PREPRINT UCRL-79217,Rev. 1

# Lawrence Livermore Laboratory

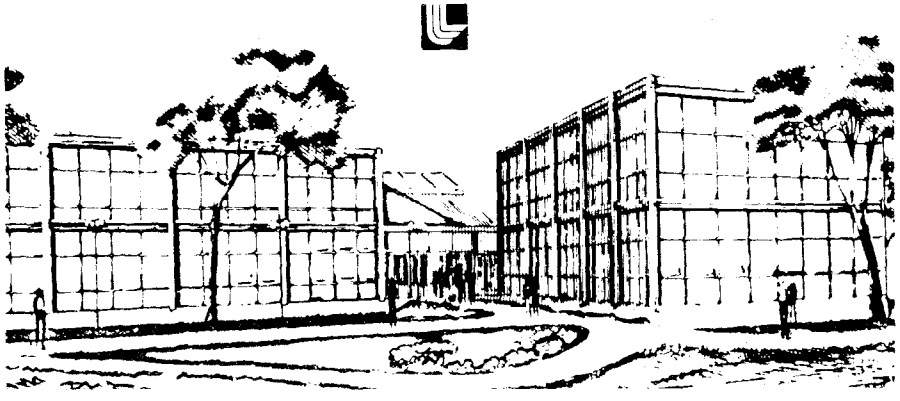
The Modeling of Adversary Action for Safeguards Effectiveness Assessment

Howard E. Lambert and Judy J. Lim

June 1977

THIS PAPER WAS PREPARED FOR SUBMISSION TO:
Institute of Nuclear Materials Management 1977 Annual Meeting, Stouffer's National Center Hotel, Arlington, VA - June 29-July 1, 1977





# THE MODELING OF ADVERSARY ACTION FOR SAFEGUARDS EFFECTIVENESS ASSESSMENT **

Howard E. Lambert and Judy J. Lim

Lawrence Livermore Laboratory
University of California
Livermore, California

ABSTRACT

In the procedure for the assessment of material control systems being developed at Lawrence Livermore Laboratory, one of the major requirements is the systematic development of adversary action sequences and stimuli. Stimuli refer to the disturbances in state or process variables that occur as the result of adversary activity, such as diversion or concealment activities. This paper presents an approach to generate adversary action sequences on the basis of graph theory and fault tree analysis. The resulting stimuli can then be generated from these sequences.

Lawrence Livermore Laboratory (LLL) is conducting a material control study for the Nuclear Regulatory Commission (NRC). This study is to develop evaluative tools by which the NRC can assess the effectiveness of a potential licensee's material control (MC) system. The purpose of the MC system is to protect against diversion of special nuclear material (SNM) by (1) limiting opportunities for diversion, (2) detecting diversion, (3) reacting to detection of diversion.

LLL is developing a multi-phase procedure (Figure 1) to assess the effectiveness of the MC system. Basically the assessment procedure entails the generation of the MC test input, the determination of the MC responses, and the analysis of the MC response results.

One of the major requirements of the procedure is the generation of adversary action sequences and the stimuli resulting from these sequences. Stimuli refer to disturbances in the state or process variables that occur as the result of adversary actions, such as diversion or concealment activities. These stimuli will be identified by the minimal cut sets obtained from fault tree analysis. The fault tree is automatically generated from directed graph models called digraphs. [2]

This paper will describe the digraph-fault tree methodology employed by LLL to generate the potential sequences of adversary actions. Fault tree analysis (FTA) has traditionally been used since the early 1960's for safety and reliability analyses in the aerospace and nuclear industries. At LLL, we plan to extend FTA to model intentional diversionary or malevolent acts. Specifically, we shall use FTA to identify the combinations of adversary activities necessary and sufficient for successful theft of special nuclear material (SNM). At each location in the plant where the adversary can gain

** 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. Energy Research and Development Administration, Contract No. W-7405-ENG-48.



