T'C

NUREG/CR-0777
UCRL-52710

A DIGRAPH-FAULT TREE METHODOLOGY FOR THE ASSESSMENT OF MATERIAL CONTROL SYSTEMS

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

Prepared for
U. S. Nuclear Regulatory Commission
by
Lawrence Livermore Laboratory

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

The views expressed in this report are not necessarily those of the U. S. Nuclear Regulatory Commission.

Available from U. S. Nuclear Regulatory Commission Washington, D. C. 20555

Available from National Technical Information Service Springfield, Virginia 22161

NUREG/CR-0777
UCRL-52710

A DIGRAPH-FAULT TREE METHODOLOGY FOR THE ASSESSMENT OF MATERIAL CONTROL SYSTEMS

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

Manuscript Submitted: May 21, 1979
Date Published:

Prepared for
Safeguards

U.S. Nuclear Regulatory Commission
Washington, D. C. 20555
Under Interagency Agreement DOE 40-550-75

NRC FIN No. A-0115
by
Lawrence Livermore Laboratory
Livermore, CA 94550

operated by University of California

for the U.S. Department of Energy

CONTENTS

FIGURES

TABLES

ACRONYMS

AES	Adversary event sets
AESS	Adversary event subsets
AGNS	Allied General Nuclear Services
CCAS	Computer-controlled access system
CCTV	Closed circuit television
DP	Differential pressure
FMEA	Failure modes and effects analysis
FTA	Fault tree analysis
FTAP	Fault Tree Analysis Program
GB	Glove box
I.D.	Identification
LS	Limit switch
MAA	Material access area
MC	Material control
MC&A	Material control and accounting
MCS	Material control system
MCSS	Material control system simulator
MTI	Moving target indicator
NFBL	Negative feedback loop
NFFL	Negative feedforward loop
NMCO	Nuclear materials control officer
NRC	Nuclear Regulatory Commission
PNSA	Plutonium nitrate storage area
PPC	Plutonium product cell
SETS	Set Equation Transformation System
SNM	Special nuclear material
SS	Security station
TDR	Theft danger rating
VP	Valve position

ABSTRACT

The Lawrence Livermore Laboratory, under contract to the United States Nuclear Regulatory Commission, is developing a procedure to assess the effectiveness of material control and accounting systems at nuclear fuel cycle facilities. The purpose of a material control and accounting system is to prevent the theft of special nuclear material such as plutonium or highly enriched uranium. This report presents the use of a directed graph and fault tree analysis methodology in the assessment procedure. This methodology is demonstrated by assessing a simulated material control system design, the Test Bed.

1.0 INTRODUCTION

The Nuclear Regulatory Commission (NRC) is responsible for the licensing of commercial nuclear facilities. Each facility is required to have a Material Control and Accounting (MC&A) system designed to protect against the theft of special nuclear material (SNM), such as plutonium or highly enriched uranium. Material control is that part of the safeguards system that encompasses management and process controls to assign and exercise responsibility for nuclear material; maintain vigilance over the material; govern its internal movement, location, and utilization; and monitor the inventory status of all material and assessment for all material. The material accounting part encompasses the procedures and systems to perform nuclear material measurements, maintain records, provide input, and perform data analysis to account for nuclear material. Since the safeguarding of nuclear materials is of grave concern, the NRC must be able to systematically evaluate the MC&A systems of nuclear facilities and to assure the public that these systems are effective. The Lawrence Livermore Laboratory (LLL) has been developing an assessment procedure to evaluate the effectiveness of MC&A systems for the Office of Nuclear Regulatory Research.[1] The assessment procedure is based on a directed graph (digraph) and fault tree methodology. This report presents the application of this methodology in the assessment of a simulated material control system design, the Test Bed.[2] The Test Bed assessment was initiated in September 1977 and completed in January 1978. It reflects LLL's perception of the problem in January 1978.

Subsequent to the Test Bed assessment, the methodology has been modified in response to the insights gained and the problems encountered in the assessment. In addition, alternative methodologies have been developed. Both of these more recent methodologies have been demonstrated on an existing fuel cycle facility.[3,4] However, the digraph-fault tree methodology has provided the framework for the more recent work; it has provided the initial solution to the most difficult portion of the assessment procedure, the systematic generation of adversary event sets.

The LLL assessment procedure is based on the concept that a safeguards system and an adversary's perturbation of the system can be modeled, and that the model can be mathematically analyzed to determine the system vulnerabilities. This procedure leads to an objective assessment (to the extent that the model can be developed objectively) that is performance-based and uniform across facilities.

Figure 1 is a block diagram of the LLL assessment procedure. The procedure requires three types of data: license applicant information, the NRC/LLL data base, and the characteristics of adversaries against whom one is protecting the system. Applicant data include the description of the physical plant, operational procedures, descriptions of SNM processing, and the details of the MC&A system. The NRC/LLL data base contains performance data on MC&A system components and serves as a standard against which the applicant data are compared. Adversary characteristics define a broad spectrum of adversary types and capabilities.

The first step in the assessment procedure is to identify the targets within the facility. The possible locations for theft-attractive SNM are identified and ranked. At the same time, performance models are developed for the components in the MC&A system. These two steps in the Test Bed assessment are described in Sections 4.1 and 4.4.

The heart of the assessment procedure is contained in the block labeled "Material control and accounting system assessment" in Fig. 1. After the facility targets have been identified, the next step is to determine the adversary actions and conditions of the material control system that can allow successful diversion of special nuclear material, that is, generate the SNM theft scenarios. Each scenario is called an adversary event set because it describes all the events that must be accomplished in order for an adversary to perpetrate a theft. Simulation of the events may be required for those adversary event sets in which timeliness and ordering of events are important for successful theft.

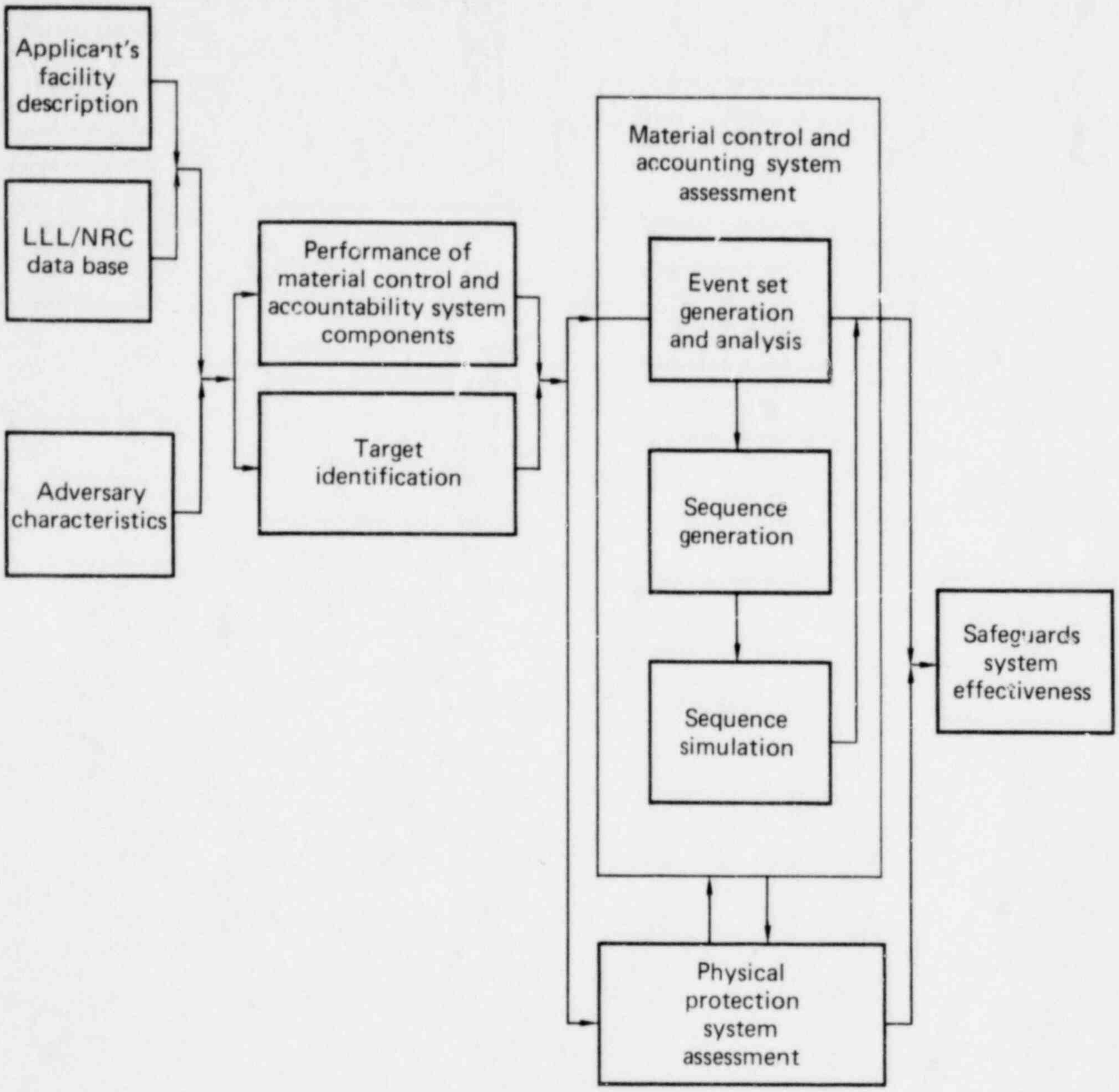

Applicant's facility description
LLL/NRC data base
Adversary characteristics
Performance of material control and accountability system components
Target identification
Material control and accounting system assessment
Event set generation and analysis
Sequence generation
Sequence simulation
Physical protection system assessment
Safeguards system effectiveness

FIG. 1. The LLL assessment procedure.

The assessment of the MC&A system must be combined with the assessment of the physical protection system.[5] The final block at the right of Fig. 1 depicts the step of determining the overall effectiveness of the safeguards system. The qualitative and quantitative analyses of the adversary event sets, the simulation results, and the results of the physical protection system assessment are integrated to provide the safeguards system reliability, sensitivity, and hardness against SNM theft.

2.0 DIGRAPH-FAULT TREE METHODOLOGY

The key in the LLL assessment procedure for evaluating the effectiveness of an MC&A system is the generation and analysis of adversary event sets. The procedure is 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[6] to assess the safety of chemical processing systems and extended by LLL to model intentional diversionary or malevolent acts by an adversary.

Figure 2 shows the procedure for the generation and analysis of adversary event sets.

2.1 GENERAL SYSTEM SCHEMATIC

The first step in the procedure (Fig. 2) is the formulation of a general schematic for system modeling. Information from piping and instrumentation diagrams, the physical plant layout, and MC&A-related procedures is used to formulate the schematic. 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.

2.2 UNIT MODEL DIGRAPHS

In the second step in Fig. 2, unit model digraphs, the basic building blocks of the procedure, are generated. Digraphs are functional cause-and-effect models that describe the relationships among various system variables and the conditions that are necessary for these relationships to exist.[6,7] In addition, digraphs can show events such as adversary actions that may nullify or change the relationships among variables. Digraphs are useful because they are multivalued network models and can readily model the dynamics of the relationships among variables. The advantage of generating unit model digraphs is that separate analyses can be performed on system components

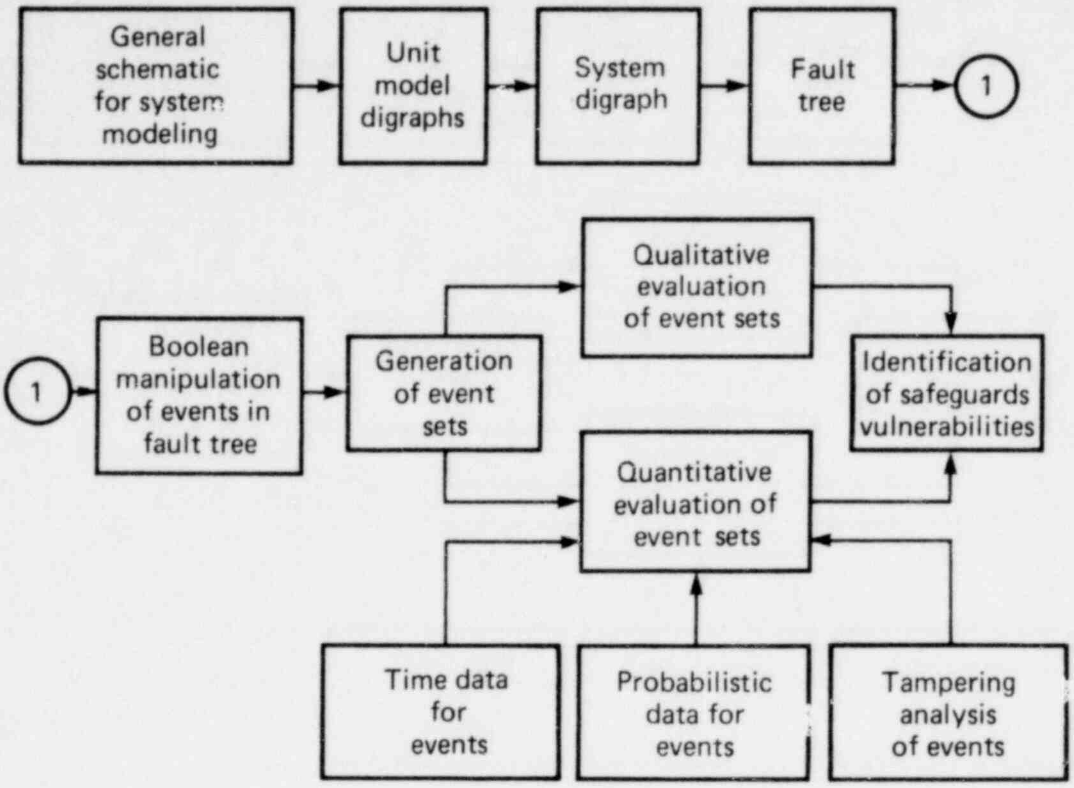

General schematic for system modeling
Unit model digraphs
System digraph
Fault tree
1
1
Boolean manipulation of events in fault tree
Generation of event sets
Qualitative evaluation of event sets
Quantitative evaluation of event sets
Identification of safeguards vulnerabilities
Time data for events
Probabilistic data for events
Tampering analysis of events

FIG. 2. Procedure for generation and analysis of adversary event sets.

without performing an entire systems analysis. These unit models are analogous to minifault trees described by Fussell, et al.,[8] and decision tables described by Salem, et al.[9]

2.3 SYSTEM DIGRAPH

The third step in Fig. 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 event being modeled). The system digraph is obtained by following in detail the cause-and-effect information flow outlined in the general system schematic. The material control and accounting system is modeled as a control system designed to counter adversary actions. All potential ways in which the material control system can respond to prevent special nuclear material theft are modeled in terms of "adversary cancellation loops" on the system digraph. These loops are similar to the negative feedback and negative feedforward loops designed to cancel disturbances in process variables.

Figure 3 shows the main elements used in the modeling of the system digraph. To divert SNM successfully, the adversary must move material out of the Test Bed from the target (a material removal node). We specify the initial conditions for the analysis, such as the particular removal node being analyzed and the adversary attributes. Given these conditions, we trace the material flow path from its source, such as a storage tank, and the adversary actions needed to induce this flow. These actions of the adversary generate a series of signals in the safeguards system, which acts to counter the adversary. The safeguards system is modeled in terms of feedback and feedforward control loops. Figure 3 shows the main feedforward control loop and continues through the reactions of the various monitors. The reactions are mapped against the plant operating procedures to obtain the anomaly states of the system. These states are used by the computer decision logic of the system to generate the appropriate safeguards system response, such as activation of the guard force, which then acts to counter the adversary.

In order to identify the safeguards system vulnerablities, the places where information flow can be prevented must be determined on the system digraph.

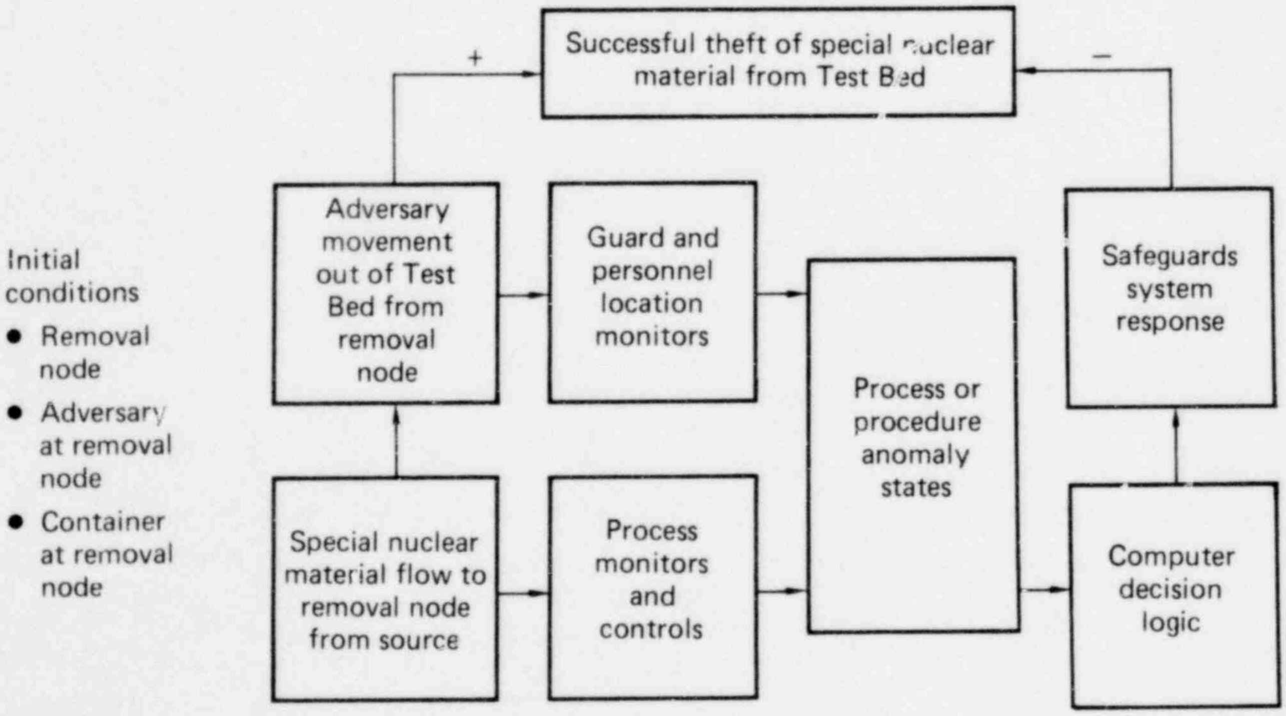

Successful theft of special nuclear material from Test Bed
+
–
Initial conditions
• Removal node
• Adversary at removal node
• Container at removal node
Adversary movement out of Test Bed from removal node
Guard and personnel location monitors
Safeguards system response
Process or procedure anomaly states
Special nuclear material flow to removal node from source
Process monitors and controls
Computer decision logic

FIG. 3. General form of system digraph for Test Bed assessment.

2.4 SYSTEM FAULT TREE

In the fourth step of Fig. 2, the system fault tree is generated from the system digraph by means of a transformation 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 material control and accounting assessment is M_{DIV}, defined by

$$M_{DIV} = \begin{cases} +1 \text{ if successful theft of} \\ \quad \text{SNM occurs,} \\ 0 \text{ otherwise.} \end{cases}$$

A zero value for a variable on the system digraph corresponds to a true or expected value. Hence, any other value corresponds to a deviation or disturbance. The top event in the system fault tree for the material control and accounting assessment is $M_{DIV} = +1$. For a disturbance in the top event variable to exist, that is $M_{DIV} = +1$, all loops in the system digraph that model the corrective actions of the MC&A system must fail.

Thus, in order for successful theft of special nuclear material to occur, all adversary cancellation loops must fail. These loops can fail for four reasons:

1. Adversary activity, including equipment tampering and collusion
2. Random monitor failure
3. Inadequate monitor measurement sensitivity
4. Human error, including slow guard response.

To find the combinations of adversary cancellation loops that must fail, we generate a fault tree from the system digraph by means of a transformation algorithm. The algorithm creates an AND logic gate in the fault tree for each cancellation loop that can fail.

Control loops in the system digraph are classified according to their response range and dynamics prior to application of the transformation algorithm. The corrective actions of loops that are too weak or too slow result in the automatic failure of these loops. The advantage of this prior loop classification is efficiency. One need not consider all the combinations of events listed above that can fail these loops.

Appendix B discusses the details of the digrapn-fault tree and methodology.

2.5 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 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 or power loss on 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 that must be reached for successful tampering to take place.

The computer codes Fault Tree Analysis Program (FTAP)[10] and the Set Equation Transformation System (SETS),[11] designed to generate and handle numerous, high-order minimal cut sets, are used to perform the qualitative analysis.

2.6 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[12] 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 is calculated for four specific cases:

1. No material control system tampering, no alarm signal generated
2. No material control system tampering, inadequate safeguards response to alarm signal
3. Material control system tampering, no alarm signal generated
4. Material control system tampering, inadequate safeguards response to alarm signal.

A sensitivity analysis is also made of the probability of successful theft for the above cases as a function of the amount of special nuclear material stolen. The 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, five adversary attributes and material control system characteristics are considered:

1. Type of tools and resources required for tampering
2. Accessibility of components to potential adversaries
3. Monitoring of equipment for tampering
4. Availability of tools and resources required for tampering
5. Personnel required for tampering.

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

The remainder of this report is divided into the following sections:

Section 3: Test Bed Description[2]

Section 4: Test Bed Assessment.

3.0 TEST BED DESCRIPTION

The event set generation and analysis procedure has been demonstrated in the assessment of a simulated material control system design in a nuclear facility, the Test Bed.[2] The Test Bed includes material balance procedures, but no other part of the material accounting system.

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

3.1 DESIGN OVERVIEW AND PHILOSOPHY

Two constraints have been internally imposed in the Test Bed design:

1. Manual plant operations: there are no automated operations and humans must perform the actual operations.
2. Humans as decision-makers: almost all active decisions relating to security system responses have human participation in the final step.

A two-part philosophy underlies the Test Bed material control (MC) system design for the nitrate storage area.

1. The first and most important part of the design philosophy is the reduction of opportunities that can lead to removal of SNM from the storage tank containment cells. This has been accomplished by the addition of check valves in the process and instrumentation lines.
2. The second aspect of the design philosophy is the monitoring of all operating procedures, critical valve positions, operating environments, and personnel in the material access area (MAA).

3.2 PLANT DESCRIPTION

The AGNS reprocessing facility is shown in Fig. 4. A nitrate-to-oxide conversion plant has been added to the basic AGNS design to provide a receiver for the nitrate product. The portion of the plant included in the Test Bed design is outlined in the plan view of Fig. 5.

The storage area is divided into four modules, each consisting of six slab storage tanks. The MAA is adjacent to the storage cell and is used for controlling the nitrate flow into, out of, and between storage tanks and for sampling the tank contents. Valving and sampling operations are conducted by means of glove boxes (GB) located on each of the three levels of the MAA, shown in Figs. 6 and 7.

Access to the MAA is through the portal control booth and the computer controlled access system (CCAS). The CCAS is under the supervision of the security station operator.

The product for the nitrate storage area is transferred from the plutonium product cell approximately twice a week in batches of 730 liters.

3.3 PERSONNEL MOVEMENT AND LOCATIONS

Figure 8 shows the entrances and exits in the Test Bed. The normal exit and entrance point to the MAA is through the normal portal and then the CCAS. Use of the CCAS requires a personal I.D. badge and a personal I.D. number. In addition, the CCAS uses closed-circuit TV (CCTV) surveillance to monitor (1) the weight of the booth and its contents, (2) the radiation level of the contents, (3) the presence of ferrous and nonferrous metals, and (4) the actual booth contents.

Entry and removal of large equipment or tools from the MAA are accomplished by a special transportation team during the maintenance mode of operation. The equipment portal doors EE_A, EE_B, $E2_R$, $E2_L$ shown in Fig. 8 are used for this purpose. During equipment removal, a guard scans the equipment and tools with hand-held radiation detectors.

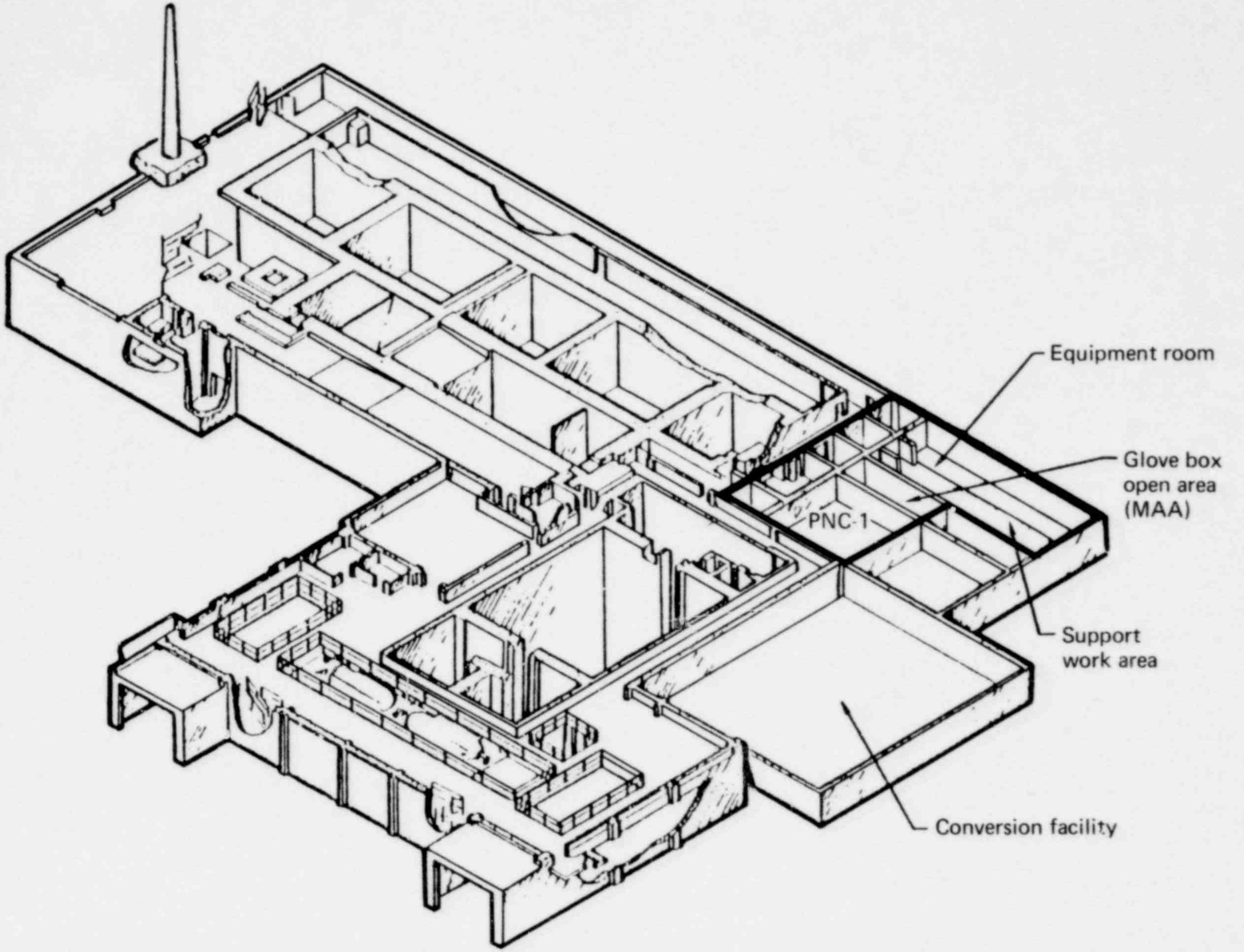


FIG. 4. Modified reprocessing facility used as Test Bed design.

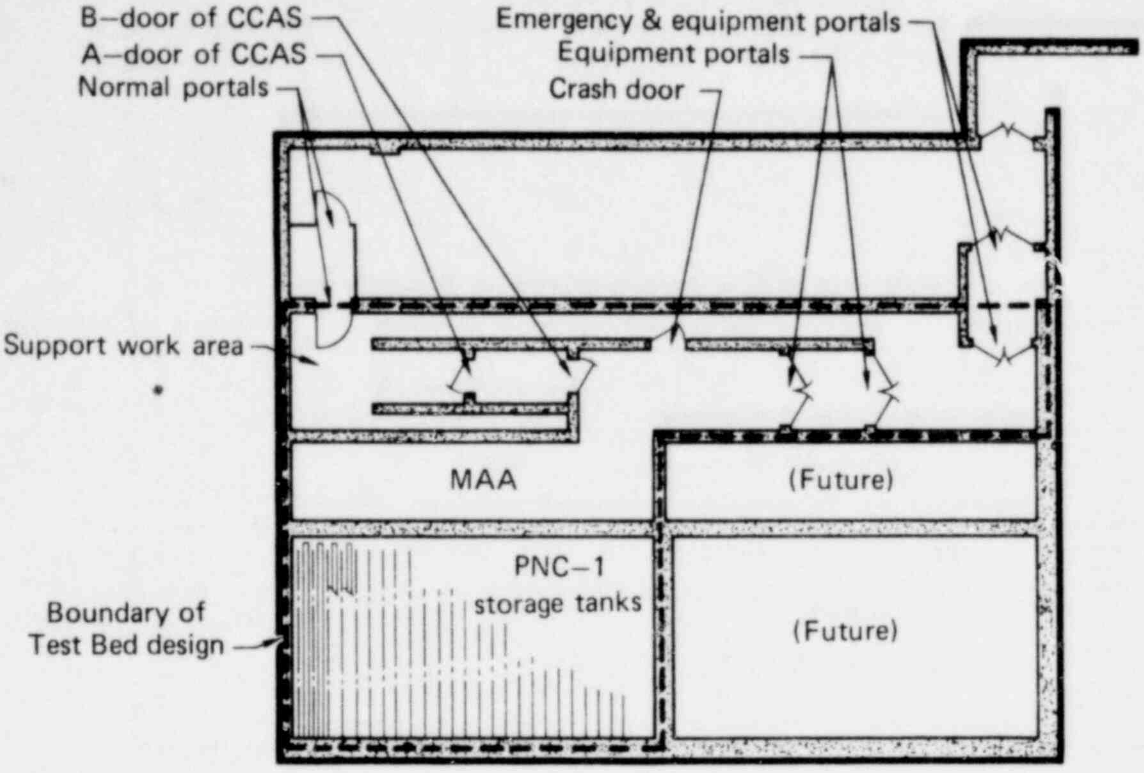


FIG. 5. Plan view of plutonium nitrate storage area.

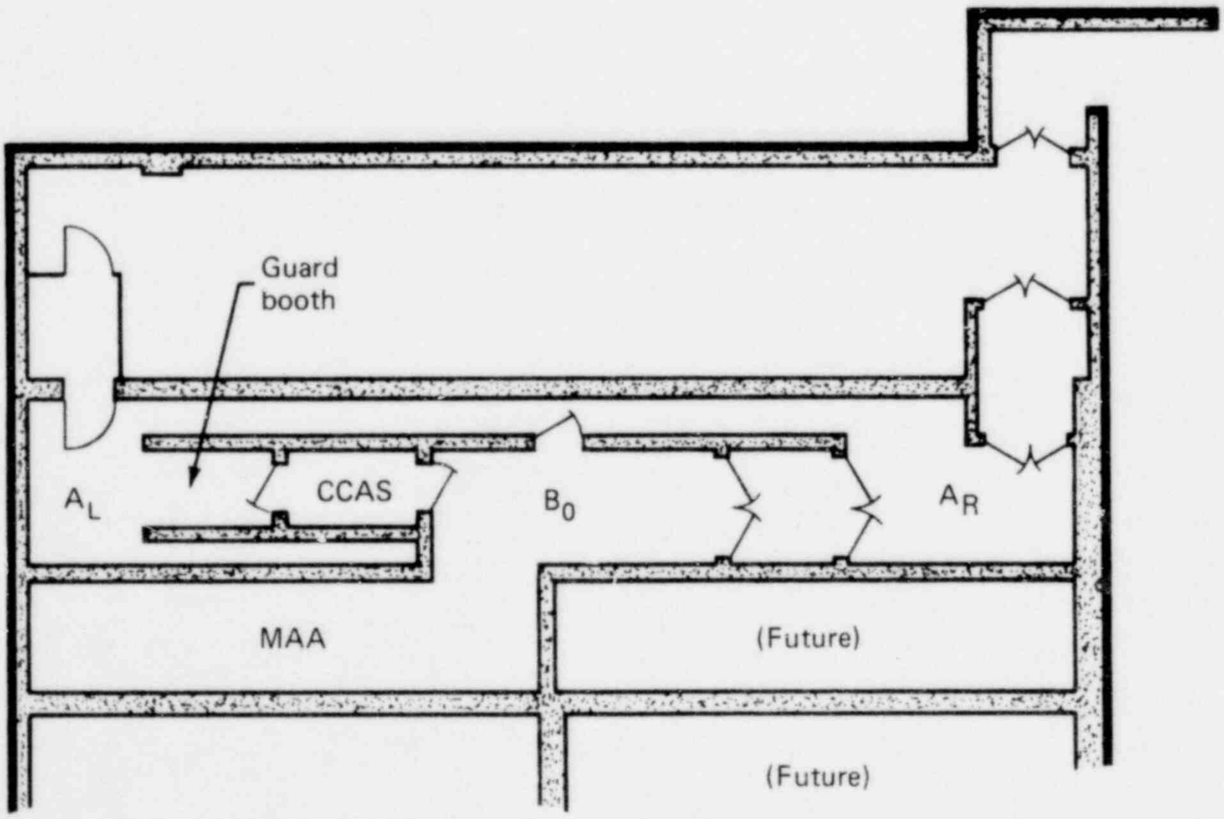


FIG. 6. Areas in the Test Bed.

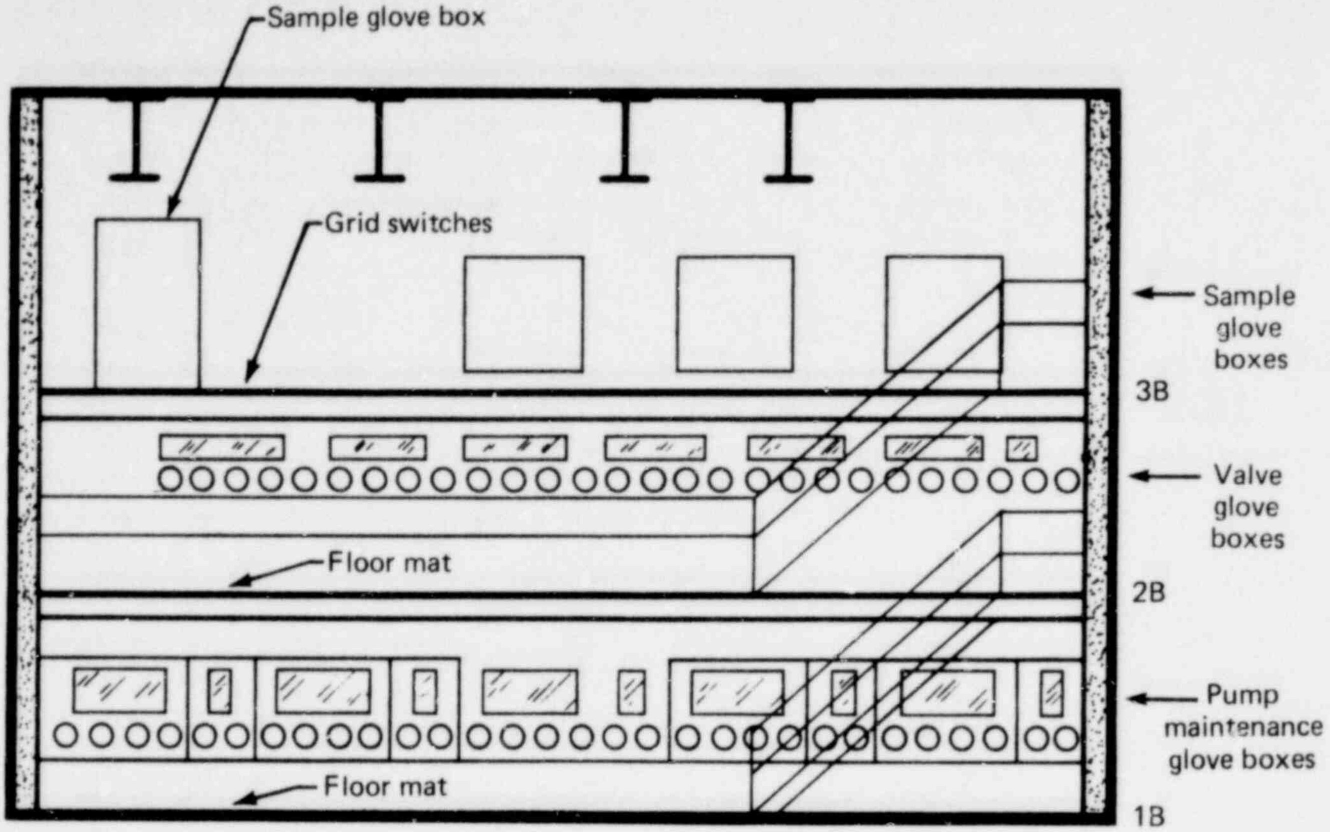


FIG. 7. Floor levels in the Test Bed.

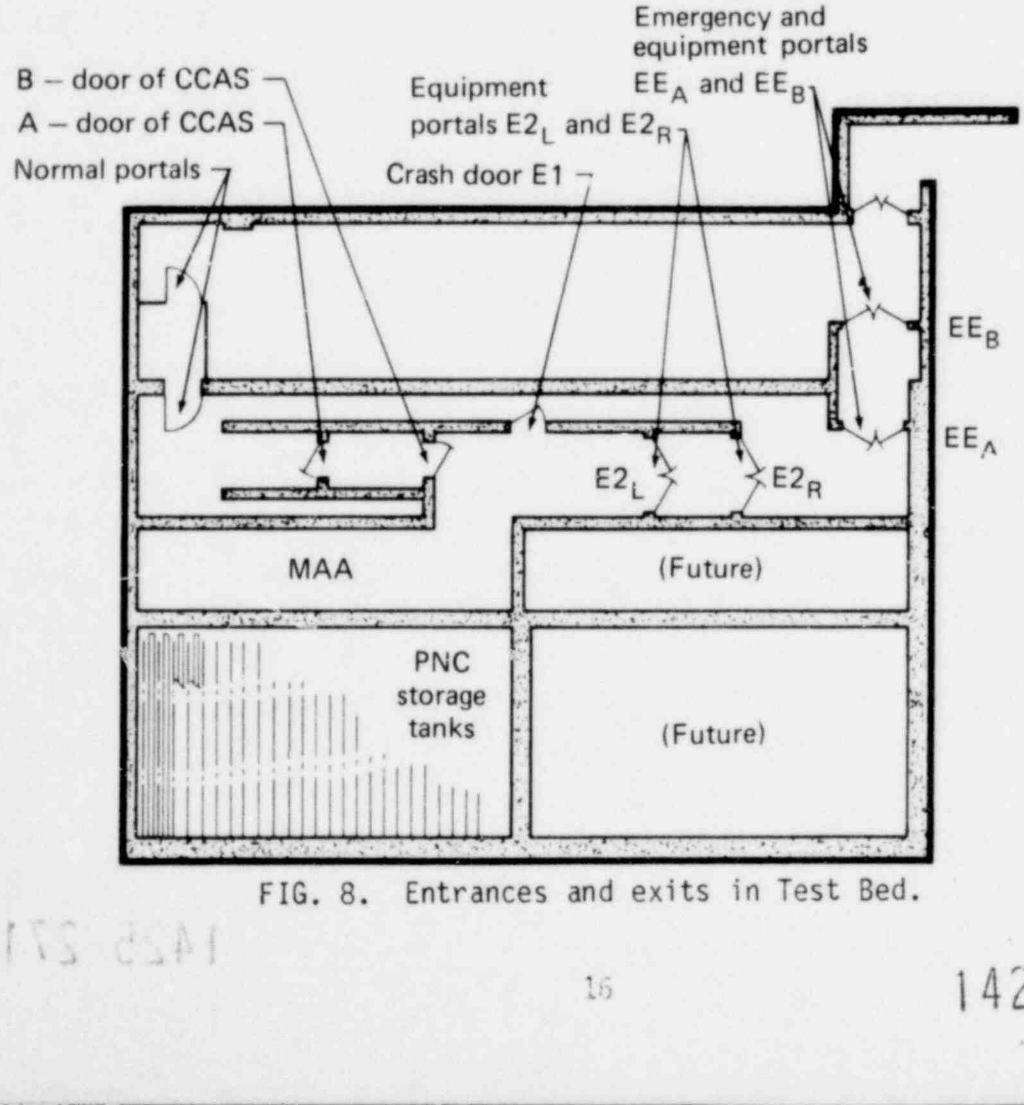


FIG. 8. Entrances and exits in Test Bed.

~~1425 271~~

The crash door, E1, is used during the emergency mode. Plant personnel can exit through the CCAS, the crash door, and the equipment portal during emergency conditions by pushing crash bars. Exit under these circumstances triggers an audible alarm and sends a signal to the MC computer system, which then generates the highest level system alarm.

The spatial resolution used in the analysis of personnel movement in and out of the MAA is determined by the material control decision logic and the fields of view of the monitoring system. These monitors include pressure mats, microwave detectors, CCTV with moving target indicators (MTI), and infrared detectors. The areas and levels A_R, A_L, CCAS, B_0, 1B, 2B, and 3B (Figs. 6 and 7) are partitioned into 14 personnel locations, as shown in Fig. 9. The corresponding monitors for each personnel location are shown in Fig. 10. The gamma, alpha, and neutron detectors are material monitoring components and can sense the presence of radiation. The metal detector senses the presence of ferrous and nonferrous metal. The glove box pressures are monitored by differential pressure sensors.

