nuclear Power Reactors to Acts of Sabotage," SAND 75-0504 Sandia Laboratories, March 1976,

(2) Memo R.B. Minogue, thru L.V. Gossick to Ben Huberman, Director of Policy Evaluation transmitting a discussion of design threat levels entitled "Basis and Rationale for Selections of a Design Threat Level for Power Reactors Sabotage Protection" prepared by SD staff, January 3, 1977,

(3) Transcript of the public hearings on the Material Access Authorization Program - "Rulemaking in the matter of 10 CFR Parts 11, 50, and 70, Docket Rm-50-7, July 10, 11, and 12, 1978."

2. DES

(a) (Category 2) SCSB - In denial of PRM 50-19, the calculated consequences of core meltdowns in PWR and BWR reactor were used to estimate the potential effectiveness of an evacuated containment to mitigate the effects of a Class 9 core meltdown accident. Risk assessment results and models (i.e., probability of the events) were not used.

(b) (Category 2) EMSB - The justification of the need for R.G. 1.139, "Guidance for Residual Heat Removal," is based in part on the WASH-1400 result that showed the probability of core melt due to system and equipment failures that result in the inability to remove fission product decay heat is higher than the probability of core melt in the event of a large LOCA. Additional bases for the regulatory position of R.G. 1.139 are provided in the discussion, and it is the view of the staff that the position would be unchanged if the WASH-1400 results had not been considered. (Note that as in the safeguards case (see 1.(a) above) the use of WASH-1400 results is a conservative action; i.e., the need for increased safety or improved safeguards is demonstrated.)

(c) (Category 3) EMSB - WASH-1400 estimates for fission product gap activity (Appendix VII) were used to affirm the use of R.G. 1.25 source terms in R.G. 1.89 to determine the radiation environment for qualifying electrical equipment. The more conservative source term of R.G. 1.25 was used in developing R.G. 1.89; hence, it is concluded that no reconsideration of the application of WASH-1400 is necessary.

(d) (Category 4) TPSB - The staff is presently reevaluating the effectiveness of existing transportation regulations in protecting the health and safety of the public. To a very great extent, that reevaluation is depending on quantitative risk assessment. There is, of course, little in common between reactor accident probabilities and transportation accident probabilities. But there is some similarity in accident consequences and post accident cleanup between the two. Therefore, the staff is using the consequence analysis portions of WASH-1400 in the transportation analyses. These uses are documented at this time in NUREG-0170 (Vol. 1) and a Sandia contractor report SAND 77-1927. The Sandia report is a precursor of a staff environmental statement.

The staff use of quantitative risk assessment in general, and WASH-1400 material in particular has been cautious and critical. Some aspects of the staff's questions on the validity of this risk assessment are addressed specifically in the overall summary and conclusions of NUREG-0170 (Vol. I, p. ix). The use of WASH-1400 material was sufficiently critical so that, in our view, no reconsideration is needed. I should point out that no rulemaking action has yet been taken on the basis of these risk assessments.

Enclosure 2

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

NOV 16 1978

MEMORANDUM FOR: Guy Arlotto, Director, Division of Engineering Standards

FROM: E. C. Marinos, Reactor Systems Standards Branch

SUBJECT: REVIEW OF REGULATORY ACTIONS AND STAFF POSITIONS WHICH RELY ON WASH-1400

The attached information is transmitted pursuant to the request for more detailed identification of licensing actions and staff positions (relied on WASH-1400) for which I have knowledge,(memorandum from D. F. Sullivan to G. Arlotto dated November 9, 1978).

The licensing actions and staff positions identified in Enclosure (I) were applied to plant reviews conducted during my assignment in NRR, until December 15, 1976. I have no knowledge of the present NRR staff plant review practices.

Enclosure (II) is a list of references to documents where licensing actions and staff positions are identified.

E. C. Marinos
E. C. Marinos
Reactor Systems Standards Branch

Enclosures: As stated

cc w/encl:
R. Minogue
H. Denton
W. Morrison
D. Sullivan
D. Bunch

REGULATORY ACTIONS AND STAFF POSITIONS WHICH RELY ON WASH-1400

Technical Issue	References
1. Pump Flywheel Missiles Generated by Reactor Coolant Pump Overspeed	Ref. 1, pg 1082, item 4.1.3 and pg 1136, item 4.4.B.
2. Separation of Electrical Equipment	Ref. 1, pg 1085, item 4.1.4.
3. Common Mode Failures	Ref. 1, pg 1132, item 4.4.A.
4. Electrical Power Grid Stability and Effects on Accident Consequences from Grid Frequency Degradation	Refs: 1, pg 1170, item 4.4.O; 3, Issue No. 9 and Issue No. 10; 5, pg 690 and pg 715.
5. Turbine Missiles	Ref 1, pg 1173, item 4.4.P.
6. Relationship Between Required Seismic Qualification of Safety Equipment and Actual Earthquake Response Spectra	Ref 1, pg 1178, item 4.4.Q.
7. D. C. Power Supplies in Nuclear Power Plants	Refs: 2; 7, Task A-30; 1, pg 1145, item 4.4.E.
8. Treatment of Non-Safety Grade Equipment in Evaluations of Postulated Steam Line Break Accidents	Refs: 3, Issue No. 1; 5, pg 690 and pg 715.
9. Loss of Offsite Power Subsequent to Manual Safety Injection Reset Following a Loca	Refs: 3, Issue No. 4; 5, pg 690 and pg 715.
10. Analysis of Postulated Reactor Coolant Pump Rotor Seizure Incidents	Refs: 3, Issue No. 5; 5, pg 690 and pg 715.
11. Protection Against Single Failures in Reactivity Control Systems	Refs: 3, Issue No. 6; 5, pg 690 and pg 715.
12. Passive Failures Following a Loss-of-Coolant Accident	Refs: 3, Issue No. 7; 5, pg 690 and pg 715.

Technical Issue	References
13. Use of Probabilistic Assessment of Reliability	Refs: 3, Issue No. 8; 5, pg 690 and pg 715.
14. Interpretation of GDC 19 "Control Room"	Refs: 3, Issue No. 11; 5, pg 690 and pg 715.
15. Load Break Switch (Generator Breakers)	Refs: 3, Issue No. 12; 5, pg 690 and pg 715; 6, pg 416 thru 423; 11; 12, pg 8-1 and Appendix E; 14.
16. Overpressurization	Refs: 3, Issue No. 15; 5, pg 690 and pg 715.
17. Passive Mechanical Valve Failures	Refs: 4, Issue No. 17; 5, pg 690.
18. Onsite A.C. Emergency Power Supply	Refs: 1, pg 1145, item 4.4.E; 8; 9, BTP 2, pg 8A-2; 10.
19. Allowable Time Periods That Redundant Safety Equipment May be Inoperable	Ref. 1, pg 1148, item 4.4.E.
20. Reliability of Safety Systems in the Normal Environment and Post-Accident Conditions	Ref. 1, pg 1161, item 4.4.L.
21. Single Failure Criterion	Ref. 13.
22. Limiting Conditions of Operation for ECCS/ECI Components	Ref. 15.
23. Impact of Component Outages on ECCS Unavailability	Refs: 16, 17 and 18.

REFERENCES

1. Investigation of Charges Relating to Nuclear Reactor Safety: Hearing Before the Joint Committee on Atomic Energy Congress of the United States, 94th Cong. 2d Sess. (February 18, 23 and 24, March 2 and 4, 1976).

2. NUREG-0305 dated July, 1977 - Technical Report on D.C. Power Supplies in Nuclear Power Plants.

3. NUREG-0138 dated November, 1976 - Staff Discussion of Fifteen Technical Issues Listed in Attachment to November 3, 1976 Memorandum from Director, NRR to NRR Staff.

4. NUREG-0153 dated December, 1976 - Staff Discussion of Twelve Additional Technical Issues Raised by Responses to November 3, 1976 Memorandum from Director, NRR to NRR Staff.

5. Regulatory Commission's Safety and Licensing Procedures: Hearing Before the Committee on Government Operations of the United States Senate, 94th Congress, 2d Session (December 13, 1976).

6. Advisory Committee on Reactor Safeguards, 190th General Meeting, February 6, 1976.

7. NUREG-0410 dated January 1, 1978 - NRC Program for the Resolution of Generic Issues Related to Nuclear Power Plants.

8. Before the Atomic Safety and Licensing Appeal Board - In the Matter of Florida Power & Light Company (St. Lucie Nuclear Power Plant, Unit 2); NRC Staff Response to Applicant's Submittal of April 3, 1978.

9. NUREG-75/087, Rev 1 - Standard Review Plan.

10. Regulatory Guide 1.108, Revision 1 dated August, 1977 - Periodic Testing of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Power Plants.

11. Proposed Technical Position on Qualification of High Interrupting Capacity Power Generator Breakers - Memorandum for R. E. Heineman from E. C. Marinos dated October 26, 1976.

12. Safety Evaluation Report - McGuire Nuclear Station, Unit 1 and 2, dated March 1978, NUREG-0422.

13. Information Report by the Office of Nuclear Reactor Regulations on the Single Failure Criterion - Memorandum for the Commissioners, thru L. V. Gossick, from E. G. Case dated August 17, 1977.

14. Recommendation for Board Notification - Memorandum for D. Vassallo from F. Schroeder dated May 24, 1978.

15. A Quantitative Approach for Establishing Limiting Conditions of Operation for ECCS/ECI Components in Commercial Nuclear Power Plants - Science Applications, Inc.; Report No. SAI-78-649-WA dated June, 1978.

16. The Impact of Component Outages on ECCS Unavailability - Science Applications, Inc.; Report No. SAI-75-550-WA dated August, 1975.

17. Amendment to "Impact of Component Outages on ECCS Unavailability" Based on NRC Surry Power Plant ECCS Reanalysis - Science Applications, Inc.; Report No. SAI-76-536-WA dated May, 1976.

18. The Impact of Component Outages on ECCS/ECI Unavailability for an Operational RESAR-3 PWR - Science Applications, Inc.; Report No. SAI-76-622-WA dated July, 1977.

SAND75-0504
Specified External Distribution Only

Safety and Security of Nuclear Power Reactors to Acts of Sabotage

Prepared by Sandia Laboratories, Albuquerque, New Mexico 87115
and Livermore, California 94550, for the United States Nuclear
Regulatory Commission under ERDA Contract E(29-1)-789

Printed March 1976

Sandia Laboratories

Nuclear Fuel Cycle Programs

SF 2900 Q(7-73)

SAND75-0504
Specified External Distribution Only
Printed March 1976

SAFETY AND SECURITY OF NUCLEAR POWER REACTORS TO ACTS OF SABOTAGE

Prepared for the
United States Nuclear Regulatory Commission
Office of Nuclear Regulatory Research

by

Sandia Laboratories
Albuquerque, New Mexico 87115
Livermore, California 94550

ABSTRACT

A study has been made of the vulnerability of U.S. commercial light water reactor power plants to sabotage. The susceptibility of nuclear plants to sabotage and the consequences of a successful attack are compared with respect to other industrial and civil targets. Recommendations are given to further reduce the vulnerability of nuclear power plants to sophisticated sabotage threats.

CONTENTS

ILLUSTRATIONS

SAFETY AND SECURITY OF NUCLEAR POWER REACTORS TO ACTS OF SABOTAGE

1. Background

Commercial nuclear power plants are designed and operated to very high standards to protect against accidents. The plants include a variety of engineered safety features which provide additional protection against a radioactive release. Consequently, the risk to the public due to accidents caused by equipment failure or operator error is very low.[1] There remains the question whether consequences created by deliberate sabotage could contribute significantly to the public risk.

In 1968 the U.S. Atomic Energy Commission sponsored an appraisal of the potential hazard of industrial sabotage in nuclear power plants.[2,3] This appraisal, directed by Dr. C. Rogers McCullough, reviewed the history of industrial sabotage and examined the motivation and extent of knowledge likely to be possessed by various types of saboteurs. An assessment was made of the likelihood and possible consequences of a number of sabotage acts and the level of damage necessary to create a public hazard. It was concluded that, although sabotage with serious consequences to the public is possible in theory, the probability of occurrence was sufficiently low that no undue risk to the health and safety of the public existed.

Recent events indicate that: (1) terrorism has increased in many parts of the world, (2) terrorists are becoming more sophisticated, and (3) a greater variety of more complex targets are being attacked. This situation demands reconsideration of the vulnerability of various civil and industrial facilities to sabotage. Thus early in 1974 the Atomic Energy Commission began at Sandia Laboratories this study on the vulnerability of nuclear power plants to sabotage. This report summarizes the objectives, methodology, results, and recommendations.

2. Study Objectives

The objectives of the study are:

(1) Evaluation of the susceptibility of nuclear plants to sabotage for a broad range of threats,

(2) Determination of the consequences of successful sabotage,

(3) Comparison of the susceptibility and the consequences with sabotage of other industrial targets,

(4) Recommendations of means by which sabotage might be prevented or its consequences mitigated.

The likelihood of sabotage attempts in nuclear power plants was not estimated.

Principal emphasis is on sabotage which could produce levels of radioactivity constituting a hazard to the lives, health, or property of the general public. Sabotage which would cause only loss to the operating utility company was not evaluated.

3. Study Methodology

Two typical U.S. commercial nuclear power plants -- one having a pressurized water reactor (PWR) and the other having a boiling water reactor (BWR) -- were studied in detail. A number of other plants of both reactor types were visited and studied in order to identify plant-to-plant differences and to assure general applicability of the results.