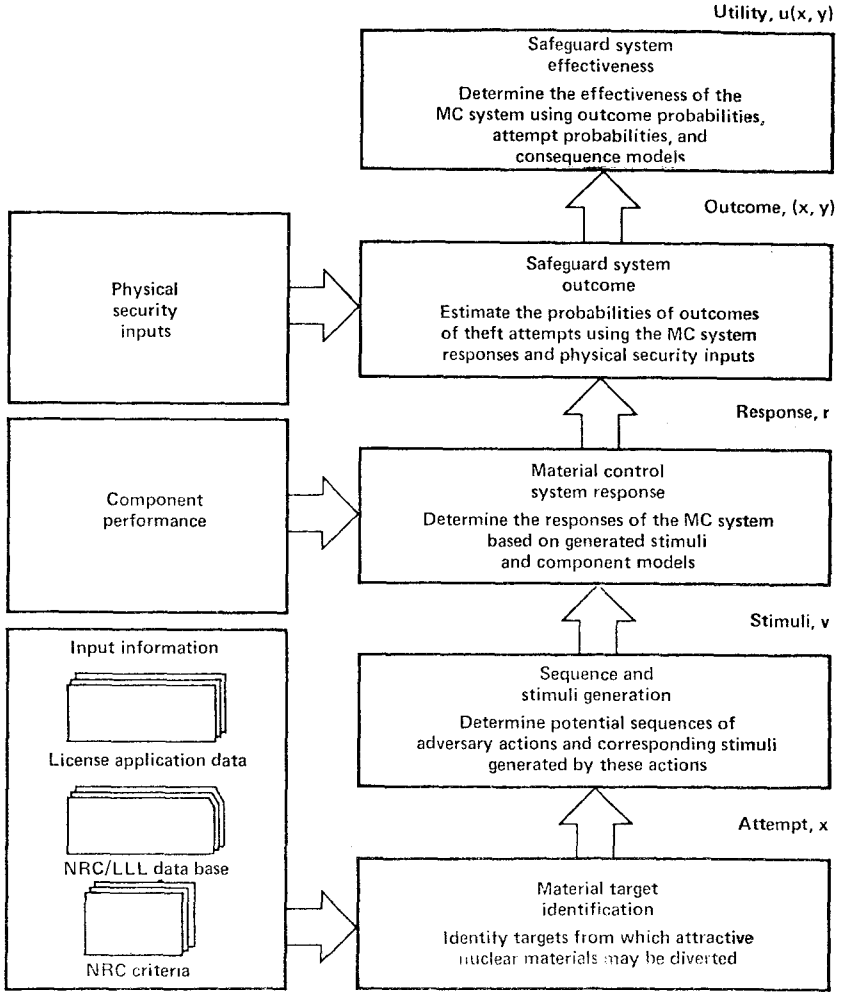



Figure 1 Procedures for the Evaluation of Material Control Systems - Overall Block Diagram

access to theft-attractive SNM, we plan to generate fault trees with top events "successful diversion of SNM." The basic events in these fault trees are (1) adversary activities such as diversion or concealment activities and (2) human error or equipment failure that can increase the adversary's probability of success. The minimal cut sets are the smallest sets of basic events necessary and sufficient for successful diversion of SNM.

To automate generation of these fault trees we plan to use an approach similar to the approach developed by Lapp and Powers [2] based on graph theory. The basic building blocks of their methodology are directed graphs models called digraphs. A digraph is a location-specific graph that depicts the normal relationship between process variables. In addition, the digraph includes events that can nullify or change the normal relationship between process variables. Thus digraphs can be extended to show the relationship between MC system variables and can facilitate modeling adversary actions. Individual digraphs can be constructed for system components and pieced together to generate a system digraph. Fault trees can then be automatically generated from a system digraph via a synthesis algorithm [2].

There are several advantages to using digraphs directly rather than manually constructing fault trees. First, a fault tree constructed from a system digraph is easier to check than a manually constructed fault tree. In a manually constructed fault tree, one must infer the cause-and-effect relationships existing between process and state variables from the event description in the fault tree. In a system digraph, one can readily follow the relationships which are clearly displayed. Secondly, digraphs reduce the problem of different analysts constructing different fault trees for the same system. The same fault tree is always obtained from a specific system digraph regardless of the analyst. Lastly, digraphs remove much of the redundant work required in the manual construction of fault trees. Only one digraph must be constructed for each particular system component. Thus the digraph may be used again and again wherever the particular component appears in the system.