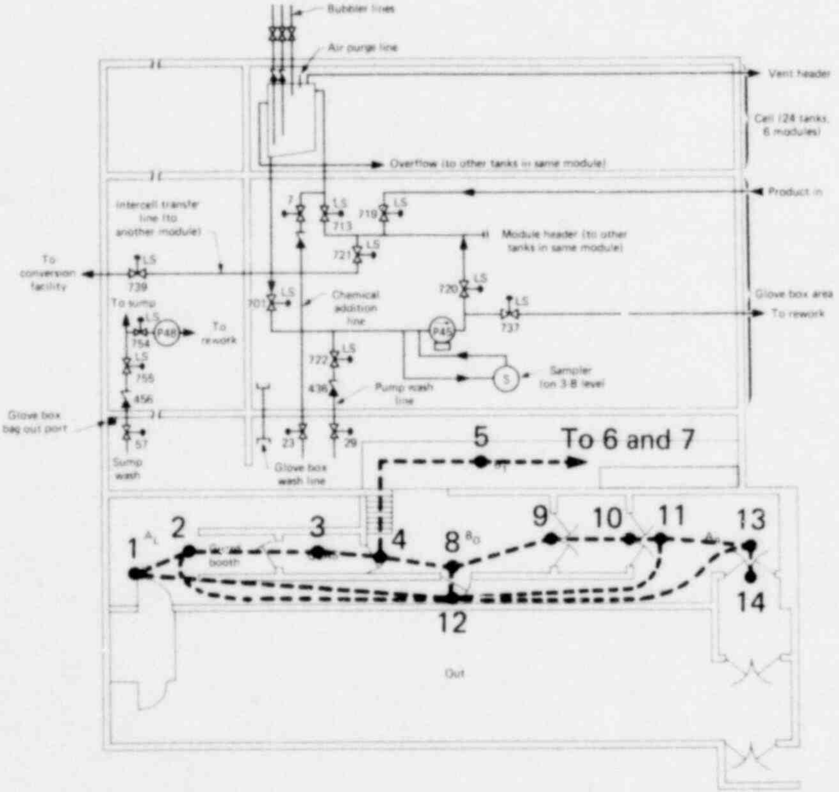


FIG. 9a. Personnel locations used in assessment.

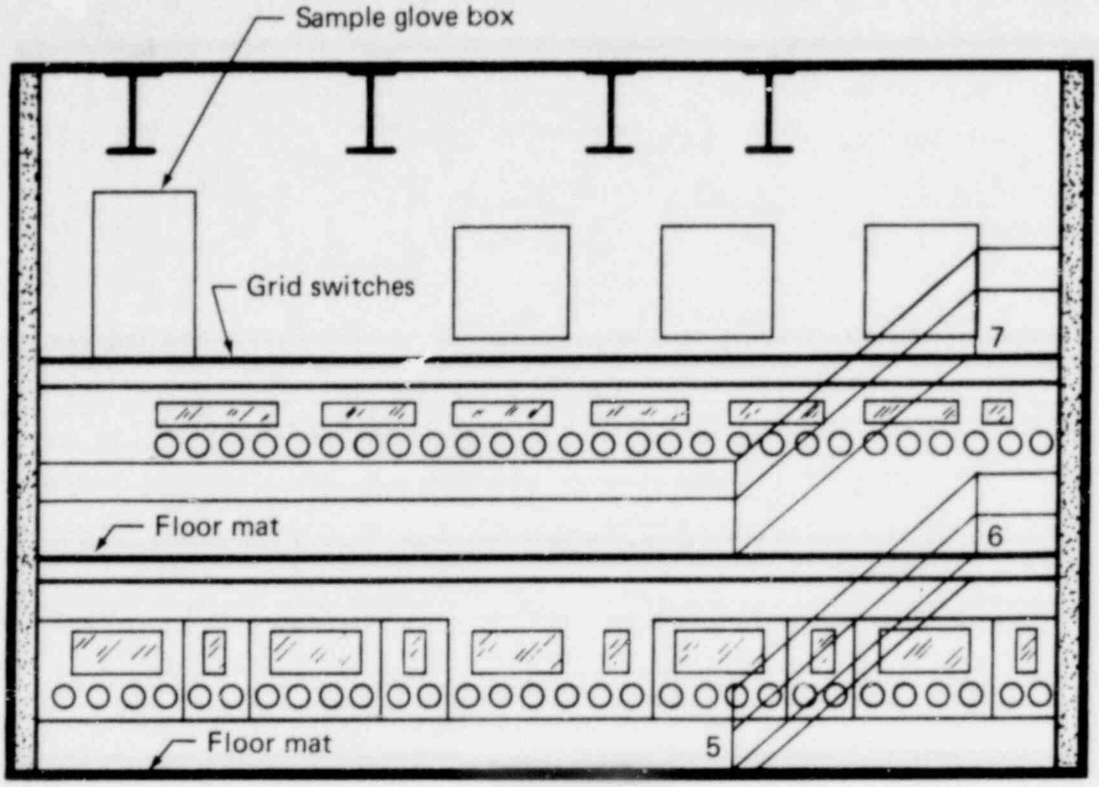


FIG. 9b. Personnel locations used in assessment.

Areas	A_L		GB and CCAS		B_O				MAA			A_R		
									1B	2B	3B			
Monitors	1	12	2	3	4	8	9	10	5	6	7	11	13	14
Pressure mat	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Microwave detector	●		●	●	●	●	●		●	●		●	●	
TV and MTI			●	●	●	●	●		●	●	●	●	●	●
Infrared detector		●	●		●							●		
Neutron detector				●										
Gamma detector				●		●	●	●						
Metal detector				●										
Alpha detector									●	●	●			
GB pressure									●	●	●			

FIG. 10. Test Bed areas and associated monitors.

3.4 SYSTEM MODES OF OPERATION

The plutonium nitrate storage area (PNSA) has eight modes of operation. The unauthorized locations for personnel during these various modes are shown in Fig. 11. The "two-man rule" is enforced for all procedures within the MAA.

The PNSA consists of a complicated piping network. For purposes of analysis, the piping network is simplified to show one representative tank with incoming and outgoing lines (Fig. 12). Pump 45 (P45) is used for product receival from the plutonium product cell, stirring and sampling, and product transfer to another tank or to the conversion facility. Table 1 lists the valves that are authorized to be opened for each mode of operation. "LS" represents a limit switch that monitors the position of the valve. The authorized duration of procedure for each mode of operation is also indicated in Fig. 13.

Unauthorized areas Mode of operation	A_L	GB and CCAS	B_O	MAA			A_R
				1B	2B	3B	
Static			●	●	●	●	
Product receival						●	
Stir and sample				*		*	
Rework						●	
Transfer	●			*		*	●
Load out						●	
Chemical addition						●	
Maintenance							

*Plant personnel cannot be at both areas at same time.

FIG. 11. Test Bed operation modes and associated unauthorized areas.

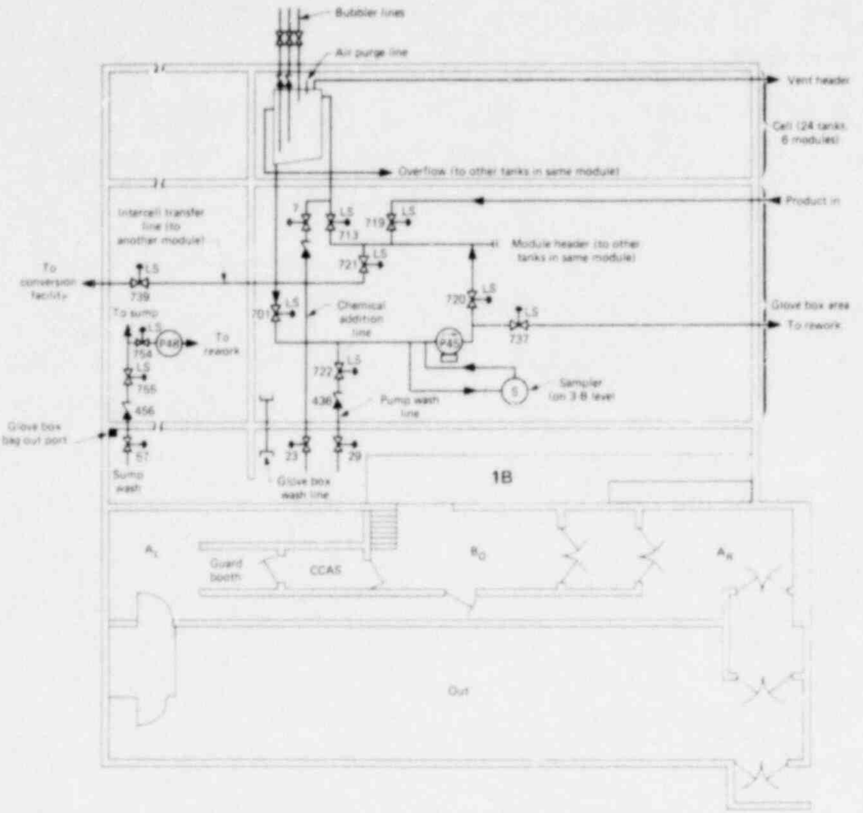


FIG. 12. System flowsheet for Test Bed assessment.

TABLE 1. Procedures for Test Bed modes of operation.

Mode of operation	Valves open	Pump 45	Authorized duration of procedure
1. Static	None	Off	N/A
2. Product receival	713 LS, 719 LS	Off	0.3-0.7 h
3. Stir and sample	701 LS, 713 LS, 720 LS	On	8-11 h
4. Rework	701 LS, 720 LS, 737 LS	On	0.3-0.7 h
5. Transfer module I to J	701-I LS, 720-I LS, 721-I LS, 721-J LS, 713-J LS	On	0.3-0.7 h
6. Load out	701 LS, 720 LS, 721 LS, 739 LS	On	0.3-0.7 h
7. Chemical addition	23, 7	Off	3-5 h
8. Maintenance (not specified)			

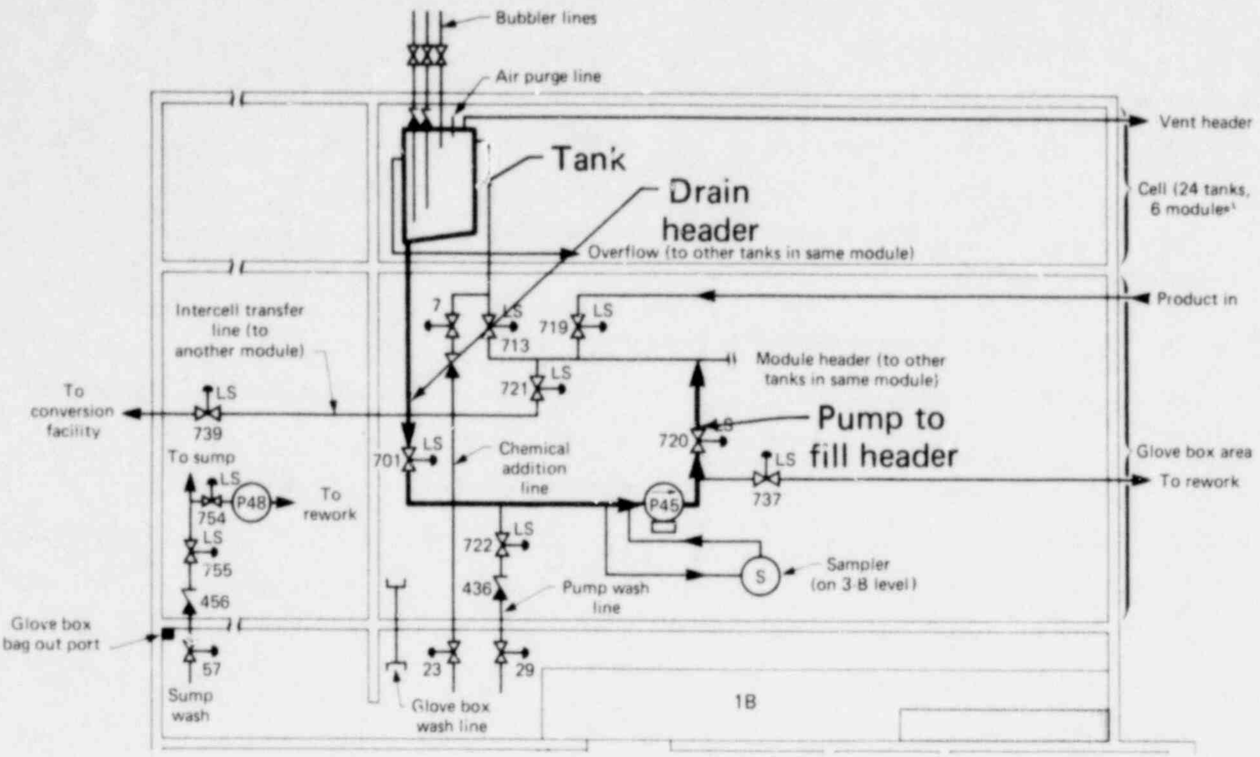


FIG. 13. Sources of SNM in Test Bed.

3.5 MATERIAL CONTROL (MC) SYSTEM

Overall control of the MC system resides in computerized material control stations, with final authority retained by the Nuclear Materials Control Officer (NMCO). Because of the importance of these computerized systems, they will be discussed first.

3.5.1 Material Control System Supervision

Material control supervision resides in two independent MC stations. The first of these, MC-1, is located in the security station and is responsible for the routine monitoring of SNM contained within the plant. The second station, MC-2, is located in the Process Control Center and is responsible for the response to certain abnormal conditions. This station also provides data to the process operator on the detailed state of the process. Each of the MC stations has its own computer system and noninterruptable power supply. The two computer systems are interconnected and have the same data in their memory. The software for the two systems is identical except for four differences:

1. Software modifications can be made only through the MC-2 system.
2. Daily work rosters can be read into the MC-2 system only.
3. Personnel authorizations and identities can be read into the MC-2 system only.
4. MC-2 can reduce the intermediate level theft danger rating (with the concurrence of MC-1), whereas MC-1 cannot do this alone.

A third computer system is located in the analytical laboratory. This laboratory data system is used to record the results of all chemical and physical analyses automatically. This system is not supplied from the noninterruptable power supply.

A fourth computer system is used to monitor and control the CCAS. This computer is located adjacent to the MC-1 station and is connected to both MC computers. This system is supplied from the noninterruptable power supply.

3.5.2 Material and Personnel Monitoring

The material and personnel monitoring components (listed in Fig. 10 and Table 1) and the CCAS are designed to detect unauthorized personnel or SNM movement. The MC computer monitors the steps performed in each operating procedure and alerts the MC operator if a discrepancy is detected between the actual and the authorized procedures.

This is accomplished by the monitoring of floor mats, glove box ports, piping and instrumentation valve positions, and the Portal Control System Booth. The MC computer system memory contains procedural sequences for all normal operating procedures. In addition, at the beginning of each work shift, the MC-2 operator loads the approximate time periods for each procedure to be performed that shift, along with the individuals authorized to perform them. The MC computer system then makes two correlations: access attempts to the MAA with those authorized, and the plant state with the expected state, as indicated in the procedure table (Table 1). Any discrepancy alerts the MC system.

3.5.3 Alert Levels

The MC System has four levels of alert called Theft Danger Ratings (TDR), as shown in Table 2. TDR-0, the lowest alert level, is the normal operating alert level of the plant. The next level, TDR-1, corresponds to a minor abnormal situation and requires only an information-gathering response from the plant MC personnel. The next higher alarm level, TDR-2, is reserved for a situation in which it appears that SNM can easily be removed from the MAA. This requires a low-level security force response in addition to an information-gathering response. The highest level, TDR-3, corresponds to an MC system assessment that diversion is occurring or has occurred. The response to a TDR-3 is a full security force response, along with the alerting of outside agencies. Table 3 shows the authorized locations for guards and health workers during TDR-2 and TDR-3 alarm states.

TABLE 2. Test Bed safeguards system response: reaction rules to TDRs.

Theft danger rating	Nature of situation	Response
TDR-0	Nominal operating conditions	
TDR-1	Possibility of diversion of SNM with relative difficulty	Guards and operators read monitors, check records, communicate with workers, send one guard out
TDR-2	Possibility of diversion of SNM with relative ease	Send one guard out, alert high-level security force
TDR-3	Direct opportunity for diversion or diversion is occurring or has occurred	Send three guards out, alert outside agencies, add special portal security procedures

TABLE 3. Guard and health worker locations in Test Bed.

TDR level	Number of guards	Authorized area for guards	Number of health workers	Authorized area for health workers
TDR-0	None		None	
TDR-1	None		None	
TDR-2	1	Guard booth	1	(Not specified)
TDR-3	3	Guard booth B_O A_R	2	(Not specified)

4.0 TEST BED ASSESSMENT

We now describe the steps taken in the assessment of the Test Bed.

4.1 TARGET IDENTIFICATION

The first step in the assessment procedure is to identify potential targets. A target is defined by a given type of SNM, the location in the plant where the SNM can be acquired (the removal node), and the conditions that will cause SNM to appear at that location. LLL has developed a computer code call PIPE[13] that uses the information in the piping and instrumentation diagrams to generate all possible removal nodes and to approximate potential flow rates.

4.1.1 Material Type

The plutonium nitrate in the Test Bed has a concentration of approximately 250 g of Pu per liter of solution and hence is a very theft-attractive material. The only exception is the solution used to wash the pumps during pump change out. In this case, the solution is nitric acid with some Pu contamination and is allowed to fall on the glove box floor.

4.1.2 Sources

Sources refer to locations where SNM is normally contained in the process. There three generic sources for the Test Bed, shown in bold lines in Fig. 13:

1. Tanks
2. Drain headers (when valves are closed)
3. Pump-to-fill header lines (when valves are closed).

4.1.3 Removal Nodes

Removal nodes are locations where an adversary can gain physical access to SNM. The removal nodes for the Test Bed are shown in Fig. 14 and enumerated in Table 4.

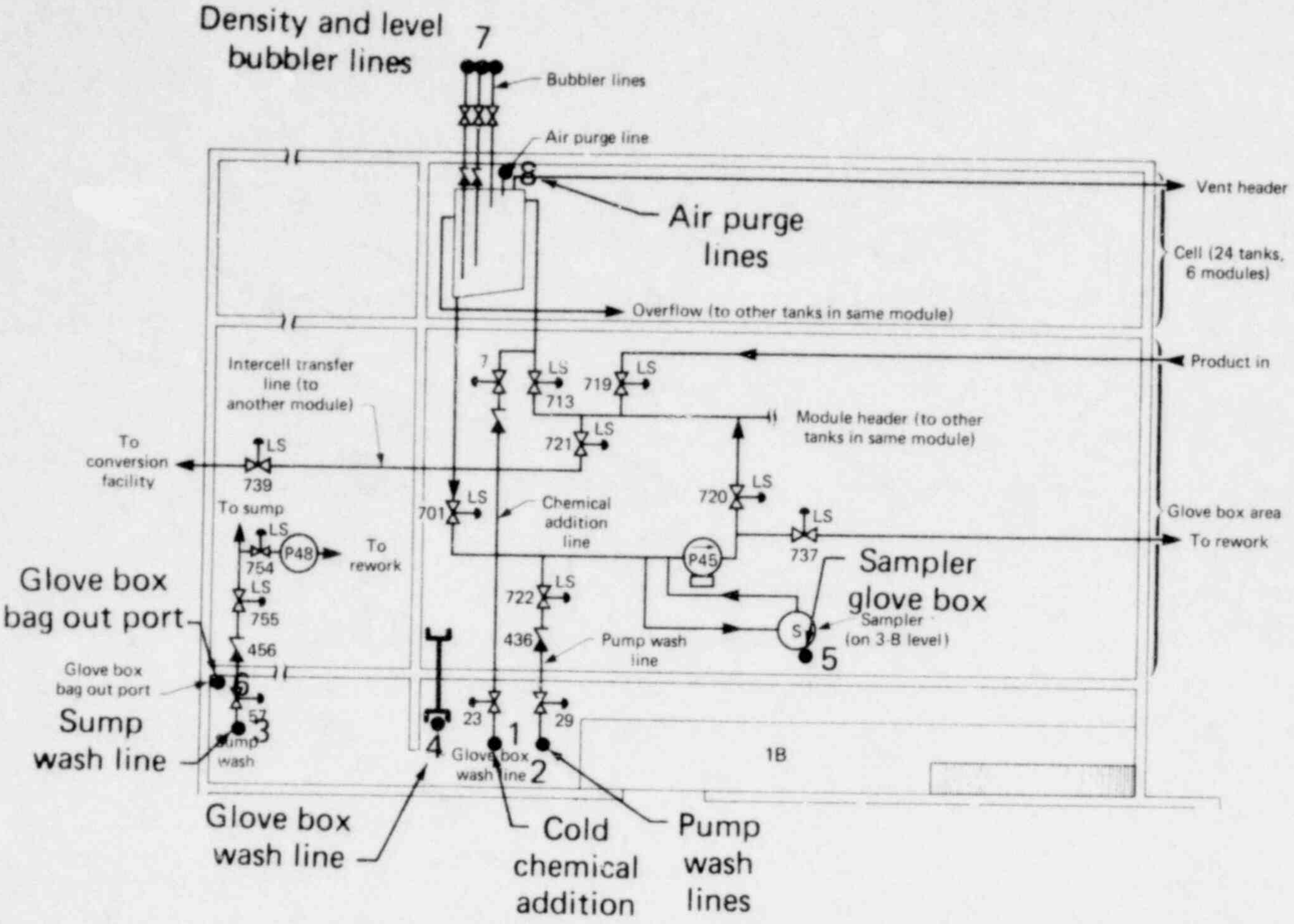


FIG. 14. Removal nodes in Test Bed.

TABLE 4. Removal nodes in Test Bed.

A removal node is the location where adversary can physically gain access to SNM.

1.	Cold chemical addition lines	24
2.	Pump wash lines	4
3.	Sump wash line	1
4.	Glove box wash line	4
5.	Sampler glove box	1
6.	Glove box bag out port	1
7.	Density and level bubbler lines	72
8.	Air purge lines	24
	Total	131

4.1.4 SNM Exit Points

An SNM exit point is a location where SNM crosses the system boundary. Within the normal process flow, there are four exit points for the Test Bed:

1. Product input line
2. Product output line
3. Vent line
4. Rework line.

All other SNM exit points require that the adversary must remove SNM from the process and that the SNM must cross the boundary of the MAA outside the normal process flow. For the Test Bed, these exit points include

5. CCAS
6. Crash door
7. Hole in wall
8. Service lines, e.g., air, electricity
9. Equipment portals (E2)
10. Emergency and equipment portal (EE)
11. Normal portal.

It is important to note that all sources, removal nodes, and exit points must be identified; otherwise the analysis is not complete and some adversary event sets would not be generated.

4.2 GENERATION OF THE SYSTEM DIGRAPH AND FAULT TREE FOR THE TEST BED

The purpose of the digraph-fault tree procedure is to systematically generate a fault tree that can be qualitatively and quantitatively evaluated. This evaluation can assist in the determination of the effectiveness of the MC&A system.

The system digraph models the interaction of the adversary with the MC&A system as he perpetrates an SNM theft. The system digraph is constructed from a collection of unit model digraphs. Appendix C gives the system digraph and unit models for the Test Bed.

The fault tree elicits and organizes the information contained in the system digraph for "Successful theft of SNM from the Test Bed." The fault tree of the Test Bed shows all combinations of events that can lead to successful theft. Appendix D, which includes five sheets of information, provides the fault tree generated for the Test Bed.

4.2.1 Analysis Assumptions

We performed our analysis for theft at only one removal node, the pump wash line (node 2 in Fig. 14, node 706 in Fig. 15). The pump wash line is located outside the pump glove box and is used for adding nitric acid during pump washout.

We further assumed that SNM is removed from the process during the product receival mode of operation and that the SNM is taken out of the MAA either during the product receival mode or the maintenance mode.

There were six other assumptions:

1. Analysis is based on the inside adversary.
2. The initial system alert state is TDR-0.
3. Response to a TDR-1 consists primarily of sending a guard to collect information on level 1 anomalies that have triggered the alarm.
4. Doors EE_A, EE_B, and $E2_L$ (Fig. 8) remain open during the maintenance mode. However, a guard is stationed at A_R during this mode and the adversary must past him in order to use doors EE_A and EE_B.
5. Since the adversary is an insider, he can gain access to the pump wash line and bring a container or other small equipment into the MAA without generating anomalous signals.
6. The analysis did not consider the failure of the two-man rule. Hence, for Test Bed procedures that require two people working

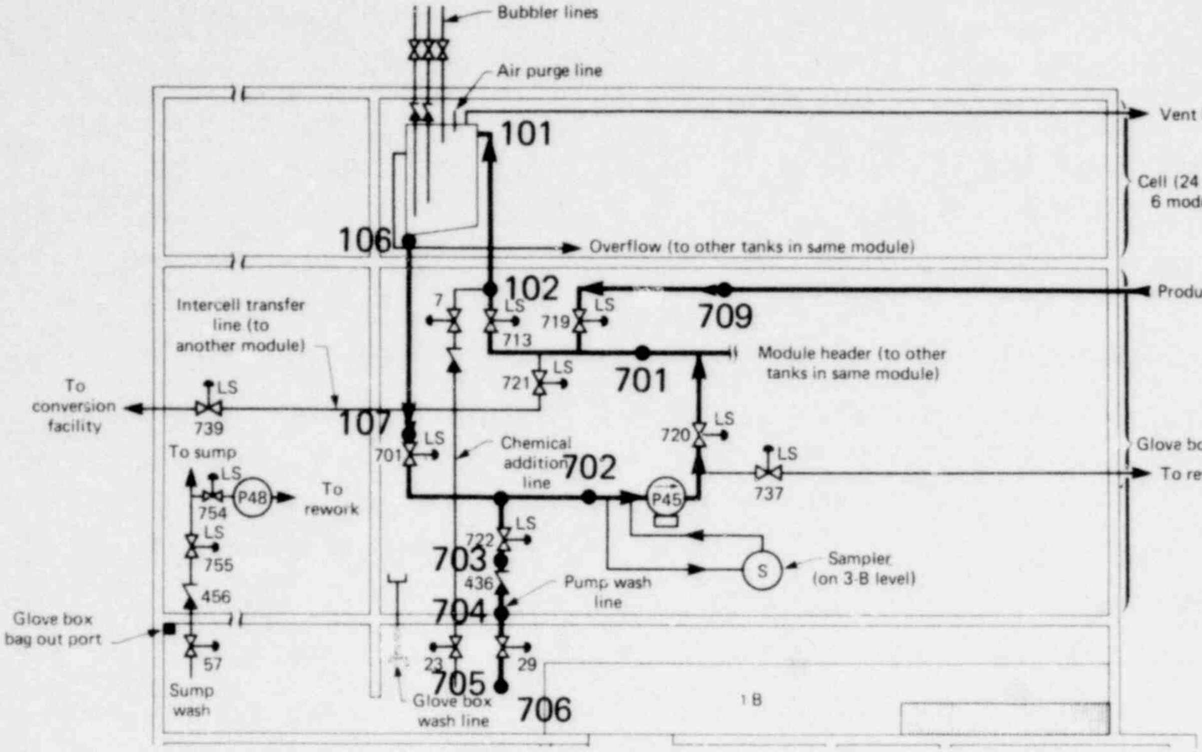


FIG. 15. Nodes for SNM flow within process. Removal node is pump wash line (706).

together, only the two people in collusion can cause the procedure to fail.

4.2.2 System Flowsheet for Product Receival Mode of Operation

Figure 15 shows the SNM flow for the product receival mode of operation. The numbering scheme listed below is used to define the nodes and valves in Fig. 15. Nodes are locations on a pipe and are separated by pipe lengths and/or valves.

Nodes and valves	Numbering scheme
Tank and piping nodes	100-600
Header line nodes	700-790
Sump line nodes	900-990
Valves without limit switches	000-399
Check valves	400-699
Valves with limit switches	700-900

The SNM product from two interim storage tanks in the plutonium product cell (PPC) is transferred by gravity feed to the PNSA. The SNM enters the PNSA through the product input line to the module header and from there into a specific tank (tank 1, module 1 for the analysis). Storage tanks are filled one at a time to a volume of approximately 730 l, which takes about 1/2 hour. After the storage tanks are filled, the contents are stirred.

As indicated in Fig. 11, levels 1B and 2B are the only locations where personnel are authorized during the product receival mode. Table 1 shows that only valves 713LS and 719LS are allowed to be opened during this mode.

The two interim storage tanks in the PPC and the storage tanks in the PNSA have differential pressure (DP) cells that measure the static pressure of the solution in each tank. The static pressure measurement is used to determine the amount of solution in each tank. Material accountability is accomplished by comparing the amount of solution transferred from the PPC with the amount received by the PNSA. Any major discrepancy indicates a potential theft.

No DP cell measurements are made while the tank is filling. Hence, SNM theft detection schemes based on mass balance discrepancies are effective only after the tank is filled. This fact makes the product receival mode of operation an attractive mode during which to steal SNM.

4.2.3 Unit Model Digraphs

The basic building blocks for the digraph-fault tree procedure are unit model digraphs. Engineering analysis is applied to process equipment, monitors, and other components of the MC system in constructing unit model digraphs. Because the analyst considers individual components, he can do an isolated or separate analysis. The total system analysis is accomplished through the solution of the complete set of interrelated unit model digraphs.

To aid in constructing the unit model digraphs, we performed a failure modes and effects analysis (FMEA) for the material monitoring components, personnel monitoring components, process equipment, and computers in the Test Bed. Particular emphasis was given to failure modes that could inactivate components in such a manner that adversary activity goes undetected. We determined the failure modes that could be induced by an adversary from collusion, reliability, and tampering analyses (described in Sections 4.3 and 4.4). Six types of information were used in these analyses:

1. Minimum and maximum times needed to perform the act
2. Required tools and equipment
3. Means by which the MC system can detect the act
4. Minimum required collusion for tampering
5. Means by which the adversary can disguise the act
6. Persons who have authorized access to the component.

Instructions and the forms used in conducting the FMEAs for the Test Bed are given in Appendix A.

It is important to note that an analyst can perform an FMEA without knowledge of digraphs. Licensees can submit FMEAs of the MC&A components in their plant. The information regarding the failure modes in these FMEAs can then be compared with the unit model digraphs in the NRC/LLL data base for discrepancies, omissions, etc.

Next, the input and output variables of the component must be identified and the relationships among these variables established on the basis of mass, momentum, and energy laws. By using these variable relationships and the information in the FMEAs, the analyst can construct a unit model digraph for the component.

The procedure described above for generating a unit model digraph of an MC&A component is outlined in Fig. 16.

The system digraph for the Test Bed is generated from a collection of unit model digraphs. Each unit model constructed for the Test Bed will now be described.

4.2.3.1 Material Flow to Pump Wash Line (Node 706). Two variables, MPU_x and $\overline{MPU}_x$, are used in the unit model digraph to describe the mass flow rate

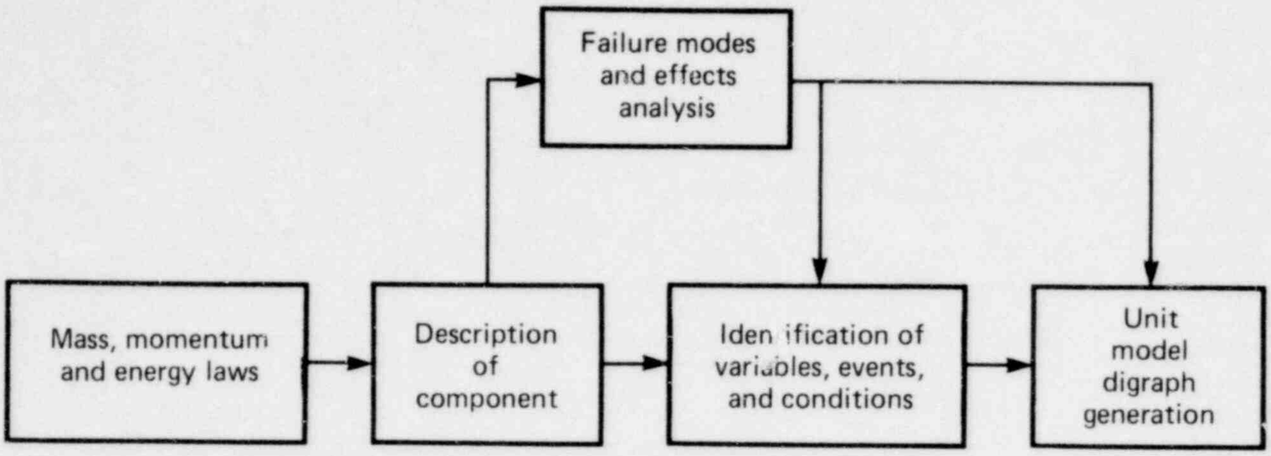

Failure modes and effects analysis
Mass, momentum and energy laws
Description of component
Iden ification of variables, events, and conditions
Unit model digraph generation

FIG. 16. Procedure for generation of unit model digraphs.

of the SNM, Pu Nitrate, to node 706. When the Pu Nitrate is contained within the piping system of the storage area, the mass flow rate of Pu Nitrate at node x is defined by:

$$MPU_x \begin{cases} +1 \text{ high mass flow rate at node } x \\ \ \ 0 \text{ normal mass flow rate at node } x \\ -1 \text{ low mass flow rate at node } x \end{cases}$$

When the Pu Nitrate is outside of the piping system and the adversary has possession of it, then the mass flow rate of Pu Nitrate is defined as:

$$\overline{MPU}_x = \begin{cases} +1 \text{ adversary has possession of SNM at node } x \\ \ \ 0 \text{ adversary does not have possession of SNM} \\ \quad \text{at node } x \end{cases}$$

A narrative description of the thinking that went into the construction of the unit model of material flow to the pump wash line, node 706, now follows. Refer to Figs. 15 and 17 and Fig. C-4 as necessary.

In order for the adversary to have possession of the Pu Nitrate at node 706 ($\overline{MPU}_{706}$ in Fig. 17), he must be present at node 706, have the container, and fill the container with Pu Nitrate. The first two conditions are initial conditions for the analysis. For the mass flow rate to occur at node 706

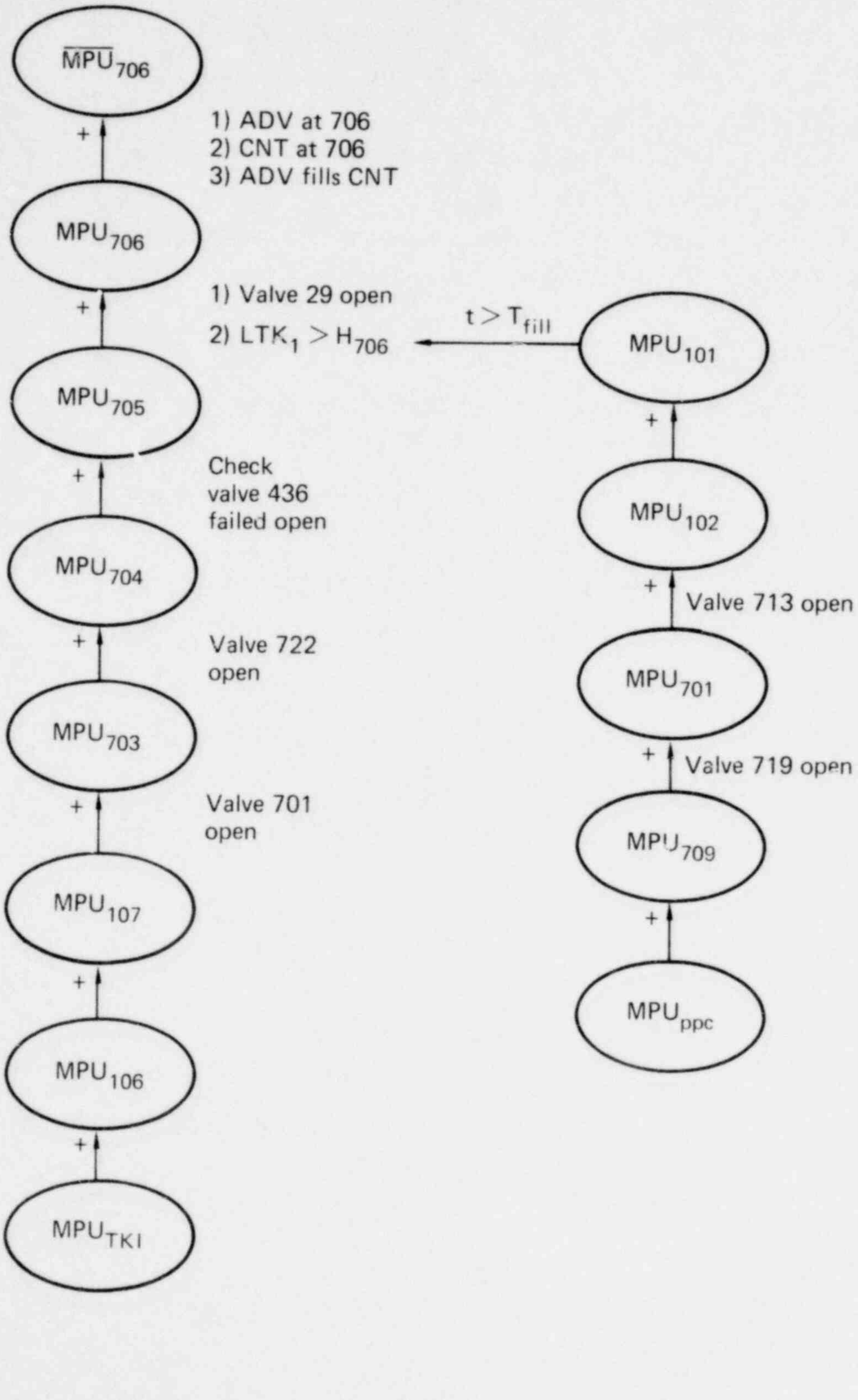


FIG. 17. Unit model of material flow to pump wash line (Node 706).

(MPU_{706}), it is necessary to have mass flow rate at node 705 (MPU_{705}) and the following conditions: valve 29 must be opened and the solution level in the tank must be higher than the level of the pump wash line ($LTK > H_{706}$). Similarly, for the mass flow rate to occur at node 705, the mass flow rate must occur at node 704, and check valve 436 must fail open. By following the cause-and-effect information shown in Fig. 15, the mass flow at node 704 is caused by flow at nodes 703, 107, and 106; and valves 722 and 701 must be opened, respectively. According to the procedure table in Table 1, the opening of valves 722 and 701 is unauthorized during the product receival mode and safeguards anomaly signals would be generated. Unit model digraphs for limit-switched valves are discussed in the next section.

Mass flow at node 106 is caused by mass flow from tank 1, which decreases the amount of solution in tank 1 (MPUTK1). If the amount stolen is larger than the detection threshold, the loss is eventually detected by the accountability measurement system. (See Section 4.2.3.9)

For the solution level in the tank to be higher than the level of the pump wash line ($LTK > H_{706}$), the mass flow from the plutonium product cell (MPU_{PPC}) through the module header (nodes 709, 702, 102, 101) is required for a time sufficient to fill the tank to that level ($t > T_{FILL}$.)

4.2.3.2 Valve Position Anomaly. The unit model digraphs for valves with limit switches (LS) are shown on sheet 5 of the system digraph in Fig. C-1. The basic information flow is from the valve position (VP) to the limit switch position to the indicated limit switch position (LS^I), which is the output signal of the limit switch circuit to the safeguards valve anomaly signal (A_v).

The variable VP is defined by:

$$VP = \begin{cases} +1 \text{ if valve is opened} \\ -1 \text{ if valve is closed} \end{cases}$$

The variables LS and LS^I are similarily defined. The conditional edge relationships between LS^I and A_v define the combinations of indicated valve positions and mode operations that can yield anomalies. For example, valves 722 or 701 produce an anomaly when opened during the product receival mode of operation, i.e., $A_V^{722} = +1$ when $LS^{I,722} = +1$ or $A_V^{701} = +1$ when $LS^{I,701} = +1$.

4.2.3.3 SNM/Adversary Movement Out of MAA. The unit model digraph of SNM flow to the pump wash line (node 706) was described in Section 4.2.3.1. A description of the modeling of the unit model digraph for SNM/adversary movement from node 706 out of the MAA is now given.

As described in Section 4.2.3.1, the movement of SNM at node x with the adversary in possession of it is denoted by the variable $\overline{MPU}_x$. As the adversary moves from location to location, he crosses areas of the MAA that appear on the system digraph (sheet 1 of Fig. C-1) as conditional edge relationships between the node variables (Fig. 18). If an area is monitored, then a control loop is activated by the conditional edge.

Figure 19 shows an example of this triggering of a control loop by a conditional edge. When an adversary moves from node 5 to node 4, he crosses a pressure mat in area B_0. The pressure mat is activated (PM-B_0) and sends a signal to the material control logic which decides that a personnel location anomaly (A^1_{PL,B_0}) has occurred if the pressure mat in B_0 has been activated while the plant is in the static mode of operation.

As the adversary crosses various locations in the plant, control loop failures must occur for successful SNM theft. These failures appear as basic events in the fault tree and hence become part of the adversary event sets.