The study methodology (see Figure 1) combines systematic analysis and empirical gaming to identify plant vulnerabilities and to determine countermeasures. Fault trees were developed to systematically inventory all combinations of sabotage actions that could lead to a radioactive release from the plant. Adversary study teams developed detailed sabotage sequences describing how sabotage operations might be accomplished. Differing amounts of information and plant access were afforded to the teams. The teams evaluated the resources required to accomplish sabotage and estimated their chances of achieving success. These results were analyzed to obtain a qualitative measure of the susceptibility of the plants to sabotage.

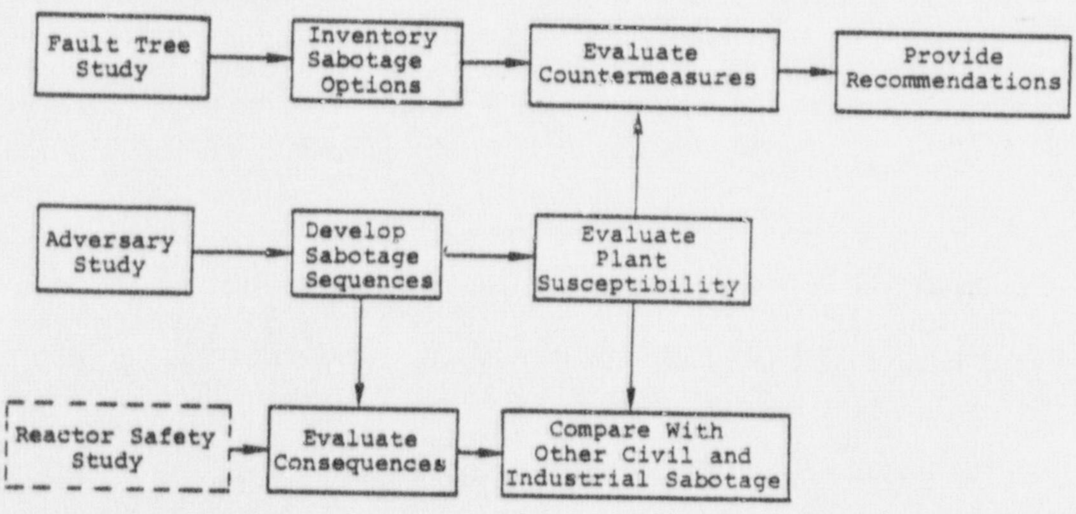

Figure 1. Study Methodology

The same combination of fault tree analysis and empirical gaming was employed to determine countermeasures to reduce the vulnerability of the plants to sabotage. The fault trees were analyzed to define conditions sufficient to prevent a radioactive release and to identify vital plant systems that should be protected. Measures to thwart sabotage were also formulated by members of the adversary teams by drawing upon their experience gained in determining how to penetrate the plant defenses.

The consequences of the sabotage sequences were estimated using data developed by the Reactor Safety Study. In order to place the study results in perspective, the adversary team members investigated the susceptibility of other targets to sabotage and estimated the consequences of an attack.

4. Study Results

4.1 Inherent Resistance of Nuclear Plants to Sabotage

The following characteristics of commercial nuclear power plants greatly increase the difficulty of releasing radioactivity by sabotage:

(1) The "defense-in-depth" concept of reactor plant design;

(2) The massive structure of the plant, which protects critical components from external attack;

(3) The safety design basis of the plant, which emphasizes system reliability, flexibility, redundancy, and protection against common mode failures; and

(4) Engineered safety features, which are added to the basic system to cope with abnormal operations or accidents.

As an example, in a commercial light water reactor plant, fuel containing the radioactive fission products is enclosed in metallic cladding and is located within a thick steel reactor vessel. The reactor vessel and coolant piping are located within a massive steel and concrete containment structure. Although, in part, the purpose of these multiple containments is to provide successive confinement of radiotoxic fission products, the containments may also serve as effective physical barriers against external threats.

Additional plant protection measures can be taken to supplement the inherent resistance of nuclear power plants to sabotage. These measures could be degraded by:

(1) Excessive dependence on perimeter security to provide sabotage protection; and

(2) Possible conflicts between safety and security in plant design and operation requirements, particularly in regard to access to vital components.

4.2 Susceptibility of Nuclear Plants to Sabotage

Acts of willful destruction occur in many industries. They may be caused by disgruntled employees during periods of discordant labor relations, by fanatics or extremists during periods of civil unrest, or by mentally deranged individuals. Such acts have rarely occurred at nuclear power plants. The sequences developed by the adversary teams and the systematic presentation of plant failure modes described by the fault trees jointly demonstrate that there is negligible chance that acts of willful destruction would result in release of radioactive materials.

Sabotage which might endanger the public could only be carried out by knowledgeable, capable personnel having a high degree of technical competence. Such an attack would require thorough planning in order to mount an effort coordinated to bypass the plant security system and to disable or destroy elements of several plant systems in the multiple plant defenses against a radioactive release.

4.3 Consequences

The elapsed time between the initiation of a sabotage-induced failure sequence and the actual release of radioactive materials varies considerably. For many credible sequences, such as long-term transient incidents, sufficient time is available after initiation for a plant damage control team to nullify or mitigate the consequences of the attack.

The Reactor Safety Study[1] developed methods to predict the magnitude of the radioactivity released and the public consequences occurring from random equipment failure and human error for various accident sequences. All sabotage options that have been identified lead to plant failure sequences that were included in the Safety Study. Therefore, sabotage cannot create consequences greater than those considered by the Safety Study.

Many factors influence the consequences: the sabotage option chosen, the operating status of the engineered safety features, the containment failure mode, the time and space variation of the wind and meteorological conditions, the site population distribution, and the extent of emergency response by on-site and off-site personnel. Control of all these factors is well beyond the capabilities of a credible sabotage operation. Evaluation of the probable consequences arising from the sequences developed by the adversary teams yielded values that are a small fraction of the maximum consequences considered by the Reactor Safety Study.

4.4 Comparison with Sabotage to Other Targets

Within the civil, industrial, and military sectors of our society are many potential targets for sabotage, which, if attacked, could result in public harm. To evaluate objectively the risk resulting from sabotage of a given target, the following factors must be known:

(1) The likelihood that sabotage will be attempted,

(2) The susceptibility of the target to sabotage, and

(3) The consequences of successful sabotage.

Reliable methods have not been developed for predicting the likelihood of attack. Thus, judgments of the seriousness of the threat must be based on perception and intuition. The latter two factors, susceptibility and consequences, are amenable to analysis. Qualitative comparisons of the relative susceptibility of various targets to sabotage and estimates of the consequences can be made. Such objective knowledge of the susceptibility of a target and the consequences of a successful attack are useful inputs in making subjective judgments of risk.

Nuclear power reactors appear far less susceptible to sabotage than most other civil or industrial targets. The technical requirements, planning, and necessary manpower and equipment are much greater for a credible sabotage attempt on a nuclear power reactor than are required for an attack on other potential industrial or civil targets. The probable consequences of successful sabotage of a power reactor are comparable to the consequences that could be produced by sabotage of many other targets. The lower susceptibility to sabotage attack of nuclear reactors reduces the likelihood of credible attacks being mounted by unsophisticated elements.

Figure 2 shows a qualitative ranking of the magnitude of susceptibility of various targets to sabotage, along with the magnitude of consequences of successful sabotage. For equal attack likelihood, targets listed near the upper right-hand corner (high susceptibility, high consequences) present the greatest risk.

CONSEQUENCES → / SUSCEPTIBILITY →	LOW	MEDIUM	HIGH
HIGH	NUCLEAR WEAPONS WARFARE CHEMICALS	DAM	WATER SUPPLY FOOD SUPPLY PUBLIC GATHERING
MEDIUM	NUCLEAR POWER REACTOR MUNITIONS DEPOT	PUBLIC BUILDING BRIDGE TUNNEL AIRPORT AND AIRCRAFT EXPLOSIVES	RAILROAD YARD AND TRAINS DOCKS AND SHIPS TOXIC CHEMICALS PETROLEUM AND NATURAL GAS
LOW	MILITARY BASE	BANK FOSSIL FUEL POWER PLANT	COMMUNICATIONS POWER TRANSMISSION

Figure 2. Comparison of Various Sabotage Targets

5. Recommendations

Recommendations have been developed to reduce further the susceptibility of nuclear power plants to sabotage. These recommendations fall into three categories: plant design, administrative control, and emergency planning.

5.1 Plant Design

In practice, sabotage protection as well as safety and operability considerations should be an integral part of nuclear power plant design.

Specific recommendations were developed for a PWR and a BWR nuclear power plant for plant design modifications to counter sabotage. The impact of these plant specific recommendations can be summarized by the following generic recommendations:

> Recommendation 1 - Systems* whose disablement, destruction, or misuse could cause a radioactive release, the immediate loss of reactor coolant, or the permanent loss of plant monitoring and control should be adequately protected by physical barriers, intrusion detection systems, and active response.

Examples are the reactor vessel and the control room. Protection of such systems should not be difficult since the safety-based design of the plant has already located these systems deep within the plant behind massive physical barriers.

> Recommendation 2 - Systems* required to provide recovery from short-term transient incidents which could lead to a radioactive release should be adequately protected by physical barriers, intrusion detection systems, and active response.

A flexible combination of physical protection and emergency plant damage control response (see Recommendation 7) is recommended to assure that transient incidents created by sabotage cannot lead to a radioactive release. Physical protection of some systems is required to prevent those transient sequences which might cause a release in times which are too short for plant damage control actions to be effective. Although these systems may be located throughout the vital area of the plants, they are highly redundant and are provided with great flexibility. Adequate protection of a required minimum set of these systems appears to require relatively minor plant modifications.

5.2 Administrative Control

Control of personnel access during shutdown, repair, or operation of nuclear power plants would preclude sabotage actions by unauthorized personnel. The

*Systems used here also denote plant features or areas.

specific recommendations that have been developed follow:

Recommendation 3 - Procedures should be developed to permit access to containment and other vital areas only by authorized personnel during shutdown, repair, or operation. Following every prolonged period of shutdown or repair, a methodical inspection of containment should be made by qualified personnel.

Recommendation 4 - Close supervision, by knowledgeable personnel, should be given to maintenance or repair being performed on equipment of vital systems or in vital areas.

Recommendation 5 - Only those persons who are required to operate, maintain, or inspect the reactor plant should be admitted to the control room.

Recommendation 6 - Plant tours for the general public should not be conducted in vital areas.

Recommendation 4 could have spinoff benefit in terms of increased plant availability and safety.

5.3 Emergency Planning

The final recommendation involves planning for emergency damage control actions which would be performed by plant operating personnel. A flexible preplanned response by trained personnel of the plant operating staff would be a very effective countermeasure against sabotage.

Recommendation 7 - Emergency plans should include a damage control team to provide effective response to acts of sabotage. Equipment required by the team should be provided and plant modifications implemented to provide features to expedite the use of the equipment. The team should be capable of restoring long-term emergency cooling to effect safe shutdown following sabotage attack.

6. Summary

Nuclear power plants have inherent resistance to sabotage due to their safety-based design and construction. A highly determined, knowledgeable, planned, and skillful effort would be required in order for saboteurs to circumvent plant security measures, create an initiating incident, and disable the engineered safety features in order to cause a radioactive release from the plant. Countermeasures involving plant design, protection systems, administrative control, and emergency planning have been recommended to provide increased protection against such sophisticated efforts.

7. References

1. Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, U.S. Nuclear Regulatory Commission, WASH-1400 (NUREG-75/014), October 1975.

2. C. R. McCullough, S. E. Turner, and R. L. Lyerly, An Appraisal of the Potential Hazard of Industrial Sabotage in Nuclear Power Plants, Southern Nuclear Engineering, Inc., SNE-51 UC-80, July 1968.

3. S. E. Turner, C. R. McCullough, and R. L. Lyerly, Industrial Sabotage in Nuclear Power Plants, Nuclear Safety, Vol. II, No. 2, March-April 1970, p. 107.

Distribution:

NRC/Office of Nuclear Regulatory Research
Division of Safeguards, Fuel Cycle and Environmental Research
J. S. Berggren
Washington, D.C. 20545 (100)

1000 G. A. Fowler
1200 W. A. Gardner
1230 W. L. Stevens
Attn: J. W. Hickman, 1233
1300 D. B. Shuster
1310 A. A. Lieber
1700 O. E. Jones
1710 V. E. Blake, Jr.
1730 H. H. Patterson
1750 J. E. Stiegler
4300 R. L. Peurifoy, Jr.
5000 A. Narath
5100 J. K. Galt
5120 G. J. Simmons
5400 A. W. Snyder
5410 D. J. McCloskey (100)
5420 J. V. Walker
5430 R. M. Jefferson
5440 H. D. Sivinski
8100 L. Gutierrez
8110 A. N. Blackwell
Attn: A. T. Jones, 8112
8300 B. F. Murphey
8320 T. S. Gold
Attn: R. L. Rinne, 8321
3141 C. A. Pepmueller, Actg. (5)
3151 W. L. Garner (3)
(ERDA/TIC) (SEDO)
8266 E. A. Aas (2)

OELD

NUCLEAR REGULATORY COMMISSION

IN THE MATTER OF:

Rulemaking in the matter of

10 CFR Parts 11, 50 & 70

Docket No. RM-50-7

Place - Washington, D. C.

