PREPRINT UCRL- 81823

CONF-780784--1

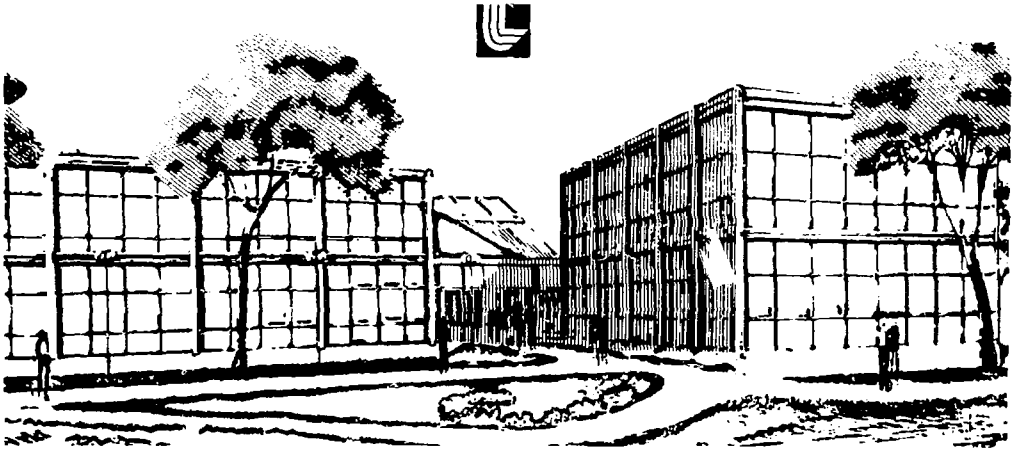
Lawrence Livermore Laboratory

Material Control Study: A Directed Graph and Fault Tree Procedure for Adversary Event Set Generation

H. E. Lambert, J. J. Lim, and F. M. Gilman

October 9, 1978

This paper was prepared for submission to:
NATO Advanced Institute: Synthesis and Analysis Methods for Safety and Reliability Studies, Urbino, Italy, July 3-14, 1978.



Material Control Study: A Directed Graph and Fault-Tree Procedure For Adversary Event Set Generation

H. E. Lambert, F. M. Gilman, and J. J. Lim*

Abstract

In work for the United States Nuclear Regulatory Commission, Lawrence Livermore Laboratory is developing an assessment procedure to evaluate the effectiveness of a potential nuclear facility licensee's material control (MC) system. The purpose of an MC system is to prevent the theft of special nuclear material such as plutonium and highly enriched uranium. The key in the assessment procedure is the generation and analysis of the adversary event sets by a directed graph and fault-tree methodology.

Introduction

The Lawrence Livermore Laboratory is conducting a Material Control and Accounting Study for the Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research. As part of their duties, the NRC is responsible for the licensing of new nuclear facilities. Since the safeguarding of nuclear materials has become increasingly important in recent years, the NRC must be able to systematically evaluate the material control systems of proposed nuclear facilities and to guarantee their effectiveness to the public. Each facility has a material control system to protect against the theft of special nuclear material, such as plutonium and uranium 235. In the two-year-old study, the Laboratory has been developing an assessment procedure to evaluate the effectiveness of a potential nuclear licensee's material control system [1].

The assessment procedure, shown in the block diagram in Figure 1, draws upon two types of data: license applicant information and the NRC/LLL data base. Applicant data include the plan of the facility physical plant, operational procedures, descriptions of special nuclear material processing, and the details of the material control and accounting system. The NRC/LLL data base will contain the mathematical models (such as models of the performance of the special nuclear material detection monitors) necessary to evaluate an applicant's submittal.

The first step in the assessment procedure is to identify targets within the facility that contain theft-attractive special nuclear material. The second step is to determine the adversary actions and conditions of the material control system that could allow successful diversion of special nuclear material, that is, generate the adversary event sets. Simulation is required for those adversary event sets where timeliness and ordering of events is important for successful diversion. The qualitative and quantitative analysis of the event sets and the simulation results allow the effectiveness of the material control system to be determined.