A brief description of the digraph-fault tree generation scheme is now given. We also present the basic terminology and notation of digraphs and the concepts of feedback and feedforward control loops.

A digraph consists of nodes and edges. Nodes in the digraph represent either state variables, process variables, or events. If one variable or event effects another variable or event, a directed arrow or edge connects the independent variable or event to the dependent one. The directed edge may either be a normal edge which indicates the relationship is normally true, or a conditional edge which indicates the relationship is true only when the condition exists.

Numbers may be placed on the directed edge to represent the gains between the two variables or events. The information to calculate these gains is obtained from $\partial Y/\partial X$, where X and Y denote the independent and dependent variables or events respectively. The magnitudes of the gains used in digraphs are quantized into five discrete values of -10, -1, 0, +1, +10. Gains of $\pm 10$ represent large or fast disturbances which are beyond the capability of a negative feedback loop to cancel. Gains of $\pm 1$ represent normal disturbances which a negative feedback loop is able to cancel. Gains of 0 indicate no relationship exists between the two variables or events.

State or process variables and abnormal events occurring at a specific



location are represented by alphanumeric labels on the nodes. For instance "T1", "P2", "M3", "FIRE at HX" represent temperature at location 1, pressure at location 2, mass flow rate at location 3, and fire at heat exchanger, respectively. The direction of the deviations in the values of state or process variables and abnormal events are denoted by "+" and "-". These deviations have magnitudes of "0", "1" and "10". A magnitude of 10 indicates a range of values that is considered large; a magnitude of 1 indicates a range of values that is considered moderate. A magnitude of 0 represents a true or expected range of values of the variable or event. Hence the same scheme of -10, -1, 0, +1, +10 is also used to represent the deviations in the values of the variables or events. For instance T1(+10) now represents a large increase in temperature at location one and P2(0) represents the true or expected value of pressure at location two.

Some variables or events may be univariant; that is, they deviate only in the positive direction or only in the negative direction. For instance, "FIRE at HX" is a univariant variable.

We now provide an example to illustrate the concepts discussed above. Consider the system shown in figure 2 of a storage tank containing plutonium nitrate solution. The level of the solution in the tank, L, is determined by measuring the difference between pressures $P_1$ and $P_2$, $\Delta P_{1-2}$, and the liquid density, $\rho$. An air supply (not shown) provides air to lines 1 and 2.

Air in line 1 enters the tank at level $L_1$. The pressure of the entering air equals the static pressure of the liquid at level $L_1$ and the atmospheric air pressure, $P_2$. Be measuring $\Delta P_{1-2}$ and $\rho$, one can determine the level of solution in the tank. A simple digraph of the differential pressure cell is given in figure 3. A gain of +1 between level, L, and pressure $P_1$, implies that a moderate increase (or decrease) in L results in a moderate increase (or decrease) in $P_1$. A potential adversary event, shown by the conditional edge labeled "line 1 pinched," results in a zero gain between L and $P_1$. This implies that if the line were pinched, an adversary could divert plutonium nitrate from the tank and no change in $P_1$ and hence indicated level, $L_I$, would result. A gain of -1 between $P_2$ and $L_I$ implies that a moderate increase (or decrease) in $P_2$ results in a moderate decrease (or increase) in $P_1$. Vacuum on line 2 is a univariant variable with value 1 if vacuum is applied, and value 0 if vacuum is not applied. The table in figure 3 illustrates information that a generic digraph or unit model of a differential pressure cell would contain. It is by no means complete, relations regarding failure modes such as leaking and plugging must also be included.

A system digraph is generated with respect to a specific top event of a fault tree. It is constructed by using the information contained in the digraphs of the individual system components and by working backwards through the cause-and-effect relationships of the variables and events. Process control must also be modeled in the system digraph, specifically feedback and feedforward control loops. The purpose of these control loops are to cancel disturbances that may occur in process variables.