Date - Monday, July 10, 1978

Pages 1 - 241

Telephone:
(202) 347-3700

ACE - FEDERAL REPORTERS, INC.

Official Reporters

444 North Capitol Street
Washington, D.C. 20001

NATIONWIDE COVERAGE - DAILY

level that we're concerned about.

DR. HALL: That's a bit of jargon. Would you say what part 100 release means?

MR. JONES: 300 rem to the thyroid, 25 rem to the whole body. That is not to say that a release less than that would not be hazardous.

DR. HALL: Let's go back.

This is a release greater than that which is imagined in the Safety Analysis Report?

MR. JONES: That is correct.

DR. HALL: Is this an accident, the magnitude of which would have been examined in WASH 1400?

MR.JONES: Yes. Although WASH 1400 did not address sabotage, it would have been.

DR. HALL: Did they make any comment about sabotage in that report?

MR. JONES: Yes, I believe they did make a comment in there to the effect that treatment of sabotage was a different situation with different probabilities and that they were not addressing them.

DR. HALL: Did they make any statement about the consequences of sabotage?

MR. JONES: I don't believe they did. I don't recall that they made any --

DR. HALL: Is that the feeling of the rest of the

panel?

Does anyone have a different view of that?

MR.JONES: I think WASH 1400 did not address sabotage consequences and make a comparison. I don't recall that. We can check that.

DR. HALL: I wish you would check that, because it is not part of this hearing record, of course,but I do remember hearing Dr. Rasmussen make some presentations and Sol Levine make some presentations of that report.

So, perhaps before, or sometime in this, if you have occasion, you might just verify it.

Carole, did you get an answer for your definition?

MS. FRINGS: Yes.

DR. HALL: In your testimony you mention that you would be exempting nonpower reactors if their inventory was less than the formula amount. Is that a correct statement?

MR. JONES: That's correct, yes.

DR. HALL: The University of Michigan asked some questions which I will paraphrase. These were submitted by Reid R. Burn. I don't know if you have them.

MR. JONES: Yes.

DR. HALL: And the questions really go to the problem of why is the quantity of material, the formula, an important consideration?

MR. JONES: The formula quantity, which is 2 kg's

Safety and Security of Nuclear Power Plants, Power Reactors to Espionage and Sabotage.

Would you summarize the conclusions of that?

DR. KNUTH: Yes, sir.

I have the report right in front of me. It is a fairly short report. It isabout 12 pages. If the Board please I can submit the entire report, have it Xerox'd for your consideration.

The general conclusion of the report is that the nuclear power plants as designed have an inherent resistance to sabotage. This is based upon the design of the plants, the defense-in-depth concept, massive structures of the plant which protect critical components; the safety design basis of the plant which emphasizes reliability, flexibility, redundancy and protection against common mode failures, and against safety features which are added to the basic features.

The results of this particular study conducted for the NRC indicate that the consequences and susceptibility for sabotage to nuclear power plants is on the low side of many other industrial targets.

And they also concluded in there that the consequences of sabotaging a nuclear power plant would be well within the small fraction of the maximum consequences considered by the Reactor Safety Study, WASH-1400, so-called. It's not only difficult to sabotage them, but the potential consequences

are low compared to many other industrial targets such as public buildings, bridges, tunnels, aircraft, so forth.

DR. HALL: Let me direct your attention to your testimony at page 5, the top of the page, where you refer to this; and then you use the word -- let me quote:

"As indicated the probable potential consequences" -- and I will stress the word "probable" -- what we are looking for is not the probable but the upper reaches; with that interpretation would you change the statement you made previously?

DR. KNUTH: Well, of course, the sabotage that gives you the highest consequences always is a poor number; and of course the Reactor Safety Study considered the number of core melt downs, those having higher consequences have a lower probability.

But this particular study did not try to attach a probability of sabotage to compare with the Reactor Safety Study. But the consequences of sabotage would be within the range of the Reactor Safety Study.

DR. HALL: Can you answer a question I asked the Staff earlier?

Did the WASH-1400 mention or discuss the sabotage problem?

DR. KNUTH: Yes, it did.

They did not, in WASH-1400, attempt to develop

probabilities of sabotage. Well, let me go back one step.

The general results of WASH-1400 showed that a core meltdown, one out of about every 150 core meltdowns, would result in something on the order of greater than 10 localities. The Reactor Safety Study did indicate that the potential consequences of sabotage acts would be within those considered in the Safety Study, they did not make any attempt to attach probability to a sabotage attempt. They just did not have the basic data to try to come up with probability numbers.

But there is a statement the consequences are within the scope of WASH-1400; yes, sir.

I believe that appears in the final appendices on responses to agencies' comments, such as the Union of Concerned Scientists, which raised this question; and in the final draft they addressed it.

DR. HALL: Yes, that confirms my memory, too.

CHAIRMAN VERKUIL: We would appreciate obtaining a copy of that report.

DR. KNUTH: Three copies for the record, sir?

CHAIRMAN VERKUIL: Yes, that would be fine.

MS. FRINGS: I have a question for Mr. Culp.

I believe on page 9 of your testimony you discuss the problem that industry really cannot afford to wait months for your people to be cleared. Could you please explain

OELD

NUCLEAR REGULATORY COMMISSION

IN THE MATTER OF:

Rulemaking, 10 CFR Parts 11, 50 & 70

Docket No. RM 50-7

Place - Washington, D. C.

Date - Wednesday, July 12, 1978 Pages 422-557

Telephone:
(202) 347-3700

ACE - FEDERAL REPORTERS, INC.

Official Reporters

444 North Capitol Street
Washington, D.C. 20001

NATIONWIDE COVERAGE - DAILY

and safety was also of concern. And we have addressed both issues in this proposed regulation.

DR. HALL: What are the consequences, then, which are contemplated in the licensing of a nuclear power plant? The national, maximum, consequences?

MR. JONES: The maximum consequence would be the core meltdown and the releases indicated in WASH-1400. I think Jim can address that.

MR. MILLER: I think the references to WASH-1400 were given earlier this morning and, of course, there are consequence tables. We are implementing the physical security as was mentioned I believe on Monday to prevent a sabotage event that could lead to a release of the magnitude of Part 100.

MR. HALL: You are saying physical security measures to prevent?

MR. MILLER: That is correct.

MR. HALL: So that even if there were an insider with evil intent he could not accomplish this?

MR. MILLER: That is the charter that is given in 7355, an insider is included in two different places; in 7355 (a)(1), wherein the insider assists in an active fashion and passive fashion to the external threat; and in 7355(a)(2) wherein he acts alone.

DR. HALL: So, then, the clearance program

DR. HALL: Let me go back then to this report. Is this report to be accepted that says an act of sabotage can be no greater than that which has been included in the envelope of accidents concerning the licensing?

MR. JONES: I believe I am correct that WASH-1400 is not the criteria for licensing reactors.

DR. HALL: Granted.

MR. JONES: All WASH-1400 says is that they have addressed the maximum occurrence, and a saboteur could not cause anything more than that. They are not saying that a saboteur could not cause that.

DR. HALL: I understand.

What is your, or the Staff's position, do you accept this report by the Sandia Laboratory as being reasonable and accurate?

MR. JONES: Yes.

DR. HALL: So that a saboteur could not cause an accident greater than that which is contemplated in the Safety Analysis Report?

MR. JONES: Right. Correct.

DR. HALL: Which is to say, I agree with you that it is implied he could cause at least that.

MR. JONES: Yes.

DR. HALL: But no more than.

MR. JONES: But no more than.

consequences be? Will there be an immediate hazard to people who live in a certain radius? Will there be a long-term possible disease impact upon people?

I really don't have any concept of what is going to happen?

MR. JONES: Both.

MS. FRINGS: Both? So, what sorts of things?

You know, I have read about, for example, as a consequence of an atomic bomb exploding, which is different?

MR. JONES: That is different.

MS. FRINGS: So, is it anything comparable? Or what other kinds of results would occur?

MR. JONES: The consequences are not quite as great or as great as an atomic bomb. Do you have data?

MR. MILLER: I think I would refer you to WASH-1400 and the consequence tables that are in that document.

DR.HALL: I don't think that is a part of the record.

MS. FRINGS: I realize that. I appreciate your referring to it; so that we can look at that so we do have something on the record for the benefit of the public who may not be looking at these documents?

DR. HALL: If you could --

MR. JONES: We will put it in the record.

DR. HALL: Excuse me, I think that would be very difficult -- and the Board, although I happen to be familiar

with nuclear materials, the Board as a majority is not. And to swamp the Board with the report of WASH-1400 would be just an unfriendly act.

(Laughter.)

MS. FRINGS: I would also submit that it is not just important for the Board to understand this. After all, this is a public hearing, and we are trying to advise the public what the consequences would be.

MR. LIEBERMAN: I was just going to add that the Executive Summary of WASH-1400 attempts, I think, to give some perspective on the question. It's not a very thick document, and that might be relevant.

The general question of the safety or the consequences of reactors is not something that can really be answered in, shall we say, twenty-five words or less. It really involves many considerations and many factors, and just to give a short summary here might really not do any of us a good service.

DR. HALL: You couldn't summarize Part 50 requirements?

MR. LIEBERMAN: We could certainly do that. Maybe Mr. Miller could speak to that.

MS. FRINGS: Before you get into that, let me just ask, is the Executive Summary written in laymen's terms or is it a technical document that only a scientist would understand?

MR. LIEBERMAN: I think it's understandable to a layman. That's the purpose of the Executive Summary.

MR. MILLER: Let's address the Executive Summary

for just a minute. The Executive Summary in the consequence area, postulating an event as you have postulated it -- maximum release, maximum sabotage event -- addresses factors such as immediate fatalities, latent fatalities, property damage from such things as contamination.

MS. FRINGS: You say it addresses them. Does it conclude that these things could occur?

MR. MILLER: It gives the exact numbers and dollar costs.

MS. FRINGS: Okay. That's the kind of thing I was interested in.

MR. MILLER: We will make those tables available from the report.

MS. FRINGS: I think that would be very helpful.

DR. HALL: Do you have any idea when you can make them available to us?

MR. LIEBERMAN: We can have it done by this afternoon or tomorrow.

CHAIRMAN VERKUIL: Is there any attempt to compare the consequences of other disasters?

MR. LIEBERMAN: That's in WASH-1400. They compare it to airplane accidents and other things of this sort.

CHAIRMAN VERKUIL: Could we extract that? I'm advised by the friendly act of my colleague here that we don't have to go into WASH-1400. Could you extract the

comparability data?

What we'd like to get a sense for is whether a similar kind of disaster could occur in a variety of other situations which would not be presumably subject to the same kind of protection you have sought.

MR. MILLER: Yes, I think most of that information is in Chapter 6, and we can supply it. It has things such as dam failures and consequences from fires and earthquakes, that type of information.

CHAIRMAN VERKUIL: That would be most helpful.

(The Board conferring.)

I wonder if we might just take a 5-minute break? We are hoping to close by around noon, as I understand this room has other uses. I believe we can. We'll take a short break now.

(Recess.)

CHAIRMAN VERKUIL: Let's reconvene, please.

MS. FRINGS: We will proceed by going into some questions on Issue 2, which is a discussion of the advantages and disadvantages of alternative programs to the screening program that has been proposed.

A couple of my questions will be based on things raised by other participants. I believe this question was raised by Westinghouse when they testified. They were making the point that the DOD and DOE programs require very

talked about the worst case, and that's what we're presenting here.

CHAIRMAN VERKUIL: I hate to get into this, but I can't avoid it.

(Laughter.)

After listening, it seemed to me that the case for application of the clearance rule is stronger now in research reactors and not in power reactors because of the fact that they're left out of the Sandia report and the fact that their physical protections are not evaluated as carefully. We now seem to be turning it on its head, because we started out leaving out research reactors, at least most of them, from the requirements of the clearance rule to begin with.

MR. MILLER: We still are. My understanding was we were talking about the higher powered research reactors, of which there are not that many.

CHAIRMAN VERKUIL: And those are the ones that seem to have, as I understand your definition, the most problems with respect to greater damage than had already been anticipated through the Sandia report or the WASH-1400 study.

The others at least were contemplated and have been dealt with in terms of risk, in terms of the safety risks that were already set aside from accidents.

MR. MILLER: May we separate the two different

things? WASH-1400 and the Sandia study that we're referring to only deal with power reactors. We cannot talk in the context of nonpower reactors in those two documents.

CHAIRMAN VERKUIL: Mr. Knuth, you introduced us to the Sandia report and requested a little time to discuss WASH-1400. Maybe it would be appropriate if you made your statement now.

No one has used the podium yet. Why don't you try it out.

DISCUSSION OF WASH-1400 BY DR. DONALD F. KNUTH, KMC, INCORPORATED.

DR. KNUTH: I just thought I'd like to make a few comments on WASH-1400.

WASH-1400 is a reactor safety study. It's a very voluminous study, using a number of man-years of effort to complete, and it looked at a number of events leading to accidents in commercial nuclear power plants.

The study took these events that could lead to core melts and looked at the equipment that would have to fail as a consequence of maloperation or just equipment failure, and it attached to that probability estimates that a particular event or sequence could lead to core melt.

The consequences that arose from any particular sequence of events were dependent to a high degree upon the various sequences that actually occured.

For example, a loss of coolant accident followed by failure of the core cooling system to eject water would lead to one set of consequences, and it would also have a set of probabilities associated with it that that could occur.