*This report was prepared for the U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research under research order No. 66-77-012 and under the auspices of the U.S. DOE, Contract No. W-7405-ENG-48.

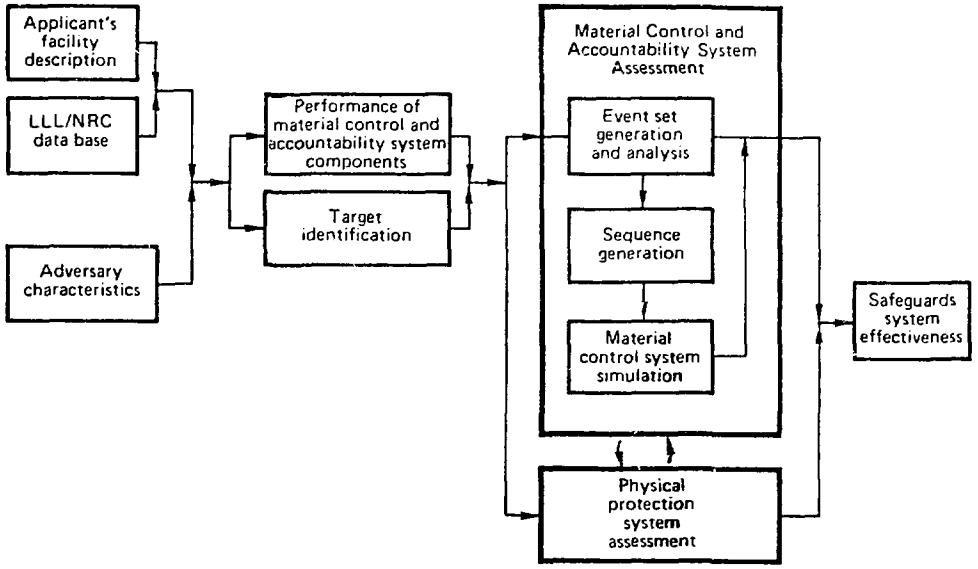


Figure 1. The LLL Assessment Procedure

Adversary Event Set Generation Procedure

The key in the LLL assessment procedure for evaluating the effectiveness of a material control system is the generation and analysis of adversary event sets. We have developed a procedure based on a directed graph (digraph) and fault-tree methodology by which the event sets can be generated and analyzed. This methodology has been used by Lapp and Powers [2] to assess the safety of chemical processing systems. We extended this methodology to model intentional diversionary or malevolent acts by an adversary so that these acts appear in the event sets.

The procedure for the generation and analysis of the event sets is described below, in detail, step by step, as delinated by the block diagram in Figure 2.

General System Schematic. The first step in the procedure (Figure 2) is the formulation of a general schematic for system modeling. Information from piping and instrumentation diagrams, the physical plant layout, and material control related procedures is used to formulate the schematic for system modeling. The general schematic delineates the unit model digraphs needed to model the system and the overall system interactions. The unit models include models of adversary movement in the facility, monitors, process equipment, and procedures.