Lapp and Powers [2] has demonstrated how to model negative feedback and negative feedforward control loops using system digraphs. A negative feedback loop (NFBL) is a path in the digraph which starts and ends at the same node. NFBL's have the property that the product of the normal gains around the feedback loop is negative. In contrast, a negative feedforward

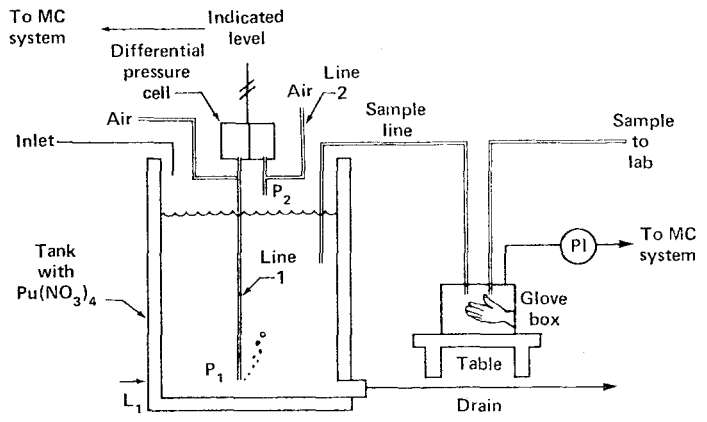
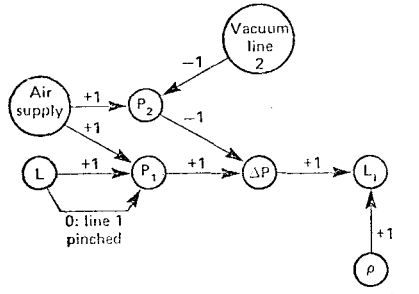



Figure 2 Tank with Bubbler




| | $P_1$ | $P_2$ | ΔP | $L_1$ |
|---|---|---|---|---|
| Air supply | +1 | +1 | | |
| L | +1 | | | |
| Vacuum line 2 | | −1 | | |
| $P_2$ | | | −1 | |
| $P_1$ | | | +1 | |
| ΔP | | | | +1 |
| ρ | | | | +1 |
| Failure: Line pinched | Change L to $P_1$ Gain to 0 | | | |

Figure 3 Digraph of Differential Pressure Cell



loop (NFFL) consists of two or more paths which start from the same node and merge together at a different node in the digraph. NFFL's have the property that the sign of the product of the normal gains on one of the paths is different from the others. For a NFFL to exist, the gains and dynamics of all branches must be equal.

We now show how all corrective actions in the MC system can be modeled using NFBL's and NFFL's. Furthermore, we also show that all control loops in the MC system digraph must fail in order for successful diversion of SNM to occur.

The use of the digraph-fault tree approach to model the MC system is best illustrated by an example. Consider the glove box in figure 2 that is used to sample plutonium nitrate from the storage tank via the sample line. A technician transfers the sample through a pneumatic sample line to the laboratory for chemical analysis. The glove box is under vacuum. In this example, it is assumed that the material control system will notify security to investigate an abnormal situation when the following stimuli are received:

1. Loss of vacuum detected by a pressure sensor on the glove box.

2. Change in level reading determined by a differential pressure cell measurement as described previously.

In addition, MC system procedures require security to inspect the glove box area at random time intervals and apphrehend any personnel diverting SNM.

The following equipment malfunctions and characteristics, human error, and adversary actions (AA) are considered in this example:

a) pressure sensors stuck
b) inadequate sensitivity in measuring instrumentation
c) no or slow response from security
d) pressure transmitting lines pinched (AA)
e) cutting and clamping of gloves (AA)
f) liquid substitution (AA)
g) applying vacuum on line 2 (AA)

The system digraph for this example is given in figure 4. Diversion can occur from the glove box if the glove box is physically penetrated, such as by cutting the gloves on the glove box. The variable chosen to be the top event node in the system digraph is $M_{DIV}$, a univariant variable defined by

$$M_{DIV} = \begin{cases} 1 \text{ if successful diversion occurs} \\ 0 \text{ otherwise} \end{cases}$$

Hence, the top event of the fault tree is a disturbance of + 1 in $M_{DIV}$, i.e., $M_{DIV} = +1$.