Another event that could lead to some core melt could be a reactor excursion by failure to scram. That could also lead to a core melt, having its consequences and having again its unique probability of occurrence.

What the study went on to do is to look at what would be the results of the most likely consequences of a core melt, and, as indicated by the staff, the most likely consequences for a core melt are fairly small. It would result in less than one fatality. It wouldn't result in any early fatalities, and the property damage is in the reports that the staff indicated they would give to you.

It went on to show also that approximately one in 150 core melts would result in consequences that could result in more than ten early deaths, and the associated latent effects and property damage and so forth are also listed in that report.

Looking at the other side of the coin, looking at sabotage, the general studies that have been made that can lead to core melt, the statements in the Sandia report, indicate that the consequences of core melt would be within

those studied in the reactor safety study.

Again in sabotage a number of chains of events are possible. A saboteur may elect to sever the primary coolant system. He may simultaneously breach the containment. A number of chains are possible.

What we've done in various studies in evaluating the consequence is to look at these various scenarios -- and there is almost an infinite array -- to determine what would a saboteur ha[illegible] to have in the way of skills to accomplish these vario[illegible] events.

[illegible]at we became convinced of is that it is very difficult for a saboteur to think through the events and to be able to sabotage sufficient equipment to cause high-consequence events, mainly because of the inherent safety design of the plant.

Not to say that it is not possible; it's just very difficult to do.

The problem we had in using WASH-1400 and trying to apply its methodology to [illegible]botage was to try to associate a probability with it. We just could not establish what the probability was that there was even a saboteur existing, or what would be the probability that a particular saboteur would pick a particular chain of events. As I say, it's almost an infinite chain. He could elect to destroy some equipment by shorting it out or what have you. What would

be the probability that an operator would detect it on a routine safety test and repair it or damage control measures in the event of that incident to mitigate the consequences? We just could not really establish the probability.

I think, in summary, the Sandia report, in discussing the various consequences -- if you will refer to page 9 of the report that I had entered into the record yesterday, there is a graphic table which attempts to establish what the consequences and susceptibility of sabotage in various industrial targets are. You will note that nuclear power plants, commercial power plants, fall essentially in the consequences they could have due to sabotage that is called medium consequences.

In that same category, a saboteur could arrive at the same consequences, whether you're talking in terms of cost in terms of lives sacrificed or in terms of dollar cost damage. He could sabotage public buildings, bridges, tunnels, airports and aircraft and so forth. There are other targets that would give even much higher consequences which would have even lower susceptibility should he choose to do so. And that is the context that I think has to be made clear, that sabotage of a nuclear power plant is difficult. The effect that it would have on the public health and safety is somewhat tenuous. It would take a very skilled saboteur to do it, and provisions are already in effect, were

placed in effect since these studies have been done. These studies were done prior to any implementation of access control and so forth that further reduce the susceptibility of plants to sabotage.

CHAIRMAN VERKUIL: Mr. Lieberman, did you have any question you might want to ask?

MR. LIEBERMAN: I just want to ask if any of the panel members have any comments to make to that.

(No response.)

DR. HALL: I'm sure, Dr. Knuth, you're not saying that because there is perhaps a greater risk from a dam that one should not take all reasonable precautions to protect a reactor power plant?

DR. KNUTH: No, sir, I'm not. I think the amount of protection provided has to be to provide reasonable assurance. I think we have achieved reasonable assurance.

I'm not suggesting that employees should not be screened for reliability. I think it should be done. The question is do you also need to have a full field background clearance for operators to go in and operate a plant, and I don't think that's necessary.

CHAIRMAN VERKUIL: Mr. Jones' observation--I think it's fair -- was that this report, or rather that WASH-1400 did not consider sabotage as an additional factor added on to accident. You say you can't calculate the probability of adding sabotage in in terms of how it might

increase risks.

DR. KNUTH: In the reactor safety study, you can have a sequence of events which lead to core melt and lead to high-consequence accidents. You can then take an engineering look at that sequence and say what is the probability that that would occur.

We know that diesels, for example, the probability that they may not start is 1 in 100. You can assign that probability. What's the probability that you lose offsite power? There are statistics to show what that probability is.

So you can take an accident-- not caused by some-one failing equipment but just occurs out of its pure orneriness -- and calculate what is the probability that this would occur. The probability then would be to an accident having certain consequences.

In the area of sabotage, you can make the statement that the consequences of core melt would not exceed those from a core melt induced by a similar method, but you cannot use the same methodology and say, "Now, what is the probability that a saboteur would be clever enough to use this particular chain?" That's where we run into difficulty. We couldn't even establish what the probability was that there was a saboteur lurking out in the real world, anyway.

I hope that helped.

CHAIRMAN VERKUIL: Thank you.

(Dr. Knuth excused.)

CHAIRMAN VERKUIL: Are there any questions for the panel?

MS. FRINGS: Mr. Miller, I would just like to see if I can understand the staff's reasoning here.

As I understand it-- we're all having communications problems, I guess -- when you license a reactor, as I understand it you are requiring that the reactor have a certain safety standard that would insure that, if an accident does occur, a certain maximum result or radiation release is the worst that could happen. Am I correct so far?

MR. MILLER: Right.

MS. FRINGS: Are you also saying that when you make that determination, you're licensing the reactor, you're only considering accidents; you're not considering sabotage?

MR. MILLER: Right.

MS. FRINGS: Now, is it true that it's the staff's opinion that consequences could be worse or could be more disastrous from an act of sabotage than from an accident? In other words, is it possible from an act of sabotage that you could have a higher radiation release or worst consequence than you could from an accident that might occur in that reactor?

MR. MILLER: No, I think Dr. Knuth stated that rather well, that as far as consequences are concerned, consequences could probably be no more than those established in WASH-1400.

MS. FRINGS: From an accident?

MR. MILLER: The type of accident that he was talking about, that's right.

However, where he did mention that there is some controversy is in the probability of a sabotage event.

MS. FRINGS: I did understand his point on that.

MR. MILLER: What we are saying is that 73.55 requires us and requires licensees to establish security programs -- I won't even call them physical security programs anymore -- to protect against an external threat and an internal threat.

In implementing that regulation, we are saying that the probability approaches 1 of an internal or external threat being there.

So let me again answer it: As far as the consequences are concerned, we agree that the consequences would be no more than WASH-1400.

DR. HALL: Did I understand you to say that there is a probability of 1 that there is a saboteur in each and every plant?

MR. MILLER: No, I did not mean that.

DR. HALL: I hope you didn't.

(Laughter.)

MR. MILLER: If I may, 73.55(a) says, and I quote. This is the General Performance Requirements:

"The licensee shall establish and maintain an onsite physical protection system and security organization which shall provide protection and high assurance against successful industrial sabotage by both of the following."

The first is external threat, perhaps aided by an internal threat, and the second is the internal threat.

CHAIRMAN VERKUIL: So you do not assign a probability to the sabotage factor?

MR. MILLER: No. We require that the onsite physical protection system and security organization provide protection against the threat levels. We do not say that the threat level is actually there.

MR. JONES: If I may try to communicate some more, WASH-1400 analyzed the probability of accidents causing a certain consequence. A sabotage event can cause that same consequence. Redundant safety systems are designed to prevent that accident from occurring. Security systems as we are proposing are designed to prevent that sabotage event from occurring, and in order to have the high assurance of prevention of that sabotage, we believe that we need

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

MEMORANDUM FOR: Harold Denton, Director, NRR
Saul Levine, Director, RES
Robert Minogue, Director, SD
Howard Shapar, Executive Legal Director
Clifford Smith, Jr., Director, NMSS
John Davis, Acting Director, IE

FROM: Lee V. Gossick
Executive Director for Operations

SUBJECT: REVIEW OF REGULATORY ACTIONS AND STAFF POSITIONS WHICH RELY ON WASH-1400

The Commission has requested (October 19, 1978 Chilk memo, attached) that the staff review the extent to which licensing and other regulatory actions or staff positions have relied on the risk assessment results and models of WASH-1400.

As a first step, you are requested to (a) survey your staff to identify those licensing and other regulatory actions or staff positions that have used or referred to the risk assessment models and results of WASH-1400 since its issuance in August 1974, and (b) have your staff provide a copy of all such documents to you. Examples of the documentation to be considered include hearing testimony, Regulatory Guides, Regulations, NUREG reports, generic issues, topical reports, and consultant or contractor reports.

Your survey should be sufficiently deep to reach all knowledgeable individual staff members in your office. Subtle as well as major reliances should be examined. Attention should be paid to past, present, and pending staff practices which led, or will lead, to regulatory actions or staff positions.

As a second step, each Office is requested to provide (1) a list identifying those actions or positions where WASH-1400 was used, categorized per Attachment 1; (2) copies of all documents identified by the survey; (3) your recommended actions and views as to whether, in view of the Lewis Committee recommendations, any of these actions or positions should be reconsidered; and (4) the effect of such reconsideration.

Please provide your response by November 20, 1978 to the Director of NRR who will coordinate the responses from a technical standpoint to highlight the most significant matters, check for consistency, and provide a report to my office by November 27, 1978. Please call Mr. Denton or Del Bunch of his staff if you have any questions. (Offices listed as cc's are requested to contribute to this review to the extent possible.)

(Signed) Lee V. Gossick

Lee V. Gossick
Executive Director for Operations

Attachments:
As stated

cc: Technical Advisor to EDO
Office of Administration
Controller
Office of International Programs
Office of Management & Program Analysis

ATTACHMENT 1

CATEGORIZATION OF LICENSING ACTIONS USING WASH-1400 VALUES AND METHODOLOGY

Category 1

Includes those actions in which an absolute value of accident risk as set forth in WASH-1400 was relied upon in the licensing process to make a specific licensing decision. Included in this category would be any reliance on an overall probability for core melting or on the probability of a given event sequence leading to core melt. A possible example is the use of the RSS to develop quantitative estimates of health risk from the coal and nuclear fuel cycles.

Category 2

Includes those actions in which the absolute values of accident risks of WASH-1400 were used in the licensing process, but when such use was restricted to relative comparisons of risks.

Included in this category would be any reliance on the overall probability of core melting of the RSS to draw comparisons between two design concepts. Possible examples are the use of the RSS to compare an FNP to a land based plant and the use of the RSS to develop perspectives on overall ATWS risks.

Category 3

Includes those actions in which the quantitative estimates or fault tree/ event tree analyses of WASH-1400 were used in the licensing process to illustrate or confirm staff conclusions on the disposition of a potential safety issue or to aid in selecting the preferred of several alternate regulatory requirements. One possible example is the NUREG-0138, Treatment of Non-safety Grade Equipment in Postulated Steam Line Break Evaluations.

Category 4

Includes those actions in which values of WASH-1400 were modified by staff to reflect different data base or experience and were then used in the licensing process.

A possible example is the adjustment of the RSS estimates of Scram unreliability in NUREG-0460.

Category 5

Includes those actions in which the event tree/fault tree methodology of WASH-1400 were used in the licensing process, but no reliance was made on the specific numerical estimates of WASH-1400.

Action - MPA/CON/ADM
Cys: Gossick
Dircks
Rehm
Denton
Levine
Davis
Minogue
Smith
Shapar
Shea
Ryan
Tucker
Hayden
Hanauer

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

OFFICE OF THE SECRETARY

October 19, 1978

MEMORANDUM FOR: Lee V. Gossick, EDO
Kenneth Pedersen, Director, OPE
James L. Kelley, Acting General Counsel
Carlton Kammerer, Director, OCA

FROM: Samuel J. Chilk, Secretary

SUBJECT: STAFF REQUIREMENTS - DISCUSSION OF RISK ASSESSMENT REVIEW GROUP REPORT, 10:40 A.M., FRIDAY, OCTOBER 13, 1978, COMMISSIONERS' CONFERENCE ROOM, D. C. OFFICE (OPEN TO PUBLIC ATTENDANCE)

The Commission requested that:

a. a draft NRC public statement be prepared which would address the Commission's current policy regarding the applicability and significance of WASH-1400 risk estimates, would indicate Commission acceptance of the Lewis Report, would indicate that the Commission is currently reviewing the use of risk assessment techniques within NRC to identify any necessary corrections, would address controversial issues associated with prior Commission statements regarding WASH-1400 and its Executive Summary, and would describe initiatives to be taken by the Commission and the NRC staff;
MPA (EDO/OPE/OGC) (SECY Suspense: Oct. 31, 1978)

b. a proposed response to Congressman Udall and other Congressional offices, as appropriate, be prepared regarding the Commission's position regarding the Lewis Report, including a description of initiatives to be taken by NRC as a result of the report's conclusions;
MPA (EDO/OGC/OPE) (SECY Suspense: Oct. 31, 1978)

c. a review be conducted of responses to Congressional correspondence to identify any NRC comments that may require revision in light of the Lewis Report;
(OPE/OCA) (SECY Suspense: Oct. 31, 1978)

d. an analysis be made of the implications of changing the Commission's previously enunciated position regarding WASH-1400 or any prior actions taken on the basis of WASH-1400 risk estimates;

MPA —— (EDO/OGC/OPE) (SECY Suspense: Nov. 15, 1978)

e. the staff should review the extent to which licensing and other regulatory actions or staff positions have relied on the risk assessment models and results of WASH-1400. The staff should review those actions and positions and state their views as to whether there should be continued reliance and the effect of discontinuing that reliance;

MPA, prepare ltr to staff for EDO —— (EDO) (SECY Suspense: Dec. 1, 1978)

f. an analysis be made of the impact of any program changes that might be necessary as a result of the Lewis Report on the Commission's FY 79 and 80 budget submissions; and

MPA/CON —— (EDO) (SECY Suspense: Nov. 15, 1978) WITS

g. an appropriate letter transmitting the Lewis Report to all prior recipients of WASH-1400 be prepared for the Secretary's signature. The proposed letter will be circulated for Commission concurrence prior to issuance.