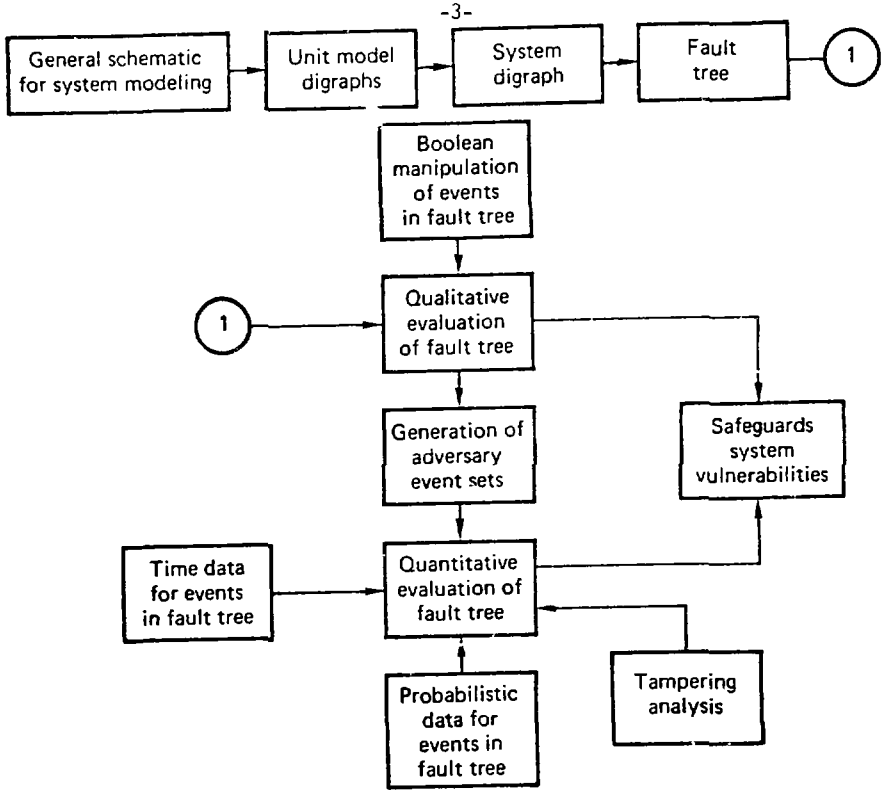


Figure 2. Procedure For Generation and Analysis of Adversary Event Sets

Unit Model Digraphs. In step 2 (Figure 2), unit model digraphs, the basic building blocks of the procedure, are generated. As described in Refs. 2 and 3, digraphs are functional cause-and-effect network models that describe the relationship between various system variables and the conditions that are necessary for these relationships to exist. In addition, digraphs can show events such as adversary actions that may nullify or change the relationships between variables. Digraphs are useful since they are multivalued network models and they can readily model the dynamics of the relationships between variables. The advantage of generating unit model digraphs is that a separate analysis can be performed on system components without performing an entire systems analysis. These unit models are analogous to mini-fault trees described by Fussell et al [4] and decision tables described by Salem et al [5].

System Digraph. The third step in Figure 2 is the generation of the system digraph, which is constructed from the unit model digraphs for a selected top event variable (the top event is the variable being modeled). The system digraph is obtained by deductively following the information flow given in the general system schematic. The material control system is modeled as a control system designed to counter the actions of the adversary. All the potential ways the material control system may respond to prevent special nuclear material theft are modeled in terms of "adversary cancellation loops" on the system digraph. These loops are similar in concept to the negative feedback and negative feedforward loops designed to cancel disturbances in process variables.

System-Fault Tree. In the fourth step (Figure 2), the system-fault tree is generated from the system digraph via a synthesis algorithm. The top event in the fault tree corresponds to a disturbance in the top event variable of the system digraph. The top event variable for the material control study is M_{DIV}, defined by

$$M_{DIV} = \begin{cases} +1 \text{ if successful diversion of} \\ \text{special nuclear material occurs} \\ 0 \text{ otherwise} \end{cases}$$

A zero value for a variable on the system digraph corresponds to a true or expected value. Any other value, hence, corresponds to a deviation or disturbance. The top event in the system fault tree for the material control study is $M_{DIV} = +1$. All loops in the system digraph that model the corrective actions of the material control system must fail for a disturbance in the top event variable to exist.

For successful diversion of special nuclear material to occur, all adversary cancellation loops must fail. These loops fail as the result of:

- random monitor failure
- inadequate monitor measurement sensitivity
- human error, including slow guard response
- adversary activity, including equipment tampering and collusion

The synthesis algorithm creates an AND logic gate in the fault tree each time a cancellation loop in the system digraph fails.

Once generated, the fault tree can be evaluated qualitatively and quantitatively to assess the vulnerabilities of the safeguard system.

