



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

AEOD/E201

JAN 12 1982

MEMORANDUM FOR: Robert F. Burnett, Director  
Division of Safeguards, NMSS

FROM: Carlyle Michelson, Director  
Office for Analysis and Evaluation  
of Operational Data

SUBJECT: METHODOLOGY FOR VITAL AREA DETERMINATION

In our meeting of July 23, 1981, we indicated that we would provide our thoughts on the vital area identification process. Based on review of selected reports, contractor meetings, and discussions between members of our staff, the following comments are provided for your consideration.

1. Generic sabotage fault trees are used for the analysis of nuclear power plants to identify vital areas and provide the basis for the proposed rule on vital area definition. Application of this technique for developing sabotage scenarios is an important part of a systematic approach for identifying vital equipment. Significant efforts have been directed toward the development and application of fault trees as exemplified by the major expenditures of resources within the safeguards research program for this purpose. However, as discussed below we believe that it is practical and necessary to identify the vulnerabilities of reactor systems and components before the application of these fault trees is undertaken.

Although the need for vulnerability studies have been recognized, the only documented vulnerability study that we are aware of is the SAI component vulnerability study. This was a commendable effort and we believe that additional studies of this general type and approach are needed. For example, vulnerability studies of safety systems, considering system interactions and common mode failures resulting from an act of sabotage, should be used to help identify fault trees which may not otherwise have been considered. In addition, transient and accident initiators may be identified which should be further analyzed through detailed fault trees, such as air systems which have not yet been properly analyzed in sabotage scenarios. Finally, we believe that additional vulnerability studies of reactor systems are needed to help define "key vital areas" as used in the proposed rule.

With regard to the generic fault trees developed by Sandia, some tests for completeness and accuracy may be beneficial. This would complement the review by RES's Division of Risk Analysis, with regard to the methodology and its application. For example, a working group of senior reactor

XA 8202/80457

JAN 12 1982

operators could provide a valuable perspective and review of the sabotage sequences including the vulnerability of systems. A second test might be to compare the fault trees to reactor operational experiences, such as events which have resulted from manual valve manipulations and system misalignment. In this regard, it is our understanding that the fault trees do not explicitly include the manipulation of manual valves. If true, this would be a significant omission in the usefulness of generic sabotage fault trees. Further, based on our review of the Beaver Valley vital area analyses, it appears that review teams consider manual valves only on an ad hoc basis during site visits.

2. We believe the major threat of sabotage to a nuclear power plant is associated with the insider or an employee of the plant who has access to the vital areas of the plant. As previously discussed, the identification of the vital areas is an important first step in the physical protection process. The second, and equally important consideration, is how should the vital area be protected against the insider threat.

The prevalent method employed to date is access control utilizing locks. Yet, access to equipment during an emergency may be critical for particular systems of certain plants to prevent damage to equipment and degradation of safety systems functions. The impact on operational safety due to physical protection measures need to be carefully evaluated as an integral step before implementing protective measures which restrict access. Since a large number of plant personnel are authorized access to all vital areas, a specific analysis should address the reduction in risk due to an insider compared to the reduction in operational safety resulting from the physical protection measures employed. This is particularly important where "compartmentalization" of equipment is involved. The impact on operational safety due to physical protection requirements continues to be a concern to the licensees and others and requires further and timely consideration.

Protecting nuclear power plants from insider threats is an extremely difficult and necessary undertaking. Based on our review of licensee reports, it appears that the number of "employee problems" has increased in recent years suggesting that the insider threat is increasing. The problem is finding a practical and effective method of safeguards. As you know, access control measures were never intended to be effective against the insider and were to be replaced or supplemented with other assurances of personnel integrity, e.g., clearances, psychological evaluations, profile identification and recognition, special application of access control measures, and design changes to protect against sabotage. Furthermore, a majority of Security Incident Reports are related to improperly secured vital area doors and improper key controls which indicates a real concern regarding the effectiveness of access control measures. In summary, we recommend that additional resources be allocated for developing and evaluating practical methods to minimize insider threats and that this activity receive budgetary priority.

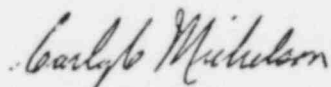
JAN 12 1982

Robert F. Burnett

- 3 -

3. The Beaver Valley study does not clearly define the criteria for identifying the type of situations to be prevented from postulated sabotage actions. For example, there are a number of other accident scenarios which could produce radiological releases. The assumptions are not provided in order to analyze the identified events with regard to such items as operator actions and credit for nonsafety-related equipment. The scope seemed incomplete in that protection of vital equipment to prevent station blackout was not considered, and randomly occurring transients in combination with a covert act of sabotage were not considered. While the events analyzed include a number of other events as subsets during power operation, events occurring during shutdown and refueling did not receive proper emphasis. Vulnerability during these conditions is increased due to the increased number of personnel on-site and reduced system operability requirements.

If you desire additional information or if we can provide additional assistance, please contact me or Wayne Lanning in my office.



Carlyle Michelson, Director  
Office for Analysis and Evaluation  
of Operational Data