ADMIN —— (EDO/SECY) (SECY Suspense: Oct. 31, 1978)

cc:
Chairman Hendrie
Commissioner Gilinsky
Commissioner Kennedy
Commissioner Bradford
Commissioner Ahearne
Director, OPA

[7590-01]

NUCLEAR REGULATORY COMMISSION

[Docket No. PRM 50-19]

CONNECTICUT CITIZEN ACTION GROUP, ET AL.

Notice of Denial of Petition for Rulemaking With Regard to Locating Nuclear Reactors Below Ground Level and Sealing Them in Heavy Vacuum Containments

On January 21, 1977, Louis J. Sirico, Jr., filed with the Nuclear Regulatory Commission a petition for rulemaking on behalf of the Connecticut Citizen Action Group, the Public Interest Research Group, Free Environment, the Iowa Public Interest Research Group, Citizens United for Responsible Energy, Iowa Federation of Women's Clubs, and the Good News General Store Cooperative, requesting the Commission to amend its regulations in 10 CFR Part 50, "Licensing of Production and Utilization Facilities."

The petitioners requested the Commission to amend 10 CFR Part 50 to require that:

1. Nuclear reactors be located below ground level; and
2. Nuclear reactors be housed in sealed buildings in which permanent heavy vacuums are maintained.[1]

A notice of filing of petition for rulemaking was published in the FEDERAL REGISTER on March 10, 1977 (42 FR 13365). The comment period expired May 9, 1977. Ten letters of public comment were received, none of which supported the petition.

In considering the petition, the Commission has reviewed existing studies on the subject, including a recently completed study which was initiated by the NRC in the spring of 1975 with Sandia Laboratories, the existing and alternative containment concepts, and an impact/value analysis of alternate concepts. The Commission has also reviewed the public comments which have been submitted.

Based on that review, which is summarized in Attachment A, the Commission does not believe that there is a sufficient basis at the present time for adopting Parts 1 and 2 of the petitioners' proposals, the effect of which would be to prohibit the licensing of any nuclear power plant which was not located underground and sealed in a heavy vacuum containment. In reaching that conclusion, the Commission is not adopting a position that underground siting or heavy vacuum containment designs could not meet present safety criteria. Rather, the position is that there is not sufficient supporting material to indicate that such designs should be made mandatory to the exclusion of all other nuclear power plant designs.

The use of heavy vacuum containments, whether above or below ground, will not ensure containment of a core melt accident, and will not appreciably increase the containment pressure retaining capability.

The Commission's review also indicated that whether a potential might exist for reducing the consequences from a Class 9 core melt accident by

[1] In addition, a third proposal in the petition, which has been separately handled, requests that a full-time Federal employee, with full authority to shut down the plant in case of any operational abnormality, always be present in a reactor's control room.

underground siting depends heavily on site-dependent parameters, plant layout, equipment design, and available technology in areas such as high pressure, rapid closing large diameter tunnel and shaft sealing systems. Accordingly, the NRC will review what further work may be appropriate on this subject, including any assurances which may be needed for consideration on a case-by-case basis of underground siting applications. This review is expected to be completed in about a year.

This conclusion not to change 10 CFR Part 50 applies to consideration of underground siting and heavy vacuum containments, both in combination as requested by the petitioners, and separately.

Therefore, in accordance with 10 CFR 2.803, the Commission has decided that sufficient reason does not exist to publish a notice of proposed rulemaking, and is hereby denying of Parts 1 and 2 of the petition. Some further explanation of the grounds for denial is set forth in Attachment A.

A copy of the petition for rulemaking and copies of the letters of comment concerning the petition are available for public inspection at the Commission's Public Document Room at 1717 H Street NW., Washington, D.C.

Dated at Washington, D.C., this 12th day of April 1978.

For the Nuclear Regulatory Commission.

SAMUEL J. CHILK,
Secretary of the Commission.

ATTACHMENT A

REVIEW OF PROPOSAL FOR UNDERGROUND SITING

Between 1958 and 1974 about a dozen feasibility studies were made on underground nuclear power plants. In addition, extensive bibliographies exist in these studies and in published articles which illustrate the extent to which this subject has been, and continues to be, discussed in the technical literature. The most recently completed study was initiated by the NRC in the spring of 1975 with Sandia Laboratories. The final study report was issued in August 1977.[1] Basically, the Sandia study concluded that there are other, more cost effective, alternatives to underground siting which would reduce direct atmospheric releases. The material and conclusions of this most recent report supplement and update the other, previously existing, studies.

Another separate study by the State of California on underground siting of reactors is in a developmental stage, and a final report is expected about April 1978.[2]

Upon reviewing the studies and articles available to date on underground siting, the following should first be noted:

1. The current NRC design requirement is that reactor containments be designed to withstand up to, and including, Class 8 Design Basis Accidents. Class 9 accidents, such as core melt, are not required because their probability of occurrence is so small that their environmental risk is extremely low.

2. Underground nuclear plants that were actually constructed are limited in number and their rated capacity ranges between 8.5 MW(e) to 266 MW(e). The experience gained from these plants is not necessarily applicable to present day base load plants of 1000 to 1200 MW(e). Large capacity underground plants may require major changes in design for equipments, such as condensers, pumps, penetrations and physical size and layout.

3. Actual experience with underground reactor siting has demonstrated operational concerns such as groundwater seepage; poor accessibility for inspection, maintenance or repair; corrosion of liners or structures, and resulted in some questioning of theoretical benefits. All three countries, Sweden, Switzerland, and France that have built underground nuclear power plants have continued to erect subsequent plants above ground. (Sample Comment: "Despite the experiences from the Plowshare program, the achievement of acceptable leak tightness following a class 9 accident in an underground plant appears to be doubtful because of multiple accesses and penetrations.")[3]

4. In spite of the numerous studies and articles on this subject, an actual, detailed engineering design for a proposed large commercial underground power reactor may be needed. As noted in one article,[4]

> * * * There are advantages and disadvantages with the siting of a nuclear plant underground, and the subject should receive greater attention in siting consideration, research and development. From the economic standpoint, there are many potential tradeoffs that will not be clear until a serious engineering effort will have taken place.

The petitioners' request that nuclear reactors be located below ground level does not identify for what specific reasons such action should be taken. Accordingly, the following assumptions have had to be made in order to be able to evaluate the proposal.

First, additional protection against, or reduction of, the risk from accidents up through Class 8 accidents (Loss of Coolant Accident) is one objective of proposing underground siting.

Second, additional protection against, or reduction of, the risk from Class 9 (core melt) accidents is another objective of proposing underground siting. Regulatory Guide 4.2,[5] in addition to defining a spectrum of Class 1 through 8 accidents, describes Class 9 accidents and their probability of occurring as:

> * * * sequences of postulated successive failures more severe than those postulated for establishing the design basis for protective systems and engineered safety features. Their consequences could be severe. However, the probability of their occurrence is so small that their environmental risk is extremely low. Defense in depth (multiple physical barriers), quality assurance for design, manufacture, and operation, continued surveillance and testing, and conservative design are all applied to provide and maintain the required high degree of assurance that potential accidents in this class are, and will remain, sufficiently remote in probability that the environmental risk is extremely low. For these reasons, it is not necessary to discuss such events in applicants' Environmental Reports.

In some cases, however, where measures can readily be incorporated into practical implementations of NRC criteria, the NRC has recommended design, or other, considerations based on parameters which are in excess of those calculated for a Class 8 LOCA. One such example is extending instrumentation ranges to be capable of reading containment atmospheric parameters at levels equivalent to those which would exist at estimated containment building structural limits—such as three to four times design pressure levels.

In considering the petitioners' proposal for underground siting as it relates to the safety of the public against design basis accidents up to, and including, Class 8 (LOCA), the following points need to be considered in addition to those already noted.

1. Present above ground containments are designed to contain the pressures and temperatures resulting from such accidents.

2. Since current containments are designed to withstand Class 8 (LOCA)

[1] Copies of the report, entitled NUREG-0255, "Underground Siting of Nuclear Power Plants: Potential Benefits and Penalties," August, 1977 may be obtained from The National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, Va. 22161, printed $9, microfiche $3.

[2] Copies of the report of the California Study on Underground Siting may be obtained after April 1978 from Energy Resources Conservation and Development Commission, 1111 Howe Avenue, Sacramento, Calif. 95825 (Publication Unit 916-322-3725).

[3] Discussion in Nuclear Safety, Vol. 16, No. 4, July to August 1975, pp. 434, 435, re: "Underground Nuclear Plant Siting: A Technical and Safety Assessment," by Crowley, Doan, and McCreath, Nuclear Safety, Vol. 15, No. 5, September to October 1974, pp. 519-534.

[4] Id.

[5] R.G. 4.2, revision 2, "Preparation of Environmental Reports for Nuclear Power Stations," issued April 1976.

pressures, if any releases of containment volume to the atmosphere were to occur either before, during, or after a Class 8 (LOCA) accident they would be directed, by plant design, through the elevated release point of the filtered ventilation system. Equivalent releases from underground containments would also have to be made from an above ground stack, and there would be a resultant release to the environment similar to that from an above ground containment.

3. Some advantages may be argued for the extra "hardening" of the facility which would result if it were below ground, such as protection against tornadoes, airplane crashes, etc. However, all of the disadvantages which result from the current state of the technology (or lack of it) of constructing and operating such plants below ground still apply.

While it thus seems clear that for accidents up to and including Class 8 LOCA accidents there is no present need for requiring underground siting, and that no identifiable potentially significant increase in safety to the public would result, this is not quite so clear for Class 9 core melt accidents. Current studies and experience indicate that whether a potential might exist for reducing the risk from a Class 9 core melt accident by underground siting depends heavily on site-dependent parameters, plant layout, equipment design, and available technology in areas such as high pressure, rapid closing, large diameter tunnel and shaft sealing systems.

In addition to these variables, the drawbacks of underground siting must be considered—in either a generic study, or consideration of a specific license application. Other design alternatives to underground siting, such as filtered atmospheric venting or compartment venting, appear to promise an equal measure of reduction of risk from a Class 9 core melt occurrence, and with lower costs.

Review of Proposal for Heavy Vacuum Containments

In reviewing this proposal, it is again necessary to make certain assumptions, since the petition is not explicit as to its rationale.

First, it is assumed that the intent of this proposal is to go beyond the current requirements for containment of LOCA-type accidents up through Class 8 accidents, and to require containment of a Class 9 (core melt) accident.

As noted in the underground siting discussion, such a design requirement is not a part of NRC regulations or policy. However, for purposes of reviewing the effectiveness of this proposal, it will be assumed that such a condition exists due to insufficient cooling of reactor core and containment with a resulting core meltdown.

Second, in the absence of a definition in the petition of what would constitute a heavy vacuum, it will be assumed that this level is about 1 psia, which is a practical technological limit and the level used at the Pickering CANDU reactors, which employ a vacuum building.[6] Also, 1 psia maximizes the potential benefits which could be postulated from the petitioners' proposal.

Third, the assumed design objective is to have containment walls and dome capable of remaining leaktight before, during and after core melt with respect to direct release of fission products, while assuming that the core will melt through the containment floor into the soils or rock on which the containment building rests.

In WASH-1400,[7] an analysis of core melt sequences, probabilities and consequences are presented in Appendix VIII, "Physical Processes in Reactor Meltdown Accidents" and its sub-Appendix E, "Containment Failure Modes Evaluations." Of interest in evaluating this proposal is the following information from those references:

	Current pressurized-water reactor (PWR)	Current boiling-water reactor (BWR)
	Pounds per square inch absolute	
Calculated class 8 accident pressure	56	56
Containment design pressure	60	71
Calculated containment failure pressure	100±15	175±25
Estimated class 9 accident pressure	~140	~250

When comparing the pressure reduction derived from the second assumption above with the WASH-1400 figures given above, it can be seen that the additional pressure margin provided by maintaining a 1 psia vacuum on current-day containments is very small. Heavy vacuum would reduce any accident pressure in the containment by about 14 psi. It is also apparent that the objective stated in the third assumption of avoiding direct release of fission products through the containment walls or dome under core meltdown conditions cannot be met by using a heavy vacuum containment. The pressure would still build to a level two to three times greater than the pressure for which the current containment structures are designed.

[6] "Vacuum Containment Systems for Multi-Unit Nuclear Power Stations" by E. W. Fee and G. E. Shaw, VII Congres International, "Le Confinement de la Radioactivite dans, l'Utilisation of l'Energie Nucleaire," Versailles, 28-31 Mai 1974, Societe Francaise de Radioprotection.

[7] WASH-1400 (NUREG-75/104), "Reactor Safety Study," October 1975.

To attempt to design the current generation of containments to withstand three times their current design pressures would be costly and would still be ineffective. Even if a stronger containment were built, the maximum result would be to permit the core to melt through the base mat before the continuing pressure buildup would otherwise eventually breach the containment structure. Also, increasing the containment building volume to limit the resulting pressures to a level resembling current design pressure levels would have the same drawbacks as the stronger containment concept.