Qualitative Analysis. The qualitative analysis of the fault tree provides much valuable information without using numerical data. It includes performing Boolean manipulations of the basic events, generating the adversary event sets, structurally ranking the basic events, determining the collusion requirements, and evaluating the effect of power loss on the material control system.

A structural ranking of the basic events in the event sets helps to identify important basic events for further analysis. This type of ranking is a function of the number of event sets in which a basic event appears in and the relative length of those event sets.

Common cause analysis is used to determine the collusion requirements (how many and who) and the effects of power loss of key components of the material control system for successful special nuclear material theft. In addition, a vital location analysis can be performed to determine the locations which must be visited for successful tampering.

The computer codes Fault-Tree Analysis Program (FTAP)[6] and the Set Equation Transformation System (SETS)[7], designed to generate and handle numerous, high-ordered minimal cut sets, are used to perform the qualitative analysis.

Quantitative Analysis. To further identify the weaknesses of the material control system, a quantitative analysis is performed. This analysis assesses the impact of material control system components with various failure rates and detection probabilities, the effect of maintenance policies, and the ease with which component tampering can occur. The IMPORTANCE computer code [8] is used to perform the quantitative assessment.

Inputs required for the quantitative analysis are a listing of all event sets, probability data for the basic events, and the assumption of statistical independence of the basic events.

The probability of successful theft of special nuclear material can be calculated for four specific cases:

(1) No material control system tampering, no alarm signal generated.
(2) No material control system tampering, slow safeguards response.
(3) Material control system tampering, no alarm signal generated.
(4) Material control system tampering, slow safeguards response.

A sensitivity analysis of the probability of successful theft for the above cases as a function of the amount of special nuclear material stolen is also done. Quantities of special nuclear material investigated are 0.5 g, 200 g, and 5 kg. The maximum expected performance of the material control system occurs when there is no system tampering. However, clever adversaries may tamper with the material control system to render it ineffective. In the tampering analysis, the following adversary attributes and material control system characteristics are considered:

- Type of tools and resources required for tampering
- Accessibility of components to potential adversaries
- Monitoring of equipment for tampering
- Availability of tools and resources required for tampering
- Personnel required for tampering

The probability of successful tampering is then a function of the probability that each of the above can occur with either no or slow material control system response.

Demonstration of the Event Set Generation Procedure

The event set generation and analysis procedure has been applied in the assessment of the material control system in a prototype nuclear facility, the Test Bed.[9]

The Test Bed is based upon the plutonium nitrate storage area of the AGNS facility in Barnwell, S.C., but with substantial modifications. These modifications are added to further develop and test the assessment procedure and are not criticisms or "fixes" to the AGNS current design. The modifications include the addition of check valves, limit switches on valves, a computer-controlled access system, computerized material control and accounting and procedure monitoring logic, and other safeguards components.

The general form of the system digraph for the Test Bed is shown in Figure 3. The arrows represent information flow with regard to (1) movement of special nuclear material and people, and (2) the material control system response which acts to prevent the theft of special nuclear material. The initial conditions of the Test Bed assessment are shown on the left of Figure 3.

