LA-UR -82-2831

Conf-821037--17



MASTER

LA-UR--82-2831

DE83 000602

TITLE: REACTOR SABOTAGE VULNERABILITY AND VITAL-EQUIPMENT IDENTIFICATION

AUTHOR(S): J. M. Boudreau and R. A. Haarman

SUBMITTED TO: Tenth Water Reactor Safety Research Information Meeting, Washington, DC, October 15, 1982



Los Alamos Los Alamos National Laboratory
Los Alamos, New Mexico 87545

# REACTOR SABOTAGE VULNERABILITY AND VITAL EQUIPMENT IDENTIFICATION

by

J. M. Boudreau and R. A. Haarman
Los Alamos National Laboratory

## Abstract

Two ongoing programs at Los Alamos, the Vital Area Analysis Program and the Reactor Sabotage Vulnerability Program, are discussed. The Laboratory has been providing the Nuclear Regulatory Commission with technical support in identifying the vital areas at nuclear power plants through the use of sabotage fault trees. This procedure is being expanded to provide support for the Reactor Sabotage Vulnerability Assessment Program. A re-examination of some of the original system modeling assumptions, including a survey of the applicable research, is underway. A description of the survey work and the computerized data bases being used is provided. This program is expected to result in refinements in the existing procedures.

## Introduction

This paper will discuss briefly the work performed by the Los Alamos National Laboratory for the Vital Area Analysis (VAA) Program. It also will outline the newly initiated Reactor Sabotage Vulnerability Program. Both of these programs are being performed under contract for the Nuclear Regulatory Commission (NRC).

Since 1979 Los Alamos has been providing the NRC with technical support for determining the locations of vital areas, as defined in 10 CFR 73, for all power reactors in the United States. The NRC now is considering expanding the vital area analysis procedure to provide support for the Reactor Sabotage Vulnerability Assessment Program. A re-examination of certain assumptions currently used by Los Alamos or proposed by the NRC relating to reactor sabotage is required to extend the previous work.

## Vital Area Analysis Program

Since the Vital Area Analysis (VAA) Program's inception in 1979, Los Alamos has visited almost all of the operating reactors and approximately 10 plants undergoing their operating license review as part of the Laboratory's Vital Area Analysis Program.[1] The results of the program are used as a resource by the NRC licensing staff to identify vital equipment and areas at the plants that require protection and to verify the licensee-identified vital areas.

The method used to perform the analysis focuses on the fault-tree approach to systematically identify the sabotage scenarios and equipment locations in the plant.[2] The vital area fault-tree methodology was developed by Sandia National Laboratories, Albuquerque (SNLA), in the early 1970s for the NRC's Office of Nuclear Regulatory Research (RES).[3] Starting in 1979, the method was applied to specific plants by Los Alamos for the Office of Nuclear Reactor Regulation (NRR) and most recently for the Office of Nuclear Material Safety and Safeguards (NMSS). This technique has proved to be an excellent tool for performing detailed and systematic analyses of complex plants.

The vital area fault-tree methodology uses the SETS computer code to solve the massive fault trees to provide the results in a usable format. SNLA is continuing its efforts in modifying the code to provide time-saving techniques for computer usage, and cooperation between SNLA and Los Alamos is required to provide interaction between the developer of the code and its user. The formation of the fault tree is central to the whole program. The accurate representation of the plant is essential for credible results. Solving the fault tree requires sophisticated numerical manipulation, and computers are well suited to the process.