The factor which will reduce the effectiveness of the heavy vacuum concept to contain core melt regardless of containment design pressure, is that the air pressent inside a containment which is under atmospheric pressure is a relatively minor contributor to the potential maximum pressure. The major contributors to the final pressure are the steam, hydrogen generated by the metal-water reactions, and non-condensible carbon dioxide generated by the action of the molten core on the concrete foundation mat. Removal of this air, therefore, would not significantly affect the post-accident pressure.

The Canadian CANDU reactor system at Pickering is mentioned in the petition as an example of a nuclear power plant employing a heavy vacuum concept. Some clarification needs to be made regarding this reference.

The Pickering type of vacuum system is designed to accommodate the same general type of accidents as our domestic reactors, i.e., up to and including Class 8 accidents as we would define them. It is not intended to be designed for, nor is it capable of protecting against, the direct release of fission products from the containment system following a core meltdown.[8]

Instead, a CANDU vacuum building has been constructed only when there are economic benefits to be gained by then being able to design the containment building for the lower pressure level which results from the post-accident pressure being shared by the containment and vacuum buildings. Therefore, on the basis of economics, a supplementary, common vacuum building has been employed only at multi-unit CANDU sites such as Pickering and Bruce.[9]

[FR Doc. 78-10382 Filed 4-18-78; 8:45 am]

[8] Id. No. 6.

[9] Id. No. 6.

U.S. ATOMIC ENERGY COMMISSION

November 1974

REGULATORY GUIDE

DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 1.89

QUALIFICATION OF CLASS IE EQUIPMENT FOR NUCLEAR POWER PLANTS

A. INTRODUCTION

Criterion III, "Design Control," of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50, "Licensing of Production and Utilization Facilities," requires that design control measures provide for verifying the adequacy of a specific design feature by design reviews, by calculational methods, or by suitable qualification testing of a prototype unit under the most adverse conditions. This regulatory guide describes a method acceptable to the Regulatory staff for complying with the Commission's regulations with regard to design verification of Class IE equipment for service in light-water-cooled and gas-cooled nuclear power plants.

B. DISCUSSION

IEEE Std 323-1974, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations,"[1] dated February 28, 1974, was prepared by Subcommittee 2, Equipment Qualification, of the Nuclear Power Engineering Committee of the Institute of Electrical and Electronics Engineers, Inc., (IEEE) and subsequently was approved by the IEEE Standards Board on December 13, 1973. The standard describes basic procedures for qualifying Class IE equipment and interfaces that are to be used in nuclear power plants and components or equipment of any interface whose failure could adversely affect any class IE equipment.

The requirements delineated include principles, procedures, and methods of qualification which, when satisfied, will confirm the adequacy of the equipment design for the performance of Class IE functions under normal, abnormal, design-basis-event, post-design-basis-event, and containment-test conditions.

C. REGULATORY POSITION

The procedures described in IEEE Std 323-1974, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations,"[1] dated February 28, 1974, for qualifying Class IE equipment for service in light-water-cooled and gas-cooled nuclear power plants are generally acceptable and provide an adequate basis for complying with design verification requirements of Criterion III of Appendix B to 10 CFR Part 50 to verify adequacy of design under the most adverse design conditions subject to the following:

1. Reference is made in IEEE Std 323-1974, Sections 2, 6.3.2(5), and 6.3.5, to IEEE Std 344-1971, "Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations." The specific applicability or acceptability of IEEE Std 344 will be covered separately in other regulatory guides, where appropriate.
2. The radiological source term for qualification tests in a nuclear radiation environment should be based on the same source term as that used in Regulatory Guide 1.7 (Safety Guide 7, 3/10/71) for BWRs and PWRs. An equivalent source term (i.e., 100% of the noble gases, 50% of the halogens, and 1% of the remaining solids developed from maximum full-power operation of the core) should be used for HTGRs. The containment size should be taken into account in each case. For exposed organic materials, calculations should take into account both beta and gamma radiation.

[1] Copies may be obtained from the Institute of Electrical and Electronics Engineers, Inc., United Engineering Center, 345 East 47th Street, New York, New York 10017.

D. IMPLEMENTATION

The purpose of this section is to provide information to applicants and licensees regarding the Regulatory staff's plans for utilizing this regulatory guide.

This guide reflects current regulatory practice. Therefore, except in those cases in which the applicant proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, this guide will be used by the Regulatory staff in evaluating all construction permit applications for which the issue date of the Safety Evaluation Report (SER) is July 1, 1974, or after.

For those construction permit applications for which an SER was issued prior to July 1, 1974, the Regulatory staff may, subsequent to issuance of the construction permit (or operating license), reevaluate the Safety Analysis Report on a case-by-case basis to assure that acceptable methods for qualification of Class IE equipment have been specified in purchase orders executed for such equipment on or after November 15, 1974.

U.S. NUCLEAR REGULATORY COMMISSION

May 1978

REGULATORY GUIDE

OFFICE OF STANDARDS DEVELOPMENT

REGULATORY GUIDE 1.139

GUIDANCE FOR RESIDUAL HEAT REMOVAL

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

JAN 3 1977

MEMORANDUM FOR: Ben Huberman, Director
Office of Policy Evaluation

THRU: Lee V. Gossick
Executive Director for Operations

FROM: Robert B. Minogue, Director
Office of Standards Development

SUBJECT: SECY 76-242C - PHYSICAL PROTECTION OF NUCLEAR POWER REACTORS AGAINST INDUSTRIAL SABOTAGE

This responds to your memorandum of December 23, 1976. It provides a more detailed writeup of the basis for the selection of design threat levels for use in regulating the protection of nuclear power reactors against sabotage. Design threat levels for use in 10 CFR Part 73, §73.55(a), were tentatively chosen by the Commission following Policy Session 76-55 of December 14, 1976, as indicated by the Secretary's memorandum to the Executive Director for Operations dated December 17, 1976 (including the revised version of December 23, 1976). The threat levels are stated in the context of general performance requirements which are supplementary to a number of specific requirements contained in §73.55.

Attached is a paper describing the factors considered in arriving at the basis and rationale for selection of design threat levels for power reactor sabotage protection. Our consideration of those factors indicates that there is conservatism in the Commission's tentatively selected general performance requirements. I believe that this paper is sufficient to support the proposed Statement of Considerations contained in my December 22 memorandum to the Secretary, including the correction pages we submitted on December 30 in response to the Secretary's December 23 revision of his December 17 memorandum.

This paper has been concurred in by NRR. Copies of the final draft were provided to NMSS and IE. All comments received were incorporated.

Robert B. Minogue

Robert B. Minogue, Director
Office of Standards Development

Enclosure: As stated

Contact: R. J. Mattson
443-6953

cc's: See next page

ENCLOSURE 3

cc's w/encl: Chairman Rowden
Commissioner Gilinsky
Commissioner Kennedy
Commissioner Mason
P. L. Strauss
S. J. Chilk
K. R. Chapman
B. C. Rusche
E. Volgenau
H. K. Shapar

BASIS AND RATIONALE FOR SELECTION OF A DESIGN THREAT LEVEL FOR POWER REACTOR SABOTAGE PROTECTION

December 30, 1976

This paper is to describe more fully the rationale for the level of physical protection at nuclear power reactors than previously has been provided (1)(2)(3)(4)(5).[1/] In understanding that rationale, it will be necessary to consider studies and analyses having general safeguards significance; i.e., significance for both the protection of materials from theft and protection of facilities from sabotage. Because of this, it will also be necessary to examine certain specific attributes of power reactors, their vulnerability to sabotage, and the potential consequences of their sabotage. The thrust of this paper is principally one of summarizing and documenting what has been said before in Commission papers, staff memoranda, and policy discussions over the past 10 years, leading to this stage of policy formation for power reactor sabotage protection.

The decision process for choosing design threat levels is of a predominantly judgmental and qualitative nature. Because of this, the historical longevity of certain design threat levels and of their linguistic construction adds credence to their acceptability and validity. For this reason, we will begin by summarizing the origins and the evolution of the design threat concept.

Considerations of threat level date back to the earliest regulatory action involving reactor sabotage which occurred in the licensing of the Turkey Point plant in 1967. Since 1967 there has been considerable change in AEC and then NRC policy, licensing practice, and understanding of the

1/ Numbers in parenthesis refer to references listed at the end of this paper.

security requirements for power reactors. Such change generally originated from two sources--increased capability for analysis and change in the incidence and type of malevolent acts in society. Some of the change resulted in changes in what have come to be known as design threat levels.

Before summarizing the principal milestones in this evolutionary process, we will define more precisely what is meant by design threat levels. The concept is directly analogous to the concept of design basis accidents used in our regulation of reactor safety. The need for these analogous concepts of design basis events arises because of the natural continuum of all possible events. In the case of sabotage, the events of interest are malevolent actions involving a potentially infinite number of permutations and combinations of many variables, such as the number of people, their skills, arms, tactics, motives, and timing, and the facility's operating status. Rather than study an infinite array of possible events, we choose a few design basis events (either accidents or threats) so as to reasonably characterize the total continuum of possible events within certain reasonable bounds. Thus, for example, in safety regulation, we require safety system design against an instantaneous double-ended pipe break but not a pressure vessel failure. The overall result is that designing for the double-ended pipe break provides protection against a wide spectrum of possible loss of coolant accidents, including pressure vessel failures of a certain limited character.

In this paper we are concerned with the analogous situation of developing the rationale by which to choose design threat levels for reactor physical protection against a spectrum of possible sabotage threats. Obviously the

nature of the vulnerability of power reactors, the potential consequences associated with their sabotage, and societal or political limitations on the resources which could be brought to bear in their attempted destruction will figure in the selection of reasonable bounds for the design threat levels. However, once specific threat levels are chosen, protection against sabotage will not in reality be limited to those events. It will also exist for threats which are larger and smaller, simpler and more sophisticated than the design threats. That is, we will be protecting against a continuum of threats, contained within reasonable bounds, with varying levels of confidence in that protection depending upon the position of a real threat within the continuum of possible threats. Corollary to this is the fact that implicit design level threats which underlie existing licensing practice provide some confidence, albeit unquantified and insufficient, of protection against the generally higher threats now being considered for inclusion in §73.55.

We will now proceed with an enumeration of the important historical milestones in the evolution of design threats for reactor sabotage protection.

In 1967 the Atomic Energy Commission (AEC) issued an order (6) concerning sabotage protection at Florida Power and Light Company's Turkey Point Units 3 and 4. The order stated that physical security requirements were to be addressed by the utility during its application for an operating license, and that the utility would not be required to protect against sabotage perpetrated by enemies of the United States. At that time, no detailed regulations and guides existed to say how this protection was to be accomplished or to more precisely characterize the threat.

A study which has come to be known as the McCullough study (7) was completed in 1968 for the AEC. It was a study of the degree of hazard to the public health and safety that could be created by industrial sabotage of a commercial nuclear power reactor of then current design. The study concluded that: (a) plant security measures cannot guarantee immunity from sabotage, but they can serve certain important deterrent functions, and (b) engineered safety features and protective systems at nuclear power plants impede simple acts of sabotage from creating a public hazard. The study considered sabotage acts by an insider, specifically acts which might be motivated by a dispute between labor and management. The McCullough study included an in-depth investigation of industrial sabotage in the United States. This investigation was combined with an estimate of the future role of nuclear power in the U.S. to conclude that a potential domestic threat level would be comprised of tactically unskilled but armed individuals who had extensive expertise and experience in the use of high explosives, motivated to cause damage but with no real intent to harm the public. The one exception was the potential psychopath with a motive of mass killings.

In the reactor case work of the late 1960's and early 1970's, there was rapid development of a licensing review practice which did not explicitly treat design threat levels. However, in the case-specific decision process there was a need to answer threat related questions, a good example of which was whether to arm guards. By about 1973 the AEC Regulatory staff had begun to describe design level threats in more specific terms for its internal use in making safeguards decisions. For example, security objectives were used

by the staff in developing specific requirements for SNM transportation systems to protect them against a continuum of threats. That continuum was characterized by three specific statements of threats of a discrete nature; viz, two armed individuals, a squad size group, and a paramilitary group. (8)

Considerations of design threat levels as applied to reactor physical protection were included in the 1973 ANSI Standard N18.17, "Industrial Security for Nuclear Power Plants". (9) That standard was endorsed in Regulatory Guide 1.17, also in 1973. (10) The standard contained specifications of what are now called design threats, as follows:

> "(a) A single disgruntled employee who is authorized to have access to the plant and who is familiar with the details of construction and operation of the plant;
>
> "(b) A single fanatic or mentally deranged person, either an authorized employee or an outsider, whose knowledge of the plant may range from none to intimate familiarity;
>
> "(c) A small group of discordant individuals, not normally authorized access to the plant, who are intent on perpetrating acts of sabotage or seizing control of the plant;
>
> "(d) Spontaneous and undisciplined actions of a relatively large group of people involved in mob activities associated with acts of civil disturbance. Although it is clear that other potential threats may exist or develop, conscientious application of measures designed to protect against the threats discussed above will provide substantial protection against other postulated threats."

In endorsing these words, Regulatory Guide 1.17 further required the arming of guards at nuclear power plants for three reasons which were documented in an October 1973 letter providing further elaboration of the design threats, as follows: (11)

"(a) To provide a deterrent against sabotage attempts,

"(b) To give the security force the capability to neutralize an attempt with force by several individuals (otherwise the entire plant might be at the mercy of one armed man), and

"(c) Most importantly, to give the security force a means of self-defense so that they can protect themselves while summoning help from the local authorities."