The generation of the system digraph is now explained in more detail. The system digraph will model the material flow, the process, and the material control system. In order that deductive logic be applied, it is important to note that the modeling of material flow proceeds backwards from the acquisition point to the material source. The basic procedure for generation of the system digraph follows. 1) Generation of the "normal" system digraph

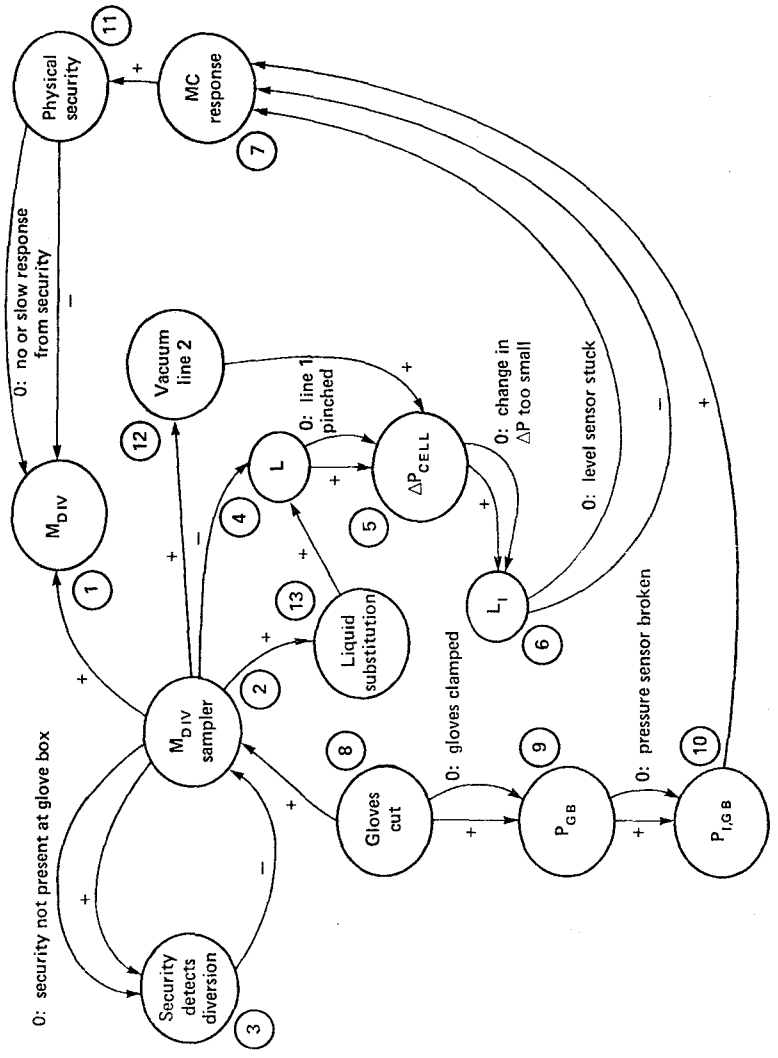



Figure 4. System Diagraph



including the feedback and feedforward loops that indicate the corrective actions taken by the MC system in response to detection of adversary activity. 2) Identification of adversary activities, equipment failures, and human error that can inactivate the effect of control loops in the "normal" digraph, e.g., inactivating sensors or security actions. 3) Investigation of the means by which the adversary can create NFFL's to cancel the effect of an adversary activity on the "normal" system digraph. 4) Generation of the system digraph for each acquisition point by combining 2) and 3).

In figure 4, corrective actions by the material control system occur by one negative feedback loop, NFBL, and two negative feedforward loops, NFFL's.

| | PATHS |
|---|---|
| NFBL | |
| Security detecting adversary at Glove Box | Nodes 2, 3, 2 (product of gains is -1) |
| NFFL #1 | |
| Response to change in Level | Nodes 2, 1 (Product of gains is +1)<br>Nodes 2, 4, 5, 6, 7, 11, 1 (Product of gains is -1) |
| NFFL #2 | |
| Response to change in Glove Box pressure | Nodes 8, 2, 1 (Product of gains is +1)<br>Nodes 8, 9, 10, 7, 11, 1 (Product of gains is - 1) |

This example assumes that, the presence of the adversary diverting material at the glove box causes security to apprehend the adversary. This situation is is best modeled by feedback loops. Hence, the disturbance of the adversary as shown in the digraph is canceled, i.e., $M_{DIV,\ SAMPLER} = +1$ becomes $M_{DIV,\ SAMPLER} = 0$.