Los Alamos uses a multistep procedure in the VAA program that is intended to efficiently gather the necessary data for input to the fault tree. This technique consists of an FSAR review, a site visit, data reduction, formation of a fault tree, and a computer solution. Los Alamos engineers spend time at each plant to gather the site-specific information needed to develop the tree. The initial fault-tree formation uses a combination of generic subtrees to represent the plant. However, experience has shown that all plants differ

widely in site-specific data, hence the fault-tree development tends to be an iterative process that concludes with a unique fault tree for each plant. The plant personnel who provide the most useful information are members of the operating, training, licensing, and maintenance staff. A typical site visit is 1 week long and starts with discussions with plant-systems-oriented personnel to establish the initiating events and the system mitigating capabilities. During the discussions, the operating procedures are reviewed to determine system and operator responses. Once the appropriate systems are identified, the Piping and Instrumentation Diagrams, Electrical Single Line drawings, and associated control system drawings are examined and physical locations are noted. Los Alamos engineers make verification inspections of selected equipment locations throughout the plant and maintenance personnel are consulted for various appraisals of component vulnerabilities. The information then is brought back to Los Alamos where the engineers develop the complete trees for eventual computer input. The results are compared with the information received at the plants, and often the plant personnel are consulted again to provide a double check on the input data before submitting the results to the NRC. The entire process takes approximately 6--10 weeks to complete.

Sabotage fault trees differ from safety fault trees in one important area--single failure criteria are not considered for sabotage-related scenarios because the saboteur is not restricted to damaging a single piece of equipment. This has led to the inclusion of multiple-failure scenarios in the sabotage fault trees, which provides a different set of assumptions than might be found on a safety tree. Because most light-water reactor safety work has been done assuming single-failure criteria and system interactions in the sabotage mode are not as well understood, there has been a tendency to use conservative assumptions in the sabotage trees. A good example of this was in the case of whether to permit a plant to use the feed-and-bleed mode of recovery in the event it has lost its feedwater capability. In 1978, calculations were performed using the Los Alamos TRAC (Transient Reactor Analysis Code) for a B&W plant to determine whether the plant should be given credit for using feed and bleed as an alternate procedure to auxiliary feedwater in a safeguards situation.[4] This run was made because the vital area designation impact was significant and it involved multiple failures that had not been considered before in the safety area. Not until after the TMI incident,

where a similar scenario was involved, was the feed-and-bleed scenario more fully developed. Generally, the sabotage tree will not include credit for recovery modes that have not been reviewed and approved by the NRC. Here again the flexibility of the tree and computers make changes fairly simple; the analyst is able to focus on the localized problem and use the computer to perform the impact analysis in a straightforward approach.

The most difficult part of the sabotage tree to develop is in the area of determining the system or combination of systems that is required to mitigate various saboteur-initiated incidents. The difficulty is a result of the lack of information in the safety area when multiple failures are considered. It should be stressed that this lack of information does not cause the vital area analysis results to be wrong in the sense that areas that contain vital equipment are not identified, but rather it is entirely possible that more safeguards requirements are put in areas of the plant where they are not required. The case of "better too many than not enough" may appear to satisfy the notion of security. However, when plant operations are considered, these safeguards requirements may affect safety adversely.

It is intended that the reactor sabotage vulnerability and vital equipment identification programs will concentrate on providing the most recent research work applicable to the fault tree formation and thereby eliminate unnecessary conservatism.

## Reactor Sabotage Vulnerability Program

As mentioned earlier, the NRC's reactor sabotage vulnerability assessment program is based on the VAA procedure. To extend the work previously performed by Los Alamos, a re-examination of some of the original assumptions about the way certain systems are modeled is needed To meet this end, the NRC recently has funded additional work at the Laboratory. The objectives of this work are (1) to identify and characterize the existing information regarding the original assumptions, (2) to determine additional research requirements, and (3) to identify the specific aspects of the existing vital area analysis and reactor sabotage vulnerability assessment procedures that should be refined.