Six adversary exit paths out of the MAA from node 706 are obtained from the unit model digraph of adversary movement:

1.	ANODE 706	APM-B1	APM-BO	CBE1HIT	APM-AL	ANODE 1
2.	ANODE 706	APM-B1	APM-BO	AA-DHIT	ALCCAS	ANODE 1
3.	ANODE 706	APM-B1	APM-BO	APM-AR	TPEQMM	ANODE 14
4.	ANODE 706	APM-B1	APM-BO	ACCAS	CCASOK	ANODE 1

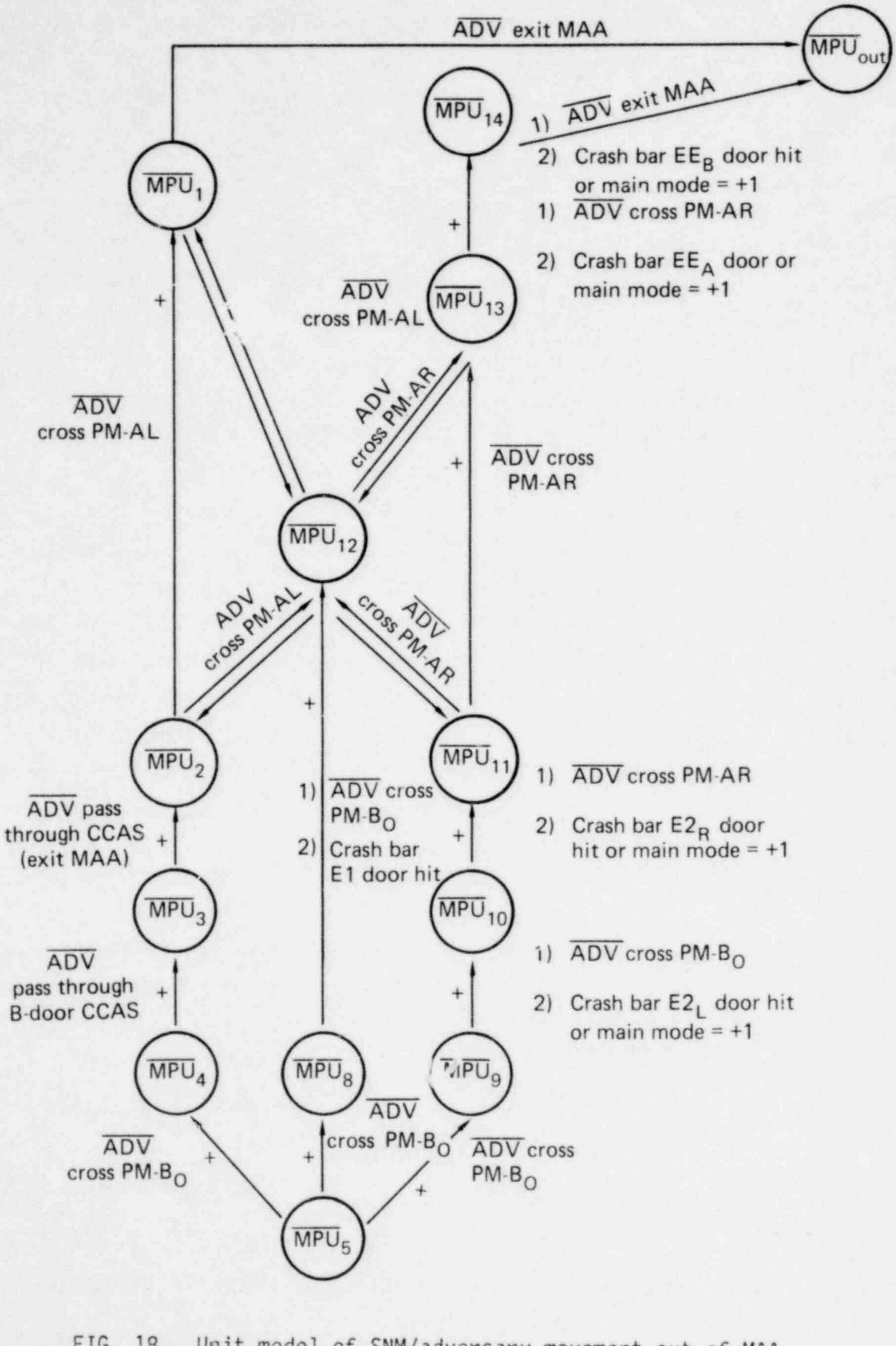

$\overline{\text{ADV}}$ exit MAA
$\overline{\text{MPU}}_{\text{out}}$
$\overline{\text{MPU}}_{14}$
1) $\overline{\text{ADV}}$ exit MAA
2) Crash bar EE_B door hit or main mode = +1
$\overline{\text{MPU}}_1$
+
1) $\overline{\text{ADV}}$ cross PM-AR
2) Crash bar EE_A door or main mode = +1
+
ADV cross PM-AL
$\overline{\text{MPU}}_{13}$
$\overline{\text{ADV}}$ cross PM-AL
ADV cross PM-AR
+
$\overline{\text{ADV}}$ cross PM-AR
$\overline{\text{MPU}}_{12}$
ADV cross PM-AL
$\overline{\text{ADV}}$ cross PM-AR
+
$\overline{\text{MPU}}_2$
$\overline{\text{MPU}}_{11}$
1) $\overline{\text{ADV}}$ cross PM-AR
2) Crash bar E2_R door hit or main mode = +1
$\overline{\text{ADV}}$ pass through CCAS (exit MAA)
+
1) $\overline{\text{ADV}}$ cross PM-B_O
2) Crash bar E1 door hit
+
$\overline{\text{MPU}}_3$
$\overline{\text{MPU}}_{10}$
1) $\overline{\text{ADV}}$ cross PM-B_O
2) Crash bar E2_L door hit or main mode = +1
$\overline{\text{ADV}}$ pass through B-door CCAS
+
+
$\overline{\text{MPU}}_4$
$\overline{\text{MPU}}_8$
$\overline{\text{MPU}}_9$
$\overline{\text{ADV}}$ cross PM-B_O
$\overline{\text{ADV}}$ cross PM-B_O
+
+
$\overline{\text{ADV}}$ cross PM-B_O
+
$\overline{\text{MPU}}_5$

FIG. 18. Unit model of SNM/adversary movement out of MAA.

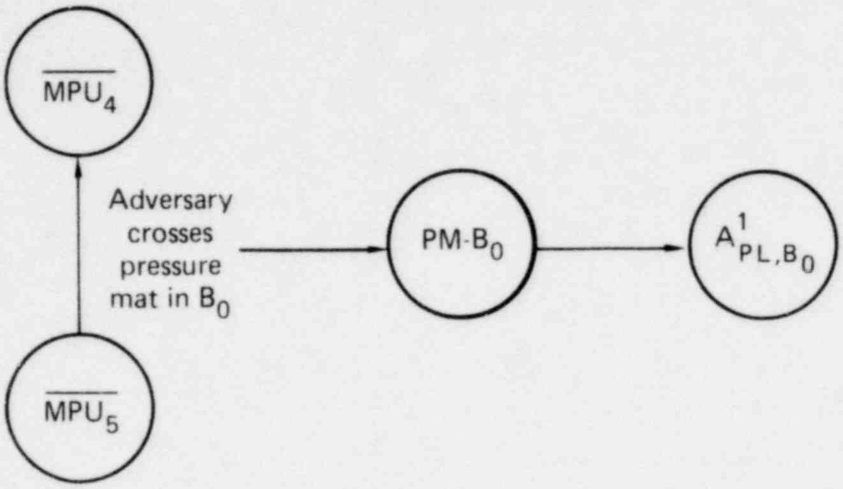


FIG. 19. Control loop triggered by conditional edge.

5. ANODE 706 APM-B1 APM-BO CBE1HIT APM-AR CBEEBHIT
CBEEAHIT ANODE 14
6. ANODE 706 APM-B1 APM-BO CBE2LHIT CBE2RHIT APM-AR
CBEEBHIT CBEEAHIT ANODE 14

The alphanumeric designators used to describe the paths are defined in Appendix E, Table of Basic Event Definitions and Probabilities for the Fault Tree.

4.2.3.4 MC Decision Logic. As described in Section 3.5.3, the material control system has four levels of alert: TDR-0, TDR-1, TDR-2, and TDR-3. These alarm states result from output signals produced by the MC monitors upon the detection of anomalies.

The MC decision logic is organized in a redundant, hierarchical manner (Fig. 20). It processes information from a variety of monitors, local-level logic subsystems, MC computer systems, and human decision makers. The important individuals involved in decision-making are the plant manager, the nuclear materials control officer (NMCO), the MC-1 operator (MC-1, O), and the MC-2 operator (MC-2, O).

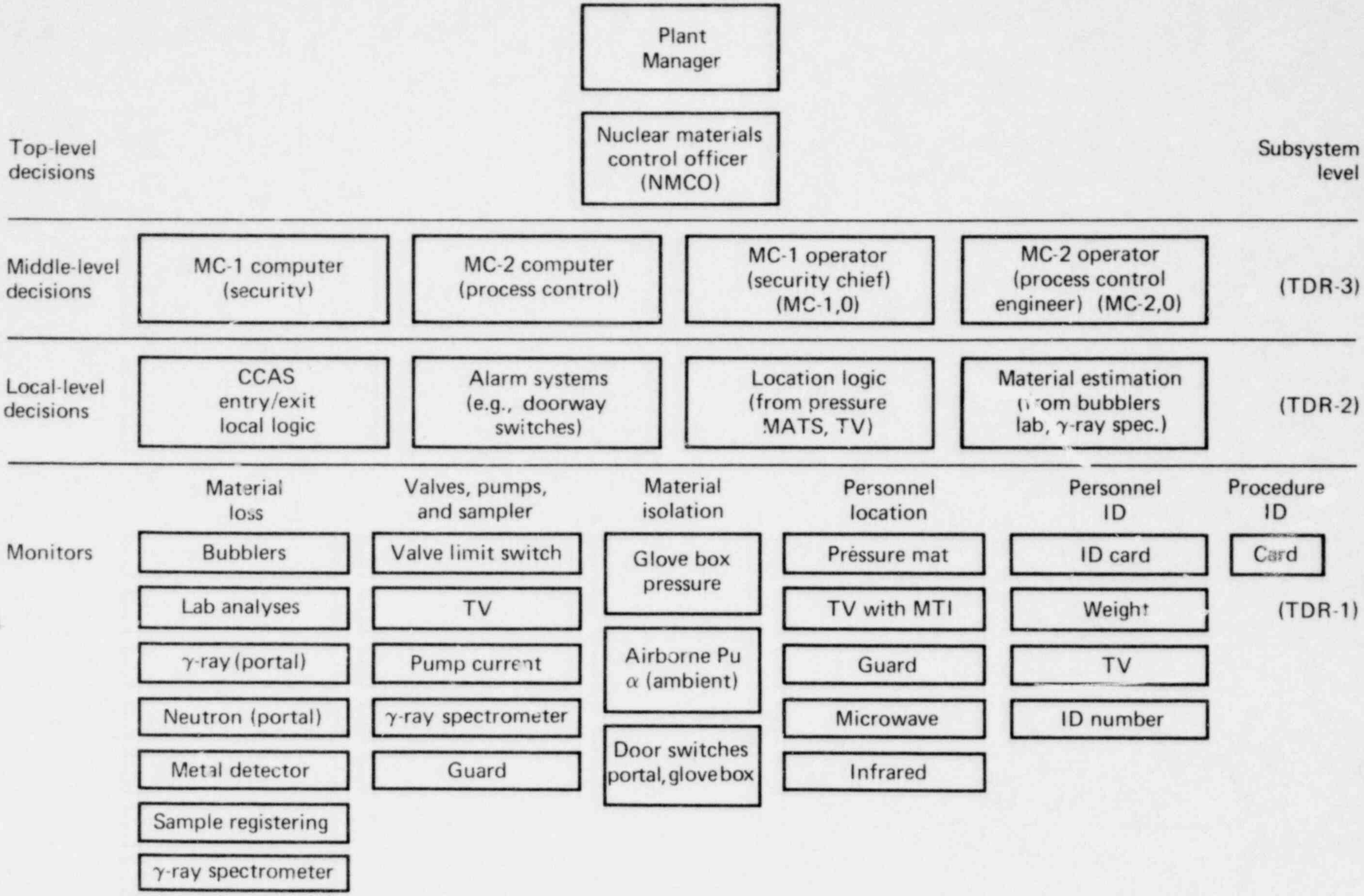


FIG. 20. Material control system hierarchy.

TDR levels are generated according to the MC decision logic given in Fig. 21. These levels are generated through electrical signals from sensors or subsystems, as received by the MC-1 and MC-2 computers or by the direct action of human operators.

In addition to the direct influence of operators and the effects of single anomalies, there are two principal methods of generating TDR levels. First, certain combinations of anomalies produce TDR levels. In Fig. 21, the anomaly variable A_j^i is defined by

$$A_j^i = \begin{cases} 1 & \text{alarm state exists} \\ 0 & \text{normal state exists} \end{cases} ,$$

where the superscript i indicates the TDR level produced by the anomaly and the subscript j indicates the monitor or operator source. The next higher TDR level is generated automatically when the system has remained at an abnormal alert state longer than a specified period of time. A TDR-1 state persisting longer than 15 minutes gives rise to a TDR-2 state; a TDR-2 state lasting longer than 30 minutes causes a TDR-3 state. These rules are indicated in Fig. 21.

The MC safeguards system response rules to the various TDR levels are delineated in Tables 2 and 3. The number and location of guards in the MAA are specified for each TDR state.

The unit model digraph for the MC decision logic is shown in generic form in Fig. 22. The digraph specific to the Test Bed is shown on the right-hand side of sheet 1 of the system digraph in Fig. C-1, in which conditions with regard to alarm states and timing appear on positive edges. There are four ways in which normal information flow can be nullified that appear on zero edges:

1. Adversary activity, i.e., equipment tampering
2. Inadequate monitor sensitivity
3. Random monitor failure
4. Human failure, i.e., slow guard response.

Alternatively, information flow can be nullified by adversary cancellation loops. An adversary cancellation loop refers to actions by an adversary that cancel the effect of his disturbance on the system when attempting to perpetrate an SNM theft. An example is theft of Pu Nitrate from a storage

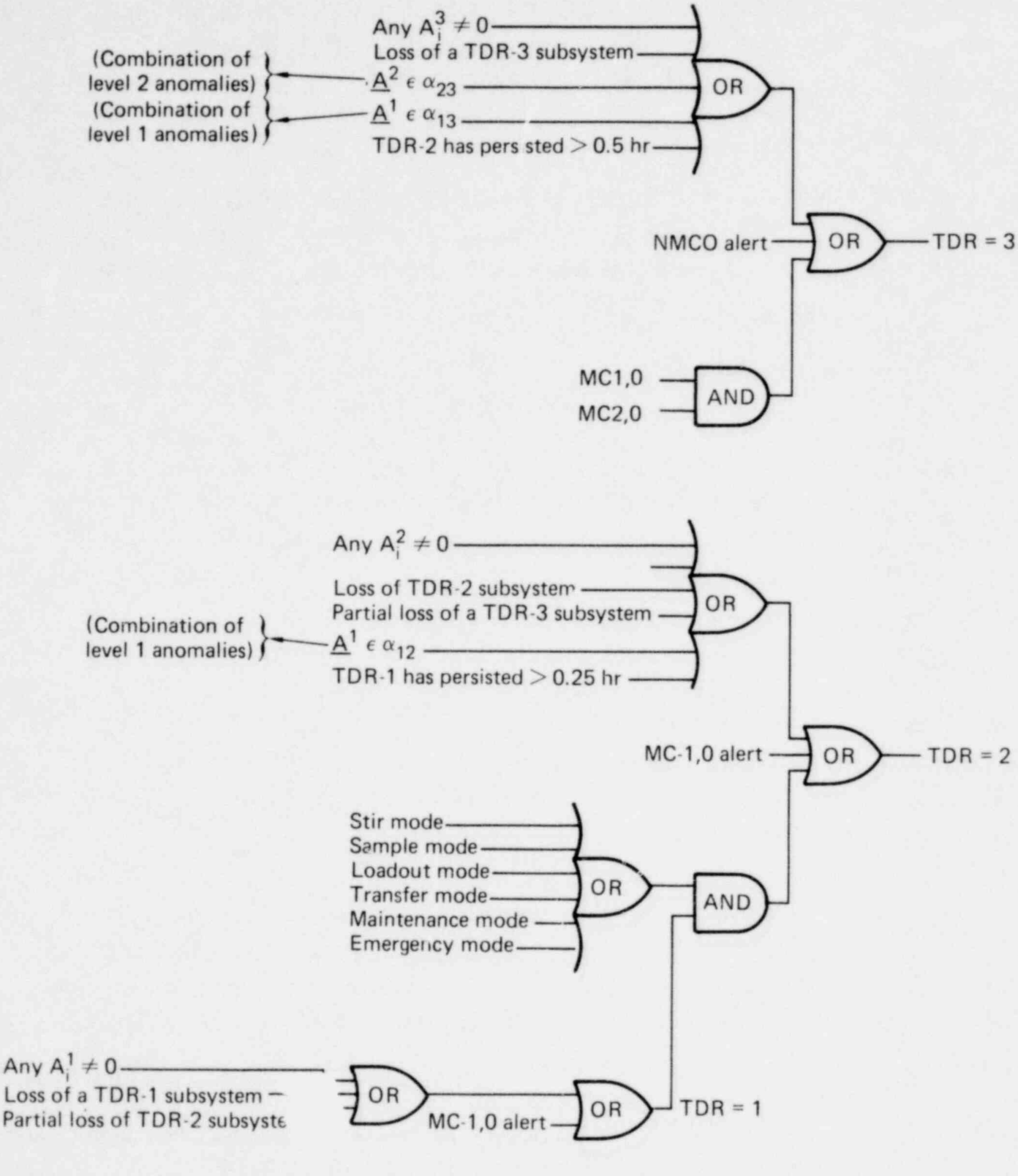

Any $A_i^3 \neq 0$
Loss of a TDR-3 subsystem
(Combination of level 2 anomalies)
$\underline{A}^2 \epsilon \alpha_{23}$
(Combination of level 1 anomalies)
$\underline{A}^1 \epsilon \alpha_{13}$
TDR-2 has pers sted > 0.5 hr
OR
NMCO alert
OR
TDR = 3
MC1,0
MC2,0
AND
Any $A_i^2 \neq 0$
Loss of TDR-2 subsystem
Partial loss of a TDR-3 subsystem
(Combination of level 1 anomalies)
$\underline{A}^1 \epsilon \alpha_{12}$
TDR-1 has persisted > 0.25 hr
OR
MC-1,0 alert
OR
TDR = 2
Stir mode
Sample mode
Loadout mode
Transfer mode
Maintenance mode
Emergency mode
OR
AND
Any $A_i^1 \neq 0$
Loss of a TDR-1 subsystem
Partial loss of TDR-2 subsyste
OR
MC-1,0 alert
OR
TDR = 1

FIG. 21. MC decision logic.

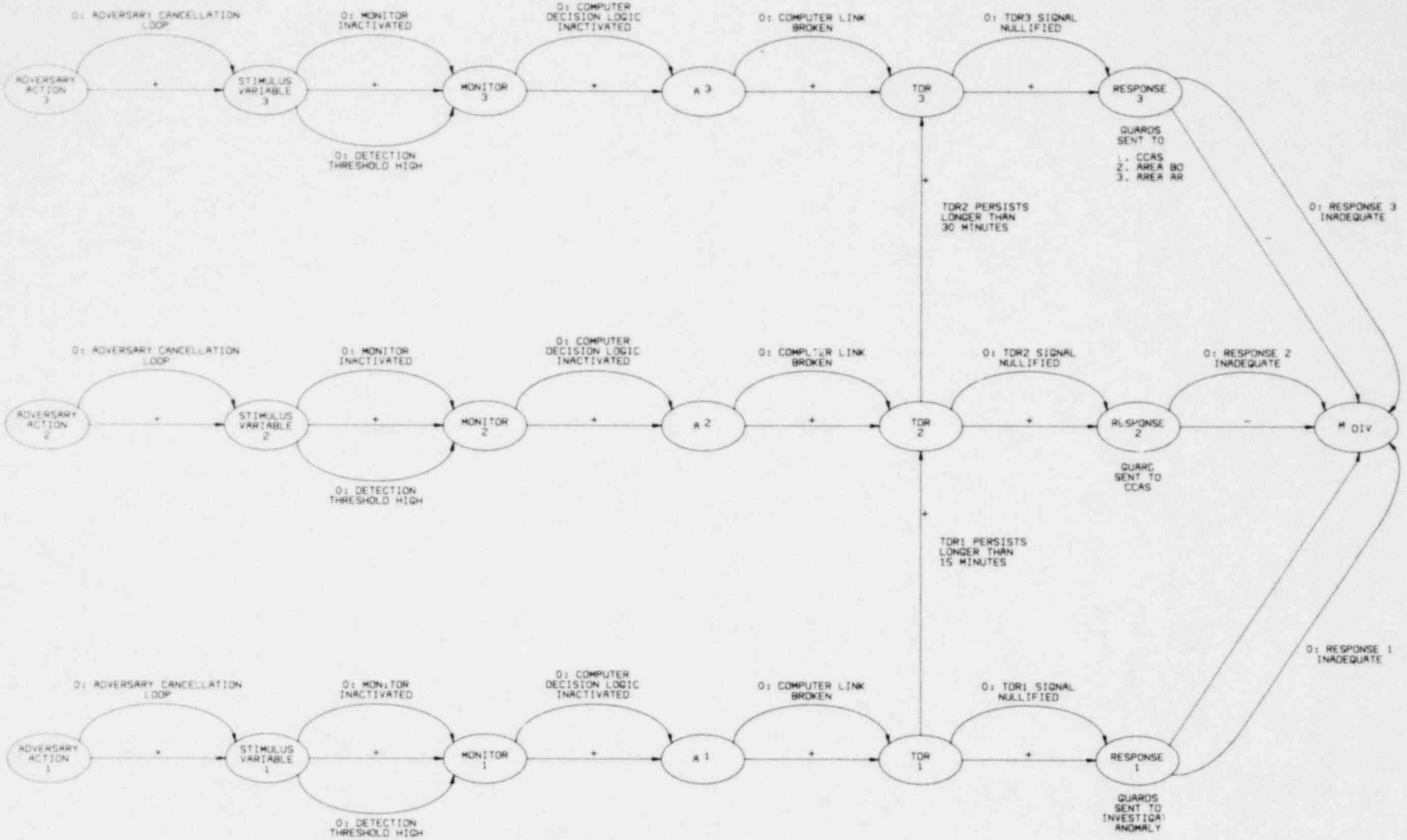


FIG. 22. Unit model of decision logic with generic failure modes.

tank, with simultaneous liquid substitution. An adversary cancellation loop is modeled as a branch of a <u>feedforward loop</u> on the system digraph (see Appendix B for details).

4.2.3.5 <u>Guard Response to TDR Levels</u>. The unit model digraph of guard response to the various TDR levels is shown in Fig. 23. Response rules dictate that a guard be sent to the CCAS whenever the TDR alarm state is greater than 1 and that an additional guard be sent to each of areas B_0 and A_R when the alarm state TDR-3 exists.

For a guard to fail at the assigned locations, either of the two conditions must occur:

1. A guard is not sent to the assigned location because the indicated alarm state does not require it.
2. A guard is dispatched to the assigned location and fails to apprehend the adversary.

Condition 1 implies that the system alarm state is TDR-0 or TDR-1 whenever the adversary exits via the CCAS. Condition 2 implies that a guard is sent to the assigned location but fails to apprehend the adversary for one of five reasons:

1. Guard not present
2. Guard fails to observe
3. Guard fails to detect
4. Guard in collusion
5. Guard disabled.

The above guard failures appear as zero edges in the unit model digraph of a stationed guard given in Fig. 24.

4.2.3.6 <u>Procedural Nonevents and Anomalies</u>. Test Bed procedures require certain valves to be opened and certain locations to be visited during the various modes of operation. For example, during the product receival mode of operation, valves 713 and 719 must be opened and level 2B must be visited. If these actions are not performed by the end of the procedure (i.e., nonevents), level 1 anomalies are produced. The unit model digraphs for the procedural nonevents and anomalies are shown on sheet 3 of the system digraph in Fig. C-1.

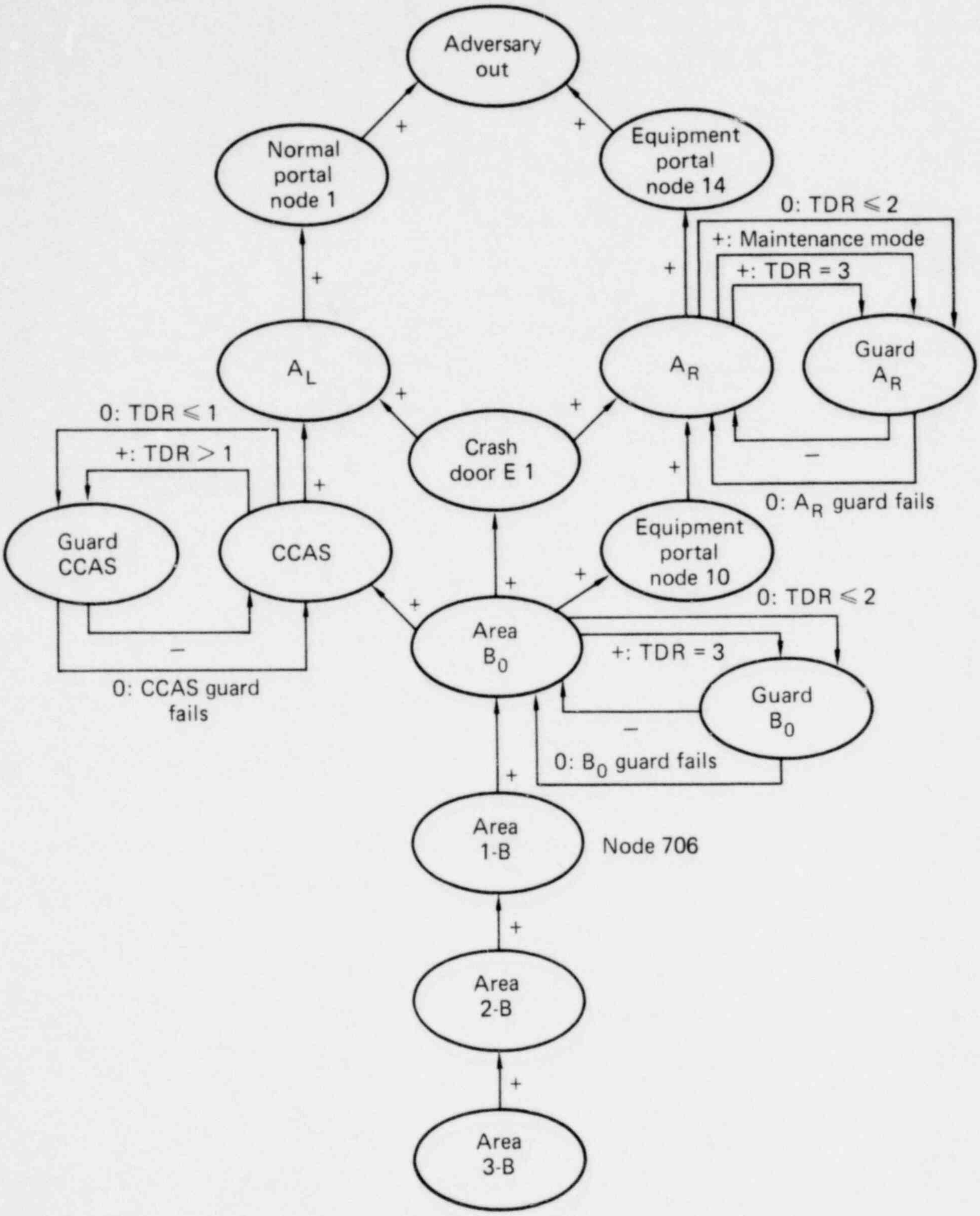


FIG. 23. Unit model of guard response to TDR levels.

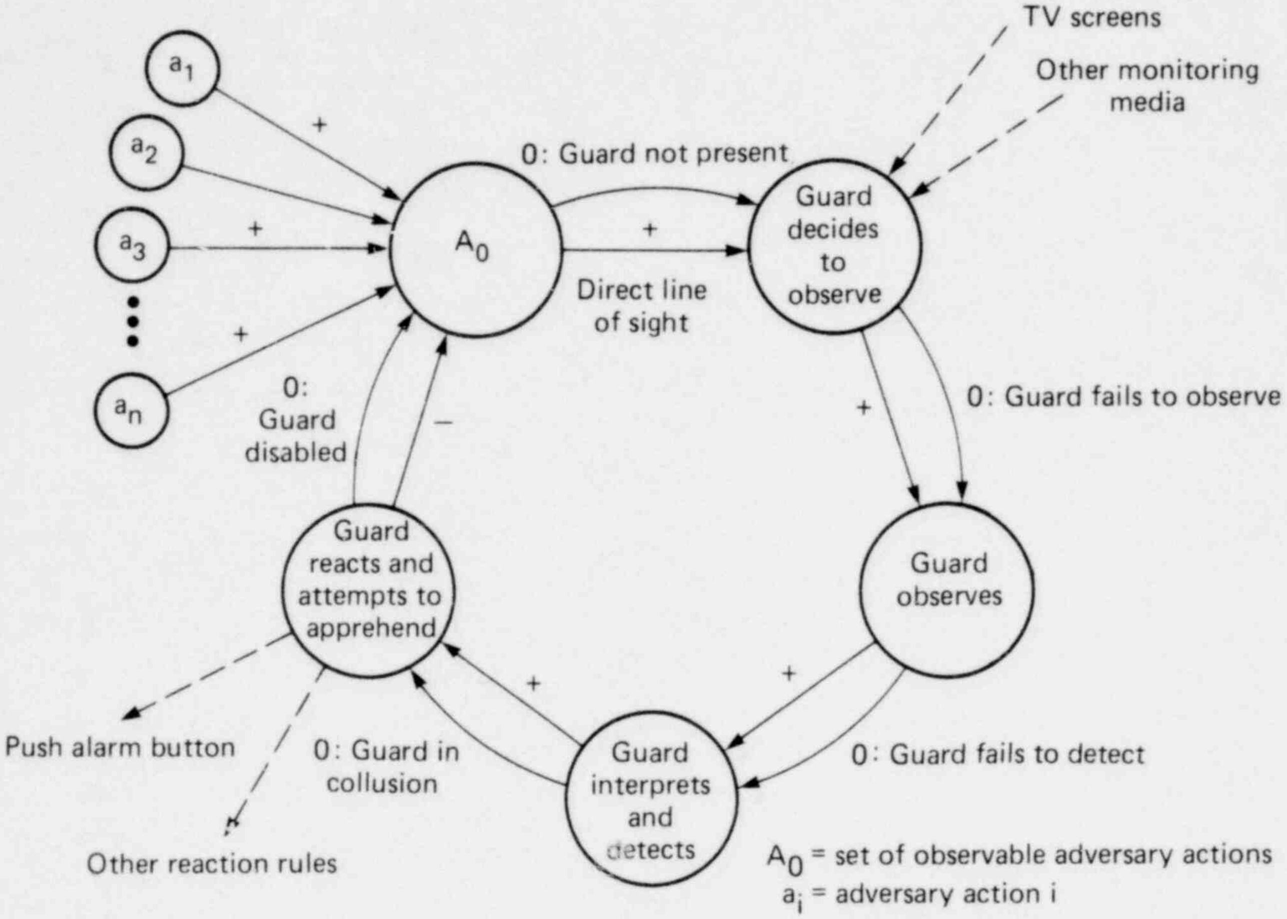


FIG. 24. Unit model of guard at station.

The modeling of nonevents requires the comparison of the set of locations actually visited during some procedure K, denoted by $\left\{L_K\right\}$, with the set of locations required to be visited for that procedure, denoted by $\left\{\tilde{L}_K\right\}$. The comparison must yield $\left\{\tilde{L}_K - L_K\right\}$ equal to the null set in order for no anomaly to be generated.

A similar set of definitions and approaches is used on the valve positions during the various modes of operation. $\tilde{\underline{V}}_K$ denotes the vector of valve positions authorized for procedure K, and $\underline{V}_K$ denotes the vector of valve positions at the end of procedure K. Hence, $\left\{\tilde{\underline{V}}_K - \underline{V}_K\right\}$ must equal the zero vector for no anomalies to be produced.

Verification that $\left\{\tilde{L}_K - L_K\right\}$ yields the null set and $\left\{\tilde{\underline{V}}_K - \underline{V}_K\right\}$ yields the zero vector is accomplished by establishing boundary conditions during the construction of the fault tree. (See Section 4.2.4.)

4.2.3.7 Differential Pressure Cells. One of the key material monitoring devices is the differential pressure (DP) cells. The differential pressure cell measurements are used to determine the solution level in each storage tank. These measurements are also used during the static mode of operation to obtain an estimate of solution mass in the tank. The unit model digraph of the operation of the DP cells is given on sheet 4 of Appendix C. A description of the DP cells used in the construction of the unit model follows.

Each storage tank has two DP cells, I and II (Fig. 25). An air supply provides air for the system through lines 1, 2, and 3. DP cell I measures the difference between pressures at points 2A and 1A. This measurement is expressed by

$$P_I = P_{2A} - P_{1A} \quad ,$$

where

$$P_{2A} = \rho g L + P_{\text{ambient}}$$

$$P_{1A} = P_{\text{ambient}} \quad .$$

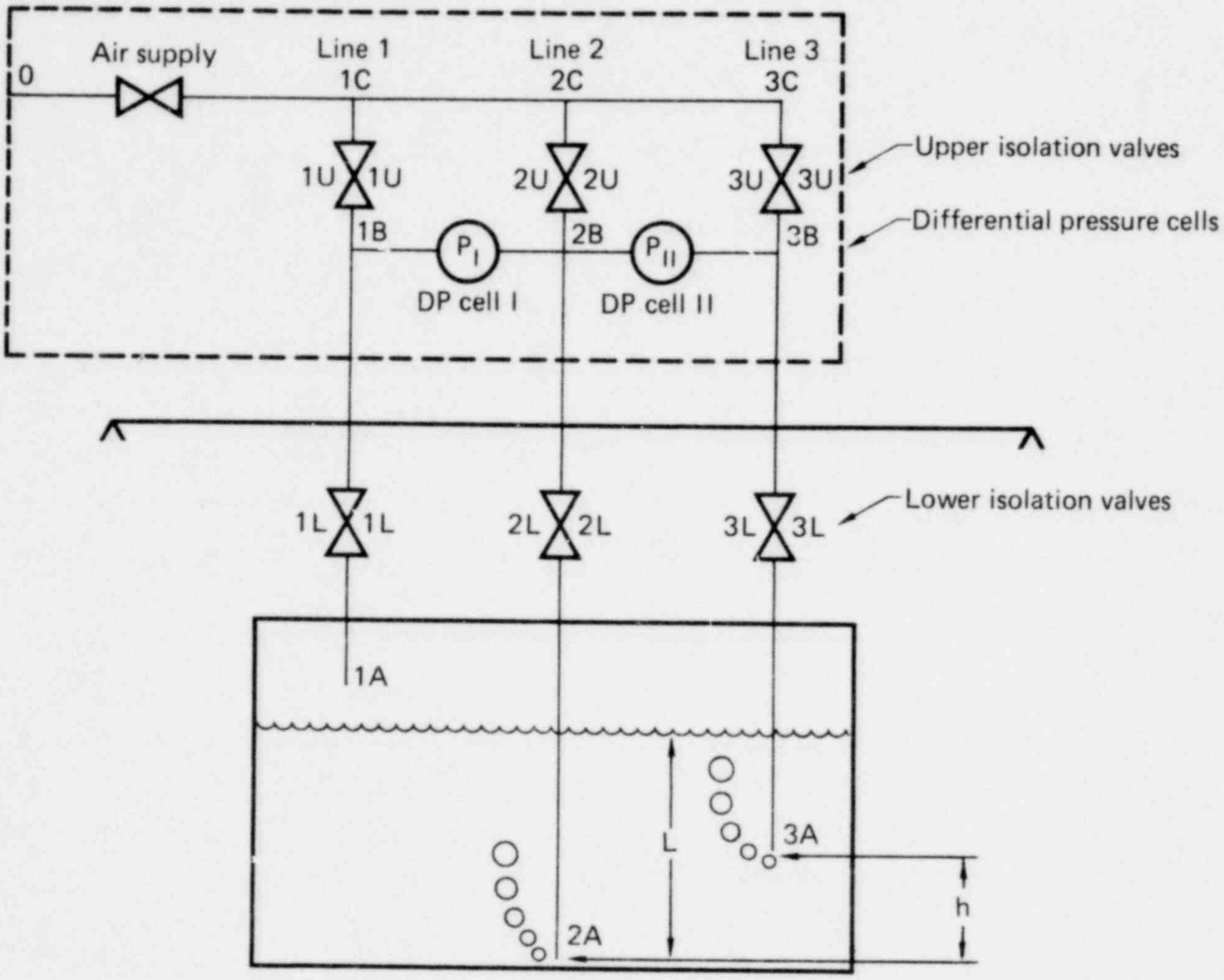


FIG. 25. Storage tank with differential pressure cells.

1425 301

Hence,

$$P_I = \rho g L \quad ,$$

where ρ is the density of the solution, g is the gravitational constant, and L is the length of line 2 submerged in the solution.

DP cell II measures the difference between pressures at points 2A and 3A; this measurement is given by

$$P_{II} = P_{2A} - P_{3A} \quad ,$$

where

$$P_{2A} = \rho g L + P_{ambient}$$

$$P_{3A} = \rho g (L-h) + P_{ambient}$$

and h is the difference in length between lines 2 and 3, and ρ, g, L are as previously defined. Thus,

$$P_{II} = \rho g h \quad .$$

Consequently, measuring P_{II} determines the value of ρ since both g and h are known constants. Once ρ is known, then L can be determined by measuring P_I. L serves as an estimate of the solution level in the tank, and ρL is the estimate of solution mass in the tank.

The digraph on sheet 4 of Fig. C-1 embodies the relationships described above. Bidirectional edges connect the pressure variables, because pressure communicates both upstream and downstream. Various failure modes and the closing of isolation valves 2L and 3L are also shown on the digraph. Closing these two valves maintains a constant pressure drop across DP cells I and II and allows SNM to be removed from the tank without causing the estimated solution level to decrease. However, closure of the isolation valves is not included in the analysis for two reasons:

1. A smooth rather than a "noisy" level indication would be detected by the material estimation system as an anomaly.
2. Isolation valves 2L and 3L are located below floor level 3B, which is covered by metal grids with microswitches that would detect any disturbance on the grids.

4.2.3.8 Material Estimation Detectors. The unit model digraph of the material estimation detectors is given on sheet 4 of Fig. C-1. A description of these estimation detectors follows.

Measurements from the DP cells, P_I and P_{II}, are statistically smoothed by means of a Kalman filter to estimate the mass of solution in the tank. The accuracy of the measurements used to obtain the mass estimate corresponds to a standard deviation of 237 g of solution. Hence, the instrumentation accuracy is a limiting factor in detecting solution mass changes as a result of SNM theft; other limiting factors are tank solution radiolysis and uncertainties in the evaporation rate.

Three estimation detectors receive the output of the Kalman filter and perform statistical hypothesis testing to determine whether SNM theft has occurred. There are three detectors:

1. Nominal Detector
   This detector has a low false-alarm rate and operates on a 30-minute smoothing interval. Detection by this system causes an A^2 anomaly level in the MC system.
2. High Sensitivity Detector
   This detector, which has a higher false-alarm rate, is used to provide a fast detection response when the MC logic is in a TDR-1, TDR-2, or TDR-3 state.
3. Large Diversion Detector
   This is continuously operating detector with a very low false-alarm rate. It is used to set off an alarm on the detection of gross diversion.

4.2.3.9 Material Balance for the Product Receival Mode. The plutonium product cell (PPC) contains three storage tanks, each with a 416-liter capacity.

Whenever two of the tanks in the PPC are full, the product receival mode of operation is initiated, and 730 liters are transferred from the PPC to storage tanks in the plutonium nitrate storage area (PNSA).

Each tank in the PPC and each storage tank in the PNSA have a pneumatic bubbler system (the DP cells are part of this system) that estimates the solution mass in the tank. Laboratory analyses of samples determine the density and concentration of SNM product in each of the two PPC tanks.

When the transfer of product is made, the mass of the transferred solution is compared with the estimated solution mass in the storage tank in the PNSA. This mass balance of solution is accomplished by using a 30-minute smoothing interval. Consequently, SNM theft during the product receival mode can be detected, at the very earliest, 30 minutes after the storage tank in the PNSA has been filled unless it is a large theft. The time to detection is probably much longer, because two to three hours are required to homogenize the contents of the tanks. If SNM theft with substitution of material of the same density as the stolen material occurs, then this theft cannot be detected until the tank has been stirred and solution samples have been sent to the laboratory for the determination of plutonium concentration. Thus, a mass balance to detect SNM theft with material substitution can be completed only approximately two days after the product receival mode is finished. In any event, if the material estimates are within the 2σ allowed error band, SNM theft will not be detected.

These time conditions and measurement sensitivities are shown on the edges in the unit model digraph for material balance during the product receival mode (sheet 6 of Fig. C-1).

4.2.4 System Digraph for Test Bed Assessment

The system digraph is generated by connecting the unit models described in the previous section. Appendix C gives the system digraph of the Test Bed.

A total of 157 control loops appear in the system digraph. Thus, a total of 157 safeguards signals (i.e., stimuli) may be generated when an adversary attempts to steal SNM from tank 1. Each control loop is initiated by an adversary action and is normally terminated by a defined system response. These control loops are the negative branches of feedforward or feedback loops (See Appendix B). Adversary cancellation loops are formed when zero edges and the ways by which information flow can be manipulated are added to these loops.