In the case of the two negative feedforward loops, an adversary activity creates a disturbance in a process variable, i.e., a stimulus, which initiates the material control system to notify security. There may be a finite time delay before the adversary is apprehended or he may not be caught in the act at all. In either case a response must be considered and this situation is best modeled by negative feedforward loops.

In the case of NFFL #1, the adversary diverts material which causes a + 1 disturbance in $M_{DIV}$ (as verified by examining the path with nodes 2 and 1 with gain of + 1). However, diversion of material should cause the solution level to go down and alert security resulting in a -1 corrective action at node 1. (A + 1 disturbance entering the path with nodes 2, 4, 5, 6, 7, 11, 1 becomes - 1 at node 1 since the net gain of this path is - 1). Hence, the adversary with the plutonium nitrate should be apprehended and a + 1 disturbance in $M_{DIV}$ is cancelled, i.e., $M_{DIV} = 0$.

The effect of these loops must be nullified for successful diversion of SNM to occur. This can occur in two ways.

1. Adversary activity, equipment failure, or human error causes a zero gain on these loops.

2. The adversary himself cancels the effect of his disturbance by creating negative feedforward loops.

As an example of two above, the adversary can divert material and substitute liquid as shown by

| NFFL #3 | PATHS |
|---|---|
| Diverts SNM and adds liquid to keep level constant | Nodes 2, 4<br>Nodes 2, 13, 4 |

Another example of a NFFL is shown by NFFL #4. The adversary(s) can withdraw liquid and simultaneously apply a vacuum on line two to keep the differential cell pressure, $\Delta P_{CELL}$, and hence, the indicated level, $L_I$, constant.

| NFFL #4 | PATHS |
|---|---|
| Cancel effect on indicated level by applying a vacuum | Nodes 2, 4, 5<br>Nodes 2, 12, 5 |

A fault tree is constructed in figure 5 with the top event "Successful diversion of SNM, i.e., $M_{DIV} = +1$. It is generated using the Lapp-Powers fault tree synthesis algorithm.[2] The minimal cut sets of the fault tree are listed in Table 1. They represent the possible combinations of adversary activities and events that can result in successful diversion of SNM.

The modeling of operational and monitoring procedures has not been described in this paper. However, these procedures can be modeled in the same generic fashion as is illustrated by the digraph in figure 4. The people in procedures can be modeled as operators or monitors, and concealment activities such as falsification of records can be shown as zero gains on the digraph.

A general methodology is now specified for the generation of the minimal cut sets which result in successful diversion of SNM.

1) Identification of the locations or sources of theft-attractive SNM in the plant (Material Target Identification in figure 1).

2) Identification of all potential acquisition points of attractive SNM in the plant.

3) Generation of a system digraph for each acquisition point in the plant with the top event node, $M_{DIV}$, diversion of SNM from the specified acquisition point.

4) Synthesis of a fault tree from the system digraph with the top event, $M_{DIV} = +1$, at each acquisition node.

5) Obtaining the minimal cut sets from the fault tree.

Once the minimal cut sets are obtained, they are examined to assess the likelihood of successful diversion of SNM. These minimal cut sets indicate