In early 1974 the security plans at all operating reactors were reviewed in accordance with the guidance of Regulatory Guide 1.17. The experience gained in these licensing actions was reflected in the November 1975 publication by NRR of the reactor Standard Review Plan, Section 13.6, "Industrial Security" (12), which required a finding that Regulatory Guide 1.17, or equivalent, was met. Hence, there was traceability from design threat levels to licensing requirements. The drafting of 10 CFR Part 73, §73.55 for issuance in proposed form in November 1974 relied upon those design threat levels; i.e., ANSI N18.17, above, as elaborated in reference (11). However, the design threat levels were not explicitly stated in the regulation issued for public comment.

Other safeguards actions which occurred in parallel with those specific to power reactor sabotage protection underscored the important role that design threat levels had come to play in the regulatory decision-making process. Two examples are noteworthy here.

In its May 9, 1974, review of the "Special Safeguards Study" (13)(14), the AEC Regulatory staff emphasized the usefulness and desirability of "design basis incidents" (or threats as we call them today). That staff review specifically noted that protection against a squad size attack assisted by

inside personnel raised an important issue of facility vulnerability to internal subversion of either the operating staff or the guard force, an issue which required attention and correction (something which three years later remains to be accomplished in the regulations for power plant sabotage protection). Subsequent licensing actions and regulatory guide development responded to this need to provide better treatment of the inside threat.

Another important safeguards consideration concerning clearances paralleled the changes described above in reactor sabotage protection. Consideration of the inside threat at both reactors and fuel cycle facilities led the AEC Regulatory staff to recognize the potential value of clearances for persons in the commercial sector having access to or control over SNM. Clearances are known to increase the assurance of personnel reliability, thus mitigating the threat of action by single individuals or conspiracies of individuals having "insider" privileges. Legislative authority for such clearances was granted in an amendment to the Atomic Energy Act in 1974.

In January of 1975 the AEC Regulatory staff issued Regulatory Guide 5.43, "Plant Security Force Duties" (15). This guide contained specifications on the capabilities of the security organization which were compatible with ANSI N18.17, Regulatory Guide 1.17, and the proposed regulation §73.55. It required that the security organization be capable of the following:

"(a) Preventing any successful theft or act of sabotage by one or two armed individuals or a group of unarmed people.

"(b) Delaying the attack of an armed group up to squad size sufficiently long to allow notification of and response by law enforcement authorities so that the attempted theft or sabotage is thwarted or stolen material is promptly recovered.

"(c) Defending itself in the event of a well-planned attack, executed in a disciplined and organized manner sufficiently well to communicate with law enforcement authorities to advise them of the attack and its scope and furnish information to be used as a basis for countermeasures and a properly escalated response by local, State or Federal counterforces either to prevent removal of the material or recover it or to initiate appropriate postsabotage action."

In the last two years, much new work has been accomplished in safeguards. Our sophistication in safeguards analysis has grown in response to the formation of NRC with a definitive legislative mandate in this area. There has been an addition of considerable inhouse safeguards expertise and associated increases in resources for safeguards research and contractual assistance. From the work performed with the considerably augmented resources, there has accumulated an impressive array of studies providing new knowledge which bears on the selection of design threat levels for sabotage protection of nuclear power plants. These studies range from assessments of the history, trends, motivation, and capabilities of malevolent groups in the United States and worldwide, to detailed engineering studies of the vulnerability of reactors from a design perspective and from a physical security system perspective, to onsite visits to operating nuclear power plants to assess the capability and practicability of meeting certain design threat levels. The salient features of this body of knowledge as it pertains to the design threat level required for protection of nuclear power plants against sabotage will be summarized in the next few pages.

At the outset it is important to acknowledge that the principal policy change flowing from the recent work of the NRC staff is the apparent need to provide explicit statements of design threat levels in our regulatory requirements for safeguards. In the choosing of the specific wording of such

explicit statements, some debate has occurred. At the Commission level many discussions have centered on understanding the various design threat levels proposed for nuclear power plant sabotage protection and for theft protection for strategic quantities of special nuclear material (SSNM). Within the staff there also has been discussion of the more detailed aspects of design threat levels; e.g., the degree to which automatic weapons, barrier penetration devices, or assault vehicles might be used by potential saboteurs has been considered at length.

We cannot in this paper, because of the time and the scope limitations on its writing, justify the selection of the design threat levels for the myriad of facilities for which NRC has safeguards responsibility or cognizance. Those facilities range from peaceful to military applications, they serve government, academic, and commercial purposes, and their development status ranges from laboratory to full-scale production models.

This paper is narrowly concerned with the rationale and basis for the sabotage protection to be required for the approximately 60 commercial nuclear power plants operating in the United States today, and others in the near term. In that regard, this paper has been drafted in full cognizance of closely allied policy documents concerning other broader NRC safeguards responsibilities, including the reports by the Division of Safeguards describing the joint ERDA/NRC task force work (16), the NMSS policy papers concerning implementation of the recommendations flowing from the work of the task force (17), and the safeguards supplement to GESMO (18). We believe that the judgments being made for nuclear power plant sabotage protection are consistent with those documents at their present stage of development, as

described below. Clearly, the analyses, policy thinking, and data contained in these documents are a part of the basis for the judgments being reached now on design level threats for nuclear power plant sabotage protection.

We will now briefly outline the salient features of the existing body of knowledge in the threat assessment area as that knowledge applies to protection of nuclear power reactors against sabotage. The organization of the material proceeds from general considerations to those more specific to the present day situation in the United States.

For the various types of malevolent groups (criminal, terrorist, revolutionary, guerrilla, etc.) operating in situations other than open warfare, there is no known correlation between tactics, motivations, or objectives and any desire to kill large numbers of individuals. This conclusion is based upon communications by NRC staff with knowledgeable individuals in the FBI, CIA, NSA, and DIA as well as studies performed by the BDM Corporation and the Mitre Corporation. For example, of the 4478 incidents of armed attack, arson, bombing, kidnapping, and hijacking studied by BDM, none attempted nor resulted in killing numbers of individuals comparable to the potential deaths resulting from reactor sabotage with radiological consequences (19). Moreover, in studying malevolent groups and the possible psychology of nuclear terrorism, no case could be made for mass killing as a logical, consistent, method of any group to achieve its ends (19-22). Of course, the threat of mass killing or destruction exists, however the fulfillment of such a threat does not appear to be consistent with the goals of any known past or present group (19)(21)(22). Groups and individuals with trivial or non-existent resources and poorly defined objectives have often threatened mass killings, but this seems to be an

expression of frustration and impotence rather than a realizable commitment to mass killings (19)(21)(23)(24)(25).

The size, capability, and the acceptability of methods used by a malevolent group depend upon the level of popular support for the group. In general, the larger the base of support sought or needed by the group, the more "respectable" and "traditional" its methods become. Criminal groups are an exception because they necessarily operate covertly, attracting a minimum of attention to themselves. These conclusions are derived from examining both the characteristics and the evolution of a number of malevolent groups. As one example of this concept, in its earlier days the PLO engaged in numerous skyjackings, but as it gained recognition and influence as being representative of the Palistinians, its official policy moderated (26). However, extremely alienated or frustrated groups are inclined to bizarre and desperate acts, especially acts of vengeance (21)(26)(27).

Large, well-organized, para-military-type groups apparently are tolerated only in areas with a high degree of social and political disfunction. In a relatively stable society, domestic terrorist or revolutionary groups are limited by circumstance (funding, support, need to avoid retaliation by general populace) to relatively unsophisticated, symbolic acts carried out by a few individuals and resulting in little, if any, loss of life. This conclusion follows from knowledge of the political and social environment in which terrorist and revolutionary groups have operated (21)(26).

A classic example of a group overstepping acceptable bounds is the fate of Uraguay's Tupamaros (28). A study of the specific objective of revolutionary and terrorist acts in the context of the society fostering those groups reveals a strong correlation between the realizable group objectives, the size of a group, and the types of acts (29).

Of the possible methods to carry out mass killings or destruction, the use of chemical or biological agents is easier, more certain of success, and less likely to endanger or expose the perpetrators, than is the sabotage of a nuclear power reactor. This statement is primarily based upon a study by Mission Research Corporation (formerly ADCON) which discussed the threat of mass casualties and makes a detailed comparison of chemical, biological, and radiological means of inflicting mass casualties and destruction (30). It is also supported by a similar conclusion of a recent reactor vulnerability study by Sandia Corporation (31). In addition, both BDM and Mitre conclude that sabotage of a nuclear power reactor is a difficult task requiring a high level of technical sophistication (32)(33). Staff communication with the FBI and CIA lead us to conclude that there is no knowledge of any group in the U.S. presently possessing the required degree of technical knowledge, resources and motive to sabotage nuclear power plants so as to cause radiological hazard to the public. However, these same sources are quick to point out that technical knowledge and sophistication have been easily acquired by certain groups in the past, and this presumably could be done again if nuclear action became a desirable motive to such a group. It should be noted that the routine actions of the FBI and CIA provide an intelligence capability which is designed to detect

change in the character or the motives of such groups in the U.S. Groups not known to the intelligence community are usually unknown because of small cellular organizations -- a factor which severely restricts the capacities and options of the group.

There is no history of or evidence for any known group intending or attempting to kill large numbers of individuals by use of special nuclear material or sabotage of a nuclear power plant. Reference 26 has an extensive discussion on motivations, from which this conclusion is drawn (34). In addition, Reference 26 discusses the characteristics of sabotage specifically as it relates to mass destruction (35).

There is no evidence of any malevolent group in the U.S. today with a history of "true" terrorist or revolutionary activity. That is, while symbolic acts of violence directed at selected individuals or institutions and of a disruptive nature have occurred, violent terrorist or revolutionary activities indiscriminantly directed against the lives of people or the stability of the government have only appeared in the radical literature. This conclusion is inferred by the staff from the representative group studies done by Mitre (21) and it follows from the motivation analysis done by BDM (22)(26)(35). The acts which have occurred in the U.S., and which are generally mistermed "terrorist" or "revolutionary" by the press have been largely limited to bombings and threats, with occasional attacks by ethno-centric revolutionary groups on police - an identifiable "enemy" more or less acceptable as a target to the "community" within which the group operated (36). Although various groups take credit for a variety of mishaps and acts of others, the bombings and attacks which have occurred have taken place covertly, and the individuals involved have attempted to

avoid directly exposing themselves (32). Moreover, there is no history of attacks on essential, protected industrial facilities in the U.S., even though, historically, these are prime targets for the revolutionary aiming at disruption or disability of the government (26). Finally, staff discussions with the FBI lead us to conclude at present there is no evidence of any known group in the U.S. with the resources, knowledge, and motives required for carrying out a concerted assault against any reasonably well-protected facility.

Of the possibilities for sabotage of a nuclear power plant, we judge that the greatest risk is portended by the actions of an insider. This conclusion is based on the fact that reactor sabotage could be accomplished by a lone individual with sufficient knowledge and access to vital equipment (31)(43). The conclusion is also supported by observation and study of the motives and actions of past malevolent groups, especially those in the U.S. (38). Acts of sabotage which have occurred at industrial facilities (e.g., the fire at Indian Point Number 2) generally involve one to three individuals, with at least one person being an employee or former employee, targeted at easily accessible equipment or structures, with no apparent attempt to cause casualties. Here there arises a corollary risk which is the act of symbolic protest or disruption without the intent to kill by the dissident insider, but which results in damage beyond that intended and leads to an unintended release of radioactive material (36).

Ultimately, the intentions of a malevolent group and its ability to carry out its intentions are more strongly dependent upon the nature and stability of the society which fosters the group than on the numbers characteristically or potentially involved in any specific activity of the group. This conclusion is reached upon observation and study of the acts and motives of a number of malevolent groups. Generally, it must be presumed that a well-established group can acquire whatever resources are necessary to carry out the acts it deems appropriate. Societal turmoil, moreover, can generate groups for specific short-term ends (e.g., reactor sabotage), either spontaneously or by splintering from already established organizations. A high frustration level in a society as a whole will tend to produce numbers of psychopathic and sociopathic individuals who could conceivably attempt nuclear action for a large variety of reasons (36). Fortunately, the history of such issue-intensive groups and individuals indicates that they are intrinsically limited in their capabilities, by both the nature of the personalities involved (24), and the restraints imposed by the day-to-day exercise of the instruments of law and order in a stable society (26). Furthermore, the desire for public acceptability as "instruments of the people" and the effective operation of the intelligence community severely restrict the options available to well-established groups. The history of the Black Panthers is a good example of a combination of effective intelligence and community pressure causing fundamental changes in an established "revolutionary" organization.

Considerations of the unique characteristics of nuclear power plants have also figured in the development of design threat levels for use in regulating sabotage protection. Principally, the considerations have involved questions of vulnerability and consequences. In the following paragraphs, we will summarize the salient features of these considerations.

The most likely consequences of successful sabotage of a nuclear power plant are significantly less than the conceivably extreme consequences associated with other possible malevolent acts, including theft of SSNM and subsequent detonation of an illicit nuclear weapon. The consequences of reactor sabotage leading to core meltdown would be comparable to those described for accidental core meltdowns, i.e., ranging between at most 3,300 fatalities and the more likely result of less than one (31) (40). Other studies have estimated that a nuclear explosion with a 100 ton yield could kill promptly as many as 50,000 people depending on the location (41). The consequences of a one kiloton nuclear explosion have been estimated to be prompt fatalities of the order of a few hundred thousand individuals, depending on the location (42). Biological pathogens such as anthrax spores disseminated in an aerosol form in the New York City area have been estimated to be capable of causing up to 600,000 prompt fatalities (42).