Those control loops representating the MC system responding to signals generated by personnel location monitors are inactivated for two reasons:

1. An insider can steal SNM without visiting any unauthorized locations during the product receival mode of operation.
2. An insider can visit the required locations specified by procedures for the product receival mode.

Thus, no personnel location anomalies are produced when SNM theft occurs during the product receival mode.

In addition, the control loop that models the dispatching of a guard to area B_0 during a level 3 alarm is inactivated because of time constraints. (See Fig. 9 for facility layout.) In particular, the adversary must perform three acts prior to crossing area B_0. To perpetrate an SNM theft, he must open valve 701, open valve 722, and fill the container with SNM from the storage tank. Although the first two acts produce level 1 alarms, a level 3 alarm is not generated until the level 1 alarms have persisted longer than 45 minutes. Furthermore, an SNM loss from the storage tank cannot be detected by the material estimator until at least 30 minutes after the tank is filled; hence, a level 3 alarm would not be produced until then. In short, the adversary can exit the MAA long before any level 3 alarm is produced.

Consequently, the control loops that have an SNM theft preventive function are those involving monitors, alarms, and procedures for MAA entry or exit and SNM movement. These relevant control loops are the loops the adversary must inactivate to ensure a successful SNM theft.

The construction of the system fault tree for the Test Bed assessment is based upon the failure of these relevant control loops.

4.2.5 System Fault Tree for Test Bed Assessment

The system fault tree for the Test Bed assessment is generated from the system digraph by means of a transformation algorithm based upon the adversary inactivation, or cancellation, of the safeguards system control loops. Appendix D shows the fault tree for the Test Bed assessment. The fault tree consists of 113 basic events and 126 logic gates, of which 64 are AND gates and 62 are OR gates.

In generating the fault tree, all relevant control loops are first identified on the system digraph. Then, the transformation algorithm is applied by starting from the top event variable (the variable of interest) in the system digraph. In this case, the top event is successful SNM theft from the Test Bed. The basic operator in the algorithm used to obtain the adversary cancellation loops is shown in Fig. 26. Repeated application of this operator yields the fault tree.

Adversary cancellation of the control loops can have two results:

1. No safeguards system response
2. Inadequate safeguards system response.

Events that lead to these two outcomes in the Test Bed assessment are shown in the operator in Fig. 26. This operator allows the distinction to be made between failure events that generate no safeguards system response and events that nullify the response when a monitor signal is received.

As shown on the bottom of Fig. 26, three generic failure modes which lead to no MC monitor signal are considered:

1. Random failure
2. Failure caused by adversary tampering
3. Failure caused by monitor insensitivity.

The first failure mode is caused by an internal failure and is known as a primary failure in standard fault tree analysis (FTA). The second failure mode results from failure outside the design envelop of the component and is referred to as a secondary failure. The third failure mode represents the insensitivity of a component in detecting stimulus input and is not considered in standard FTA.

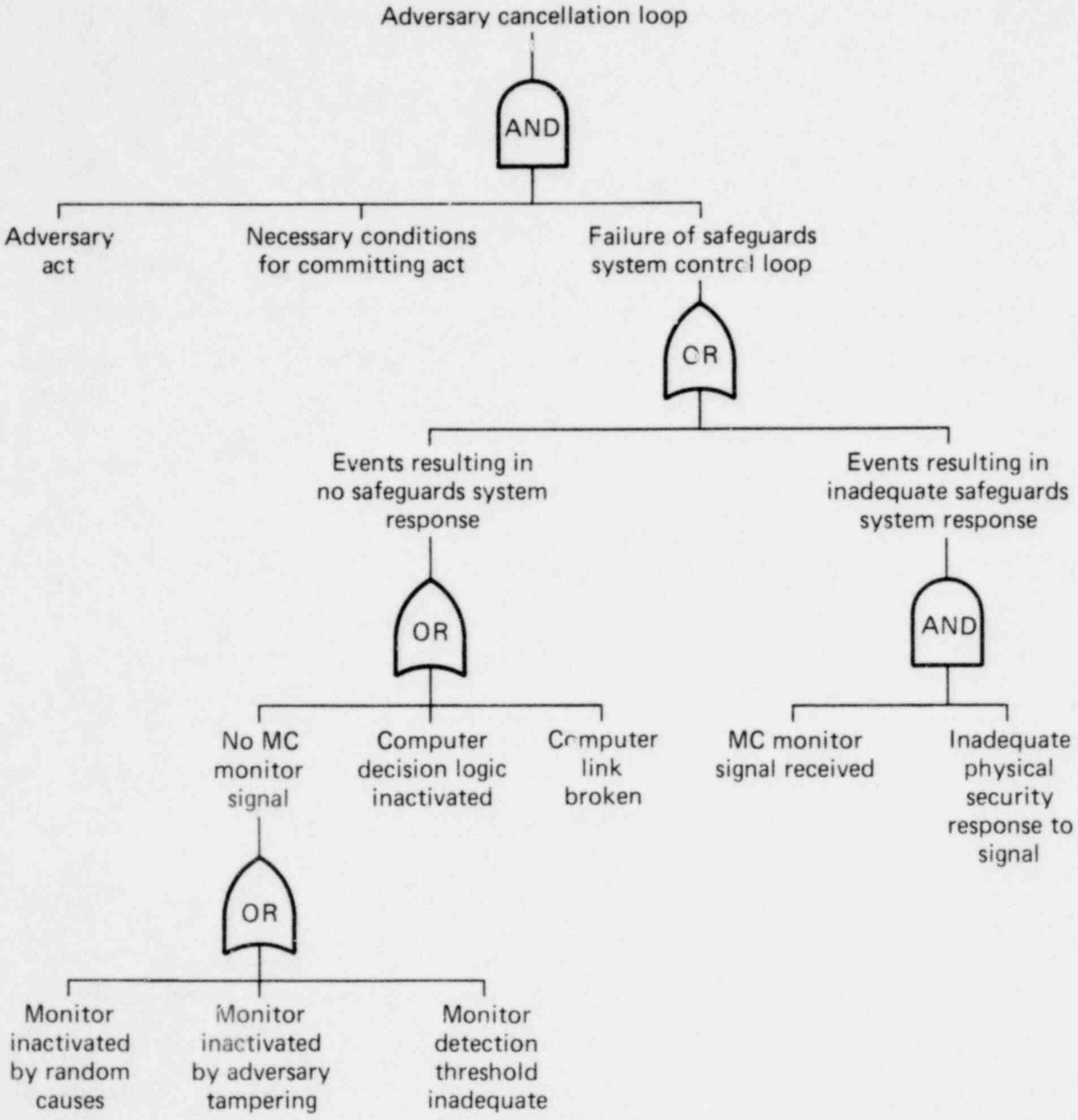

Adversary cancellation loop
AND
Adversary act
Necessary conditions for committing act
Failure of safeguards system control loop
OR
Events resulting in no safeguards system response
Events resulting in inadequate safeguards system response
OR
AND
No MC monitor signal
Computer decision logic inactivated
Computer link broken
MC monitor signal received
Inadequate physical security response to signal
OR
Monitor inactivated by random causes
Monitor inactivated by adversary tampering
Monitor detection threshold inadequate

FIG. 26. Basic fault tree operator for obtaining adversary cancellation loops.

The fault tree in Appendix D describes how successful theft of SNM from the Test Bed can occur when SNM is removed from the pump wash line during the product receival mode of operation.

Sheet 1 of the fault tree indicates three ways in which an adversary can successfully exit the MAA with SNM:

1. Through the CCAS during the product receival mode
2. Through the emergency doors during the product receival mode
3. Through the equipment portals during the maintenance mode.

Sheet 2 of the fault tree describes in detail how an adversary can successfully exit the CCAS with SNM. Basically, he can exit the CCAS by three techniques:

1. Pushing the crash bar in the CCAS
2. Cancelling the control loops triggered by anomalous signals generated while exiting the CCAS (see Fig. 26)
3. Colluding with the MC-1 and/or MC-2 operators.

It is also necessary for the success of any of these three techniques that the CCAS guard respond inadequately.

Sheets 3, 4, and 5 show how SNM is successfully removed from node 706 (the pump wash line) during the product receival mode of operation. The adversary must perform five actions:

1. Open valve 722
2. Open valve 701
3. Fail check valve 436 open
4. Cancel control loops triggered by limit switches on valves 722 and 701
5. Cancel control loops triggered (after some time delay) by the material estimation system.

Special consideration is needed in the construction of the fault tree for failure of the CCAS guard (right side of Sheet 2). The CCAS guard can fail in only two possible ways:

1. A guard has never been dispatched to the CCAS because the system TDR state is less than or equal to TDR-1.

2. A guard is sent to the CCAS when a TDR-2 or TDR-3 alarm is generated and fails to apprehend the adversary.

Thus, boundary conditions concerning the system alarm state are imposed in order to obtain a correct fault tree. Figure 27 shows the two boundary conditions imposed:

1. System alarm state less than or equal to 1 (TDR $\leq$ 1)
2. System alarm state greater than 1 (TDR > 1).

These boundary conditions constrain the ways in which the adversary cancels the safeguards information flow or control loops. For instance, if TDR $\leq$ 1 then all adversary acts and monitor failures occurring prior to the time of adversary exit must generate a TDR alarm no greater than 1. In addition, only two types of situations lead to an alarm state of TDR-1 (see unit model of MC decision logic, Fig. 22).

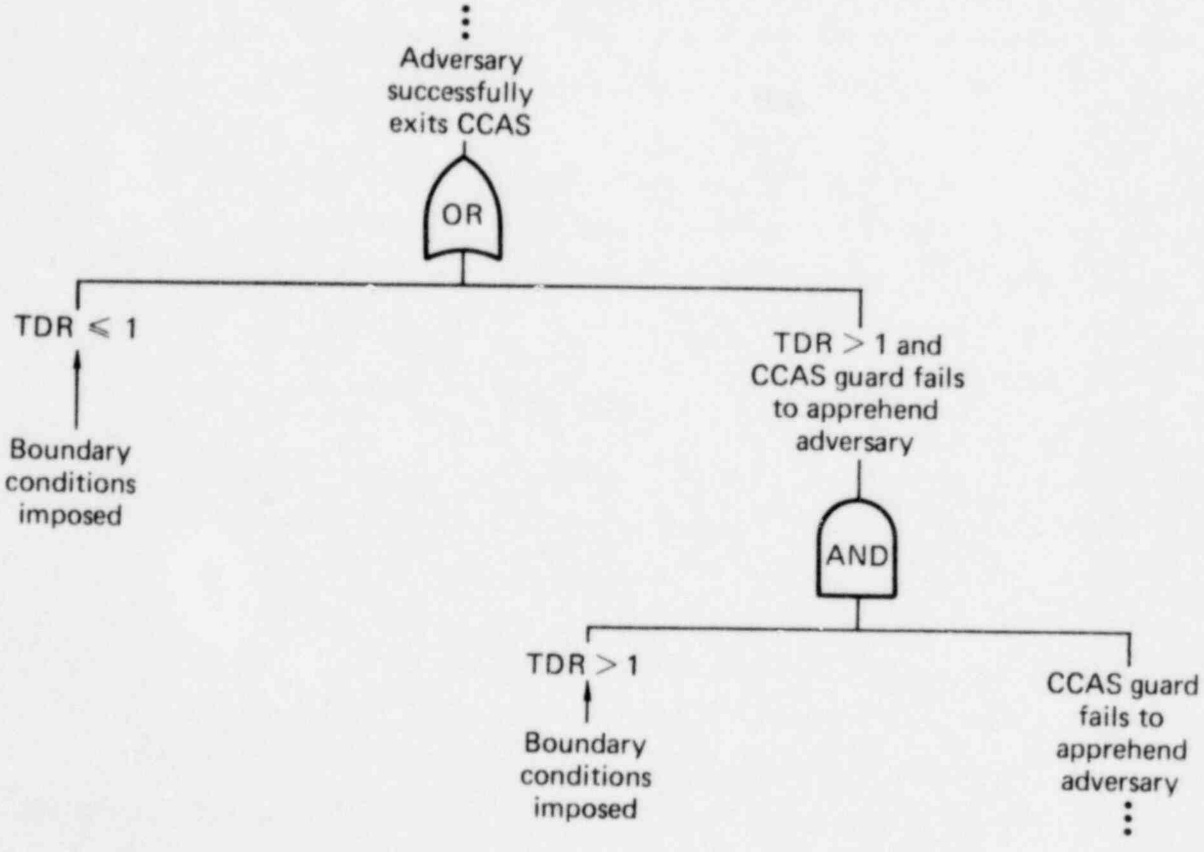

Adversary successfully exits CCAS
OR
TDR ≤ 1
Boundary conditions imposed
TDR > 1 and CCAS guard fails to apprehend adversary
AND
TDR > 1
Boundary conditions imposed
CCAS guard fails to apprehend adversary

FIG. 27. Use of boundary conditions in construction of fault tree.

1. If an adversary performs an act that generates a TDR-1 alarm, then he must exit the CCAS within 15 minutes after the act. Otherwise, a TDR-1 alarm persisting more than 15 minutes produces a TDR-2 alarm. Alternatively, an adversary can nullify the safeguards information flow in such a way that a level 1 response is not generated.
2. If an adversary commits an act that generates a TDR-2 or TDR-3 alarm, then he must nullify the safeguards information flow in such a way that a level 2 or 3 response is not generated.

Thus, the dynamics of the control loops in the system digraph must be examined to determine if the above situations can occur, i.e., if the adversary can exit the MAA with SNM before a TDR-2 alarm is generated. In the case of SNM theft from the pump wash line during the product receival mode, the adversary can accomplish this.

The following timing condition must be satisfied by each adversary act of type 1 (that is, an act which, if detected, will generate a level 1 alarm).

$$T_1 + T_2 + \dots T_n < 15 \text{ min} \quad ,$$

where n is the number of acts an adversary must perform to perpetrate an SNM theft prior to exiting the CCAS, and T_i is the duration of adversary act i. This timing constraint is graphically shown in Fig. 28.

4.3 QUALITATIVE ANALYSIS OF THE FAULT TREE FOR THE TEST BED

Qualitative analysis of the fault tree is the use of nonnumerical methods to elicit important information contained in the tree. Although there are many types of qualitative analyses, three were selected for the Test Bed assessment:

1. The generation of minimal cut sets
2. Structural analysis of the fault tree
3. Common-cause analysis of the cut sets.

Each of these three methods is discussed below, along with the outputs for the Test Bed assessment.

1425 311

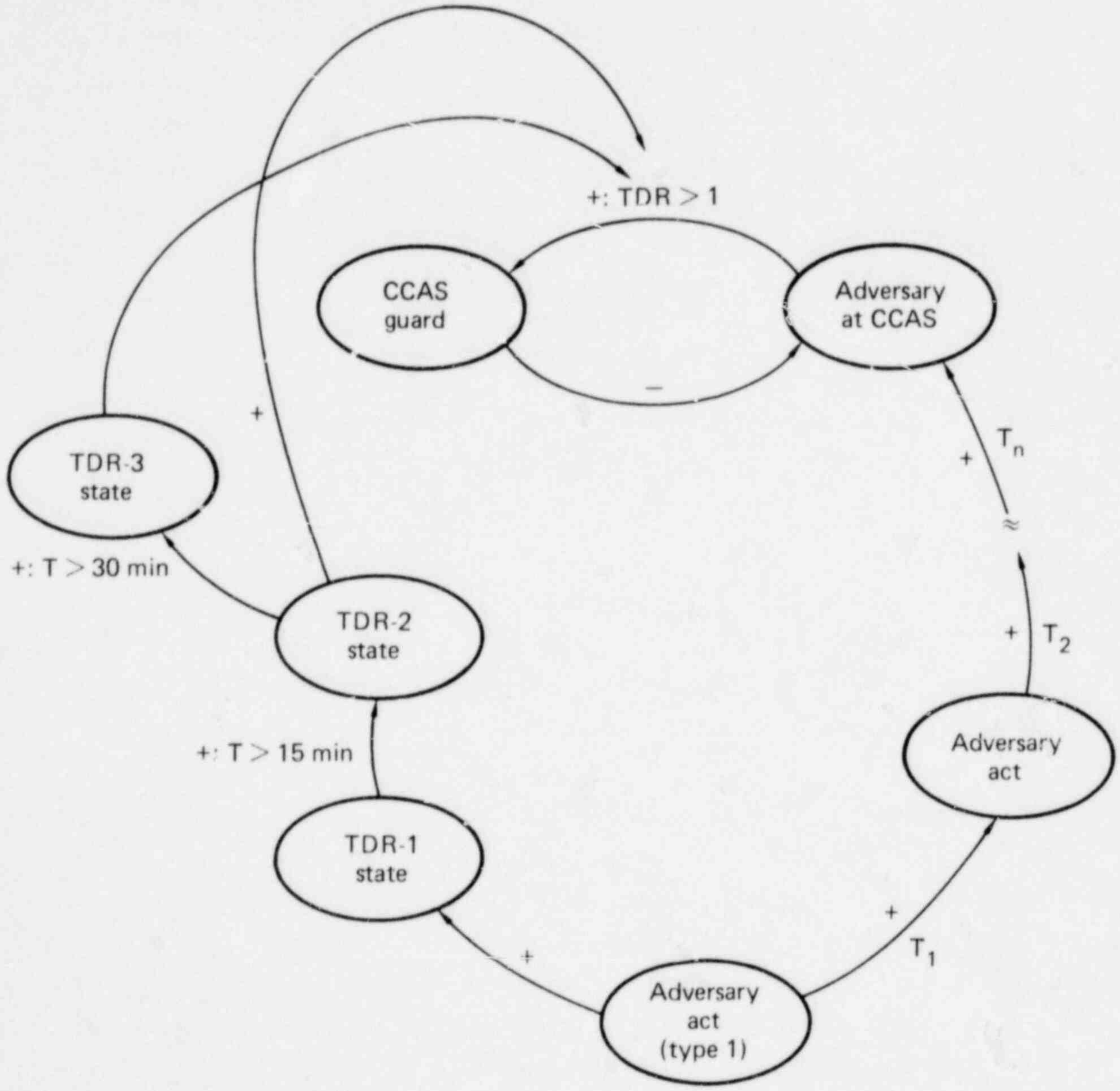


FIG. 28. Consideration of control loop dynamics in the system digraph.

4.3.1 Generation of Minimal Cut Sets

In fault tree terminology, a minimal cut set is a set of basic events that ensures the occurrence of the top event (the event of interest for which the fault tree is constructed); it cannot be reduced and still cause the occurrence of the top event. For the Test Bed assessment, the top event is successful theft of SNM from the Test Bed. Basic events are the lowest resolution events in the fault tree, e.g., equipment failure and adversary acts. The minimal cut sets for the Test Bed fault tree represent the minimum sets of system conditions and adversary acts that will allow SNM theft to occur; they are called adversary event sets (AES). The AES are required for both the qualitative and quantitative analyses that provide the results of the assessment. The AES are generated by the computer codes, Fault Tree Analysis Program (FTAP),[10] and the Set Equation Transformation System (SETS).[11]

4.3.1.1 Adversary Event Sets. Two categories of AES for the Test Bed were generated. The first category was AES for successful SNM theft with no MC alarms generated, i.e., no detection. The second category was AES for successful SNM theft with inadequate safeguards systems response, given that MC alarm(s) occurred.

For each category of AES, two types of situations were considered:

1. SNM theft in which only random equipment failures occurred
2. SNM theft in which both random equipment failures and intentional equipment tampering occurred.

Thus, four distinct groups of AES were generated for the Test Bed assessment. Let S_1, S_2, S_3, and S_4 denote these groups and be defined by

S_1 = those event sets of SNM theft with no alarm generated by the safeguards system, only random failures occurring

S_2 = those event sets of SNM theft with inadequate safeguards system response, only random failures occurring

S_3 = those event sets of SNM theft with no alarm generated by the safeguards system, adversary tampering occurring

S_4 = those event sets of SNM theft with inadequate safeguards system response, adversary tampering occurring.

Thus, S_1 and S_3 are AES where adversary acts cause <u>no</u> alarm signal to be generated by the MC system, and S_2 and S_4 are AES where <u>at least one</u> alarm signal is generated but the MC response is inadequate.

These four groups form a partition that covers all possible scenarios for an adversary to perpetrate a SNM theft by removing material from the pump wash line in the Test Bed. Let S denote all these possible scenarios. For the Test Bed assessment, S consists of 814,042 AES.

Then,

$$S = S_1 \quad S_2 \quad S_3 \quad S_4$$

and

$$S_i \quad S_j = \emptyset \text{ for } i \neq j \quad ,$$

where represents the union over sets and represents the intersection over sets.

Each AES contains the following types of information: adversary access to the SNM, adversary acquisition of the SNM, adversary removal of the SNM from the Test Bed, and adversary inactivation of the safeguards system to allow these acts. Each AES contains between 21 and 28 basic events.

Listed below is one of the AES generated for the Test Bed assessment.

ANODE 7Ø6, CONAT7Ø6, MPU7Ø9, PRMODE, V7130, V7190, TGTTKFIL, AFILLCON, TLEVEL-1, V7Ø10, V7220, CV4360, V290, NORETDR1, APM-B1, APM-BO, APM-AR, CBE2LHIT, CBE2RHIT, CBEEAHIT, CBEEBHIT, NORETDR3

The description of the alphanumeric designators of the basic events is given in Appendix E.

The description of the above AES now follows:

An adversary with a container is at node 706, the pump wash line. (ANODE 7Ø6, CONAT7Ø6) SNM is coming through the product inlet line (NPU7Ø9). The Test Bed is in the product receival mode (PRMODE). As required by the operating procedures for the product receival mode, valves 713 and 719 must be opened in order to have SNM coming through the inlet line (V7130, V7190).

Sufficient time has elasped since the start of the product receival mode to fill the tank to such a level as to allow mass flow to the pump wash line (TGTTKFIL). The adversary must open valves 701, 722, and 29, which are normally closed during the product receival mode (V7Ø1O, V7220, V290) and fail check valve 436 open (CV4360) so that SNM will flow to node 706.

The adversary fills the container with the SNM (AFILLCON) and the amount of solution mass in the tank decreases (TLEVEL-1).

The opening of valves 701 and 722 generates a TDR-1 alarm that concludes with an inadequate guard response (NORETDR1). The adversary then leaves the MAA (APM-B1, APM-BO, APM-AR) and exits the Test Bed through the emergency and equipment portals by hitting the crash bars (CBE2LHIT, CBE2RHIT, CBEEAHIT, CBEEBHIT). Finally, the use of the crash bars generates a TDR-3 alarm, which receives an inadequate guard response (NORETDR3).

It is clear that the "scenario" given by an AES is very descriptive and contains the necessary system conditions and adversary acts required for successful theft. In short, each AES contains five types of information:

1. Initial conditions of the analysis
2. Adversary access to the SNM
3. Adversary acquisition of the SNM
4. Adversary removal of SNM from the Test Bed
5. Adversary inactivation of the safeguards system.

Since there are an extremely large number of AES (814,042 for the Test Bed), an analyst cannot and would not want to thoroughly inspect each individual AES. Hence, adversary event subsets (AESS) are generated to abstract important information from the AES.

4.3.1.2 Adversary Event Subsets. Adversary Event Subsets (AESS) are smaller and shorter listings of adversary event sets that contain specific information. Two examples of AESS generated for the Test Bed assessment are the adversary exit paths from the facility and the sets of monitors that must be inactivated in order for successful SNM theft to occur.

The procedure for obtaining the AESS involves the use of the TRUE-FALSE option in FTAP.[10] This option allows the analyst to set the value of the basic events to either 1 (TRUE) or 0 (FALSE). If a basic event is set to TRUE, it logically occurs but does not physically appear in the event sets and hence allows further minimization to produce the subsets. If a basic event is set to FALSE, any event set containing the event is eliminated. An example of the application of TRUE-FALSE option appears in Fig. 29. (The AES in S_1 and S_3 are generated using the FALSE option, and the AES in S_2 and S_4 result from using the TRUE option.)

Original cutsets	{1, 2, 3, 4, 5}
	{1, 3, 5}
	{2, 4}

New cutsets after application of TRUE option for events 1 and 4	{2, 3, 5}
	{3, 5}
	{2}

New cutsets after application of FALSE option for event 2	{1, 3, 5}

FIG. 29. Example of application of TRUE-FALSE option.

The TRUE option was used to produce the adversary exit paths; all the basic events containing no path information were set to TRUE. As a result, six exit paths out of the Test Bed from node 706 (pump wash line) were generated:

1. ANODE 706 APM-B1 APM-BO CBE1HIT APM-AL ANODE 1
2. ANODE 706 APM-B1 APM-BO AA-DHIT ALCCAS ANODE 1
3. ANODE 706 APM-B1 APM-BO APM-AR TPEQMM ANODE 14
4. ANODE 706 APM-B1 APM-BO ACCAS CCASOK ANODE 1
5. ANODE 706 APM-B1 APM-BO CBE1HIT APM-AR CBEEBHIT CBEEAHIT ANODE 14
6. ANODE 706 APM-B1 APM-BO CBE2LHIT CBE2RHIT APM-AR CBEEAHIT CBEEAHIT ANODE 14

The alphanumeric designators used to describe the paths are defined in Appendix E.

Each path begins at the pump wash line (node 706) and ends at nodes on the system boundary (nodes 1 or 14). See Fig. 8, which shows the emergency crash doors. Path 3 involves exit during the maintenance mode where theft of SNM occurs during product receival but the SNM remains within the MAA until the maintenance mode of operation. Path 4 is the normal exit through the CCAS during the product receival mode.

The TRUE option was also used to obtain the sets of monitors that must be inactivated for successful SNM theft. All basic events not related to the operation of the MC&A monitors were set to TRUE. This particular application of the TRUE option reduced the 814,042 AES to a much more tractable 286 monitor subsets that must be inactivated. In addition, the subsets now consist of 2 to 8 basic events rather than the original 21 to 28 basic events.

A partial listing of these monitor subsets is given below:

1. CDLI CV436IT
2. ALARMIT CV436IT TDR1-G
3. CV436IT TDR1-G TDR3-G
4. ALARMLX CV436IT TDR1-G

1425 317

5.	ALARMIT	CV436IT	LS701IT	LS722CIT
6.	CV436IT	LS701IT	LS722CIT	TDR3-G
7.	ALARMIT	CV436IT	LS701CIT	LS722IT
8.	CV436IT	LS701CIT	LS722CIT	TDR3-G
9.	ALARMIT	CV436IT	LS701IT	LS722IT
10.	ALARMLX	CV436IT	LS701IT	LS722CIT

The alphanumeric designators used to describe the monitor subsets are also defined in Appendix E.

Many types of event subsets, as specified by the analyst, can be obtained through the application of the TRUE-FALSE option on the AES. These event subsets select and concentrate certain information contained in the AES, and in general aid in making the qualitative analysis manageable.

4.3.2 Structural Importance of Basic Events

The relative importance of each basic event to the occurrence of the top event, successful SNM theft from the Test Bed, provides valuable information about the safeguards system. This information can be used to upgrade the safeguards system design.

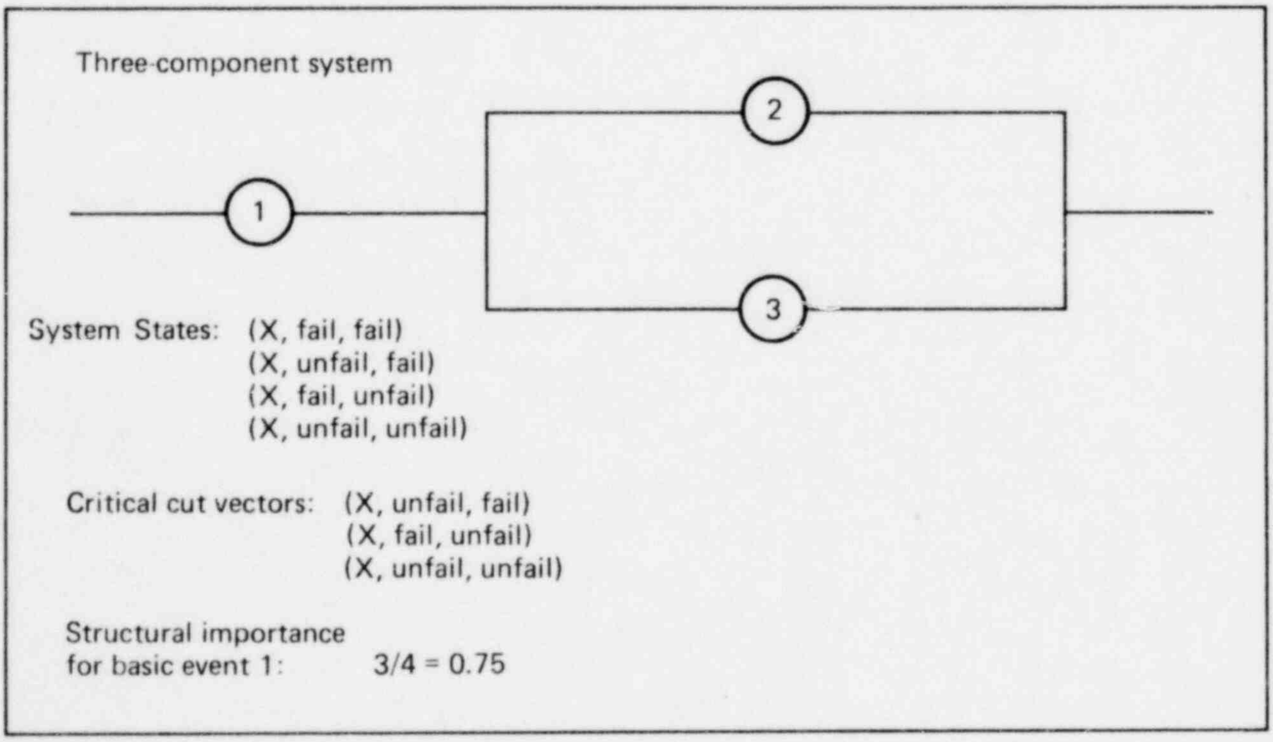
One measure of relative importance is Birnbaum's measure of structural importance.[14]

This measure of structural importance considers both the frequency with which a basic event appears in the AES and the length of the corresponding AES. Formally, the structural importance of basic event i is the ratio of the number of critical cut vectors for basic event i to the total number of system states. A cut vector is a vector containing all basic events specified either in the failed or unfailed state such that the system is failed. A critical cut vector for basic event i is a cut vector such that if event i occurs, the system passes from the unfailed to the failed state. Since the state of basic event i is fixed in the determination of its structural importance, the total number of the system states is 2^{n-1} where n is the number of basic events.

Figure 30 gives an example of the determination of the structural importance of a basic event for a three-component system.

The rankings of the structural importance for the basic events in the Test Bed assessment are shown in Table 5. The alphanumeric designators used to describe the basic events are defined in Table D-1, Table of Basic Event Definitions and Probabilities for System Fault Tree, in Appendix D. When the basic events pertaining to adversary path are set aside, the most important events are CDE1HIT, CV436IT, CV436IR, and CCASOK. This then indicates that the crash door E1, check valve 436, and the CCAS should be among the first items to harden when one attempts to improve the safeguards system.

The rankings of the basic event structural importance for the Test Bed assessment are generated by the IMPORTANCE computer code.[12]



System States: (X, fail, fail)
(X, unfail, fail)
(X, fail, unfail)
(X, unfail, unfail)

Critical cut vectors: (X, unfail, fail)
(X, fail, unfail)
(X, unfail, unfail)

Structural importance
for basic event 1: 3/4 = 0.75

FIG. 30. Determination of basic event structural importance.

TABLE 5. Basic event structural importance rankings for Test Bed assessment.

Birnbaum's Measure of Structural Importance

Number of System States = $9.0C7 \times 10^{15}$

RANK	BASIC EVENT	IMPORTANCE
1	APM-B0	5.451E-01
1	APM-B1	5.451E-01
2	ANODE1	4.357E-01
2	APM-AL	4.357E-01
3	TPHESM	3.641E-01
4	TPNETM	3.268E-01
5	CBE1HIT	3.113E-01
6	CV43GIT	2.674E-01
6	CV43GIR	2.674E-01
7	CCASOK	1.545E-01
8	LS701CIT	1.226E-01
9	LS722IT	1.226E-01
9	LS722IR	1.226E-01
10	LS701IT	1.228E-01
10	LS701CIR	1.228E-01
10	LS722CIT	1.226E-01
11	LS722CIR	1.226E-01
11	LS701IR	1.226E-01
12	ALARMIT	1.056E-01
13	ALARMIR	1.056E-01
14	ALARMLX	1.055E-01
15	ANODE14	1.029E-01
15	APM-AR	1.029E-01
16	ACCAS	1.029E-01
17	CBEEAHIT	6.855E-02
17	CBEEBHIT	6.855E-02
18	RDCCASIR	5.140E-02
19	RDCCASLX	5.140E-02
20	RDCCASIT	5.140E-02
21	ALCCAS	5.140E-02
21	AA-DHIT	5.140E-02
22	CDLI	4.094E-02
23	MDCCASIT	3.654E-02
24	MDCCASIR	3.654E-02
24	MDCCASLX	3.654E-02
25	NOMCCAS	3.654E-02
26	TPEQMM	3.427E-02
26	CSMMRMAA	3.427E-02
26	GFAIL13	3.427E-02
27	CBE2LHIT	3.426E-02
27	CBE2RHIT	3.426E-02
28	WEIGHTIR	3.162E-02
28	WEIGHTIT	3.162E-02
28	WEIGHTOK	3.162E-02
29	CDALRMLX	1.581E-02
29	CDALRMIR	1.581E-02
29	CDALRMIT	1.581E-02
30	GAMB01IR	1.054E-02
30	GAMB01IT	1.054E-02
30	GAMB01LX	1.054E-02
31	GAMB02HI	8.564E-03
31	GAMB02IR	8.564E-03
31	GAMB02IT	8.564E-03
31	GAMB02LX	8.564E-03

It should be noted that structural importance calculations provide a relative measure of the basic event importances only when all basic events have the same probability of occurrence. These calculations do not incorporate the true basic event probabilities as do probabilistic importance calculations. Basic event rankings based on probabilistic importance can vary significantly from rankings based on structural importance. (See section 4.4.3.)

4.3.3 Common-Cause Analysis of the Adversary Event Sets

Common-cause analysis is a method of redefining the original basic events in terms of new basic events that are usually more "global." These new basic events are more "global" in the sense that the original events can usually be expressed by far fewer of the new events. Hence, the number of minimum cut sets, or adversary event sets, is significantly reduced.

Two types of common-cause analyses were done in the Test Bed assessment:

1. Power and utility failure analysis
2. Collusion analysis.

These two analyses were performed by using the computer code FTAP.[10]

4.3.3.1 Power/Utility Failure Analysis. The "new" events used to replace the corresponding basic events in the AES to determine the effects of power/utility failures on the safeguards system were the following power/utility sources:

1. P-MAIN : Main AC power, i.e., off-site power and two on-site diesel generators
2. P-CCAS : Back-up CCAS power
3. P-COMP : Back-up computer power
4. P-GAM : Power to gamma detector
5. P-DPCELL : Power to differential pressure cell
6. P-LS : Power to limit switches
7. P-PM : Power to pressure mat
8. A-DPCELL : Air to differential pressure cell.

The results of the power/utility failure analysis indicate that these failures would not significantly aid the adversary in his theft attempt. Any loss of a power/utility source causes an automatic system alarm. Moreover, the Test Bed contingency plans require a physical security response to an alarm generated by a power/utility failure.

An example of the event sets produced in the power/utility failure analysis is shown in Table 6. The definitions of the basic events are given in Appendix E. Note that every event set contains at least one TDR alarm signal resulting from some power/utility loss.

TABLE 6. Example of event sets from the power/utility failure analysis.

1.	AFILLCON	ANODE706	CONAT706	CV436IT	MPU709	PRMODE		
	P-MAIN	TDR3-PM	V7130					
2.	AFILLCON	ANODE706	CONAT706	MPU709	PROMODE	P-CCAS		
	P-MAIN	TDR3-PM	V7130					
3.	AFILLCON	ANODE706	CONAT706	CSNMRMAA	CV436IT	GFAIL13	MPU709	
	PRMODE	P-MAIN	TDR3-PM	TPEQMM	V7130			
4.	AFILLCON	ANODE706	CONAT706	CSNMRMAA	CV436IT	GFAIL13	MPU709	
	PRMODE	P-LS	SRGAMB01	TDR1-PLS	TDR3-G	TPEQMM	V7130	
5.	AFILLCON	ANODE706	CONAT706	CSNMRMAA	CV436IT	GFAIL13	MPU709	
	PRMODE	P-GAM	P-LS	TDR1-PG	TDR1-PLS	TPEQMM	V7130	
6.	AFILLCON	ANODE706	CONAT706	CSNMRMAA	CV436IT	GFAIL13	MPU709	
	PRMODE	P-GAM	SRLS701	SRLS722	TDR1-G	TDR1-PG	PEQMM	V7130

4.3.3.2 Collusion Analysis. The collusion analysis is done by substituting facility personnel, or combinations thereof, for the basic events that they can perform. The list of facility personnel used in the collusion analysis for the Test Bed is given below:

SF01, SF02	: storage facility operators 1 and 2
MAIN	: maintenance personnel with access to monitors and electrical systems
COMP-OP	: computer operator with intimate knowledge of and access to computer software and hardware

MC1-OP, MC2-OP : material control officers 1 (security) and 2 (process)

NMCO : nuclear materials control officer

GUARD-AR, GUARD-BO, GUARD-CCAS : guards located at nodes AR, BO, and CCAS

LAB-TECH : laboratory analysis technician

The collusion analysis shows the minimum number of people and their identity who can accomplish successful SNM theft. Some examples of the collusion requirements for SNM theft from the Test Bed are shown in Table 7. Three people in collusion are needed in order to perpetrate an SNM theft such that the Test Bed safeguards system is unalerted. Two people in collusion can successfully steal SNM, but the safeguards system would be in an alarmed state when they exit the Test Bed. Note that the key individuals for both cases are the storage facility operators 1 and 2 (SFO1, SFO2) who must always be in collusion in order to effect a successful theft. These collusion results assume that the two-man rule works perfectly, that partners do not disable one another.

TABLE 7. Example of event sets from collusion analysis #1.

1.	NMCO	SFO1	SFO2	
2.	COMP-OP	SFO1	SFO2	
3.	MAIN	SFO1	SFO2	
4.	SFO1	SFO2	SRCB	
	SRLS701	SRLS722	TDR1-G	TDR3-G
5.	CSNMRMAA	GUARDAR	SFO1	SFO2
	SRGAMBO1	SRLS701	SRLS722	
	TDR1-G	TDR3-G	TPEQMM	

There were 24 event sets containing between 3 and 13 basic events that were found in the collusion analysis. A breakdown of these event sets and their length follows.

Number of events sets from collusion analysis #1	Length of event sets
3	3
1	7
1	10
1	11
2	12
16	13
24 total	

In a case in which the adversary(ies) has (have) knowledge and takes advantage of certain random failures in the safeguards system, two people in collusion are needed to perpetrate an SNM theft without the safeguards system being alerted. Table 8 provides the Test Bed collusion results for this case. Note that the two key individuals are again the storage facility operators 1 and 2 (SF01, SF02).

There were a total of 149 event sets, each containing between 9 and 13 basic events, produced in the collusion analysis for this case. A breakdown is given on the next page.

TABLE 8. Example of event sets from collusion analysis #2.

1.	LS701CIR	LS722IR	RDCCASIR	SF01	SF02
2.	LS701IR	LS722CIR	RDCCASIR	SF01	SF02
3.	ALARMIR	LS701CIR	LS722CIR	SF01	SF02
4.	ALARMIR	LS701IR	LS722CIR	SF01	SF02
5.	LS701IR	LS722IR	RDCCASIR	SF01	SF02
6	ALARMIR	LS701CIR	LS722IR	SF01	SF02
7.	LS701CIR	LS722CIR	RDCCASIR	SF01	SF02
8.	ALARMIR	LS701IR	LS722IR	SF01	SF02

Number of events sets from collusion analysis #2	Length of event sets
3	3
8	5
9	6
9	7
9	8
31	9
33	10
1	11
22	12
24	13
149 total	

4.4 QUANTITATIVE FAULT TREE ANALYSIS FOR THE TEST BED ASSESSMENT

Probabilistic analysis can provide more information about the performance of the MC system. The impact of four factors can be assessed using probabilistic analysis:

1. Different failure rates of MC components
2. Effect of component maintenance policies
3. Varying detection probabilities of monitors
4. Ease with which tampering with a component can occur.

The importance of probabilistic analysis is not so much the absolute numbers that result but the sensitivity analysis, which indicates the relative strengths and weaknesses of the the MC system in quantitative terms.

Three inputs are required for probabilistic analysis:

1. Boolean representation for the top event, e.g., listing of the minimum cut sets
2. Probabilistic data for the basic events
3. Assumptions regarding the statistical dependency of basic events.

The probability of successful theft of SNM from the Test Bed was calculated for four specific cases (corresponding to the groups of event sets, i.e., S_1, S_2, S_3, S_4):

1. SNM theft with no detection by the safeguards system, only random failures occurring
2. SNM theft with inadequate safeguards system response, only random failures occurring
3. SNM theft with no detection by the safeguards system, adversary tampering occurring
4. SNM theft with inadequate safeguards system response, adversary tampering occurring.

Since the probability of successful theft of SNM depends upon the amount of SNM diverted and whether or not material was used to shield the SNM, six situations were considered for each case:

1. 0.5 g Pu stolen, shielding used
2. 0.5 g Pu stolen, no shielding used
3. 200 g Pu stolen, shielding used
4. 200 g Pu stolen, no shielding used
5. 5 Kg Pu stolen, shielding used
6. 5 Kg Pu stolen, no shielding used.