To meet these objectives, Los Alamos first will survey and analyze the research and engineering studies that can assist in identifying the vulnerability of reactors to sabotage of the following types of equipment.

a. Individual safety-related cables in cable trays
b. Complete cable trays
c. Systems during shutdown or refueling conditions
d. Sensor systems, instrumentation, and nonsafety related control systems
e. Spatially-extended systems and components (that is, piping, electrical distribution, and HVAC systems)
f. Air systems
g. Electrical equipment by grounding or lifting of grounds

In addition, Los Alamos will identify and analyze any research that:

a. relates best-estimate analyses of plant responses to system failures to the corresponding FSAR analysis;
b. discusses effective inclusion of random events, such as anticipated transients, in fault-tree methodologies;
c. addresses possible system failures after which stable hot shutdown cannot be maintained indefinitely; and
d. considers the use of nonsafety-related equipment, unanalyzed procedures, or operator ingenuity to recover from system failures.

If issues are identified for which no research or insufficient research is being conducted to support a defensible conclusion, this situation will be reported to the NRC as early as possible. It is expected that the survey will highlight needed changes in the assumptions that will affect the results of the VAA or the reactor sabotage vulnerability assessment. These issues will be prioritized according to their anticipated effect. The required refinements to the existing procedures, including the development of modifications to the fault trees, then will be made one by one.

Before Los Alamos concludes that a particular issue has no effect on the results of the analysis, the assumption will be tested. Using the information gained from the survey, Los Alamos will model the system or component and its failure effects in a fault tree and will make a demonstration run. The results

of the modified fault-tree analysis then can be compared with the original results. If the results agree, the issue will be removed from further consideration.

The survey phase of this work is expected to be completed in the spring of 1983 with the follow-on work possibly extending into 1985. The survey work was begun in August of this year. One of the major resources we have available for this effort is a computerized information retrieval system. In fact there are two such systems we are using--DOE's RECON system and the Dialog system. RECON is composed of approximately 40 individual data bases. Dialog has approximately 150 data bases in its system. Some examples of the data bases important to this study are shown in Table I. To date, we have done searches on all of these data bases. We are now in the process of reviewing the results and selecting the reports from those identified that are really appropriate. The format we selected for the printout includes an abstract, which makes the report selection easier, and all the keywords and categories under which the report was filled. This is helpful in identifying words or expressions that might have been missed on the first search and allows us to go back and refine or expand our search techniques.

We are hoping that as we go through the reports we can identify authors or institutions that have done a fair amount of work on the selected topics. The next, or possibly concurrent, phase of our efforts will be to contact these people directly to be sure we have the most up-to-date information on the subject. In this regard, I would like to encourage each of you to suggest reports you know of or other data bases or people actively working in this area that may be of assistance here.

Table I

INFORMATION RETRIEVAL SYSTEMS

DOE/RECON
Energy Data Base (EDB)
Nuclear Safety Information Center (NSIC)
Nuclear Science Abstracts (NSA)
Research in Progress (RIP)

DIALOG
National Technical Information Service (NTIS)
Electric Power Database (EPRI)
Doe Energy
Smithsonian Science Information Exchange (SSIE)

## Conclusion

This program will result in the original analysis assumptions either being confirmed or modified. Once the required refinements are incorporated into the VAA and reactor sabotage vulnerability assessment procedures, it is expected that the NRC will be able to use the results with greater confidence that all the vital areas and equipment have been identified. In addition, some of the unnecessary conservativeness of the analyses may be removed and thus reduce the possibility of safeguards requirements adversely affecting the safe operation of the plants.

## REFERENCES


1. W. A. Bradley, R. A. Haarman, and D. G. Rose, "Keeping Reactors Safe from Sabotage," Los Alamos Science 2 (2), 120-131 (1981).

2. G. B. Varnado and R. A. Haarman, "Vital Area Analysis for Nuclear Power Plants," Los Alamos National Laboratory report LA-UR-80-2407 (August 1980).

3. G. B. Varnado and N. R. Ortiz, "Fault Tree Analysis for Vital Area Identification," Journal of the Institute of Nuclear Materials Management, Fall, 438-447 (1979).

4. J. W. Bolstad and R. A. Haarman, "Summary of Thermal-Hydraulic Calculations for a Pressurized Water Reactor," Los Alamos National Laboratory report LA-8361-MS, NUREG/CR-1480 (May 1980).