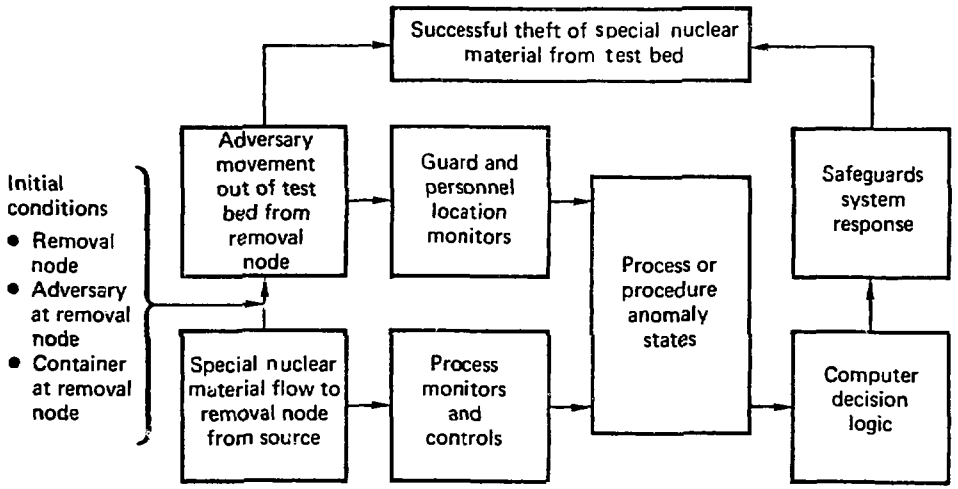


Figure 3. General Form of System Digraph for Test Bed

The fault tree generated from the system digraph by the synthesis algorithm contained 125 gate events and 113 basic events. The qualitative analysis of the fault tree generated 814,042 event sets for the case of a slow safeguards response and 4,736 event sets for the case of no safeguards response. These adversary event sets ranged in length from 18 basic events to 42 basic events. These event sets were very descriptive and contained all the adversary acts necessary for successful diversion including the route for adversary movement in and out of the facility.

The collusion analysis established that successful diversion can occur only if three particular plant personnel are in collusion or two persons if random failures occur.

The IMPORTANCE computer code determined the probability of each basic event in contributing to the probability of successful diversion. The ranking of these basic events found the following vulnerable points in the Test Bed:

- computer hardware and software
- remote control panel
- crash door alarms
- maintenance policies

Although the Test Bed is a facility with an automated and sophisticated material control system, the assessment has found several basic weaknesses. A similar assessment can determine the effect of strengthening the aforementioned areas. Thus, the Test Bed demonstration has shown the directed graph-fault tree procedure (Figure 3) is not only an effective assessment tool but also a valuable design tool. The procedure can also be used for safety and reliability analysis.

Future Activities

In the future, the adversary event set generation procedure described in this article will be used to assess the effectiveness of an existing nuclear facility handling special nuclear material. In addition, the assessment procedure will be automated as much as possible. Fault tree computer codes FTAP, SETS, and IMPORTANCE currently exist to qualitatively and quantitatively evaluate fault trees. Computer codes to perform the front end of the procedure, i.e., the manipulation, storage and generation of unit model digraphs, and system fault trees, are currently in the developmental stages.

REFERENCES

1. A. Maimoni, "Safeguards Research: Assessing Material Control and Accounting System," Energy and Technology Review, Lawrence Livermore Laboratory, Rept. UCRL-52000-77-11/12 (1977).

2. S. A. Lapp and G. J. Powers, "Computer Aided Synthesis of Fault Trees" in IEEE Trans on Rel. R-26 (1)(1977).

3. H. E. Lambert and J. J. Lim, The Modeling of Adversary Action for Safeguards Effectiveness Assessment, Lawrence Livermore Laboratory, Rept. UCRL-79217, Rev. 1 (1977).

4. J. B. Fussell et al., A Collection of Methods for Reliability and Safety Engineering, Idaho National Engineering Laboratory, Idaho Falls, Rept. ANCR-1273 (1976).

5. S. L. Salem, G. E. Apostolakis, and D. Okrent, "A New Methodology for the Computer the Computer-Aided Construction of Fault Trees," Annals of Nuclear Energy, 4 (1977) 417-433.

6. R. Willie, Fault Tree Analysis Program, Operations Research Center Report No. ORC 78-14, University of California, Berkeley (1978).

7. R. B. Worrell, Set Equation Transformation System (SETS), Sandia Laboratories, Albuquerque, New Mexico, Rept. SLA-73-0028A (1974).

8. H. E. Lambert and F. M. Gilman, The IMPORTANCE Computer Code, Lawrence Livermore Laboratory, Rept. UCRL-79269 (1977).

9. I. J. Sacks, et al., Material Control System Design: Test Bed Nitrate Storage Area (TBNSA), Lawrence Livermore Laboratory, Rept. UCID-17525-77-3 (1978).