Hence, 24 different theft cases were considered in the probability calculations for the Test Bed. It should be noted that the concentration of the solution to be stolen is 250 g Pu per liter of solution.

Certain assumptions were made about the adversary attributes in the calculation of the above probabilities. It is assumed that the adversary possesses complete knowledge of the safeguards system. In particular, he knows about random failures when they occur. The special assumptions and considerations used in the calculation of these probabilities when tampering occurs are discussed in Section 4.4.2.

4.4.1 Data Needed for Quantitative Fault Tree Analysis

Probabilistic data are needed for the three types of monitor failures. (See bottom of Fig. 26.) The first type of monitor failure is failure caused by random causes. Here, reliability parameters that depend upon the maintenance policies must be determined. The second type is failure caused by tampering. Here, the characteristics of the adversary, his resources, etc., must be used. The third type of failure is the nonperformance of the monitor caused by the intensity and duration of the stimulus input. Here, operating thresholds must be used. Data about guard performance include such factors as probabilities of inadequate guard responses to the various TDR alarm states.

The methods by which these probabilistic data were obtained will now be discussed.

4.4.1.1 Reliability Parameters. To determine reliability characteristics of components in the Test Bed, the unavailability of the component (the probability that a component is in a failure state when the adversary attempts to steal SNM) must be calculated. To calculate the unavailability of each component, the following reliability parameters are needed:

Parameter	Source
λ, failure rate,[*] conditional probability of failure	Test Bed Design Document[2] Reactor Safety Study[15] IEEE Standard 500[16]
τ_d, mean detection time of failure τ_i, inspection interval τ_r, mean repair time	Test Bed Design Document[2] Conservative engineering judgment

The sources of data for these parameters are shown above. In many cases, inspection intervals (τ_i) were not specified for the Test Bed and were derived on the basis of conservative engineering judgment. Both τ_i and τ_d are important parameters, because they indicate the amount of time an MC component can fail before detection of the failure occurs. These parameters are also important in the tampering analysis of components in Section 4.4.1.5.

[*] λ is also known as the hazard rate.

Three different maintenance policies were assumed for MC components in the Test Bed:

1. No repair
2. Repair, announced failure
3. Repair, unannounced failure.

An announced failure is a failure that is monitored. For example, an alarm, annunciator, light, or some other signal alerts the operator when a failure occurs. An unannounced failure is a failure that is not monitored but is revealed during periodic inspections or tests of the system.

4.4.1.2 MC Component Unavailability. The calculation of component unavailability using the reliability parameters and maintenance policies described in the previous section will now be discussed. Only failures due to random causes will be considered in these calculations; consideration of failure caused by tampering is given in Section 4.4.1.5.

Let $q_i(t)$ denote the unavailability of component i at time t. If component i has a constant failure rate, λ_i, then it can be shown that

$$q_i(t) = 1 - e^{-\lambda_i t} \quad .$$

If λ_i is not constant and is a function of time, i.e., $\lambda_i(t)$, then a conservative approximation may be made by assigning λ_i the maximum value of $\lambda_i(t)$ over (0, t).

For a maintenance policy with no repair, the unavailability of component i can be approximated by

$$q_i(t) = 1 - e^{\lambda_i t} \lessapprox \lambda_i t \quad .$$

Consider check valve 436 in the Test Bed as an example. This valve must fail open if SNM theft from the pump wash line is to happen. Since the Test Bed Design Document[2] did not specify an inspection interval for the check valve, a valve failure is expected to last the entire life of the system once it occurs (i.e., no repair). The failure rate for reverse leakage through a check valve is 3×10^{-7}/hour, as given in the Reactor Safety Study.[15] Hence, the probability of check valve failures ranges from 0 to 7.8 × 10^{-2} for a plant with an assumed life of 30 years. The average unavailibility of the check valve is 3.9 × 10^{-2} at 15 years. Thus, the probability of the basic event CV436IR (check valve 436 fails open due to random causes) is assigned the value 3.9 × 10^{-2}. This assignment of basic event probability is shown in Appendix E, Table of Basic Event Definitions and Probabilities for the Fault Tree.

For a maintenance policy with repair upon an announced component failure, the unavailability q(t) quickly reaches a constant value given by q_M

$$q_M = \frac{\tau_d + \tau_r}{\tau_d + \tau_r + \mu} \quad ,$$

where μ is the mean time to failure. For a constant failure rate λ, $\mu = \frac{1}{\lambda}$.

As an example of announced failure in the Test Bed, consider the gamma detector in area B_0. Since information on the background radiation is updated every quarter hour, failure of the gamma detector is detected only at the end of the quarter-hour interval. Thus, $\tau_d = 0.25$ hour. The repair time, τ_r, is assumed to be four hours and $\lambda = 1.4 \times 10^{-5}$/h.[16] Using these values in the expression for q_M, we get

$$q_M = \frac{0.25 + 4}{0.25 + 4 + 1/1.4 \times 10^{-5}} = 6.3 \times 10^{-5}$$

for the gamma detector in area B_0. (See assignment of basic event probabilities in Appendix E.)

A maintenance policy with repair but unannounced failures usually includes periodic inspections or tests of each component at time intervals of τ_i. Then the unavailability of component j increases from a low of $q_j(t = 0)$ 0 immediately after any repairs resulting from the inspection or the test to a high of q_j $(t = \tau_i)$ λ_j τ_i immediately before the next test. The average component unavailability during the interval between inspections on tests is thus approximately $\lambda_j \tau_i / 2$ and is applicable only if a demand for the component to function occurs uniformly at any time in the interval.

If the component is found to have failed during an inspection or test, then it will remain down during the necessary repair time, τ_r. Thus, the average component unavailability q_T for a maintenance policy with repair but unannounced failures and periodic inspections or tests is given by

$$q_T = \lambda\tau_i/2 + \lambda\tau_r \quad .$$

As an example of an unannounced failure in the Test Bed, consider valve 701 with limit switch contacts. Failure of the limit switch contacts to operate is detected when there is demand for valve 701 to be opened or closed. Since valve 701 is opened during the stir and sample mode, the rework mode, the transfer mode, and the load out mode, valve 701 is opened once every 13 days on the average.

Using the failure rate, λ, for limit switches from the Reactor Safety Study[15] of 10^{-4}/demand or 3×10^{-7}/h when based on one demand every 13 days and an assumed repair time of 4 hours, we get

$$q_T = \frac{(3 \times 10^{-7})(13)(24)}{2} + (3 \times 10^{-7})(4)$$

$$q_T = 4.8 \times 10^{-5} \quad .$$

(The assignment of probabilities to basic events corresponding to limit switches inactivated by random causes is given in Appendix E.)

4.4.1.3 MC Component Detection Insensitivity Performance. Monitors whose performance is a function of stimulus input are now discussed. In this case, the monitor is operational but does not detect the stimulus input (i.e., detection threshold inadequate). For the Test Bed, the performance of six monitors with the indicated stimulus input were of concern:

Monitor	Stimulus
1. gamma detector	1. amount of SNM stolen amount of shielding material
2. material estimation detectors	2. amount of SNM stolen amount of liquid substitution

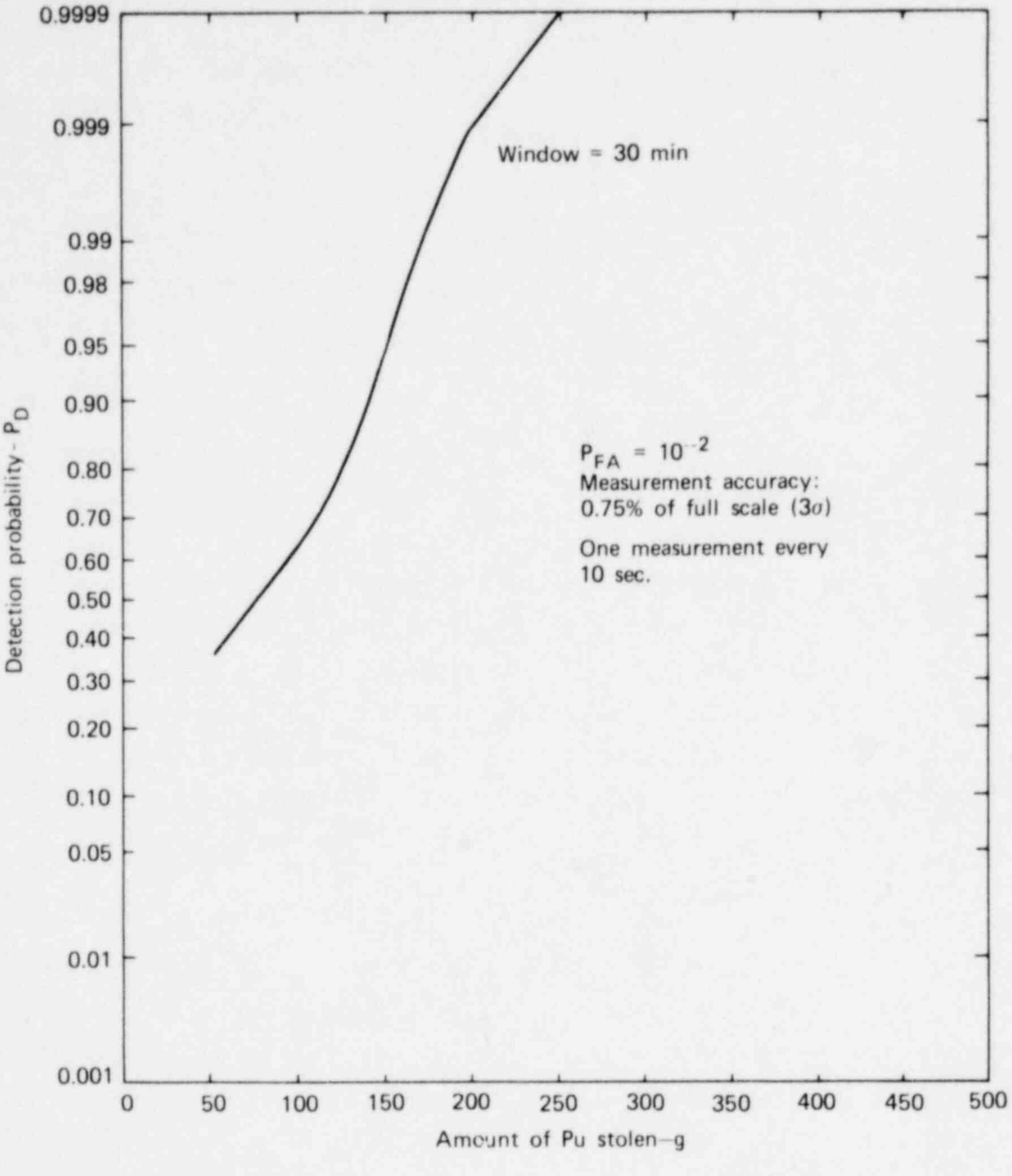
3. differential pressure cells	3. amount of SNM stolen amount of liquid substitution
4. metal detector	4. amount of ferrous metal amount of nonferrous metal
5. weight platform	5. weight of contents in CCAS . amount of SNM stolen . amount of shielding material
6. laboratory analysis for Pu concentration	6. amount of liquid substitution

Figure 31 illustrates the sensitivity of the probability of detection, P_D, for a material estimation detector as a function of the amount of SNM stolen.

4.4.1.4 Guard Response Probabilities. The probabilities of an adequate (or inadequate) guard response to various TDR alarms in the Test Bed were determined by computer runs on the Material Control System Simulator (MCSS).[17] Inputs to the simulator were the adversary event sets. All basic events in the event sets were either assigned point probabilities as calculated in the manner described in Sections 4.4.1.2 and 4.4.1.3, or assumed to be uniformly distributed random variables over a range of values set by knowledgeable experts.

The results of the MCSS output for guard response probabilities are summarized in Table 9. These results were used to assign probabilities to those basic events corresponding to guard responses. Due to the overlap in TDR alarms, that is TDR-1 alarms sometimes initiating TDR-3 alarms, the probabilities are not additive.

4.4.1.5 Tampering Analysis of MC Components. An approach similar to a common-cause analysis was used to treat tampering in the analysis qualitatively and quantitatively. The fundamental factors included in the successful tampering of an MC component are whether or not the required tools and resources can be brought to the location where the tampering occurs, without detection by the MC system; whether or not the adversary can gain access to the MC component without detection by the MC system; whether or not the adversary can prevent the MC component from performing its proper function; and whether or not the



P_{FA} = The false alarm probability is the probability that the detector will produce an alarm signal for no theft.

P_D = The detection probability is the probability that a theft of X grams of plutonium will produce an alarm signal f.om the detector.

FIG. 31. Single PNC tank diversion detection performance.

TABLE 9. MCSS results for guard response probabilities.

Probability of no interruption	0.095
Probability of no interruption within MAA resulting from physical security response to TDR-1 alarm	0.12
Probability of no interruption within MAA resulting from physical security response to TDR-3 alarm (includes TDR-1 alarms)	0.90
The following values were assumed for the uniform random variables of	
TDR-1 response	3-5 min
TDR-3 response	0.5-1.5 min

MC response is inadequate when tampering occurs. These factors are shown in Fig. 32, Fault Tree Expansion Operator for Tamnering Analysis. This operator is used to expand the basic event "Monitor Inactivated by Adversary Tampering" shown in Fig. 26.

The TRUE/FALSE option in the computer code FTAP[10] is used to simplify and reduce the number of events to be assigned probabilities in the quantitative analysis of tampering. Event A in Fig. 32 addresses the resources required by the adversary for tampering. If none are required, event A is set to TRUE. Event B considers the accessibility of the MC component to various individuals. If an insider, such as a maintenance man, can gain access to the component, event B is set to TRUE. Event C considers the difficulty in tampering with the MC component to prevent it from functioning properly and whether or not the component is monitored for tampering. If it is monitored, then the monitoring component must be defeated for successful tampering. Event D refers to the response of the MC system when tampering occurs. If there is no inspection of the MC component, then event 1 is set to TRUE. If theft can occur within the component inspection or detection interval, then event 2 is set to TRUE. If an adversary can disable and repair the component within the inspection interval, then event 3 is set to TRUE. Otherwise, one must consider the adequacy of the MC response, that is, event 4.

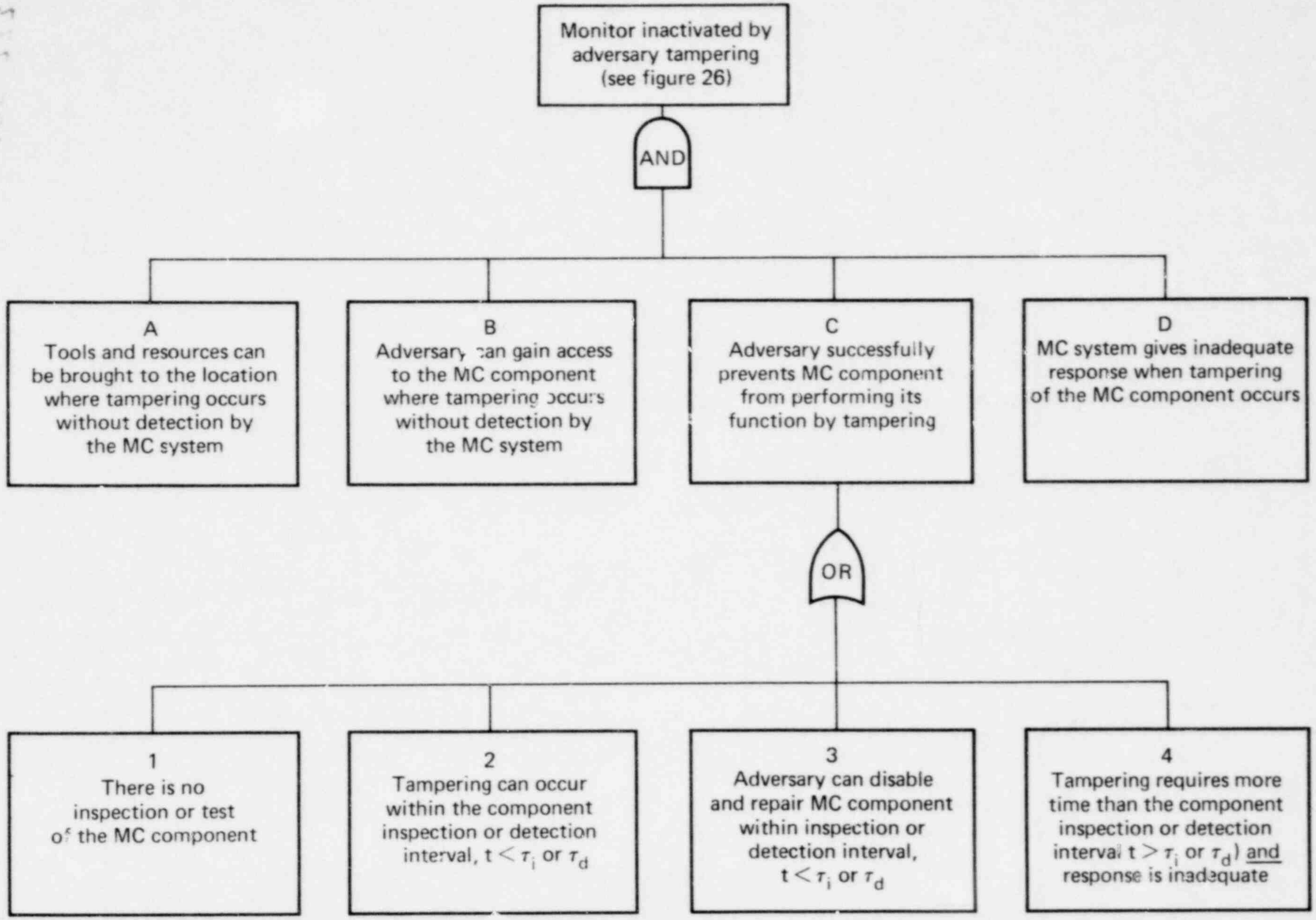

Monitor inactivated by adversary tampering (see figure 26)
AND
A
Tools and resources can be brought to the location where tampering occurs without detection by the MC system
B
Adversary can gain access to the MC component where tampering occurs without detection by the MC system
C
Adversary successfully prevents MC component from performing its function by tampering
D
MC system gives inadequate response when tampering of the MC component occurs
OR
1
There is no inspection or test of the MC component
2
Tampering can occur within the component inspection or detection interval, t < τi or τd
3
Adversary can disable and repair MC component within inspection or detection interval, t < τi or τd
4
Tampering requires more time than the component inspection or detection interval t > τi or τd) and response is inadequate

FIG. 32. Fault tree expansion operator for tampering analysis.

Thus far, the analysis has been deterministic. Setting various events to TRUE in the analysis reduces the number of events to be assigned probabilities in the quantitative analysis. Then, probabilities are assigned on the basis of conservative engineering judgment.

As an example of the assignment of probabilities to tampering events, consider the event of check valve 436 failing open because of tampering. The check valve can be failed open by plastic tubing, a wedge, or suspended solids. Because the adversary must bring resources into the MAA, which is monitored by pressure mats and CCTVs, a probability of 0.1 is assigned to event A (see Fig. 32). Since an insider, such as a storage facility operator or a maintenance man, can gain access to the check valve, event B is set to TRUE. Since the inspection procedure is not specified for the check valve, event 1 and hence event D are set to TRUE. Furthermore, since the check valve is not monitored, event C is also set to TRUE. Thus, according to this procedure, the event, for instance "check valve 436 fails open due to tampering" (CV436IR), is assigned a probability of 0.1.

As another example, consider the event of inactivation of valve 722 limit switch circuitry. The limit switch circuit can be energized by jumper cables. Because there are no monitors on the remote control panel where the circuit is located (see Fig. 33), event A is set to TRUE. Event B is set to TRUE because a person such as a maintenance man can gain access to the cabinet containing the remote control panel. Since the adversary can defeat the microswitch on the cabinet door, event C is set to TRUE. Event D is set to TRUE because an adversary can remove the jumper cables before the next mode of operation (i.e., event 4 is set to TRUE). Consequently, a probability of 1 is assigned to the events of inactivating the limit switch circuits (i.e., LS701IT and LS722IT). The scenario just described is one of the critical vulnerabilities discovered in the assessment of the Test Bed.

Other events involving MC component tampering were assigned probabilities according to the procedure described in this section.

1425 335

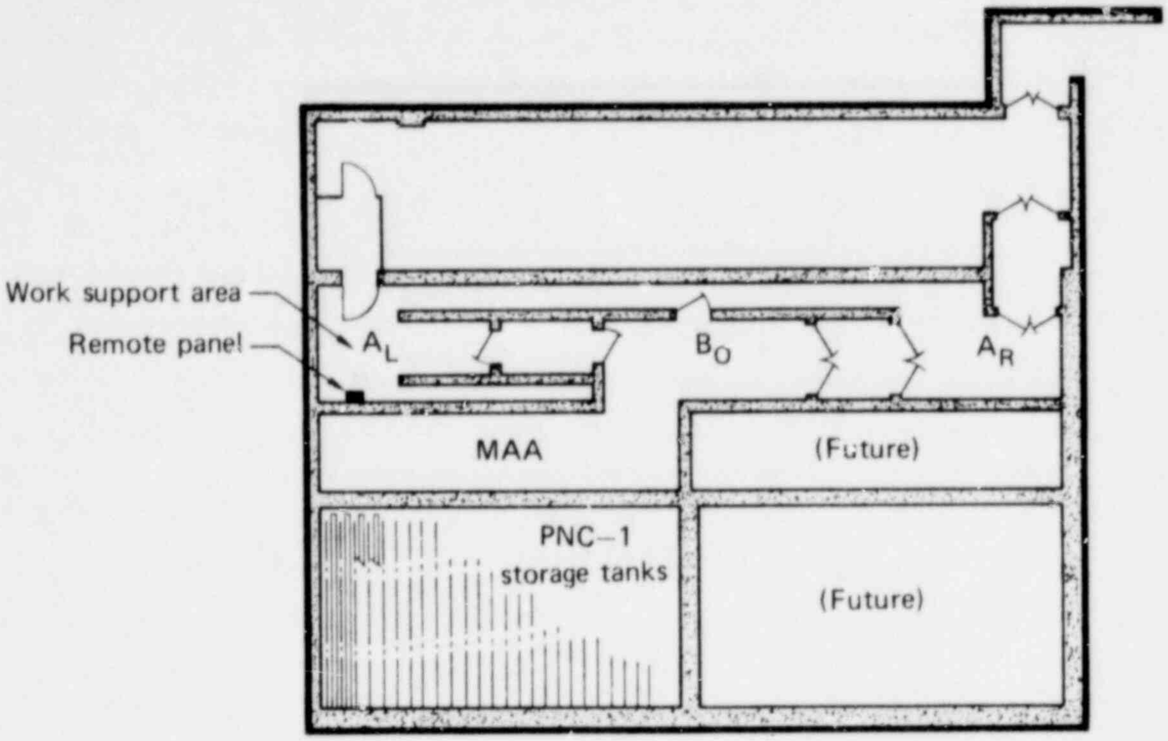


FIG. 33. Location of remote control panel for limit switch circuits.

4.4.2 Calculation of the Probability of Successful SNM Theft from the Test Bed

The probability of successful SNM theft from the Test Bed can be calculated using the adversary event sets and the data described in the previous section. Distinct calculations are made for two cases:

1. Probability of successful SNM theft with no safeguards system tampering occurring
2. Probability of successful SNM theft with safeguards system tampering occurring.

The calculation for the first case employs component reliability data; the calculation for the second case is based upon data determined in the tampering analysis of components.

1425 336

4.4.2.1 Probability of Successful SNM Theft: No Tampering Case. For the case of no MC system tampering, the probability of successful SNM theft is based upon the probabilities of occurrence of adversary event sets in S_1 and S_2 where

S_1 = those event sets of SNM theft with no alarm detection by the safeguards system, only random failures occurring

S_2 = those event sets of SNM theft with inadequate safeguards system response, only random failures occurring.

Let $P(S_i)$ denote the probability of an adversary event set in S_i occurring, i = 1 and 2. $P(S_1)$ then provides a measure of the detection capability of the safeguards system, and $P(S_2)$ gives a measure of the response capability.

$P(S_i)$ is determined on the basis of the average safeguards system unavailability. Here a distinction must be made for system unavailability and system unreliability. Unavailability is the probability that the system is vulnerable at time t, whereas unreliability is the probability that the system is vulnerable over an interval of time (0, t). The system is defined to be vulnerable when all MC components specified in an adversary event set occur. In general, system unavailability will be less than system unreliability.

The adversary is assumed to possess complete knowledge and take advantage of all random failures of the MC system. Hence, whenever the system becomes vulnerable, successful SNM theft can be effected.

Thus, in calculating $P(S_i)$, all basic events that are not random MC component failures are random assigned a probability of 1. Also, all failures are assumed to be statistically independent. Then $P(S_i)$ for i = 1 and 2 is given by

$P(S_i)$ = the probability of the union of adversary event sets in S_i, or

$$P(S_i) = 1 - \prod_{K_j \epsilon S_i} \left[1 - P(K_j)\right] \quad ,$$

where

$P(K_j)$ = the probability of the occurrence of event set K_j,

$$P(K_j) = \prod_{n \varepsilon K_j} q_n$$

where

q_n = the probability of failure of MC component n, and

$n \varepsilon K_j$ means for all components contained in event set K_j, and

$K_j \varepsilon S_i$ means for all event sets contained in the set S_i.

It should be noted that $P(S_i)$ is a conservative measure, because it allows the adversary to choose any event set (i.e., scenario) or combination thereof to perpetrate his theft. In essence, his choice becomes immaterial.

For the Test Bed assessment,

$$P(S_1) = 3.9 \times 10^{-5}$$

$$P(S_2) = 4.3 \times 10^{-5} \quad .$$

(The IMPORTANCE Computer Code[12] was used to calculate $P(S_1)$ and $P(S_2)$.) Because S_1 and S_2 are disjoint sets (that is, $S_1 \quad S_2 = \emptyset$) the combination of these two probabilities then yields:

Probability of successful SNM theft with *no* safeguards system tampering occurring	$= P(S_1) + P(S_2)(1 - P(S_1))$ $= 8.16 \times 10^{-5}$

This probability is a measure of the likelihood of a natural vulnerability existing in the safeguards system in the Test Bed.

4.4.2.2 *Probability of Successful SNM Theft: Tampering Case*. For the case of adversary tampering with the MC system, the probability of successful SNM theft is based upon the adversary event sets contained in S_3 and S_4 where

S_3 = those event sets of SNM theft with no alarm generated by the safeguards system, adversary tampering occurring

S_4 = those event sets of SNM theft with inadequate safeguards system response, adversary tampering occurring.

Let $P(S_i)$ denote the probability of successful SNM theft occurring by means of an event set (i.e., scenario) in S_i, $i = 3$ and 4. $P(S_3)$ gives a measure of the *detection* capability of the safeguards system when the adversary has tampered with the detection components, and $P(S_4)$ yields a measure of the *response* capability when the response components have been tampered with.

The adversary's choice of the event set (i.e., scenario) by which he perpetrates a SNM theft is an important factor in the calculation of the probability of successful theft when tampering is involved. It is clear that an adversary will want to do what is most advantageous for himself. Thus, a reasonable adversary strategy for stealing SNM is to use the event set with the high probability of success. By assigning a probability of 1 to all basic events that are not MC component failures, a probability of failure based on unavailability calculations for all *random* MC component failures and based on the tampering analysis for all MC component failures *caused by tampering*, $P(S_i)$, is determined by the following expression, for $i = 3$ and 4:

$$P(S_i) = \max_{K_j \varepsilon S_i} (P(K_j))$$

where

$$P(K_j) = \prod_{n \varepsilon K_j} Q_n$$

and

Q_n = the probability of the failure of component n, given that the adversary tampers with it. Adversary tampering includes both explicit tampering with the component and the taking advantage of the random failure of the component.

For the Test Bed assessment,

$$P(S_3) = 0.08$$

$$P(S_4) = 0.08 \quad .$$

The IMPORTANCE Computer Code[12] was used to calculate $P(S_3)$ and $P(S_4)$. Because S_3 and S_4 are also disjoint sets (that is, $S_3 \cap S_4 = \emptyset$,) the combination of these two probabilities gives:

$$\text{Probability of successful SNM theft with safeguards system tampering occurring} = P(S_3) + P(S_4)(1 - P(S_3)) = 0.15 \quad .$$

The complement of the above probability (i.e., 1 - 0.15 = 0.85) provides a measure of the effectiveness of the Test Bed safeguards system in preventing SNM theft when the adversary does tamper with the system.

However, if the adversary should be able to make multiple attempts, then another measure for $P(S_3)$ and $P(S_4)$ is the probability of the union of all event sets in S_3 and S_4, respectively (see Section 4.4.2.1). Using the same probability assignments for basic events employed in calculating $P(S_3)$ and $P(S_4)$, we obtain for the Test Bed assessment

$$P^\star(S_3) = 0.30$$
$$P^\star(S_4) = 0.35 \quad ,$$

where the ★ indicates a multiple attempt strategy. Then the effectiveness of the Test Bed safeguards system in preventing SNM theft against a tampering adversary who may make multiple attempts is $1 - P^\star(S_3) + P^\star(S_4)(1 - P^\star(S_3))$, or 0.46. Thus, this measure indicates that an adversary who is able to make multiple attempts has a much better chance of successfully stealing SNM from the Test Bed.

4.4.3 Strengths and Weaknesses of the Test Bed in Quantitative Terms

The probability of successful SNM theft from the Test Bed was calculated for the four cases given below.

	No Tampering	Tampering
No alarm generated	$P(S_1) = 3.9 \times 10^{-5}$	$P(S_3) = 0.08$ $P^*(S_3) = 0.30$
Inadequate response, given alarm occurred	$P(S_2) = 4.3 \times 10^{-5}$	$P(S_4) = 0.08$ $P^*(S_4) = 0.35$

It is not the absolute probabilities that provide important information about the system strengths and weaknesses, but rather the order of magnitude of the probabilities and the relative differences between probabilities for the tampering and no tampering cases. The magnitudes of the probabilities of successful SNM theft for the no tampering case indicate that it is extremely unlikely for a natural vulnerability in the Test Bed safeguards system to exist; there is a likelihood of one in 10,000. However, if the adversary were to tamper with the safeguards system, he would improve his chances for success by a factor of 1,000. His likelihood of success then becomes one in 100. Thus, the results indicate that the adversary has a much greater chance of success if he tampers with the system rather than just await the occurrence of random failures.

The sensitivity of the probabilities of successful SNM theft to the various basic events is discussed in the remaining parts of this section. The IMPORTANCE Computer Code[12] was used to perform this sensitivity study for the Test Bed assessment.

4.4.3.1 Basic Event Importance in the No Tampering Case. A measure of the basic event that contributes the most to adversary success is obtained by using the Vesely-Fussell component importance measure.[18]

Let

$I_{n,i}$ = Vesely-Fussell measure of importance for basic event n for adversary event set group S_i, i = 1, 2,

where

$I_{n,1}$ = probability that any event set containing basic event n occurs, given that the safeguards system failed to detect the adversary.

$I_{n,2}$ = probability that any event set containing basic event n occurs, given that the safeguards system failed to stop the adversary.

Explicitly, $I_{n,i}$ is calculated by dividing the probability of the union of all event sets in S_i containing basic event n by the probability of the union of all event sets in S_i. Henceforth, in this report, $I_{n,i}$ shall be referred to as the probabilistic importance of basic event n among event sets in S_i.

The results of the basic event sensitivity study are given in Table 10 for the no tampering case in the Test Bed assessment.

Thus, the results in Table 10 indicate that the random failure of check valve 436 (CV436IR) and the unavailability of the MC computer system (CDLI) play a critical role in determining the probability of a natural vulnerability existing in the Test Bed that would lead to adversary success.

A check was made of the sensitivity of the probability of successful SNM theft to three factors:

1. Shielding material used
2. Liquid substitution employed
3. Amount of SNM stolen.

TABLE 10. Basic event importance for no tampering case.

Event set group	Basic event	Probabilistic importance
S_1 (no alarm generated)	CV436IR	1.0
	CDLI	1.0
	LS701IR	6.6×10^{-8}
	LS722IR	6.6×10^{-8}
S_2 (inadequate response given alarm)	CV436IR	1.0
	CDLI	9.0×10^{-1}
	TDR1-G	9.8×10^{-2}
	TDR2-G	9.1×10^{-2}
	RDCCASLX	4.2×10^{-3}

It was found that these factors did not influence the probability. The probability of successful SNM theft remained constant as a function of these three factors.

4.4.3.2 Basic Event Importance in the Tampering Case. For the tampering case, the Vesely-Fussell measure of component importance[18] is again used to measure the sensitivity of the probability of successful diversion to the various basic events.

Three factors were included in the tampering analysis of components:

1. Type of tools and resources required for tampering
2. Accessibility of components to potential adversaries
3. Monitoring of equipment for tampering.

Subjective judgment was applied in the assignment of basic event probabilities in the tampering case because adversary attributes must be considered. However, the Vesely-Fussell component importance measure is still appropriate because it is a ratio of probabilities. Hence, subjectivity in the probability in the numerator tends to cancel subjectivity in the probability in the denominator when the analyst is consistent in his judgment.

Table 11 gives the results of the probabilistic importance of the various basic events for the tampering case in the Test Bed assessment.

TABLE 11. Basic event importance for tampering case.

Event Set Group	Basic event	Probabilistic importance, $I_{n, i}$
S_3 (No alarm generated)	CV436IT	7.6×10^{-1}
	ALARMIT	7.3×10^{-1}
	LS722IT	6.6×10^{-1}
	LS701IT	6.5×10^{-1}
S_2 (inadequate response, given alarm)	CV436IT	7.6×10^{-1}
	ALARMIT	7.3×10^{-1}
	LS722IT	6.6×10^{-1}
	LS701IT	6.5×10^{-1}

The results indicate that check valve 436 (CV436IT), the crash bar alarms (ALARMIT), and the limit switch circuits (LS722CIT,LS701CIT) are the prime items for an adversary to tamper with in order to perpetrate a successful SNM theft.

Sensitivity studies of the probabilistic importance of basic events as a function of three factors

1. Shielding material used
2. Liquid substitution employed
3. Amount of SNM stolen

were also conducted for the no tampering case. Only the amount of SNM stolen had an impact for the cases considered.

The basic event importances given in Table 11 are for 0.5 g SNM stolen. For the theft of 200 g of SNM, an additional basic event becomes important:

ASUBHNO--substitution with equivalent density HNO_3.

If substitution did not occur, the material balance system would detect the SNM loss when the bubbler system reached steady state.

For the theft of 5 Kg SNM, the basic events above, plus another basic event, become important:

LABFALSE--Pu concentration laboratory measurements falsified.

Although HNO_3 substitution occurs, a large discrepancy would exist in the Pu concentration if the laboratory measurements were not falsified.

4.4.3.3 Summary of Strengths and Weaknesses in the Test Bed. The MC system in the Test Bed is a realistic system that provides for well-controlled SNM handling and facility operating procedures. In this assessment of a single target in the Test Bed, the MC system has three strengths:

1. It has an adequate capability of timely detection of SNM theft.
2. Collusion of a minimum of three people is needed to accomplish SNM theft with no detection.
3. The probability of successful SNM theft is less than 1 in 3 (0.08 to 0.35) given that the necessary people are already in collusion.

And in this partial assessement, the MC system has three weaknesses:

1. The remote control cabinet, which provides access to the limit switch circuitry, is not monitored during maintenance.
2. There is excessive unavailability of the MC computer system because of both hardware and software problems.
3. No inspection intervals are provided for the crash bar alarm systems and the check valves.

These weaknesses facilitate adversary tampering of necessary MC components for successful SNM theft.

1425 345

5.0 EVALUATION OF THE DIGRAPH-FAULT TREE METHODOLOGY FOR THE ASSESSMENT OF MATERIAL CONTROL SYSTEMS

The digraph-fault tree methodology shares many common elements with traditional fault tree analysis. Both involve the following elements:

1. Detailed description of the system
2. Statement of analysis assumptions
3. Study of individual system components i.e., a FMEA
4. Logic model formulation
5. Qualitative evaluation
6. Quantitive evaluation.

Because the methodology shares so many common elements with traditional FTA, it also shares the same problems. However, the addition of digraphs to the model formation stage alleviates some of these problems. In addition, the Lewis Report[19] finds that fault tree analyses should be among the principal means used to assess and revalidate existing regulatory requirements and evaluate new designs.

5.1 STRENGTHS OF THE DIGRAPH-FAULT TREE METHODOLOGY

The inclusion of digraphs in the procedure allows the analysis to be performed in a more modular fashion. Digraphs also facilitate the treatment of timing and multivalued logic.

In general, digraphs serve three purposes:

1. They aid in modeling noncoherent as well as coherent systems to determine the possible causes of the event being analyzed. When properly used, the digraphs often lead to discovery of failure combinations that might not have been recognized as causes of the event. In the safeguards problem, digraphs provide the fault tree that yields the adversary event sets.

2. They provide a convenient and efficient format in which to partition and analyze a problem when a natural decomposition of the problem is not clear.
3. They serve as a display of results. If the safeguards system design is not adequate, digraphs can be used to show what the weak points are and how they lead to undesirable events. If the design is adequate, digraphs can be used to show that all conceivable causes have been considered.

The qualitative evaluation stage in the digraph-fault tree methodology introduces the new concepts of adversary event subsets and collusion sets. The event subsets allow important information to be extracted easily from the lengthy and numerous adversary event sets. The collusion sets provide the minimum collusion requirements to accomplish the adversary event sets. The qualitative evaluation also yields a structural importance measure that ranks the basic events and adversary event sets by assuming that all basic events have an equal probability of occurrence.

However, for the case of the Test Bed, data indicate that basic events can vary by as much as a factor of 10^6 in probability of occurrence. This leads to a dramatic difference in the importance of basic events in contributing to the successful theft of SNM. The quantitive evaluation stage of the methodology provides a sensitivity analysis that points to the true strengths and weaknesses of the MC system. Quantitative analysis assesses four impacts:

1. Random monitor failures
2. Measurement insensitivity
3. Ease of tampering
4. Inadequate guard response.

Although quantitative analysis is often criticized because the needed data are inadequate, we found for the Test Bed that meaningful quantitative results can be obtained with the available data. One of these results is the ranking of important MC system components.

A subjective analysis was performed to provide data for basic events that were tampering acts. The vulnerability to tampering of each MC component was established by considering three adversary attributes and MC system characteristics:

1. Type of tools and resources required for tampering (including personnel)
2. Accessibility of components to potential adversaries
3. Monitoring of equipment for tampering.

The effect of the subjectivity of the tampering analysis is in part compensated by conservative engineering judgment and the choice of measures for basic event importance (i.e., a ratio of probabilities).

5.2 WEAKNESSES OF THE DIGRAPH-FAULT TREE METHODOLOGY

One criticism of the digraph-fault tree methodology is that although it is systematic, it is still a tedious manual process. However, the use of unit model digraphs to form the system digraph and the use of a transformation algorithm to obtain the fault tree lend themselves more readily to automation than conventional fault tree construction.[6]

Another criticism of the methodology is that the transformation algorithm used to obtain the fault tree is heuristic. However, only the validity of the output can determine the correctness of the algorithm and not the fact of whether or not it is heuristic. Furthermore, the transformation algorithm is based upon the analyst's understanding of the failure behavior of control loops and upon applying the rules of conventional fault tree construction. These rules have been extensively used, tested, and documented since the conception of FTA in the early 1960s.

Finally, the most basic criticism of the digraph-fault tree methodology is the issue of completeness, which is the most important issue in any system analysis procedure.

The digraph-fault tree methodology is analytically complete in that there is a unique mapping from the digraph to the fault tree, and another unique mapping from the fault tree to the event sets such that all the basic events in the digraph are mapped into the set of event sets. However, what cannot be claimed is that the methodology is complete with respect to the real world. This type of completeness of the digraph-fault tree methodology for material control assessment depends upon obtaining three types of information:

1. All sources, removal nodes, material routes, and exit points from the MAA
2. All monitored variables and the information flow associated with these variables
3. Ways by which these information flows can be nullified.

Each of the above items will be discussed in detail.

5.2.1 Identification of Sources, Removal Nodes, Material Routes, and Exit Points

Information regarding SNM material movement from the facility is essential. Sources, removal nodes, material routes, and exit points must be identified.

Sources refer to locations where SNM is contained normally within the system (such as pipes, tank, and vaults). Removal nodes refer to places within the MAA where the adversary can gain physical access to SNM (such as samplers, and loadout areas).

Material routes refer to the locations where SNM can be transported from the removal nodes to the exit points. In addition, the routes regarding movement of items (such as tools and containers) within the facility must be included.

Exit points refer to the places where SNM can cross the boundary of the facility. Exit points can be located within the process, such as product lines, or be located outside the process, such as vent lines and security booths. If all sources, removal nodes, material routes, and exit points are not identified, significant adversary event sets can be missed.

5.2.2 Monitored Variables and Information Flow

When an adversary attempts to steal SNM, disturbances in state or process variables will be created as a result of adversary activity. An MC system is designed to detect these disturbances and to respond to them with corrective actions. These monitored disturbances and corresponding corrective actions, which often are continuous valued variables, must be identified as discrete leveled MC system variables. Also, the gains between the MC system variables that indicate the "strength" of the relationship must be determined. Timing issues and the dynamics of the gains must also be incorporated as part of the information flow.

In order that the analysis be complete, all the modes and mechanisms of MC equipment failure must be specified. Particular emphasis must be given to failure modes of material and personnel monitoring equipment that result in loss of their detection capability. Mechanisms are physical or chemical processes by which items of equipment are inactivated. It is important to enumerate the ways by which the adversary can induce these failure mechanisms, e.g., by equipment destruction. Also, environmental conditions and human error must be identified as causes of equipment failure. For the analysis to be complete on the system level, all of the ways by which an adversary can manipulate MCS variables to cancel the effect of monitored variables must be specified. The analysis of the details of system operation and adversary manipulation of different MCS variables must include operational procedures.