The design of nuclear plants, the remote nature of their sites, and the ability to decrease and delay the public consequences of a successful reactor sabotage by reactor scram actions and by preplanned public emergency evacuation measures, all serve to decrease the relative attractiveness of reactors as targets for acts of wanton or threatened violence. Other

targets in both the civilian and the military sectors of our society are simply more vulnerable (lower risk to perpetrator) and the public consequences are more certain (30)(31)(36).

Nuclear power plants are inherently resistant to sabotage owing to such characteristics as their massive structures, the spatial layout of reactor systems, and the "defense-in-depth" concept of reactor and safety system design. The NRC staff and others (7)(13)(19)(21)(26)(43) have consistently reached this conclusion over the past 10 years of study. The conclusion owes to the innate characteristics of power reactors, the criteria for their safe design and operational control, and their required safety systems, all of which significantly reduce vulnerability to acts of sabotage which could lead to a release of radioactive materials. The following discussion elaborates the features which are most important in this regard. The design and physical nature of light water power reactors are inherently resistant to acts of violence. The fission products are enclosed in metallic clad fuel rods which are shielded by water and located in a thick steel reactor vessel. The vessel is located within a massive reinforced concrete structure with a controlled atmosphere. In addition to providing barriers to the release of radioactive materials, these design features also constitute physical hardening against destruction by sabotage. The massive reinforced concrete structures provide physical protection of vital systems from overt acts of sabotage directed at the periphery of the plant buildings. These structures are required in order to protect vital safety equipment against such things as tornadoes, earthquakes, fire, and missiles and are inherently resistant to penetration. In addition the vital systems are spatially separated within such hardened structures. The

safety design criteria for power reactors prevent or mitigate radioactive releases by requiring conservative reactor designs and safety margins, system reliability, quality assurance, redundancy, diversity, tests and inspections, and protection against common mode failures. For example, the reactor protection system is designed to automatically scram the reactor which significantly reduces the stored energy of the core and simultaneously minimizes the potential risk to the public. Such design features are necessary for sustained operation and safety over the lifetime of the plant. Engineered safety features are required and must be designed to mitigate postulated transients and accidents concurrent with an additional single failure. The design basis limits the release of fission products under abnormal reactor conditions. These systems also provide protection against most potential sabotage attempts involving a single destructive act.

The successful sabotage of a nuclear power plant to result in a public health hazard would require considerable expertise and opportunity on the part of the saboteur. The saboteur must be knowledgeable in the operation and location of the redundant, physically separated, and functionally diverse reactor systems and safety systems and must be given or seize the time required to sabotage redundant trains and systems. Generally, the susceptibility of reactors to single acts of sabotage, e.g., destruction of components such as pumps, or power supplies, do not portend a radiological risk to the public. These time requirements and the complexities of the target are significant deterrents to the potential saboteur.

Conclusion:

Having considered the breadth of information and the regulatory precedents indicated above, the staff reached a judgment through the consensus gathering process of interoffice concurrence that a general performance requirement should be explicitly stated in §73.55(a) for issuance of the regulation in effective form, as shown in Enclosure A of SECY-76-242C.(4) The staff had also conducted onsite studies of six plants to determine the practicality and effectiveness of §73.55 in meeting the proposed general performance requirements (design level threats). That work was described in SECY-76-242B.

After its examination of roughly the same information base, the Commission tentatively selected somewhat different and generally more conservative design threat levels as described in the Secretary's memorandum of December 17, 1976 (revised on December 23) to the Executive Director for Operations. The design threat levels chosen by the Commission were stated as follows;

"(a) General performance requirements

"The licensee shall establish and maintain an onsite physical protection system and security organization which will provide protection with high confidence against successful industrial sabotage by both of the following:

"A. A determined violent external assault, or attack by stealth of one to three persons with the following attributes, assistance and equipment: (1) Well trained (including military training and skills) and dedicated individuals, (2) inside assistance of one knowledgeable individual who may attempt to participate in both a passive role (e.g., provide information) and active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), (3) suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long-range accuracy, (4) hand-carried equipment, including explosives for use as tools of entry or otherwise destroying the reactor integrity, and

"B. In internal threat of one insider or one employee (in any position)."

There is an important difference between the threat levels recommended by the staff in SECY-76-242C and those tentatively chosen by the Commission. It lies in the "determined violent" nature of the threat described by the Commission. The determined violent nature is consistent with other safeguards actions already taken or planned by the Nuclear Regulatory Commission, e.g., the orders to licensees issued by the Division of Safeguards in the spring of 1976 concerning the use of deadly force. The change also provides consistency in judgment concerning the resources to be presumed available to perpetrators of theft or sabotage and their willingness to die or kill. Presumably, any group willing to commit a nuclear atrocity, whether by sabotage or by theft and detonation of a nuclear device, can be assumed to be capable of determined and violent actions with all available resources, obtained either legally or illegally. In SECY-76-242C the staff did not recommend the determined violent nature for the nuclear power plant design threat. That judgment had two bases. First, the overriding risk of sabotage to nuclear power plants, viewed in context with knowledge of their vulnerability, is the insider, acting with or without outside assistance, with motive, access, and knowledge of the plant. Second, there are differences between the potential consequences of sabotage of a power reactor versus SSNM theft and successful detonation of an illicit nuclear weapon. In reality, however, inconsistencies in the specification of threat characteristics are not as important as they first appear. For example, the difference in assault capability between three and six determined people with the same weapons probably is not as large as the

difference between three professional thieves whose overriding concern is self preservation and three determined violent terrorists willing to kill and die. In fact, such differences are not amenable to precise quantitative analysis. In recognition of this situation, and in recognition of the size of basic maneuvering units generally appearing in small unit tactics in armies throughout the world, the staff has previously preferred a more general characterization of the assault force, e.g., speaking in terms of squad size groups with paramilitary capabilities.

Based on the foregoing, the rationale for the design threat levels in the general performance requirements of §73.55(a) can be summarized as follows:

A. The determined violent assault by three persons is believed to be a conservative overestimate of the motives and capabilities of existing or past groups with malevolent interest in the United States. The conservatism is judged to be reasonable in light of the potential consequences of a successful sabotage of a nuclear power plant. The arms and other characteristics of the assault threat are estimates of what could be reasonably obtained in the U.S. by a determined violent group. The hypothesized aid by an insider is commensurate with the observed practice of dedicated, malevolent groups in the past to enhance their chances of success and to decrease the risk of injury or death of the perpetrator.

B. The requirements for protection against the lone insider are motivated primarily by the need for protection against a deranged or unstable employee. In addition, recent study concerning the possible subversion or coercion of employees is sufficient to

warrant enlargement of the inside threat specification to include all persons with inside access, independent of their position or authority. The inside threat is judged to be adequately limited to one person at this time while work is being initiated and carried to completion over the next several years to provide better information on alternatives for dealing with internal conspiracies at nuclear power plants.

REFERENCES

1. SECY-76-242, "Requirements for the Physical Protection of Nuclear Power Reactors," April 26, 1976.

2. SECY-76-242A, "Requirements for the Physical Protection of Nuclear Power Reactors," April 26, 1976.

3. SECY-76-242B, "Requirements for the Physical Protection of Nuclear Power Reactors," September 8, 1976.

4. SECY-76-242C, "Requirements for the Physical Protection of Nuclear Power Reactors," October 7, 1976.

5. Memorandum from B. Snyder to Commissioners' Assistants, "Design Basis Threats for Power Reactor Safeguards (Proposed 73.55)," December 8, 1976.

6. Memorandum and Order: In the Matter of Florida Power and Light Co., August 4, 1967. Docket Nos. 50-250 and 50-251.

7. C. Rogers McCullough, et.al, "An Appraisal of the Potential Hazard of Industrial Sabotage in Nuclear Power Plants," Southern Nuclear Engineering Report, SNE-51, July 1968.

8. Conversation with R. B. Minogue, now Director of Standards Development, concerning View Graph used in 1973 briefing of the AEC.

9. American National Standards Institute draft Standard N18.17, "Industrial Security for Nuclear Power Plants," March 23, 1973.

10. Regulatory Guide 1.17, "Protection of Nuclear Power Plants Against Industrial Sabotage," June 1973.

11. Letter to Mr. Byron Lee, Jr., of Commonwealth Edison, dated October 23, 1973, from Mr. Lester Rogers, then Director of Regulatory Standards, responding to Mr. Lee's letter of June 20, 1973, to Mr. L. Manning Muntzing, then Director of Regulation, USAEC.

12. "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," LWR Edition, Section 13.6 Industrial Security," Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, September 1975.

13. David M. Rosenbaum, et.al., "Special Safeguards Study." Congressional Record, 120, No. 59, April 30, 1974.

14. Memorandum to L. Manning Muntzing, then Director of Regulation, from D. F. Knuth, Director of Regulatory Operations, J. O'Leary, Director of Licensing, and L. Rogers, Director of Regulatory Standards, giving staff comments on Special Safeguards Study, May 9, 1974.

15. Regulatory Guide 5.43, "Plant Security Force Duties," January 1975.

16. Joint ERDA/NRC Task Force Report on Safeguards.

17. SECY-76-416A, B.

18. Safeguards Supplement to GESMO, Section 5.2.3, Chapter 5 Draft dated December 21, 1976.

19. BDM "Draft working paper B, Summary of Findings, Analysis of the Terrorist Threat to the Commercial Nuclear Industry." 12 Sept. 1975 BDM/W-75-176-TR. Also see "Analysis of Group Size" BDM/W-75-247-TR, December 1975.

20. Ibid., p. 81.

21. Mitre "The Threat to Licensed Nuclear Facilities," September 1975, MTR-7022. This report characterizes several past and existing malevolent groups.

22. BDM "Behavioral Analysis of the Terrorist Threat to Nuclear Installations, Phase 1,: BDM/W-74-043-TR, July 1974, Section IV.

23. Staff communications with H. G. Hubbard, M.D., Aberrant Behavior Center.

24. Staff communications with F. G. Harris, M.D., Aberrant Behavior Center.

25. Brian Jenkins, "Will Terrorists Go Nuclear," Paper presented at the California Seminar on Arms Control and Foreign Policy, November 1975.

26. BDM "Draft working paper C, Supportive Appendices: Analysis of the Terrorist Threat to the Commercial Nuclear Industry." BDM/W-75-176-TR (see Appendix D).

27. BDM Ref. 19, pp II-16 - II-19, P III-43.

28. Ref. 19, pp 22, 23.

29. Ref. 26, Appendixes D and F.

30. ADCON "Superviolence: The Civil Threat of Mass Destruction Weapons," A 72-034-10, 29 Sept. 72, Chapters 8,9. These findings are also supported by a number of classified documents reviewed by the staff.

31. "Safety and Security of Nuclear Power Reactors to Acts of Sabotage," Sandia Report, SAND 75-0504, March 1976.

32. Ref. 22, p 78.

33. Ref. 26, p E-9.

34. Ref. 26, pp F-21, F-23.

35. Ref. 26, pp E-43, E-44. See also Ref. 25, p 12.

36. Ref. 26, Appendix H.

37. For example, a group calling itself "Project Achilles Heel" claimed responsibility for the Indian Point 2 fire. Ref. 26, p B-19.

38. Ref. 26, Appendix F.

39. Ref. 26, Appendices F, G, H.

40. WASH-1400, "Reactor Safety Study," p 9, U.S. Nuclear Regulatory Commission, October 1975.

41. Mason Willrich and Theodore B. Taylor, "Nuclear Theft: Risks and Safeguards," pp 21-24, Ballinger, Cambridge, Mass., 1974.

42. ADCON, op.cit, Chapter 9.

43. "Summary Report of Workshop on Sabotage Protection in Nuclear Power Plant Design," Draft Sandia Report, SAND 76-0637, November 1976.

NUREG-0170
VOL. 1

FINAL ENVIRONMENTAL STATEMENT ON THE TRANSPORTATION OF RADIOACTIVE MATERIAL BY AIR AND OTHER MODES

Docket No. PR-71, 73 (40 FR 23768)

December 1977

Office of Standards Development
U. S. Nuclear Regulatory Commission

INTERIM REPORT

Accession No. 7817210145

SAND77-1927

Contract Program or Project Title: Generic Environmental Assessment on Transportation of Radioactive Materials Near or Through a Large Densely Populated Area

Subject of this Document: Transport of Radionuclides in Urban Environs: A Working Draft Assessment

Type of Document: Preliminary Report
Draft Assessment

Author(s): A.R. DuCharme, Jr. (Project Coordinator); R.E. Akins; S.L. Daniel; D.M. Ericson, Jr.; B.H. Finley, N. N. Finley; P.C. Kaestner; D.D. Sheldon; J.M. Taylor; M.S. Tierney

Date of Document: May 1978

Responsible NRC Individual and NRC Office or Division: N. Eisenberg
Transportation and Product Standards Branch
Office of Standards Development

This document was prepared primarily for preliminary or internal use. It has not received full review and approval. Since there may be substantive changes, this document should not be considered final.

Sandia Laboratories
Albuquerque, New Mexico 87185

for the

U.S. Department of Energy

Prepared for
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

under DOE Contract AT(29-1)-789
NRC FIN No. A-1077-A

INTERIM REPORT