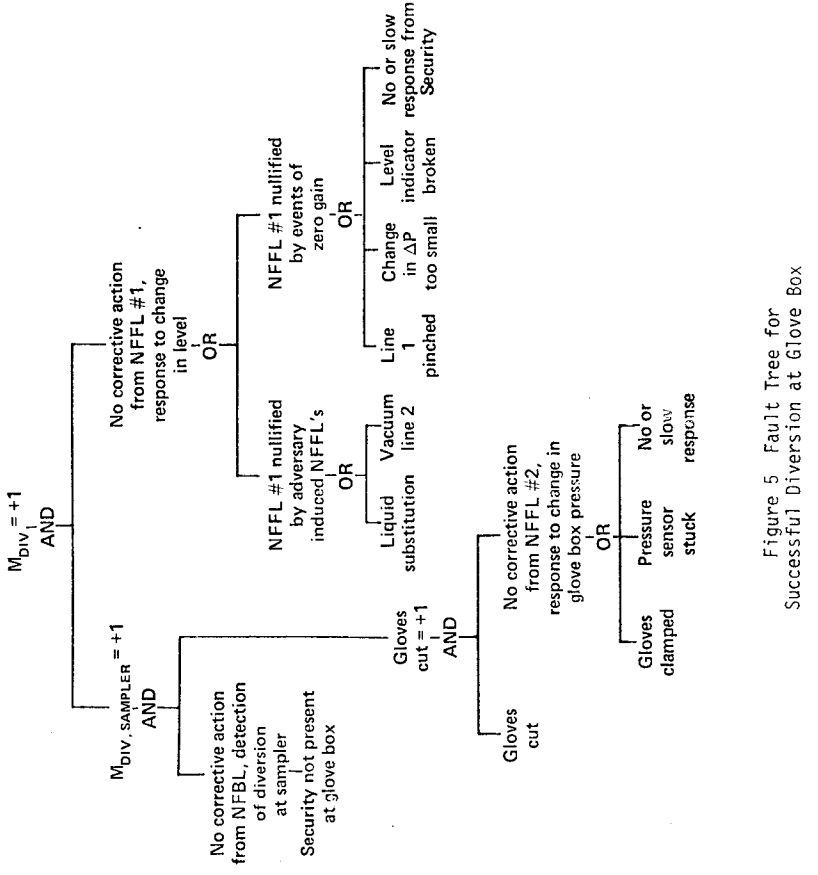



Figure 5 Fault Tree for Successful Diversion at Glove Box

TABLE 1

List of Minimal Cut Sets

| Minimal Cut Set No. | Description |
|---|---|
| 1. | {Security Not Present at G. B.* & Gloves Cut & No or Slow Response by Security} |
| 2. | {Security Not Present at G. B. & Gloves Cut & Gloves Clamped & Liquid Substitution} |
| 3. | {Security Not Present at G. B. & Gloves Cut & Gloves Clamped & Vacuum on Line 2} |
| 4. | {Security Not Present at G. B. & Gloves Cut & Gloves Clamped & Line 1 Pinched} |
| 5. | {Security Not Present at G. B. & Glove Cut & Gloves Clamped & Changed in ΔP too Small} |
| 6. | {Security Not Present at G. B. & Glove Cut & Gloves Clamped & Level Indicator Stuck} |

Minimal cut sets 7-11 are the same as minimal cut sets 2-6 respectively except the basic event "Gloves Clamped" is replaced by "Pressure Sensor Stuck."

* G. B. represents Glove Box



which feedback and feedforward loops can be inactivated and can suggest where improvements in the MC system may be made.

Information regarding the time ordering of the basic events in the minimal cut sets is required for the generation of the adversary action sequences. In addition, any dependency of a basic event on the process or material control system must be specified. Adversary action sequences that must be accomplished in collusion can be identified by a similar approach to common cause analysis in fault trees [3]. With the above information, a representative set of stimuli can be generated from the basic events in the minimal cut sets. This set will serve as a test input into the simulation model which determines the material control system response.

At LLL the philosophy is to automate the digraph-fault tree approach as much as possible in the generation of adversary action sequences. Automation of this approach will be accomplished by 1) generating a library of generic digraphs of equipment, devices, monitors, etc., 2) developing a computerized procedure to generate system digraphs from generic digraphs.

## References

1. "A Material Control Assessment Procedure", R. Adams and L. R. Spogen this proceedings

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

3. R. B. Worrell and G. R. Burdick, "Qualitative Analysis in Reliability & Safety Studies" IEEE Trans. on Rel., R-25 (3) 1976.

## Acknowledgements

The authors wish to thank Steven Lapp and Gary Powers for their help in developing the methodology presented in this paper.

*Technical Information Department*
LAWRENCE LIVERMORE LABORATORY
University of California | Livermore, California | 94550

175 938