5.3 CONCLUSION

It is conceptually impossible to be complete in a mathematical sense in the construction of any model; what matters is the approach to completeness and the ability to demonstrate with reasonable assurance that only very small contributions are omitted.[17] The digraph-fault tree methodology provides a systematic approach to completeness and assurance of the inclusion of important events in the analysis.

When the digraph-fault tree methodology is coupled with an adequate data base, it provides a viable tool with which to quantify the effectiveness of a material control system. It should be noted here that the input of well-trained analysts who are familiar with the system being assessed is critical.

In conclusion, the digraph-fault tree methodology provides a framework that can be used in making the assessment of material control systems more systematic and rational, in establishing the topography of SNM theft scenarios, and in delineating quantitative estimates of the effectiveness of the system that can be derived from existing data.

REFERENCES

1. A. Maimoni, "Safeguards Research: Assessing Material Control and Accounting Systems," Energy and Technology Review, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-52000-77-11/12 (1977).[*]
2. I. J. Sacks, et al., Material Control System Design: Test Bed Nitrate Storage Area (TBNSA), Lawrence Livermore Laboratory, Livermore, Calif., UCID-17525-77-3 (May 1978).[*]
3. F. M. Gilman, M. H. Dittmore, and J. J. Lim, Wood River Junction Vulnerability Analysis: Phase I Report, Lawrence Livermore Laboratory, Livermore, Calif., MC 79-197, to be published as a NUREG Report in 1979.
4. I. J. Sacks, A. A. Parziale, T. R. Rice, and S. L. Derby, The Structured Assessment Analysis of Facility X, Volume 1 - Executive Summary, Lawrence Livermore Laboratory, Livermore, Calif., MC 79-12-D, to be published as a NUREG Report in 1979.
5. L. D. Chapman, et al., Physical Protection of Nuclear Material in Transit, Quarterly Progress Report (October-December 1978), Report SAND 790535/Report NUREG-CRO 694.[*]
6. S. A. Lapp and G. J. Powers, "Computer-Aided Synthesis of Fault Trees," in IEEE Trans. on Reliability, R-26, 1 (April 1977).
7. H. E. Lambert and J. J. Lim, The Modeling of Adversary Action for Safeguards Effectiveness Assessment, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-79217, Rev. 1 (June 1977).[*]
8. J. B. Fussell, et al., A Collection of Methods for Reliability and Safety Engineering, Idaho National Engineering Laboratory, Idaho Falls, Idaho, ANCR-1273 (April 1976).[*]
9. S. L. Salem, G. E. Apostolakis, and D. Okrent, "A New Methodology for the Computer-Aided Construction of Fault Trees," Annals of Nuclear Energy, 4 (1977), pp. 417-433.

[*] Available through the National Technical Information Service, Springfield, Virginia 22151.

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

11. R. B. Worrell, Set Equation Transformation System (SETS), Sandia Laboratories, Albuquerque, NM, SLA-73-28A (July 1974).

12. H. E. Lambert and F. M. Gilman, The IMPORTANCE Computer Code, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-79269 (March 14, 1977).*

13. G. A. Morris, PIPE: A Computer Code for Analyzing Piping Networks, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-52441 (March 3, 1978).*

14. Z. W. Birnbaum, "On the Importance of Different Components and a Multicomponent System," in Multivariate Analysis-II, P. R. Krishnaiah, Editor (Academic Press, New York, 1969).

15. U.S. Atomic Energy Commission, Reactor Safety Study, WASH 1400 (1974).

16. IEEE Standard 500.

17. R. B. Hollstien, "A Material Control System Simulator," in Proceedings of 19th Annual INMM Meeting, VII (June 1978).

18. W. E. Vesely, "Reliability Quantification Techniques Used in the Rasmussen Study," in Reliability and Fault Tree Analysis, R. E. Barlow, J. B. Fussell, and N. D. Singpurwall, editors, SIAM (1975).

19. H. W. Lewis, et al., Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission, U.S. Nuclear Regulatory Commission, Washington, D.C., NUREG/CR-0400 (1978).*

NMS:ew

*Available through the National Technical Information Service, Springfield, Virginia 22151.

APPENDIX A

INSTRUCTIONS FOR A FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

Two types of information should be included in the FMEA whenever applicable:

1. A summary description of the device regarding its function, operating threshold, inputs, variables describing the inputs, outputs, and variables describing the outputs
2. A block diagram of the device showing inputs, outputs, and internal logic.

The FMEA is conducted in tabular form as shown Fig. A-1.

In column (1) of Table A-1, the device or component is listed with its identification number (if applicable) and its location within the plant. Column (2) refers to monitoring components that are listed in column (1). The adversary act or condition and corresponding variable the component is designed to detect or monitor are listed here. When possible, column (2) should include component performance data, i.e., measurement accuracy (variance) and detection probability as a function of stimulus input resulting from the adversary act or condition.* The component performance may simply be a threshold value; for example, the pressure switch has a threshold force of 15 lb. Any delay time between when the act is committed and when it is detected is also to be listed in column (2).

In column (3), all the potential failure modes of the device or component are listed.

In column (4), the causes of these failure modes are listed. There are four failure causes:

1. Adversary acts
2. Random equipment failure
3. Human error
4. Environmental conditions.

In column (5), the effect of the failure on the component is listed.

*If the stimulus input is a function of α amount and β type of SNM stolen, then α and β must also be specified in column (2).

(1) Component ID number and location	(2) Component function, (i.e., detection of adversary act) corresponding variable, component performance data	(3) Failure mode	(4) Cause of failure	(5) Effect of failure mode on MC component	(6) Effect of failure mode on process or MC system	(7) Reliability information maintenance policy, λ, τ, θ

Minimum, maximum time to complete act	Required tools for tampering	Minimum required collusion for tampering	Persons who have authorized access to component	Possible means by which material control system can detect act	Means by which adversary can disguise act

FIG. A-1. FMEA tabular form.

In column (6), the effect of the failure on the process or MC system is determined. Assume that all other components are working normally when the failure occurs. The mode of system operation should be specified if the effect of the failure mode varies depending on the system mode of operation.

Column (7) lists reliability or availability information. Components generally follow one of three different maintenance policies:

1. No maintenance possible
2. Maintenance or repair upon detection of failure
3. Maintenance or repair at some inspection interval.

For policy 1, the failure rate λ must be specified. For policy 2, λ must be specified as well as $\tau_d + \tau_r$, the mean detection plus mean repair or replacement time. For policy 3, λ or τ_i, the inspection interval, must be given. If reliability data are guesses, this must be indicated.

The lower part of Fig. A-1 provides information on adversary-induced failures that are specified in column (4) of the top part. The following information is to be given on the lower part of the form:

1. An estimate of the minimum and maximum amount of time required by the adversary to commit the act
2. The tools required to accomplish the act
3. The minimum number of people required in collusion to accomplish the act
4. People who have authorized access to the component
5. The means by which the MC system can detect the act
6. The means by which an adversary can disguise the act.

Appendix B

DETAILS OF THE DIGRAPH-FAULT TREE METHODOLOGY

The purpose of the digraph-fault tree methodology is to systematically produce a fault tree for qualitative and quantitative evaluation. A fault tree is a deductive Boolean logic model of a top event, which represents an undesired event, or a system state.

The top events are events such as fire, explosion, or system shutdown for safety and reliability analyses. For material control assessment, the top event can be an event such as successful theft of SNM from the facility.

Basic events provide the limit of resolution for the fault tree and define the top event. The basic events in safety and reliability analysis include human error, equipment failure, and environmental conditions. For material control assessment, the basic events also include adversary activity, such as equipment destruction and records falsification.

Historically, fault trees have been constructed manually using established rules.[1] These rules define which logic gates to use and the inputs to these gates. A number of disadvantages exist in traditional fault tree analysis (FTA).

1. Rules for manual fault tree construction do not provide for consistency checks and give no logical basis for the generation of AND gates.
2. Analysts can infer various cause-and-effect relationships when analyzing a system schematic and thus construct different fault trees for the same problem.
3. Dynamics and multivalued logic are difficult to incorporate in the FTA.

To partially alleviate these disadvantages, we adopted an approach using digraphs (directed graphs) to construct fault trees[2-4] similar to one developed by Lapp and Powers.[5-7] This approach has five advantages over traditional FTA.

1. Unit models digraphs are constructed for individual components. Cause-and-effect relationships are clearly displayed in these unit models, as well as the level of detail of modeling.
2. The system topography with regard to information flow and control loops is displayed in the system digraph.

3. Multivalued logic, the direction and deviations in system variables, is incorporated as well as component failures.
4. The dynamics of the relationships of system variables can be considered.
5. A transformation algorithm is devised that generates a fault tree from the system digraph. The algorithm states explicitly when to use AND gates, OR gates, and consistency checks in constructing the fault tree.

In the Test Bed assessment, digraphs were used to model the material control system as a system designed to counter the actions of the adversary. All potential ways in which the material control system may respond to prevent theft of SNM are modeled in terms of "adversary cancellation loops" on the system digraph. These loops are similiar to the negative branches of negative feedback and negative feedforward loops designed to cancel disturbances in process variables.

A description of the digraph-fault tree methodology as used in the assessment is now given. The basic terminology and notation used in the methodology will also be introduced.

B.1 TERMINOLOGY AND NOTATION

A digraph is a set of nodes and connecting edges. Nodes in the digraph represent variables. If one variable affects another variable, a directed arrow or edge connects the independent variable to the dependent one. The directed edge may be either a normal edge that indicates that the relationship is normally true, or a conditional edge that indicates that the relationship is true only when another variable (or condition) exists. Edges connecting any pair of nodes are mutually exclusive; only one edge relationship is true at a given time.

Numbers may be placed on the directed edge to represent the gains between the two events. These gains are based on the mathematical definition of gain, $\partial Y/\partial X$, where X and Y denote the independent and dependent variables, respectively. The magnitudes of the gains used in the digraphs for the assessment are quantized into three discrete values of -1, 0, +1. Gains of ±1 represent normal disturbances that a negative feedback loop is able to cancel.

Gains of 0 indicate the nullification of any relationship existing between the two variables,

Variables are represented by alphanumeric labels on the nodes. For instance, P2, M3, and FIRE at HX represent the variables: pressure at location 2, mass flow rate at location 3, and fire at heat exchanger. The direction of the deviations in the values of variables are denoted by "+" and "-". These deviations have magnitudes of 0 and 1. 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. The same scheme of -1, 0, and +1 is also used to represent the deviations in the values of variables. For instance, once a variable assumes a value, it becomes an event. P2 = (0) is the event of the true or expected value of pressure at location 2, and M3 = +1 is the event of a moderate mass flow rate at location 3.

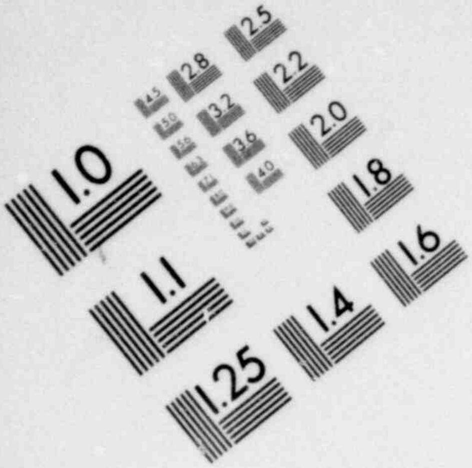
Some variables may be univariant; that is, they deviate only in the positive direction or only in the negative direction. For instance, FIRE at HX is a univariant variable.

B.2 UNIT MODEL DIGRAPHS

A schematic and a unit model digraph for a control value is shown in Fig. B-1. The nodes represent the following variables:

1. M1--mass flow rate occurring at location 1
2. M2--mass flow rate occurring at location 2
3. P3--pressure coming from location 3
4. Leak Out--air leaking out
5. Leak In--air leaking in.

Events that nullify the relationships between the above variables are shown as conditions on zero edges. The gains between variables are shown as 0 or ±1. For instance, the +1 gain between P3 and M2 states that an increase (decrease) in the air line P3 results in an increase (decrease) in the mass flow rate M2. The -1 gain between P3 and M2 indicates that if the actuator were reversed, an increase (decrease) in P3 results in a decrease (increase) in M2. The 0 gain between P3 and M2 indicates that there would be no relationship between the two variables if the valve were stuck. This discretizing of variables and gains should be calculated whenever possible using mass, energy, and momentum laws.



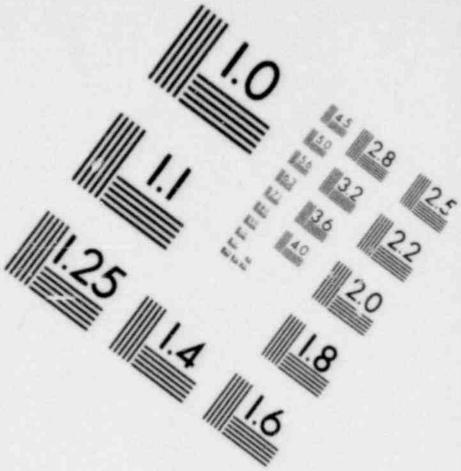
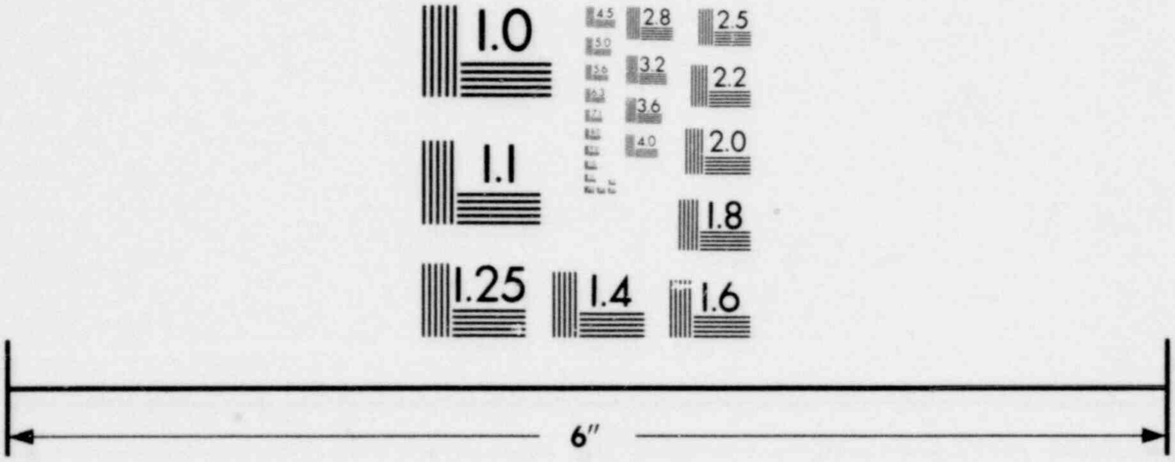
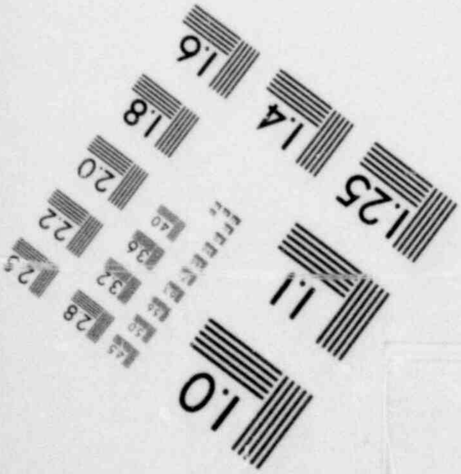
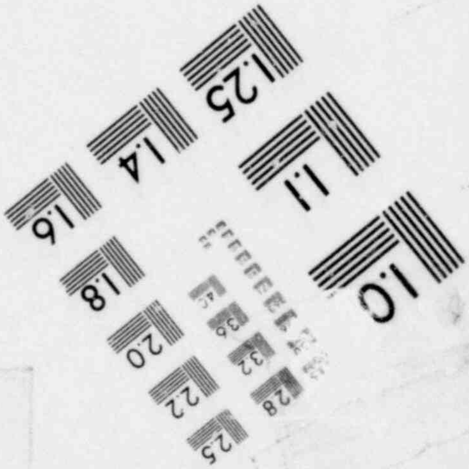
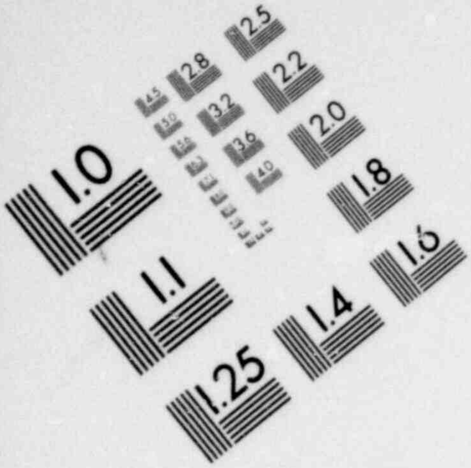


IMAGE EVALUATION TEST TARGET (MT-3)









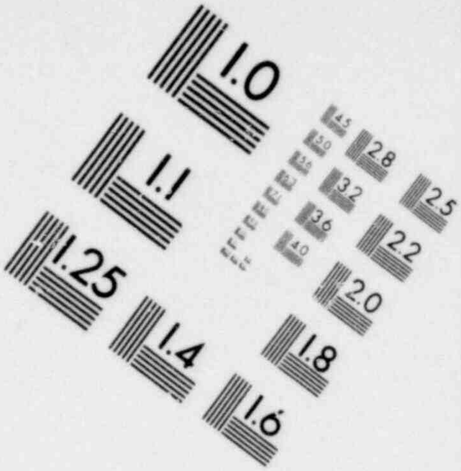
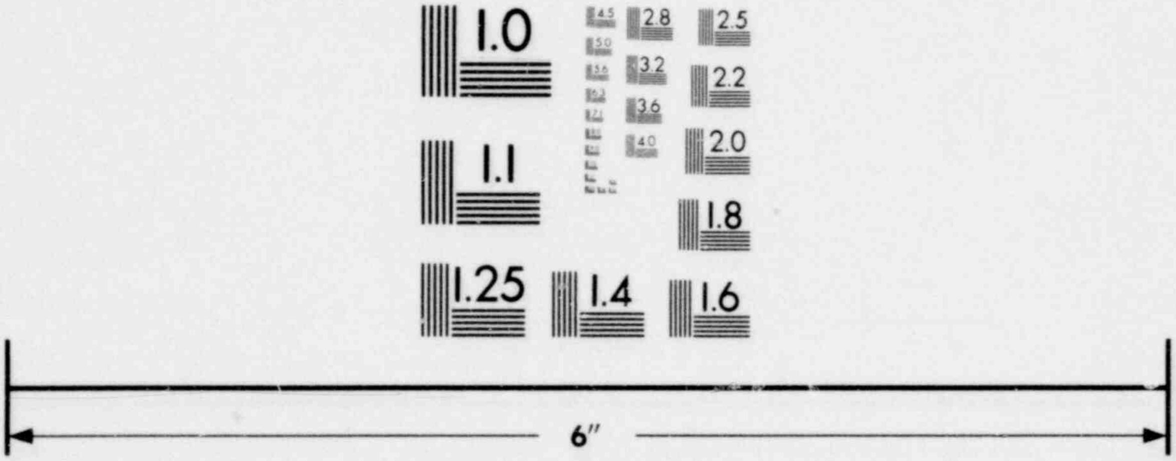
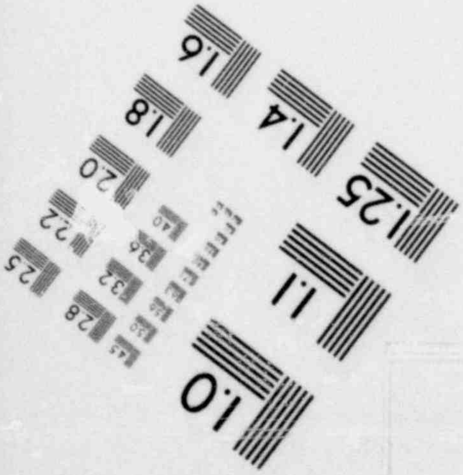
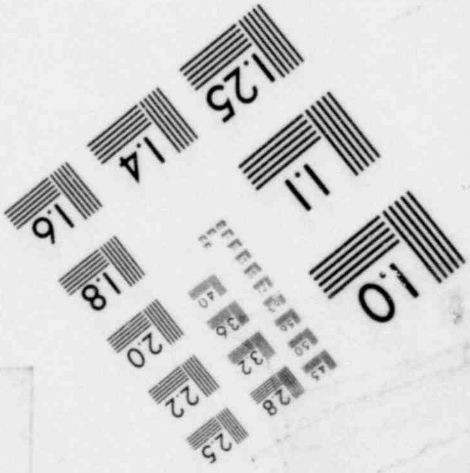
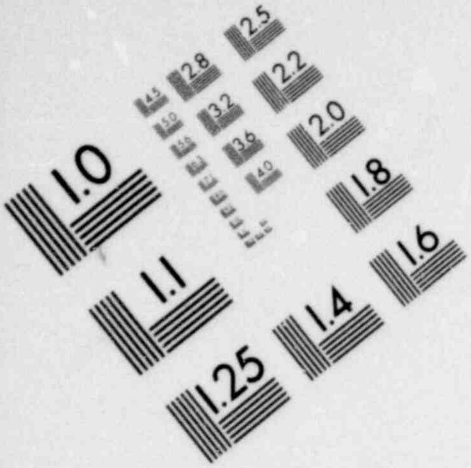


IMAGE EVALUATION
TEST TARGET (MT-3)









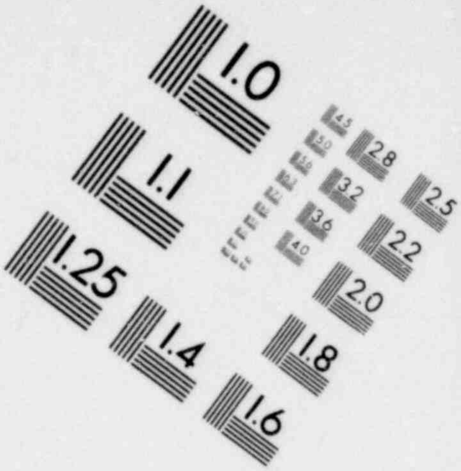
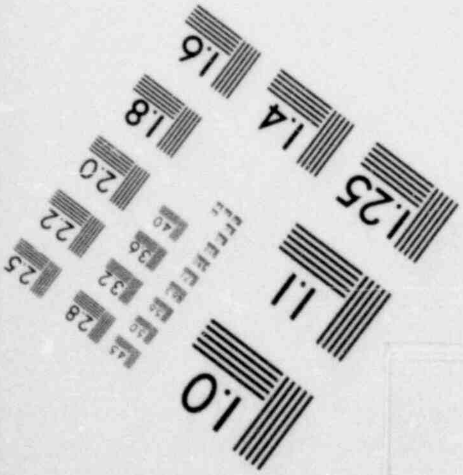
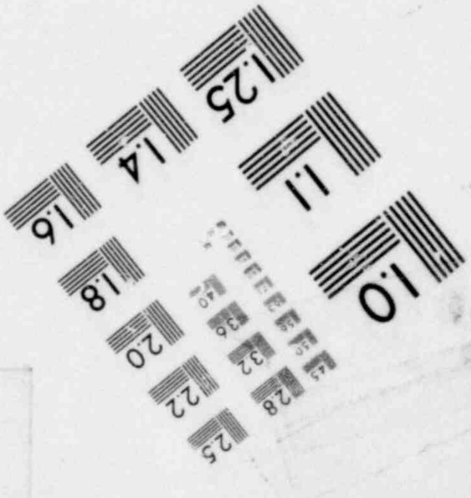
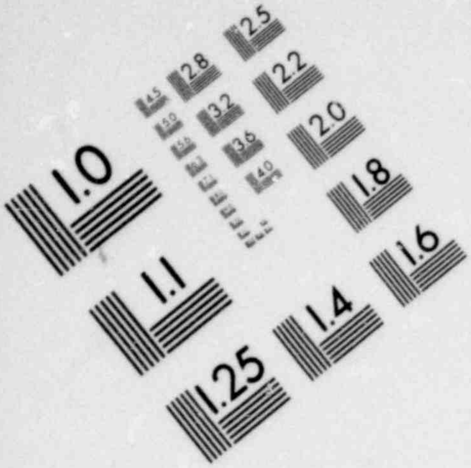


IMAGE EVALUATION TEST TARGET (MT-3)







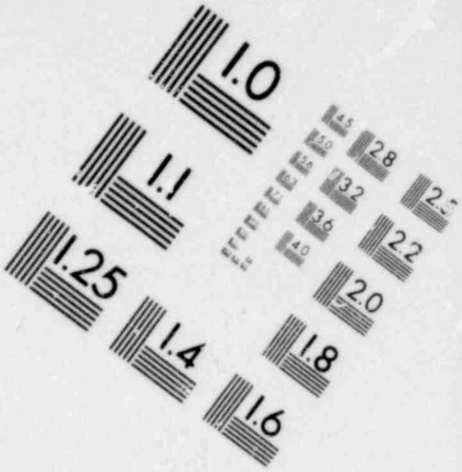
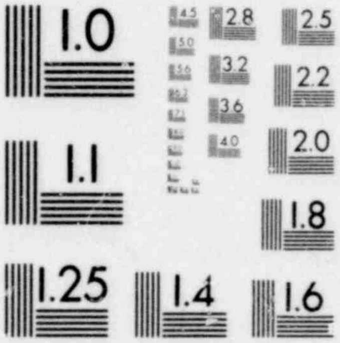
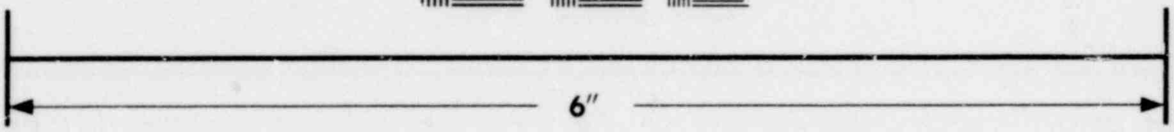
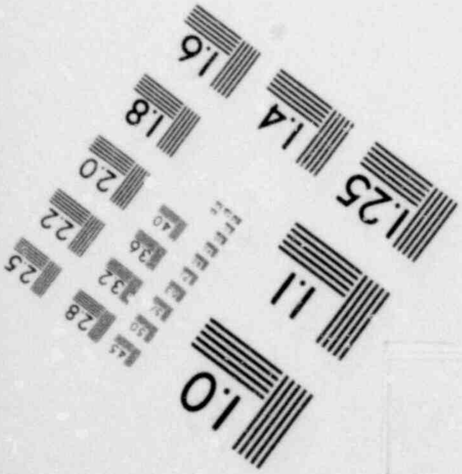
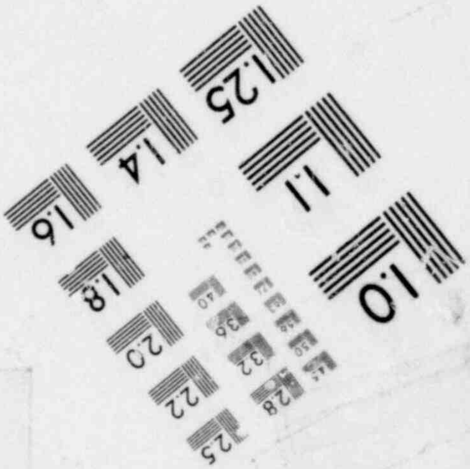


IMAGE EVALUATION TEST TARGET (MT-3)









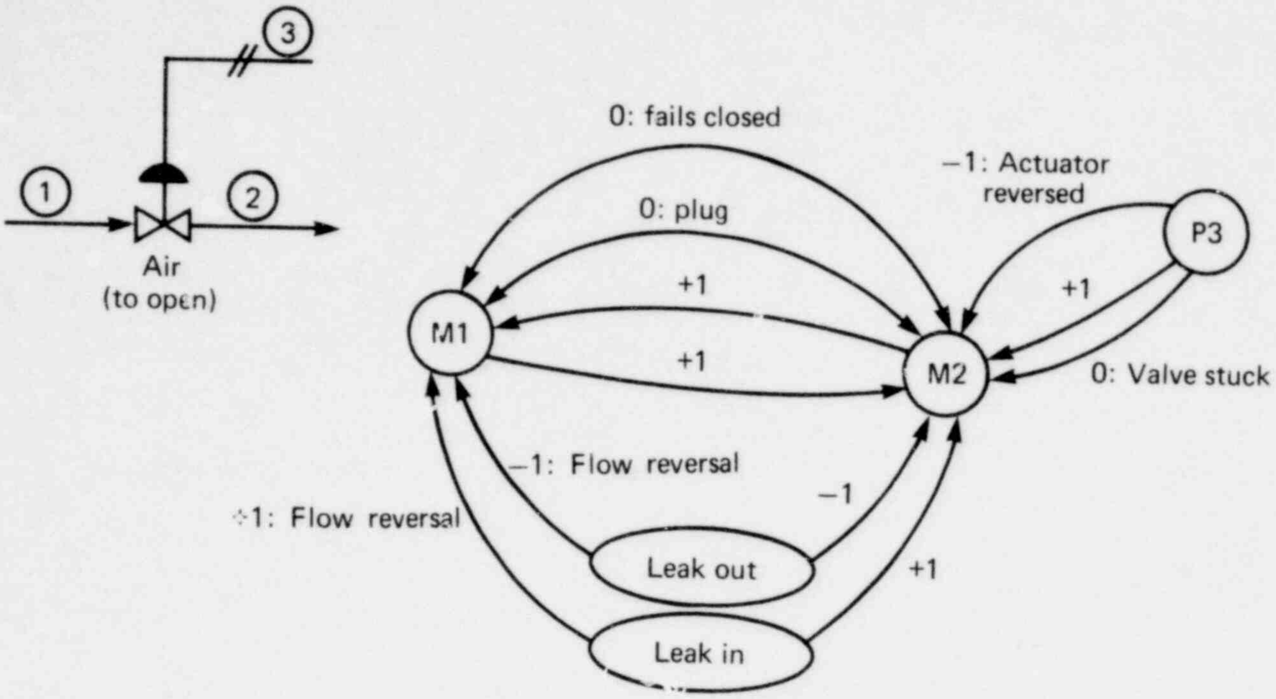


FIG. B-1. Unit model digraph of control valve.

In addition, the dynamics of gains should also be considered. Dynamics become important when determining if control loops are fast or strong enough to correct disturbances.

B.3 SYSTEM DIGRAPH

A system digraph is constructed from the unit model digraphs. By working backwards from the top event variable through the cause-and-effect relationships unit model digraphs, we can identify negative feedback and feedforward loops by tracing paths in the system digraph. A negative feedback loop is a path from a node back to itself with a net negative gain. A negative feedforward loop is two or more paths that fan out from one node and converge at another node. At least one of these paths must have a gain opposite to that of the other paths. An example of a negative feedback and feedforward loop is given in Fig. B-2.

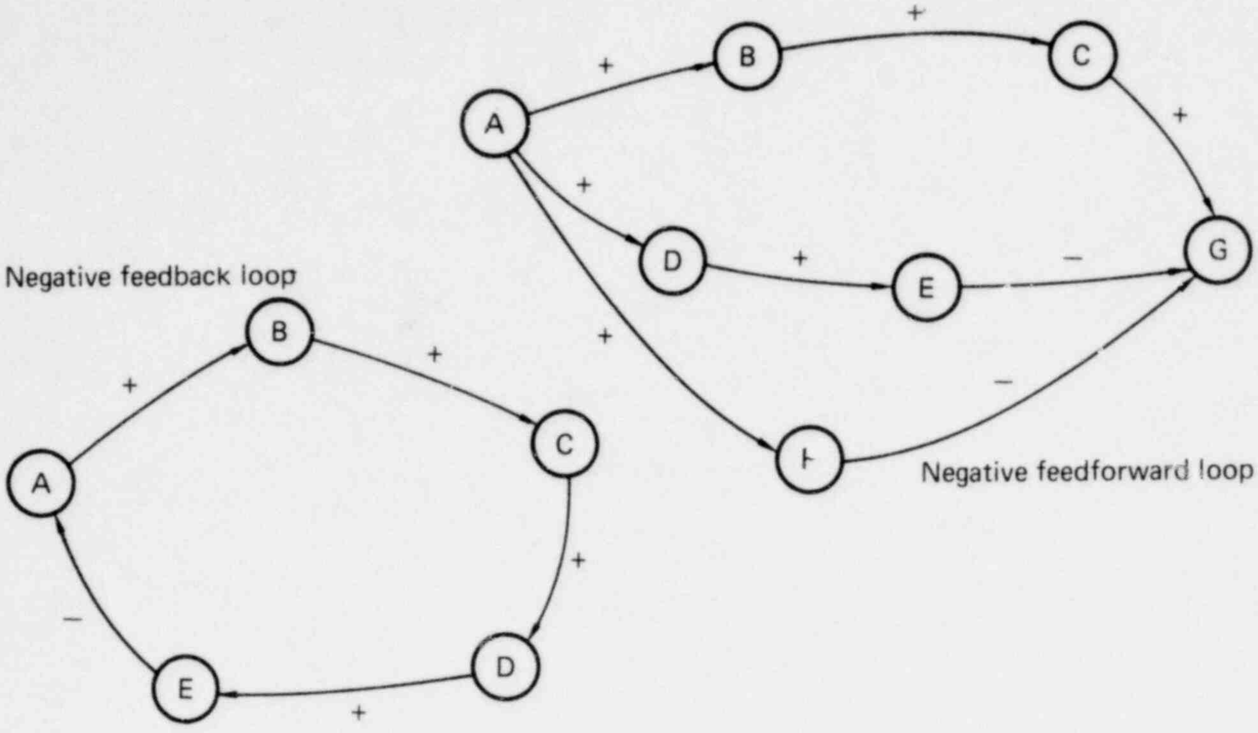


FIG. B-2. Example of negative feedback and feedforward loop.

These loops may also be initiated by an event on a conditional edge. Moreover, nested loop situations can exist when several loops share a common node or event.

The rules for constructing system digraphs from unit model digraphs are given below:

1. Start at the top event variable.
2. Select the unit model digraph(s) from which the top event variable is the output.
3. Work backward through the unit model digraphs(s) to its inputs, assembling the system digraph.
4. For each input variable on the resulting digraph, repeat step 3 until variables are encountered that have no further inputs (i.e., system boundary conditions or failure modes).
5. If loops exist in the system, it is possible to pass through the same unit digraph twice. The same rules given in steps 3 and 4 should be followed. Do not trace variables that have already been developed.

6. Variables that are conditions on edges are developed in the same manner as input variables.

The resulting system digraph can be used for the output variable having either values +1 or -1. The only part of a system digraph that explicitly denotes variable values are events on conditional edges.

Consider the Facility Z example in Fig. B-3, which is representative of the system digraph generation for the Test Bed assessment. The numbered nodes represent portals. Node 1 is a portal through which personnel can enter or exit the facility. It is monitored by a guard in a booth. Nodes 2 and 3 are portals connecting the areas inside the plant. Node 4 is an emergency door that permits exit but not entry. Areas 2 and 3 are covered with pressure mats that have microswitches that close when 15 or more pounds of force are exerted on them. The closing of these switches transmits a signal to the security

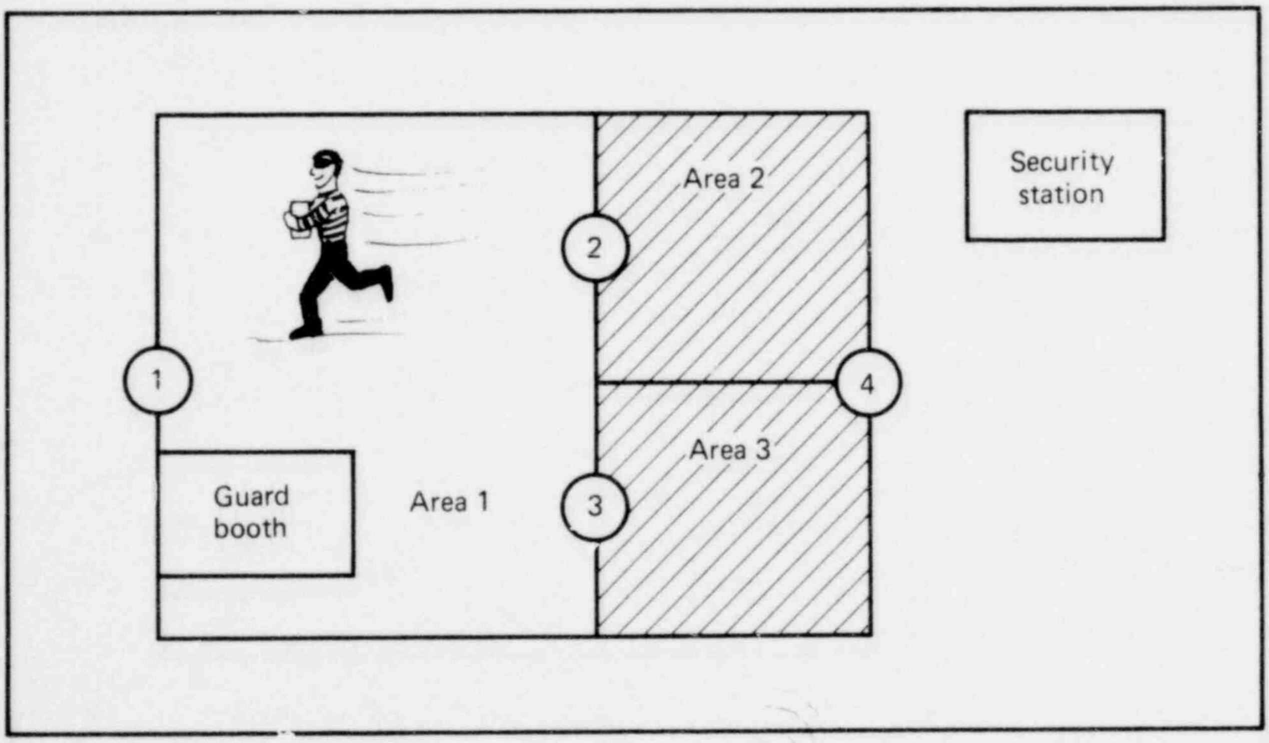


FIG. B-3. Facility Z.

station which ther dispatches a guard to node 4. An adversary with SNM is in area 1 and wishes to exit the facility.

The top event chosen for the example problem is "successful SNM theft from Facility Z." The top event variable is $MSNM_{OUT}$, defined by

$$MSNM_{OUT} = \begin{cases} +1 & \text{Adversary removes SNM from Facility Z} \\ 0 & \text{Otherwise.} \end{cases}$$

Hence, successful theft is the adversary removal of SNM from the boundary of the facility. The +1 state corresponds to a disturbance or unexpected system state (i.e., successful theft); the 0 state represents the expected system state (i.e., nonoccurrence of theft).

Three unit model digraphs can be constructed for the Facility Z problem:

1. Adversary movement through the facility
2. Guard at station
3. Facility safeguards information flow.

The unit model digraph for adversary movement through the facility is shown in Fig. B-4. The unit model shows three different routes obtained by applying basic reachability. The event $\overline{MSNM}_i$ denotes the presence of the adversary with SNM at portal i.

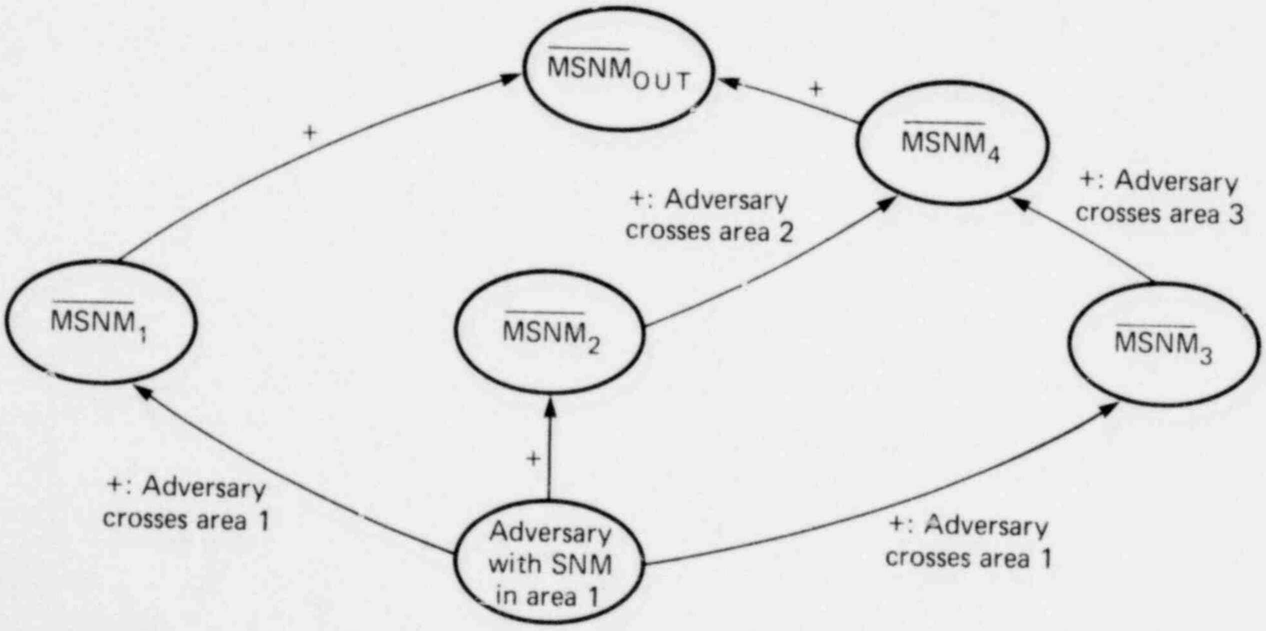

$\overline{MSNM}_{OUT}$
+
+
$\overline{MSNM}_4$
+: Adversary crosses area 2
+: Adversary crosses area 3
$\overline{MSNM}_1$
$\overline{MSNM}_2$
$\overline{MSNM}_3$
+
+: Adversary crosses area 1
Adversary with SNM in area 1
+: Adversary crosses area 1

FIG. B-4. Unit model digraph of adversary movement through Facility Z.

The unit model digraph for a stationed guard is given in Fig. B-5. This is the same model as in Fig. 24.

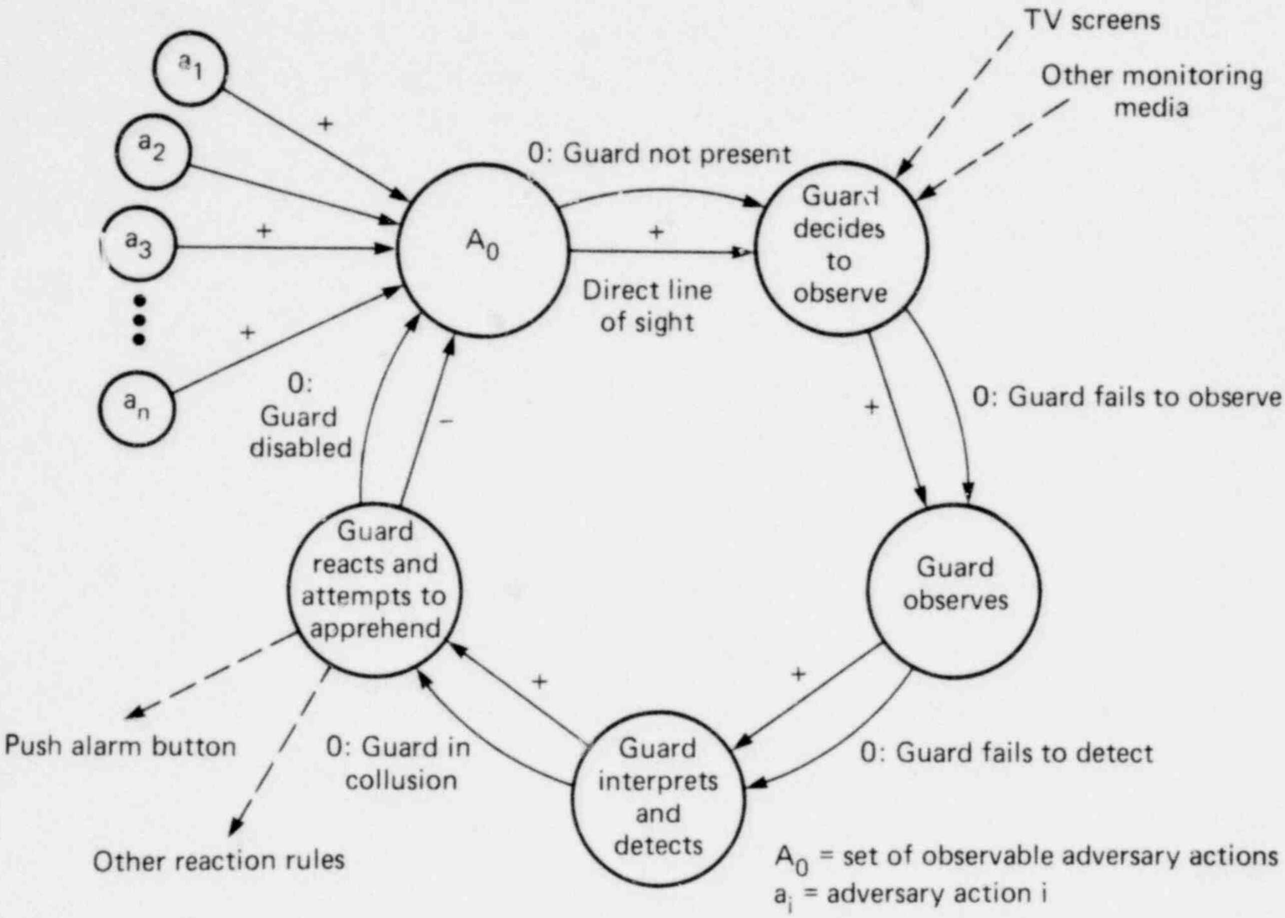


FIG. B-5. Unit model digraph of guard at station.

The unit model digraph for the safeguards information flow in Facility Z is given in Fig. B-6. When the adversary crosses areas 2 or 3, he creates a stimulus of a force greater than 15 lb, which triggers the pressure mats to transmit a signal to the security station (SS). Upon receipt of the signal, a guard is dispatched to portal 4 to prevent anyone exiting the facility with SNM (hence the negative gain).

The flow of information represented in Fig. B-6 is generic to the modeling of the MC decision logic of the Test Bed. (Refer to Section 4.2.3.4.)

By applying the rules described previously to these three unit model digraphs, the system digraph for successful SNM theft from Facility Z can be obtained. The top event is $\overline{\mathrm{MSNM}}_{\mathrm{OUT}} = +1$; the event $\overline{\mathrm{MSNM}}_{\mathrm{OUT}}$ appears in the unit model of adversary movement and also on the unit model of safeguards information flow. Its inputs are $\overline{\mathrm{MSNM}}_4$ and $\overline{\mathrm{MSNM}}_1$. By following the rules and working strictly from output to input variables (i.e., backward), we can construct the system digraph shown in Fig. B-7.

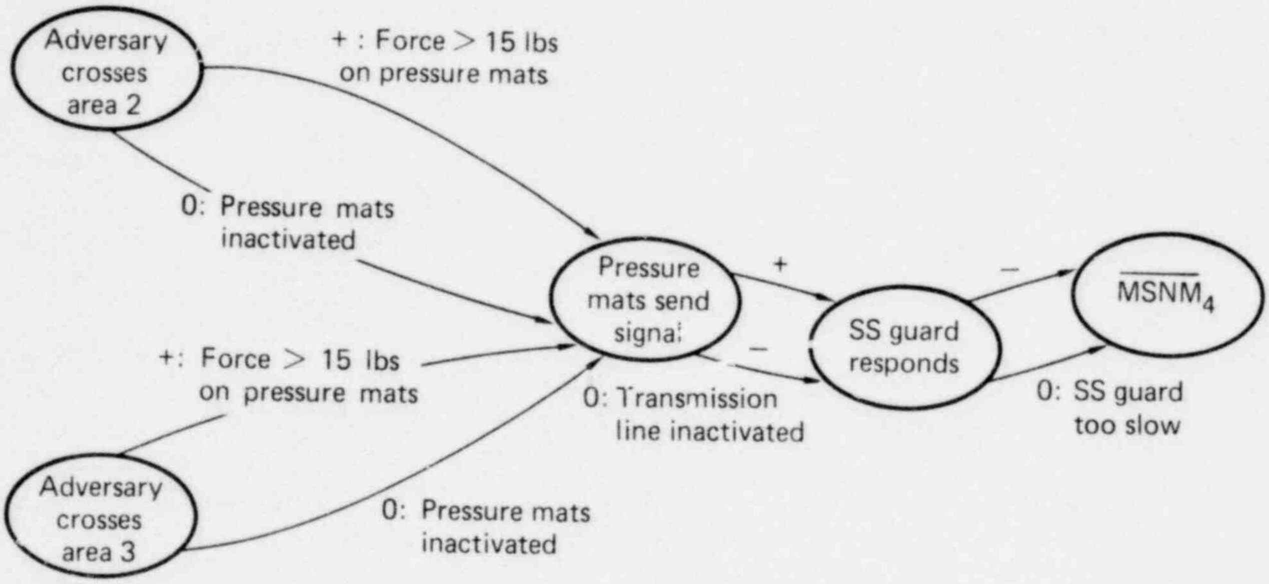

Adversary crosses area 2
+ : Force > 15 lbs on pressure mats
0: Pressure mats inactivated
Pressure mats send signal
+
–
SS guard responds
–
$\overline{\mathrm{MSNM}}_4$
+: Force > 15 lbs on pressure mats
0: Transmission line inactivated
0: SS guard too slow
Adversary crosses area 3
0: Pressure mats inactivated

FIG. B-6. Unit model digraph of safeguards information flow at Facility Z.

The system digraph in Fig. B-7 has one negative feedback loop (NFBL) and two negative feedforward loops (NFFL). The NFBL consists of nodes I, J, K, L, and H. NFFL 1 consists of the following paths: A, B and A, D, E, B.

NFFL 2 consists of the paths C, B and C, D, E, B. Note that the NFFLs are edged-fired by events A and C. Most NFFLs on the Test Bed system digraph are edge-fired.

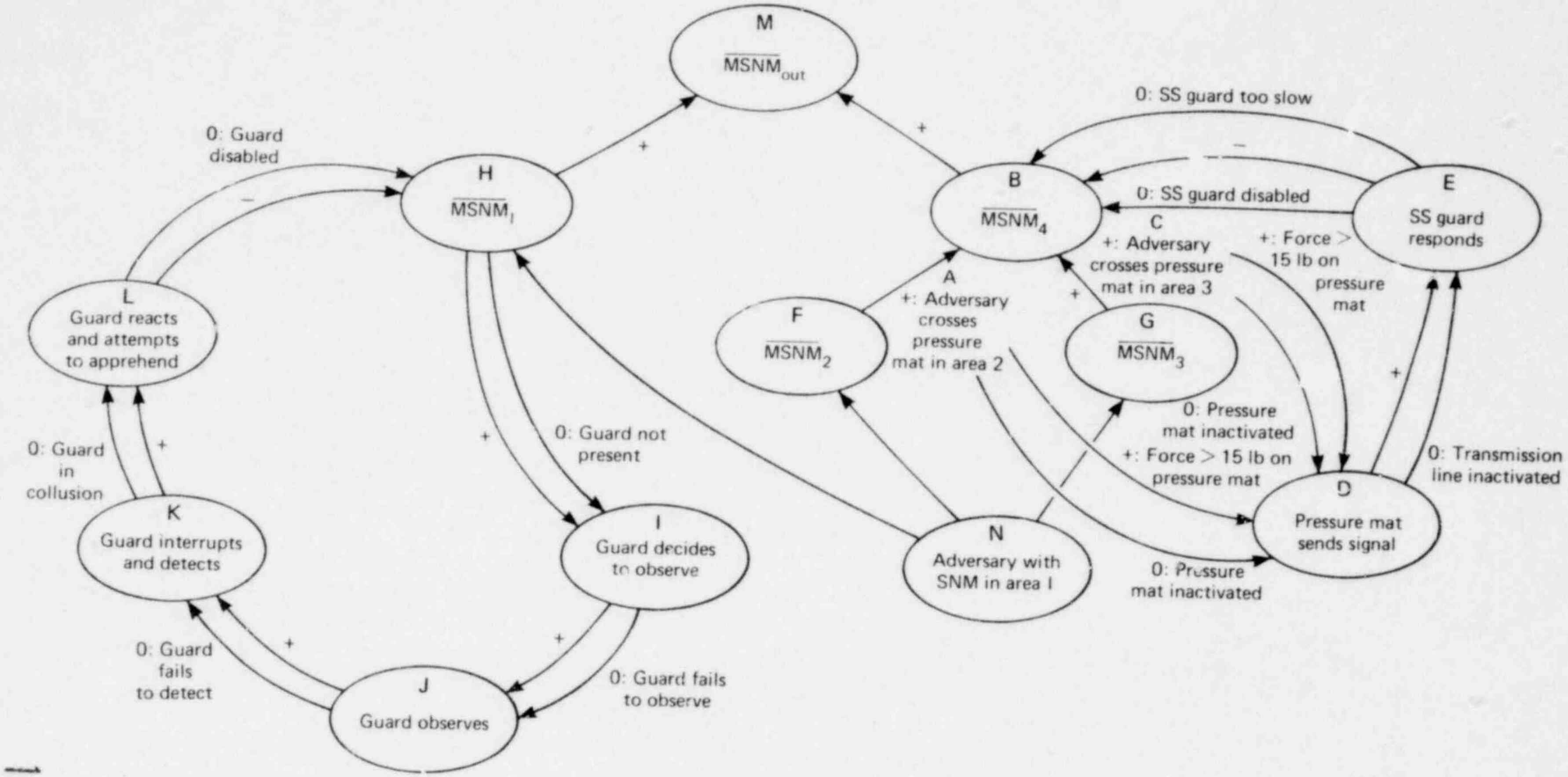

M
$\overline{MSNM}_{out}$
0: Guard disabled
–
+
H
$\overline{MSNM}_{I}$
+
0: SS guard too slow
–
B
$\overline{MSNM}_{4}$
0: SS guard disabled
E
SS guard responds
L
Guard reacts and attempts to apprehend
C
+: Adversary crosses pressure mat in area 3
+: Force > 15 lb on pressure mat
A
+: Adversary crosses pressure mat in area 2
F
$\overline{MSNM}_{2}$
+
G
$\overline{MSNM}_{3}$
+
0: Guard in collusion
+
+
0: Guard not present
0: Pressure mat inactivated
+: Force > 15 lb on pressure mat
0: Transmission line inactivated
K
Guard interrupts and detects
I
Guard decides to observe
N
Adversary with SNM in area I
D
Pressure mat sends signal
0: Pressure mat inactivated
0: Guard fails to detect
+
+
0: Guard fails to observe
J
Guard observes

FIG. B-7. System digraph for SNM theft from Facility Z.

A direct analogy between loop structure and an MC system can be drawn. The guard at the booth in Facility Z is there to prevent SNM theft from the facility at the location and time of occurrence. Hence, the stationed guard is modeled as a negative feedback control loop. On the other hand, the guard from the security station responds to signals generated within the facility and prevents theft of SNM at a different time and location than where the signals are generated. Hence, this guard is modeled as a negative feedforward control loop.

The dynamics of all gains (i.e., relationships) in the system digraph in Fig. B-7 are assumed to be instantaneous except for gains between nodes representing adversary movement through the facility and the movement of the guard from the security station to node 4. In these cases, transit times between nodes can be assigned so that the dynamics of the loop structure can be evaluated for construction of the fault tree.

B.4 FAULT TREE SYNTHESIS

Given the system digraph in Fig. B-7, we now need to construct the fault tree for the top event, successful SNM theft from Facility Z.

The first step is to identify all the loops in the system digraph. As described, there are two NFFLs representing a security station guard responding to signals generated from the pressure mats and one NFBL representing a guard at the booth apprehending an adversary with SNM.

The two NFFLs involve dynamics. If the transit time of the adversary out of the facility is less than the transit time of the security station guard, then these two loops fail. For example, NFFL 2 fails if $T_{A,B} < T_{E,B}$ and NFFL 2 fails if $T_{C,B} < T_{E,B}$, where $T_{I,J}$ is the transition time from node I to node J. The implication of the above inequalities will be considered below when the adversary event sets are generated from the fault tree.

Once the NFFLs and the NFBLs are identified and their dynamics determined, a transformation algorithm is applied to the system digraph to obtain the fault tree.

The basic rationale of the algorithm for material control assessment may be stated as follows: In order for the top event of successful SNM theft to occur, certain combinations of basic events must happen. Thus, all control loops on the path from where these basic events enter the system digraph to cause the top event must be inactivated. The transformation algorithm defines the logical basis of how and why these loops are to be inactivated.

The transformation algorithm has three properties:

1. It directly deduces the fault tree from the system digraph.
2. It is based on the local conversion of the system digraph nodes and edges into a partial fault tree through the use of fault tree operators.
3. It provides consistency checks of events on NFBLs against events already developed in the tree (e.g., previous conditions in the fault tree and events within the domain of an AND gate).

The algorithm requires the fault tree operators to be recursively applied until all events in the system digraph have been developed. The criterion used to select the appropriate operator for the development of an event depends on whether or not negative feedback loops or negative feedforward loops pass through the event. The operators in the transformation algorithm are given below.

If an event is on an NFBL, the operator shown in Fig. B-8 is used.

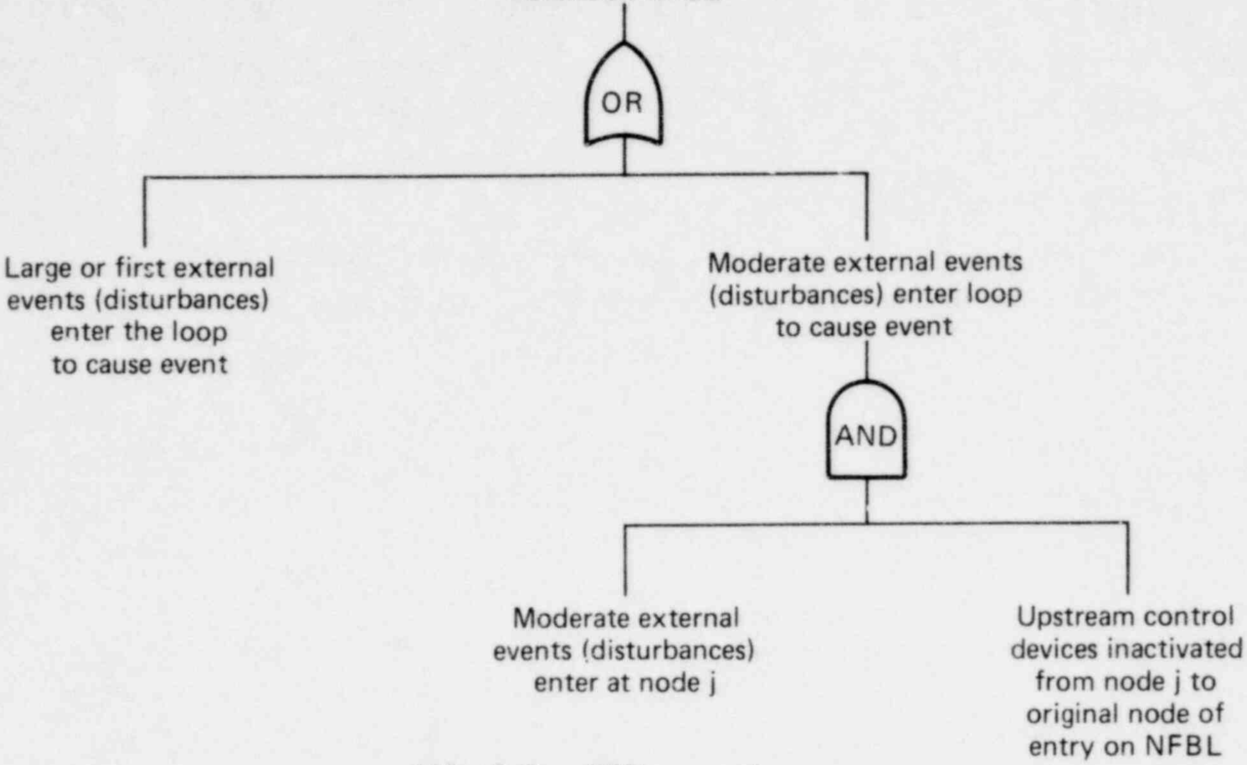

Event on NFBL
OR
Large or first external events (disturbances) enter the loop to cause event
Moderate external events (disturbances) enter loop to cause event
AND
Moderate external events (disturbances) enter at node j
Upstream control devices inactivated from node j to original node of entry on NFBL

FIG. B-8. NFBL operator.

For an event just before the start of an NFFL, the operator in Fig. B-9 is used.

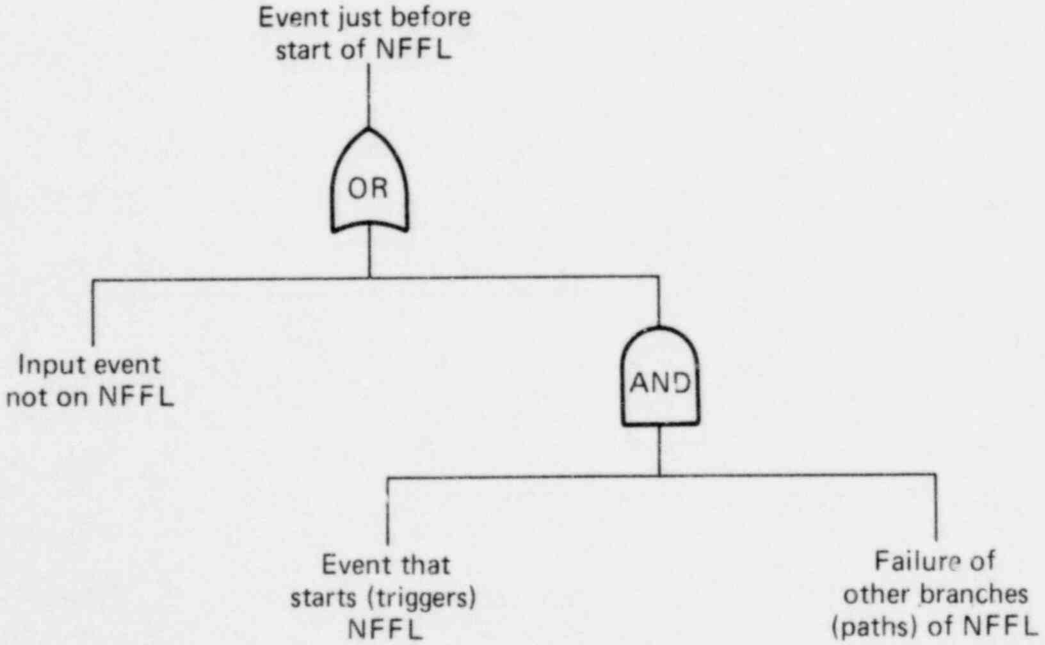

Event just before start of NFFL
OR
Input event not on NFFL
AND
Event that starts (triggers) NFFL
Failure of other branches (paths) of NFFL

FIG. B-9. Operator for event before start of NFFL.

An event whose occurrence depends on a conditional edge relationship is developed with the operator shown in Fig. B-10.

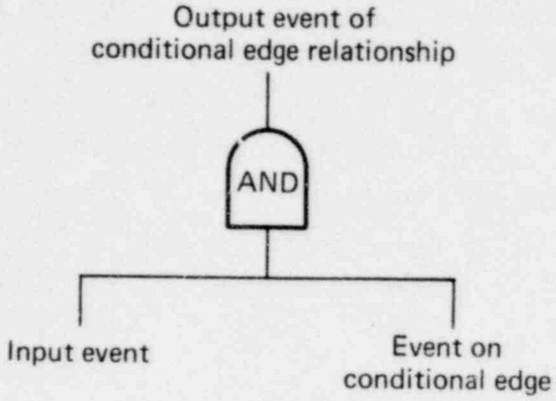

Output event of conditional edge relationship
AND
Input event
Event on conditional edge

FIG. B-10. Operator for output event depending on conditional edge relationship.

Otherwise, all other events in the system digraph are developed using the last operator as shown in Fig. B-11.

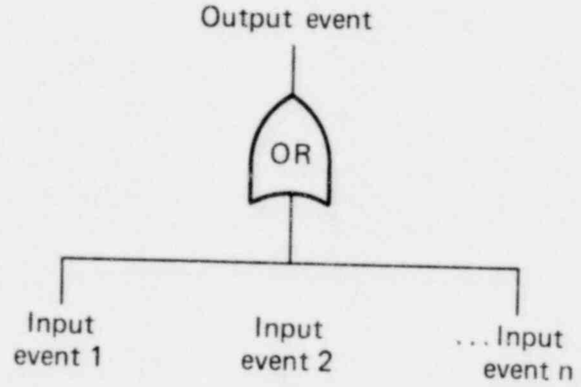


FIG. B-11. Operator for all other events.

The operators are based on the logical (AND, OR) combinations of events that could cause a particular event and on how negative feedback loops and negative feedforward loops fail. The negative feedback loop operator has two major terms. The left branch indicates that a large or fast input event (disturbance) to the NFBL will pass through the loop. The right branch denotes the fact that if a moderate event (disturbance) enters the NFBL it is also necessary (AND) to inactivate the control loop. The negative feedforward loop operator also has two major terms. The leftmost branch indicates that if the disturbing event entering the loop does not send signals down the paths of the NFFL, the loop will not cancel out the disturbance.

Otherwise (hence an OR gate), the right-hand term indicates that if the disturbing input event activates all paths of the NFFL, both the disturbance AND the failure of the other paths of the loop must occur.

The operator for events with conditional edge relationships requires the generation of an AND gate in the fault tree. Certain conditions or events must exist for one event to cause another event. Finally, if the event is not on a NFBL or NFFL or not conditionally dependent on other events, an ordinary OR gate operator is used.

Figure B-12 shows the fault tree for the system digraph of SNM theft from Facility Z. It was derived from the recursive application of the operators discussed previously. The operator invoked to develop each event and its gate structure is listed below.

Gate	Operator
G1	OR
G2	NFBL
G3	OR
G4	OR
G5	Conditional edge and NFFL
G6	Conditional edge and NFFL
G7	OR
G8	OR

Note for G2 that only the right-hand term of the NFBL operator is invoked, because there are no events for the left-hand term. Also, for G5 and G6 both the conditional edge and NFFL operators are invoked simultaneously because the conditional edge statement is also the event that starts the NFFL. G4 represents the ways in which the guard at the booth can fail, and G7 gives the ways in which the safeguards information flow can be inactivated.

The fault tree in Fig. B-12 yields 13 adversary events. The number of adversary event sets may be reduced by a dynamic analysis of the NFBLs and NFFLs in the system digraph of Facility Z. If the dynamic analysis establishes that the NFFLs always fail because of timing conditions, then G7 and G8 in the fault tree (see Fig. B-12) are not generated. Hence, the number

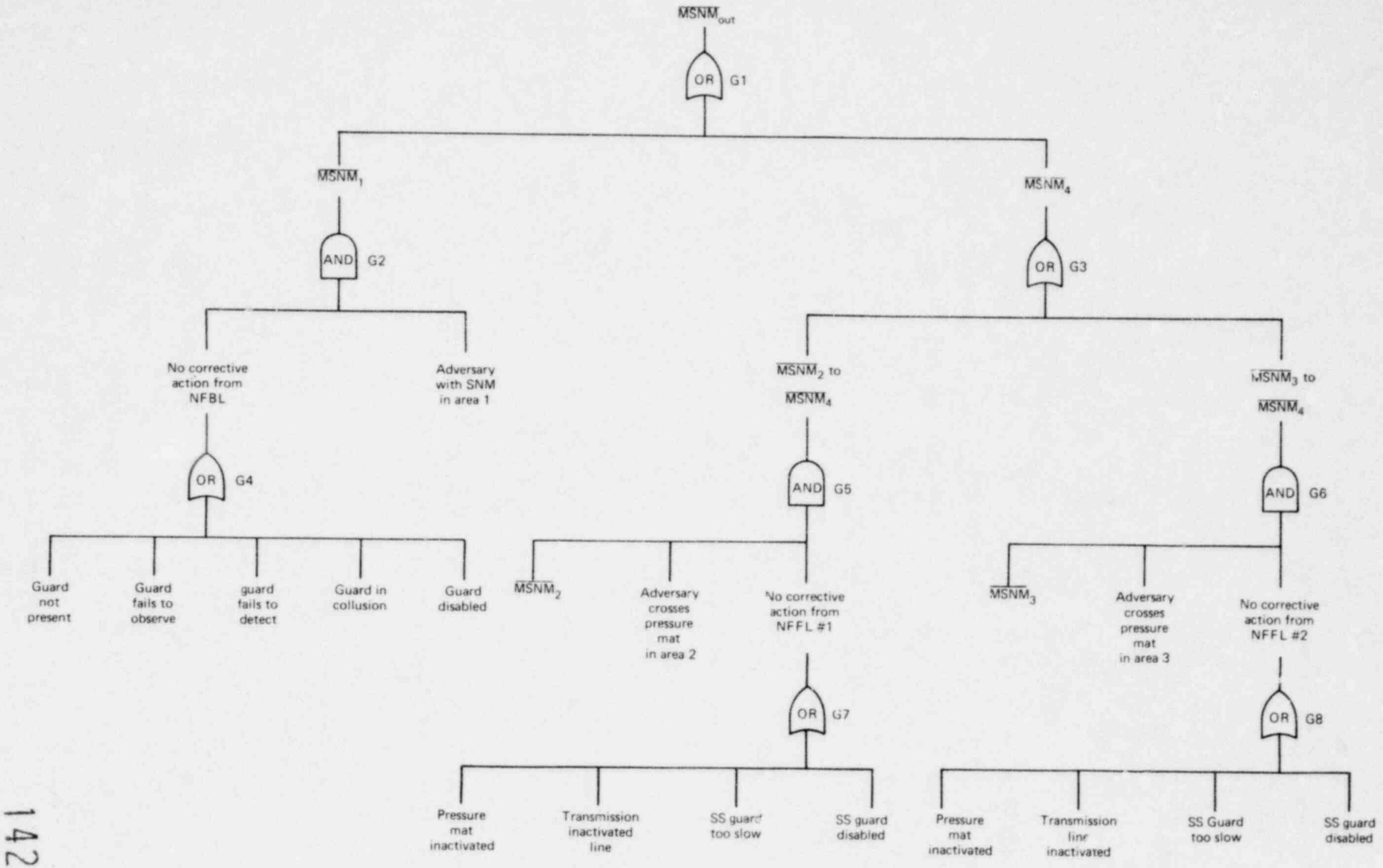

$\overline{MSNM}_{out}$
OR
G1
$\overline{MSNM}_1$
AND
G2
No corrective action from NFBL
Adversary with SNM in area 1
OR
G4
Guard not present
Guard fails to observe
guard fails to detect
Guard in collusion
Guard disabled
$\overline{MSNM}_4$
OR
G3
$\overline{MSNM}_2$ to $\overline{MSNM}_4$
AND
G5
$\overline{MSNM}_2$
Adversary crosses pressure mat in area 2
No corrective action from NFFL #1
OR
G7
Pressure mat inactivated
Transmission inactivated line
SS guard too slow
SS guard disabled
$\overline{MSNM}_3$ to $\overline{MSNM}_4$
AND
G6
$\overline{MSNM}_3$
Adversary crosses pressure mat in area 3
No corrective action from NFFL #2
OR
G8
Pressure mat inactivated
Transmission line inactivated
SS Guard too slow
SS guard disabled

FIG. B-12. Fault tree for SNM theft from Facility Z.

of adversary event sets would be reduced to seven. A dynamic analysis can reduce the number of relevant event sets. By reducing the size of the fault tree, significant savings can be made in both CPU time and storage requirements of the FTA computer codes.

B.5 CONSISTENCY CHECKS IN FTA

We now discuss the importance of consistency checks in FTA[6,8-10] for MC system assessments.

Suppose Facility Z given in Fig. B-7 has two modes of operation: the production mode and the shutdown mode. During the production mode, a guard is present at the booth, and another guard is present at a security station external to the facility. Hence, analyses presented in the previous sections are applicable for SNM theft during the production mode of operation. However, during the shutdown mode of operation, no one should be present in the facility. Only one guard is stationed outside the facility, and he is to apprehend anyone exiting the facility. Clearly, the previous analysis does not apply to the shutdown mode of operation for Facility Z.

The production and shutdown modes are mutually exclusive modes of operation. Thus, the guard not being present at the booth is a failure while the facility is in the production mode and is a boundary condition in the shutdown mode. Stated in FTA terms, events that are exclusive to one mode of operation cannot be in the domain of an AND gate with events that are exclusive to another mode of operation. Consistency checks ensure that mutually exclusive events do not appear in the domain of AND gates in fault trees.

There are several ways to perform consistency checks:

1. Inspecting each adversary event set for consistency
2. Including complemented events in the construction of the fault tree
3. Imposing boundary conditions in the construction of the fault tree.

The first approach is impractical because of the large number of event sets that are generated in real problems. The second approach requires the solution of the fault tree for prime implicants[11,12] that are computationally more difficult to find than minimal cut sets. Thus, the third approach was used in the Test Bed assessment.

Figure B-13 gives a conceptual system digraph for SNM theft from Facility Z with the two modes of operation.

The guard responses and the flow of safeguards information are summarized below for Facililty Z under the two modes of operation.

1. NFBL 1 is the same as NFBL H, I, J, K, L, in Fig. B-7 and is active only during the production mode of operation.
2. NFBL 2 is new and is active only during the shutdown mode of operation.
3. NFFLs are the same as NFFLs 1 and 2 in Fig. B-7 and are active only during the production mode of operation.

As one works backwards from the top event node in the system digraph to generate the fault tree, consistency checks cause boundary conditions to be generated that impose restrictions on events that are developed. These boundary conditions dictate in an exact way how the information flow is to be nullified. Any events that are in logical contradiction to the boundary conditions are excluded from the fault tree. As one continues to generate the fault tree, new boundary conditions may be generated and checks for logical consistency may be more restrictive.

The procedure for generating boundary conditions and consistency checks in the digraph-fault tree methodology is now described. First, a listing of all basic events in the digraph is obtained, and mutually exclusive events are identified. Second, the loop structure in the digraph and the basic events on these loops are determined. Mutually exclusive events on these loops define the boundary conditions. Third, a timing analysis of the loops must be performed to establish whether two events that are mutually exclusive at any one point in time can occur singly at different times.

Figure B-14 gives the fault tree generated for the system digraph in Fig. B-13. It shows the use of boundary conditions in implementing consistency checks. Figure B-14 shows that numerous adversary event sets containing mutually exclusive events would have been generated if boundary conditions were not imposed to serve as consistency checks.

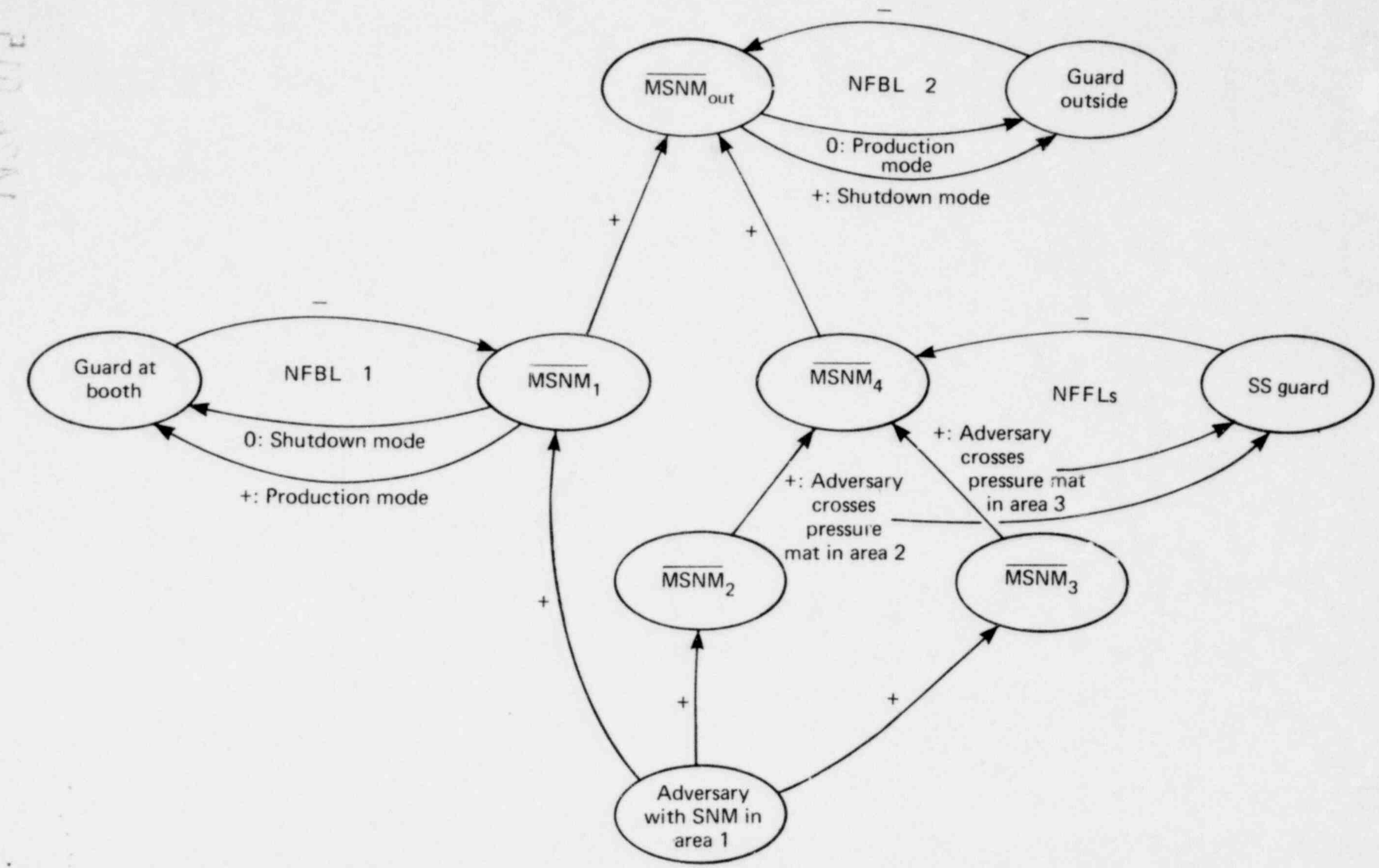

$\overline{\text{MSNM}}_{\text{out}}$
NFBL 2
Guard outside
–
0: Production mode
+: Shutdown mode
+
+
Guard at booth
NFBL 1
$\overline{\text{MSNM}}_1$
–
0: Shutdown mode
+: Production mode
$\overline{\text{MSNM}}_4$
NFFLs
SS guard
–
+: Adversary crosses pressure mat in area 3
+: Adversary crosses pressure mat in area 2
$\overline{\text{MSNM}}_2$
$\overline{\text{MSNM}}_3$
+
+
+
Adversary with SNM in area 1

FIG. B-13. Conceptual system digraph for Facility Z with two modes of operation.

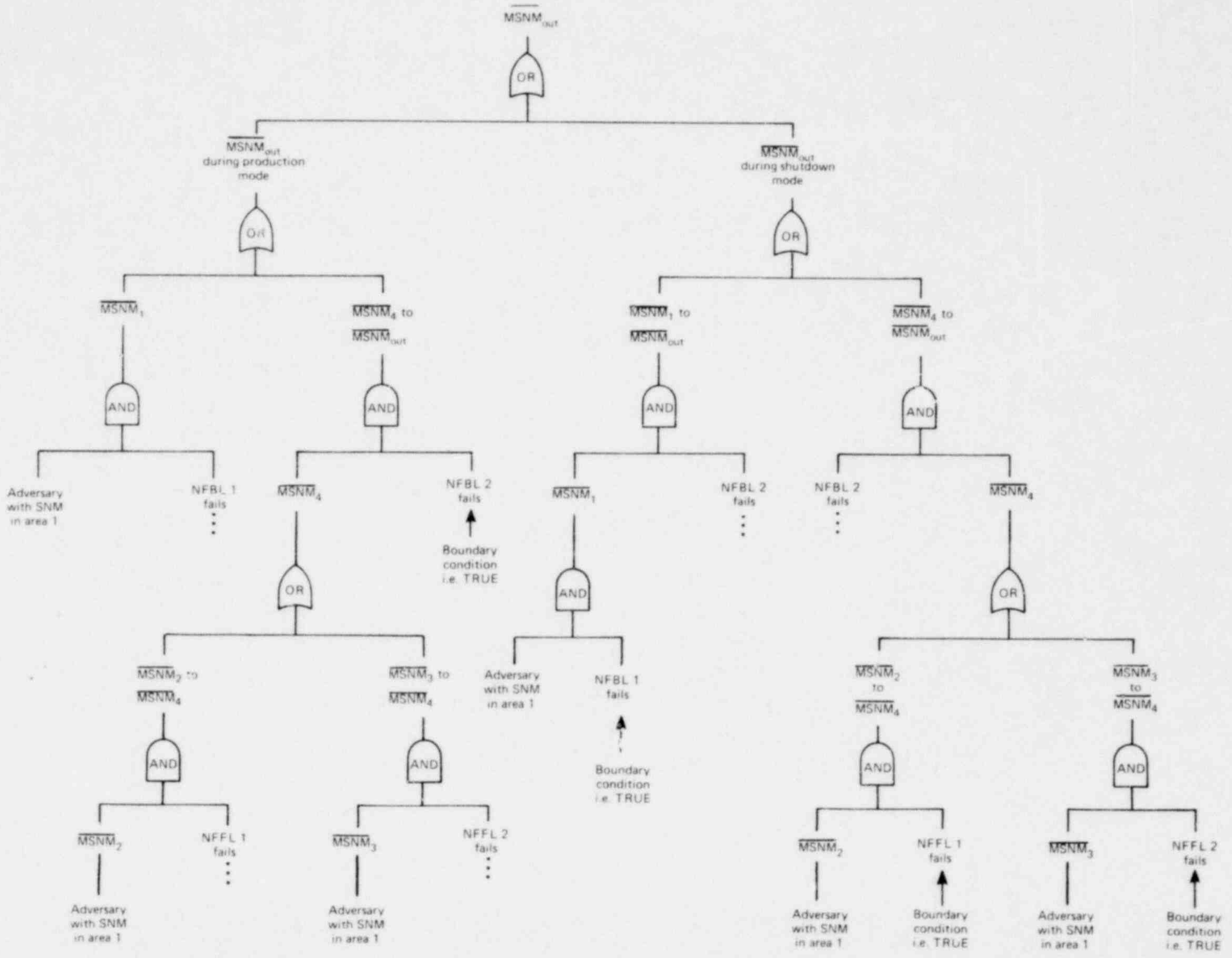

$\overline{MSNM}_{out}$
OR
$\overline{MSNM}_{out}$ during production mode
$\overline{MSNM}_{out}$ during shutdown mode
OR
OR
$\overline{MSNM}_1$
$\overline{MSNM}_4$ to $\overline{MSNM}_{out}$
$\overline{MSNM}_1$ to $\overline{MSNM}_{out}$
$\overline{MSNM}_4$ to $\overline{MSNM}_{out}$
AND
AND
AND
AND
Adversary with SNM in area 1
NFBL 1 fails
$\overline{MSNM}_4$
NFBL 2 fails
Boundary condition i.e. TRUE
$\overline{MSNM}_1$
NFBL 2 fails
NFBL 2 fails
$\overline{MSNM}_4$
OR
AND
OR
$\overline{MSNM}_2$ to $\overline{MSNM}_4$
$\overline{MSNM}_3$ to $\overline{MSNM}_4$
Adversary with SNM in area 1
NFBL 1 fails
Boundary condition i.e. TRUE
$\overline{MSNM}_2$ to $\overline{MSNM}_4$
$\overline{MSNM}_3$ to $\overline{MSNM}_4$
AND
AND
AND
AND
$\overline{MSNM}_2$
NFFL 1 fails
$\overline{MSNM}_3$
NFFL 2 fails
Adversary with SNM in area 1
Adversary with SNM in area 1
$\overline{MSNM}_2$
NFFL 1 fails
$\overline{MSNM}_3$
NFFL 2 fails
Adversary with SNM in area 1
Boundary condition i.e. TRUE
Adversary with SNM in area 1
Boundary condition i.e. TRUE

FIG. B-14. Fault tree with boundary conditions as consistency checks.

APPENDIX B

REFERENCES

1. H. E. Lambert, Systems Safety Analysis and Fault Tree Analysis, Lawrence Livermore Laboratory, Livermore, Calif., UCID 16238 (May 9, 1973).
2. "Safeguards Research: Assessing Material Control and Accounting Systems", in Energy and Technology Review, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-52000-77-11/12 (Nov-Dec., 1977), pp. 11-19.
3. H. E. Lambert, and J. J. Lim, The Modeling of Adversary Action for Safeguards Effectiveness Assessment, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-79217, Rev. 1 (June 1977).
4. F. M. Gilman, H. E. Lambert, and J. J. Lim, The Results of a Directed Graph-Fault Tree Assessment of a MCA System, Lawrence Livermore Laboratory, Calif., UCRL-80802 (1978).
5. S. A. Lapp and G. J. Powers, "Computer-Aided Synthesis of Fault-Trees," IEEE Trans. on Reliability, R-26 (April 1977), pp. 2-13.
6. S. A. Lapp and G. J. Powers, "The Synthesis of Fault Trees," in Nuclear Systems Reliability Engineering and Risk Assessment, Eds. J. B. Fussell and G. R. Burdick, SIAM (1977).
7. H. E. Lambert, "Comments on the Lapp-Powers 'Computer-Aided Synthesis of Fault Trees,'" to appear in IEEE Trans. on Reliability.
8. J. B. Fussell, Synthetic Tree Model--a Formal Methodology for Fault-Tree Construction, Aerojet Nuclear, ANCR 01098 (March 1973).
9. J. R. Taylor, "A Formalisation of Failure Mode Analysis of Control Systems," Danish Atomic Energy Commission, RISO-M-1654 (September 1973). Available from Library of the Danish Atomic Energy Commission; (Atomenergikommissionens Bibliotek); Riso; DK-4000 Roshilde, Denmark.
10. H. E. Lambert, Fault Trees for Decision Making in Systems Analysis, Lawrence Livermore Laboratory, Calif., UCRL-51829 (October 1975), p. 63.
11. R. Willie, Fault Tree Analysis Program, Operations Research Center Report, No. ORC 78-14, University of California, Berkeley (1978).
12. R. B. Worrell, Set Equation Transformation System (SETS), Sandia Laboratories, Albuquerque, N.M., SLA-73-28A (July 1974).

Appendix C

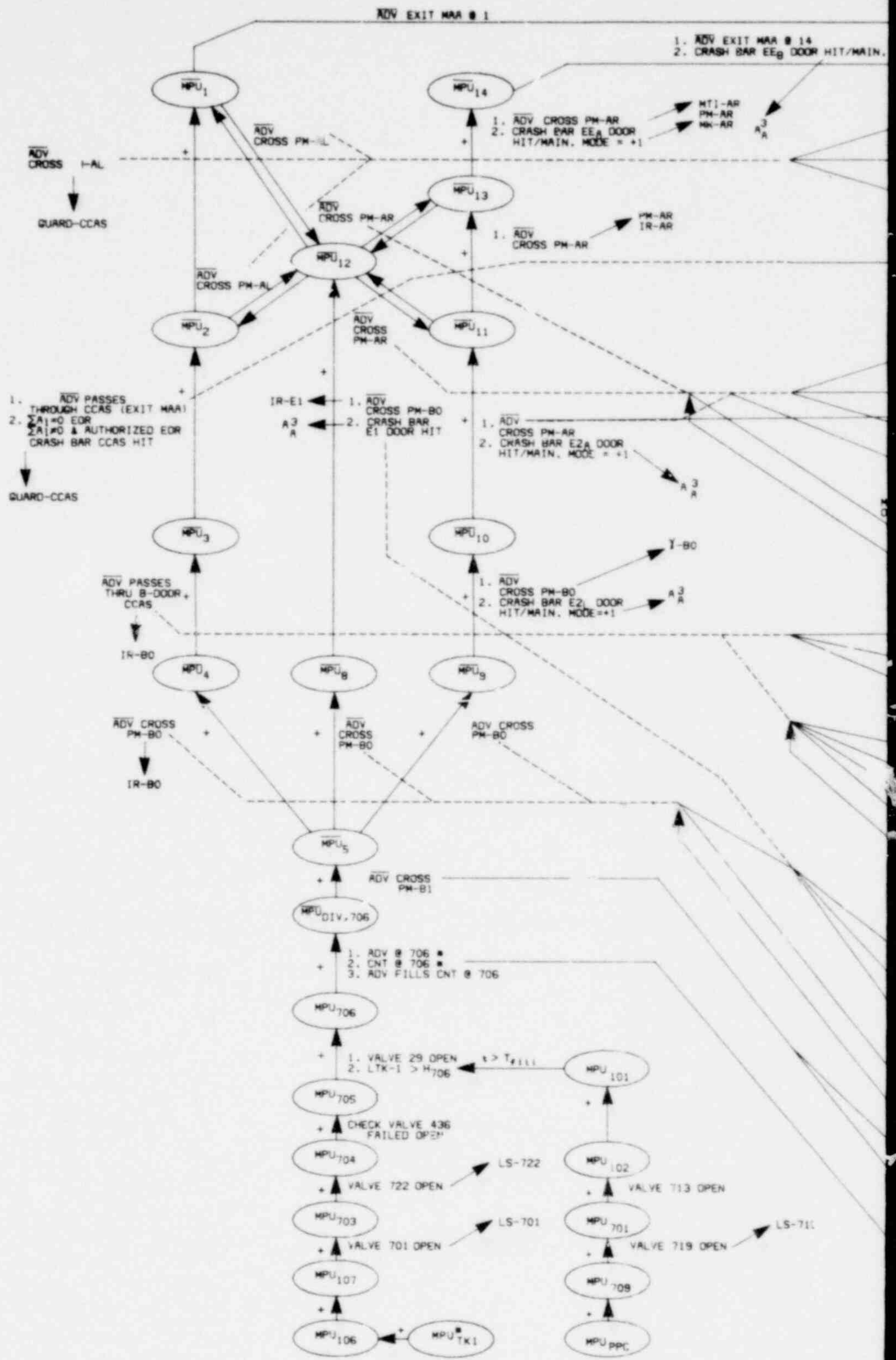
SYSTEM DIGRAPH FOR THE TEST BED ASSESSMENT

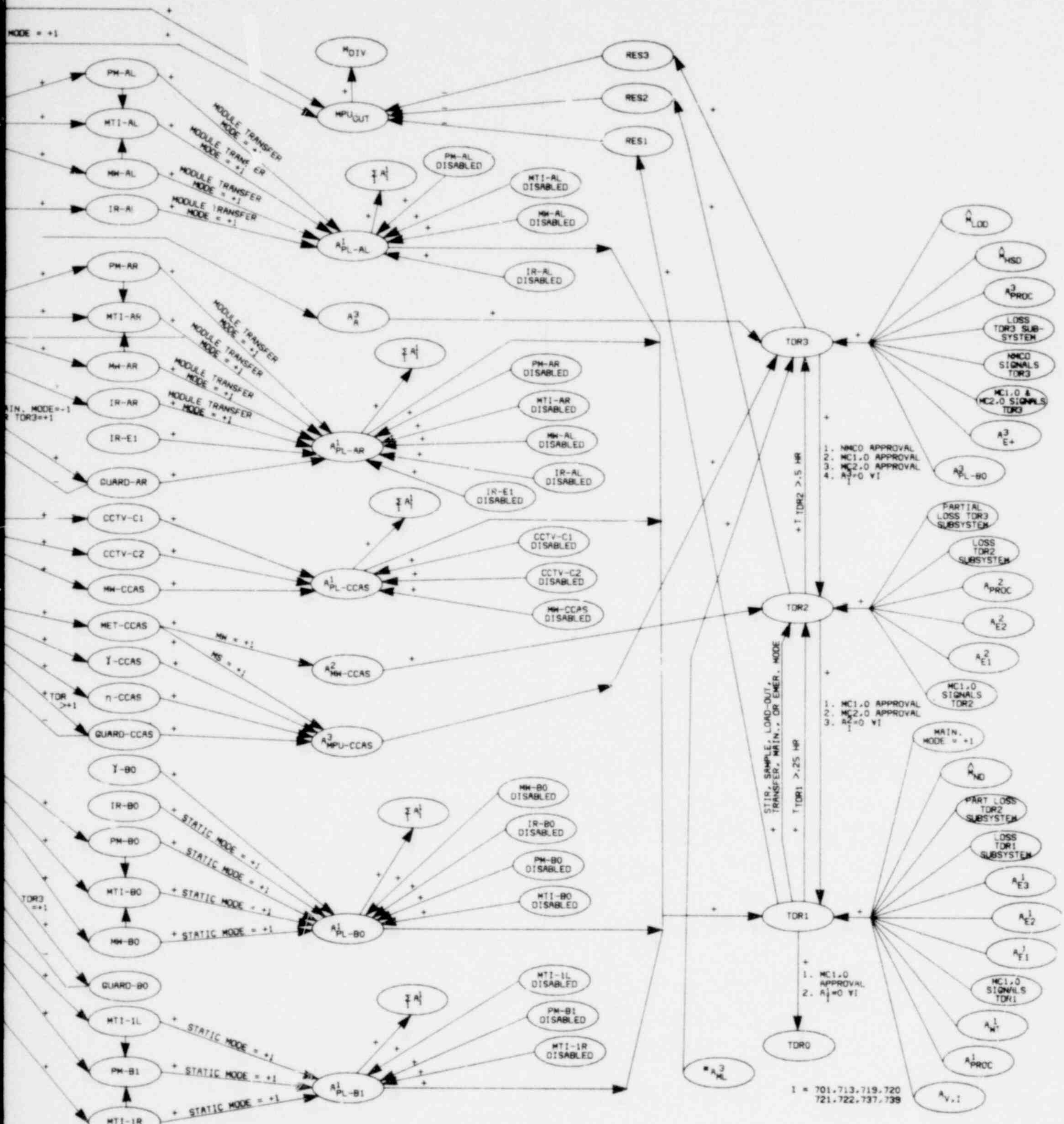
GLOSSARY FOR SYSTEM DIGRAPH

Notation	Description
^	Entrance/Exit Anomaly
A_X^I	Anomaly of Type X Which Generates a TDR Signal of Level I
A_{MW}	Portal Metal Anomaly (Weak)
A_V	Valve Position Anomaly
A_W	Weight Anomaly
A_R	Area A_R Within MAA
A_L	Area A_L Within MAA
B_0, B_1	Subdivisions of Plutonium Product Storage Area
C	Concentration
CCAS	Computer Controlled Access System
CCTV-I	Closed Circuit T.V. Detection at Location I
CNT @ I	Container at Location I
δM	Difference in Solution Mass
g	Acceleration Due to Gravity
γ-I	Gamma Detection at Location I
Guard-I	Guard at Location I
h	Difference in Elevation of Two Bubbler Lines
IR-I	Infrared Detection at Location I
L	Liquid Level of Plutonium Nitrate in Tank
LS^J	Limit Switch Position for Valve J
LS_I^J	Indicated Limit Switch Position for Valve J
MPU_{TK1}	Mass of Plutonium Nitrate in Tank 1
M	Solution Mass
M_{DIV}	Theft of Plutonium Across Boundary of MAA
MC-1, O	Security Station Operator
MC-2, O	Process Control Station Operator
MET-CCAS	Metal Detection at CCAS
$\overline{MPU}_I$	Adversary with Plutonium at Node I
MPU_I	Mass Flow Rate of Plutonium at Node I
MPU_{OUT}	Movement of Plutonium Out of the MAA
MTI_I	Motion Target Detection at Location I

GLOSSARY FOR SYSTEM DIGRAPH (continued)

Notation	Description
MW_I	Microwave Detection at Location I
NMCO	Nuclear Materials Control Officer
μCCAS	Neutron Detection in CCAS
P_X	Pressure at Location X
PM-I	Pressure Mat Detection at Location I
PFC	Plutonium Product Cell
RES 1	Guard Response Level 1
RES 2	Guard Response Level 2
RES 3	Guard Response Level 3
ρ	Density
σ	Standard Deviation
t	Present Value of Time
t_{END}	Procedure End Time
t_{START}	Procedure Start Time
TDR Ø	Theft Danger Rating Level Ø
TDR 1	Theft Danger Rating Level 1
TDR 2	Theft Danger Rating Level 2
TDR 3	Theft Danger Rating Level 3
TK 1	Tank 1
TK 2	Tank 2
(t_1, t_2)	Authorized Range of Procedure Starting Times
VP_J	Valve Position of Valve J
1-B, 2-B, 3-B	First, Second, and Third Floors of Bl Area


ADV EXIT MAA @ 1
1. ADV EXIT MAA @ 14
2. CRASH BAR EE_B DOOR HIT/MAIN.
MPU_1
MPU_14
1. ADV CROSS PM-AR
2. CRASH BAR EE_A DOOR HIT/MAIN. MODE = +1
MTI-AR
PM-AR
MK-AR
A^3_A
ADV CROSS PM-AL
ADV CROSS I-AL
GUARD-CCAS
MPU_13
ADV CROSS PM-AR
1. ADV CROSS PM-AR
PM-AR
IR-AR
MPU_12
ADV CROSS PM-AL
MPU_2
ADV CROSS PM-AR
MPU_11
1. ADV PASSES THROUGH CCAS (EXIT MAA)
2. ΣA_I=0 EOR ΣA_I≠0 & AUTHORIZED EOR CRASH BAR CCAS HIT
GUARD-CCAS
IR-E1
1. ADV CROSS PM-BO
A^3_A
2. CRASH BAR E1 DOOR HIT
1. ADV CROSS PM-AR
2. CRASH BAR E2_A DOOR HIT/MAIN. MODE = +1
A^3_A
MPU_3
MPU_10
Y-BO
ADV PASSES THRU B-DOOR CCAS
1. ADV CROSS PM-BO
2. CRASH BAR E2_L DOOR HIT/MAIN. MODE=+1
A^3_A
IR-BO
MPU_4
MPU_8
MPU_9
ADV CROSS PM-BO
ADV CROSS PM-BO
ADV CROSS PM-BO
IR-BO
MPU_5
ADV CROSS PM-B1
MPU_DIV,706
1. ADV @ 706 *
2. CNT @ 706 *
3. ADV FILLS CNT @ 706
MPU_706
1. VALVE 29 OPEN
2. LTK-1 > H_706
t > T_fill
MPU_101
MPU_705
CHECK VALVE 436 FAILED OPEN
MPU_704
VALVE 722 OPEN
LS-722
MPU_102
VALVE 713 OPEN
MPU_703
VALVE 701 OPEN
LS-701
MPU_701
VALVE 719 OPEN
LS-71
MPU_107
MPU_709
MPU_106
MPU*_TK1
MPU_PPC
+


MODE = +1
M_{DIV}
MPU_{OUT}
RES3
RES2
RES1
PM-AL
MTI-AL
MM-AL
IR-AL
MODULE TRANSFER MODE = +1
ΣA^1_i
PM-AL DISABLED
MTI-AL DISABLED
MM-AL DISABLED
IR-AL DISABLED
A^1_{PL-AL}
$\hat{M}_{LDD}$
$\hat{M}_{HSD}$
A^3_{PROC}
LOSS TDR3 SUB-SYSTEM
NMCO SIGNALS TDR3
MC1.0 & MC2.0 SIGNALS TDR3
A^3_{E+}
A^3_{PL-BO}
PM-AR
MTI-AR
MM-AR
IR-AR
IR-E1
GUARD-AR
A^3_A
TDR3
MAIN. MODE=-1
TDR3=+1
PM-AR DISABLED
MTI-AR DISABLED
MM-AL DISABLED
IR-AL DISABLED
IR-E1 DISABLED
A^1_{PL-AR}
1. NMCO APPROVAL
2. MC1.0 APPROVAL
3. MC2.0 APPROVAL
4. A^3_i=0 ∀I
+ T TDR2 >.5 HR
CCTV-C1
CCTV-C2
MM-CCAS
MET-CCAS
Y-CCAS
n-CCAS
GUARD-CCAS
CCTV-C1 DISABLED
CCTV-C2 DISABLED
MM-CCAS DISABLED
$A^1_{PL-CCAS}$
MM = +1
MS = +1
$A^2_{MM-CCAS}$
$A^3_{MPU-CCAS}$
TDR >+1
PARTIAL LOSS TDR3 SUBSYSTEM
LOSS TDR2 SUBSYSTEM
A^2_{PROC}
A^2_{E2}
A^2_{E1}
MC1.0 SIGNALS TDR2
TDR2
1. MC1.0 APPROVAL
2. MC2.0 APPROVAL
3. A^2_i=0 ∀I
STIR, SAMPLE, LOAD-OUT, TRANSFER, MAIN., OR EMER. MODE
+ T TDR1 >.25 HR
MAIN. MODE = +1
$\hat{M}_{ND}$
PART LOSS TDR2 SUBSYSTEM
LOSS TDR1 SUBSYSTEM
A^1_{E3}
A^1_{E2}
A^1_{E1}
MC1.0 SIGNALS TDR1
A^1_{W}
A^1_{PROC}
$A_{V,I}$
Y-BO
IR-BO
PM-BO
MTI-BO
MM-BO
GUARD-BO
TDR3 =+1
STATIC MODE = +1
MM-BO DISABLED
IR-BO DISABLED
PM-BO DISABLED
MTI-BO DISABLED
A^1_{PL-BO}
TDR1
1. MC1.0 APPROVAL
2. A^1_i=0 ∀I
TDR0
MTI-1L
PM-B1
MTI-1R
MTI-1L DISABLED
PM-B1 DISABLED
MTI-1R DISABLED
A^1_{PL-B1}
$*A^3_{AL}$
I = 701,713,719,720
721,722,737,739
+
-

1426 023

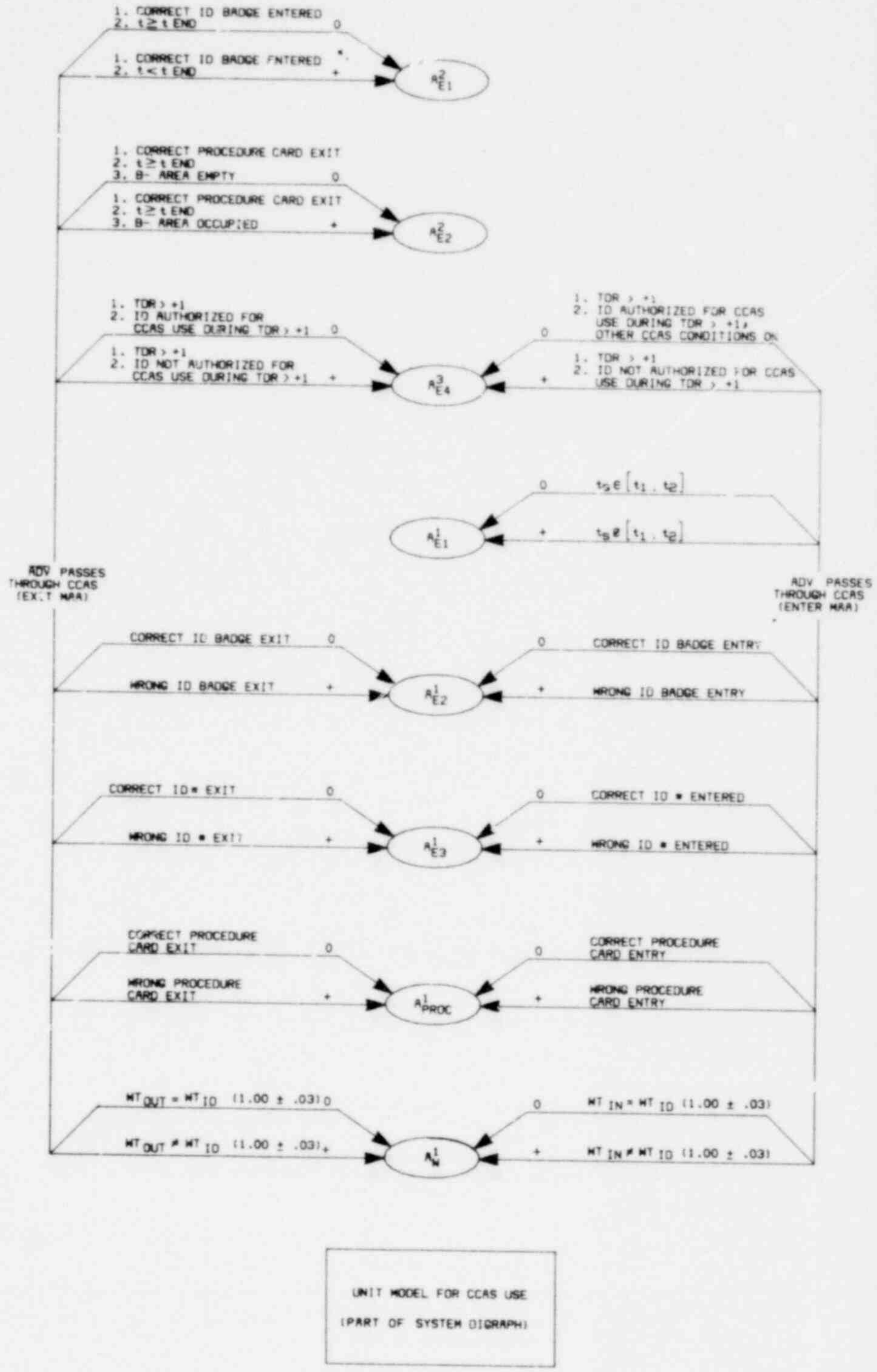
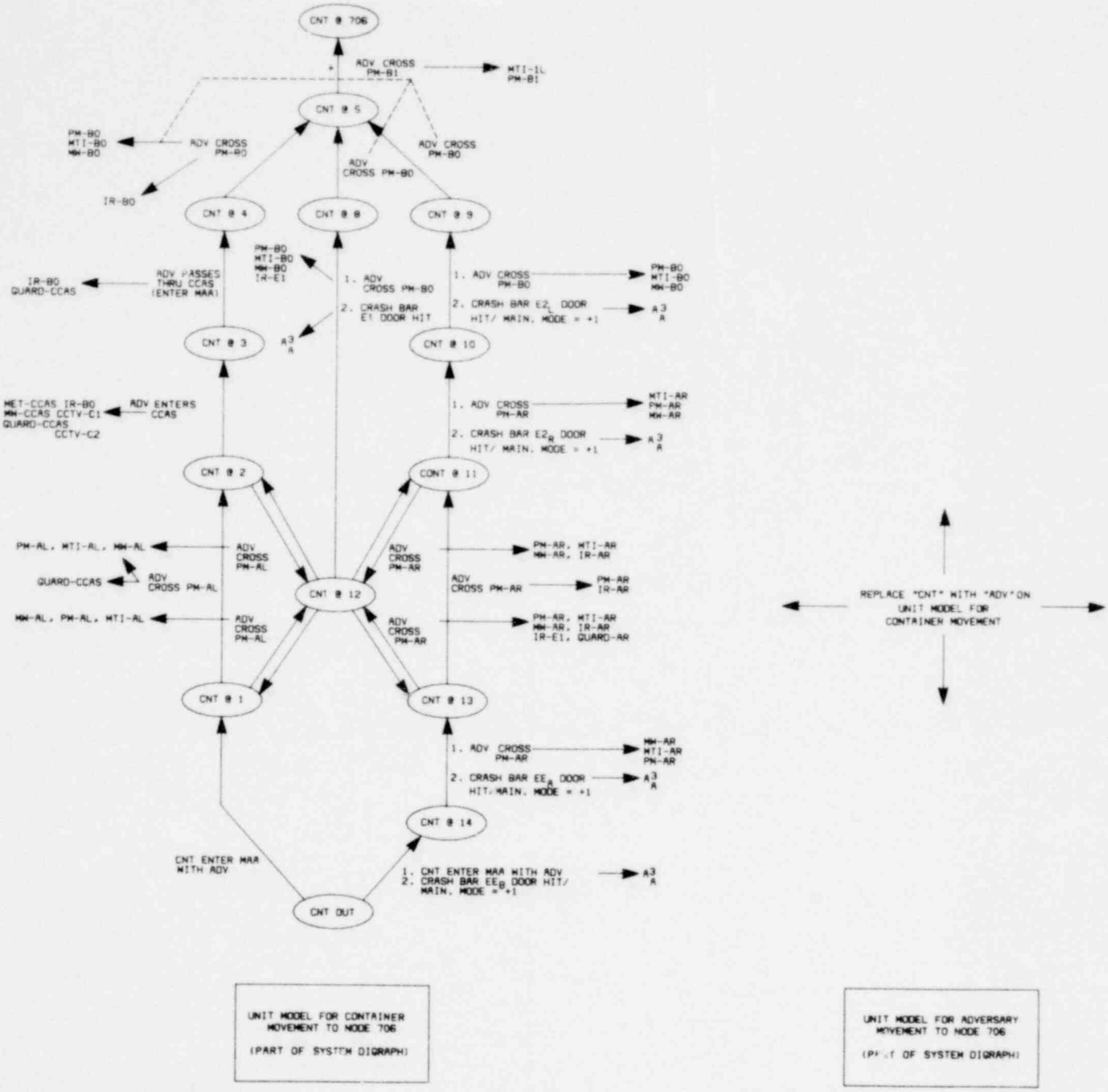

1. CORRECT ID BADGE ENTERED
2. t≥t END
0
1. CORRECT ID BADGE FNTERED
2. t<t END
+
A^2_{E1}
1. CORRECT PROCEDURE CARD EXIT
2. t≥t END
3. B- AREA EMPTY
0
1. CORRECT PROCEDURE CARD EXIT
2. t≥t END
3. B- AREA OCCUPIED
+
A^2_{E2}
1. TDR > +1
2. ID AUTHORIZED FOR CCAS USE DURING TDR > +1
0
1. TDR > +1
2. ID NOT AUTHORIZED FOR CCAS USE DURING TDR > +1
+
A^3_{E4}
1. TDR > +1
2. ID AUTHORIZED FOR CCAS USE DURING TDR > +1, OTHER CCAS CONDITIONS OK
0
1. TDR > +1
2. ID NOT AUTHORIZED FOR CCAS USE DURING TDR > +1
+
0
$t_s \in [t_1, t_2]$
A^1_{E1}
+
$t_s \notin [t_1, t_2]$
ADV PASSES THROUGH CCAS (EXIT MAA)
ADV PASSES THROUGH CCAS (ENTER MAA)
CORRECT ID BADGE EXIT
0
WRONG ID BADGE EXIT
+
A^1_{E2}
0
CORRECT ID BADGE ENTRY
+
WRONG ID BADGE ENTRY
CORRECT ID # EXIT
0
WRONG ID # EXIT
+
A^1_{E3}
0
CORRECT ID # ENTERED
+
WRONG ID # ENTERED
CORRECT PROCEDURE CARD EXIT
0
WRONG PROCEDURE CARD EXIT
+
A^1_{PROC}
0
CORRECT PROCEDURE CARD ENTRY
+
WRONG PROCEDURE CARD ENTRY
$WT_{OUT} = WT_{ID}$ (1.00 ± .03) 0
$WT_{OUT} \neq WT_{ID}$ (1.00 ± .03) +
A^1_W
0
$WT_{IN} = WT_{ID}$ (1.00 ± .03)
+
$WT_{IN} \neq WT_{ID}$ (1.00 ± .03)
UNIT MODEL FOR CCAS USE
(PART OF SYSTEM DIGRAPH)

FIG. C-1. Test Bed design



system digraph for SNM diversion at pump washout line (706).
(Sheet 2 of 6)

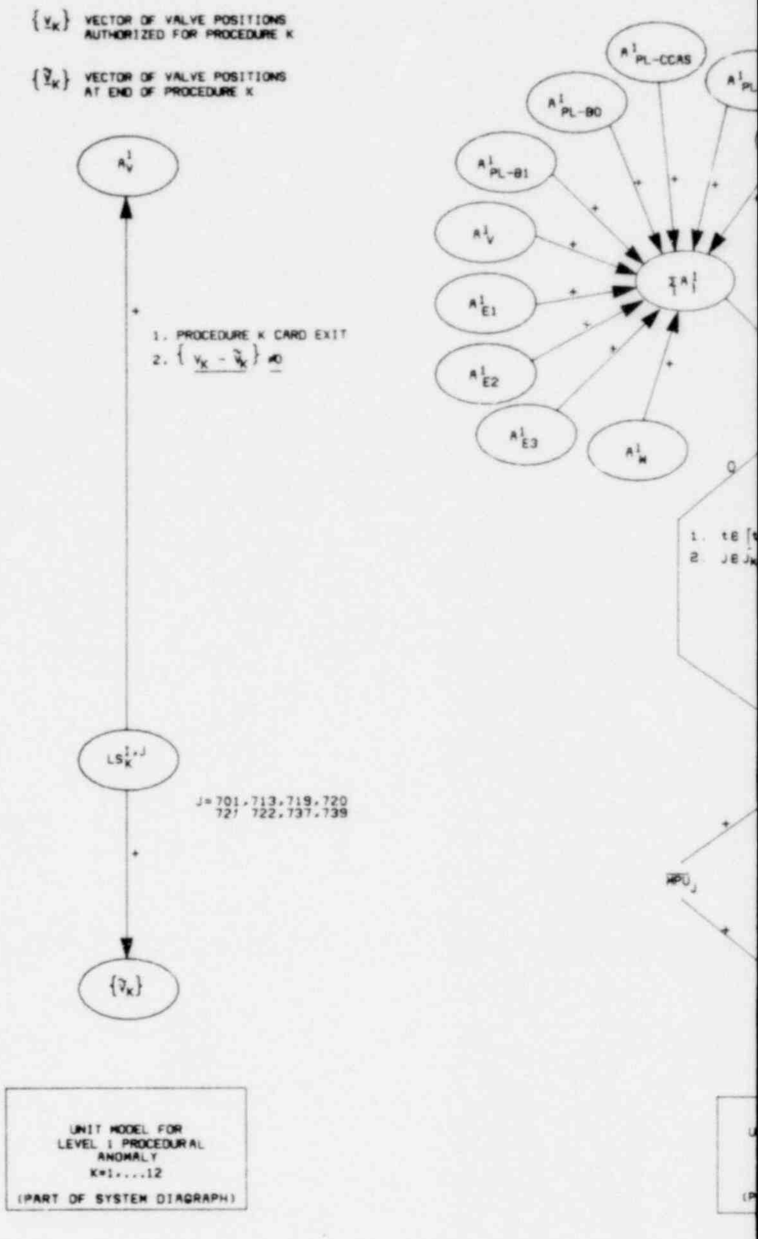
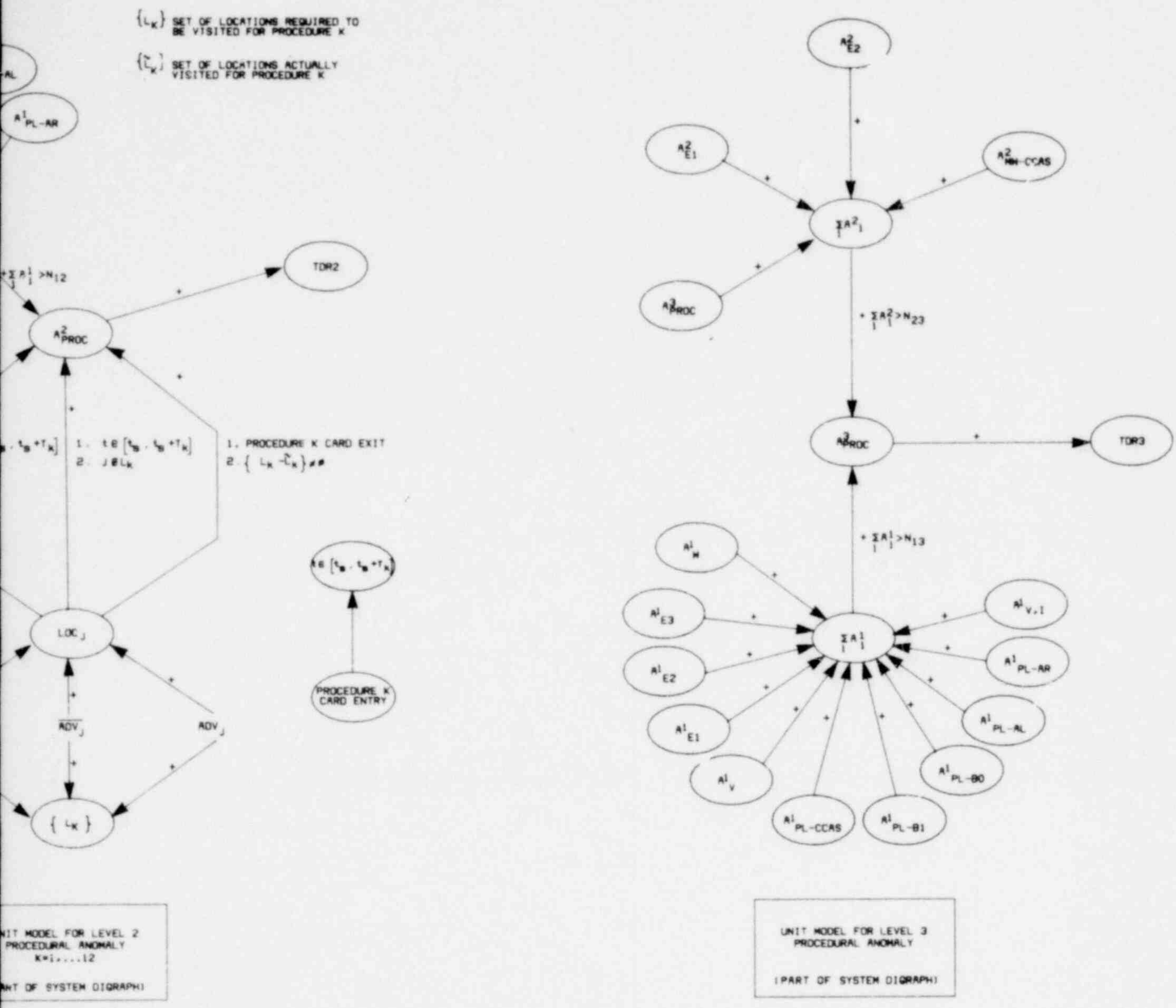

{$\underline{v}_K$} VECTOR OF VALVE POSITIONS AUTHORIZED FOR PROCEDURE K
{$\tilde{\underline{v}}_K$} VECTOR OF VALVE POSITIONS AT END OF PROCEDURE K
A^1_V
+
1. PROCEDURE K CARD EXIT
2. { $\underline{v_K - \tilde{v}_K}$ } $\underline{\neq 0}$
$LS^{I,J}_K$
J=701,713,719,720 721 722,737,739
+
{$\tilde{v}_K$}
UNIT MODEL FOR LEVEL 1 PROCEDURAL ANOMALY K=1,...,12
(PART OF SYSTEM DIAGRAPH)
$A^1_{PL-CCAS}$
A^1_{PL}
A^1_{PL-BO}
A^1_{PL-BI}
A^1_V
A^1_{E1}
A^1_{E2}
A^1_{E3}
A^1_W
$\sum_i A^1_i$
+
0
1. t∈[t
2. J∈J
$\overline{HPU}_J$
+
U
(P

Fig. C-1. Test Bed



design system digraph for SNM diversion at pump washout line (706).
(Sheet 3 of 6)

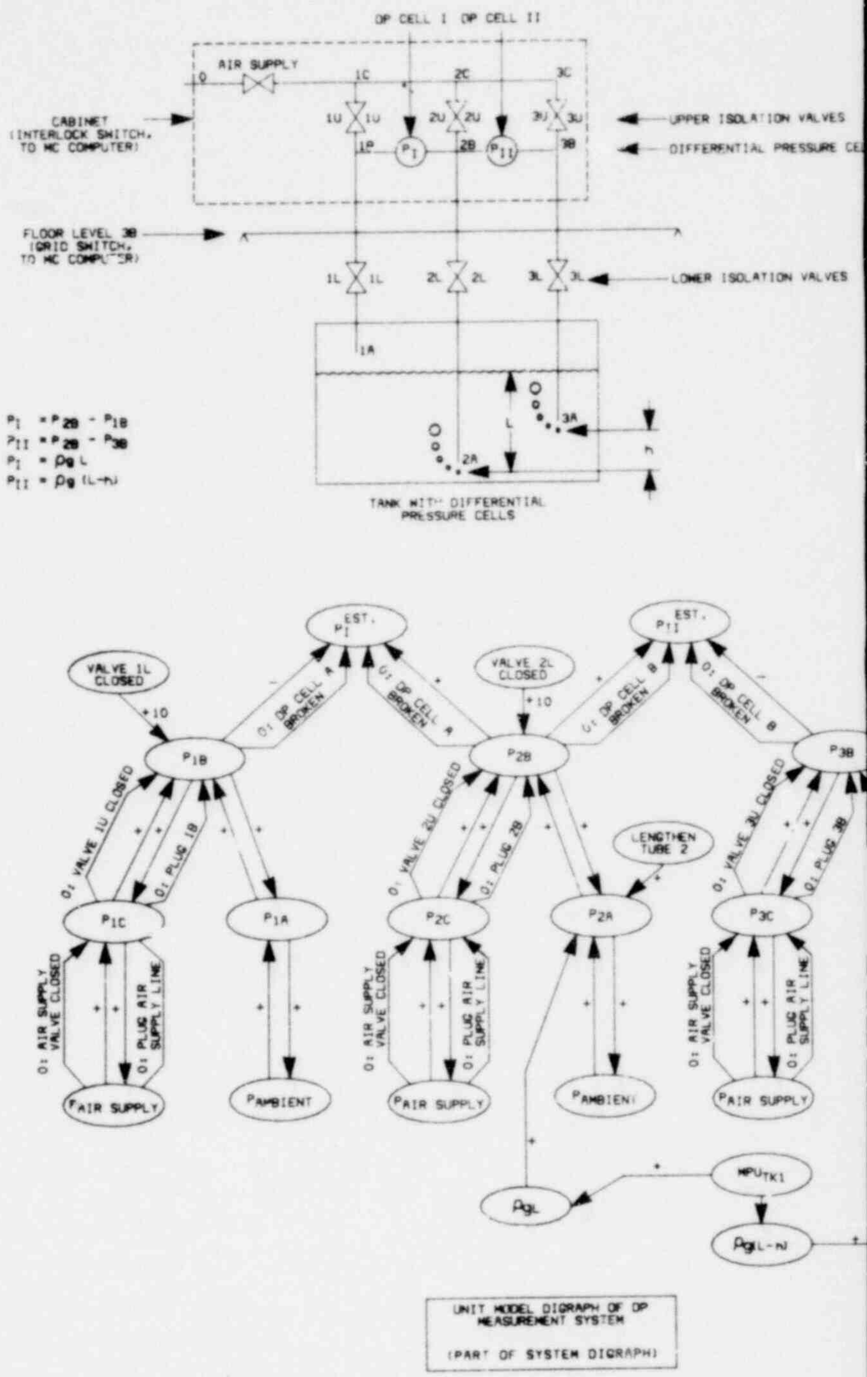
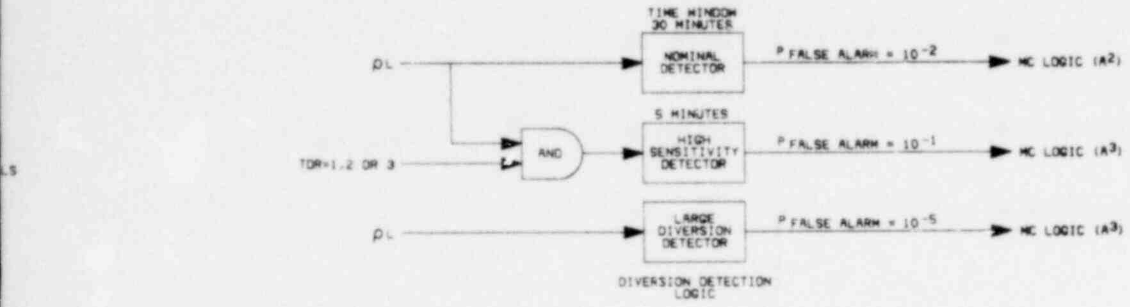


FIG. C-1. Test Bed design



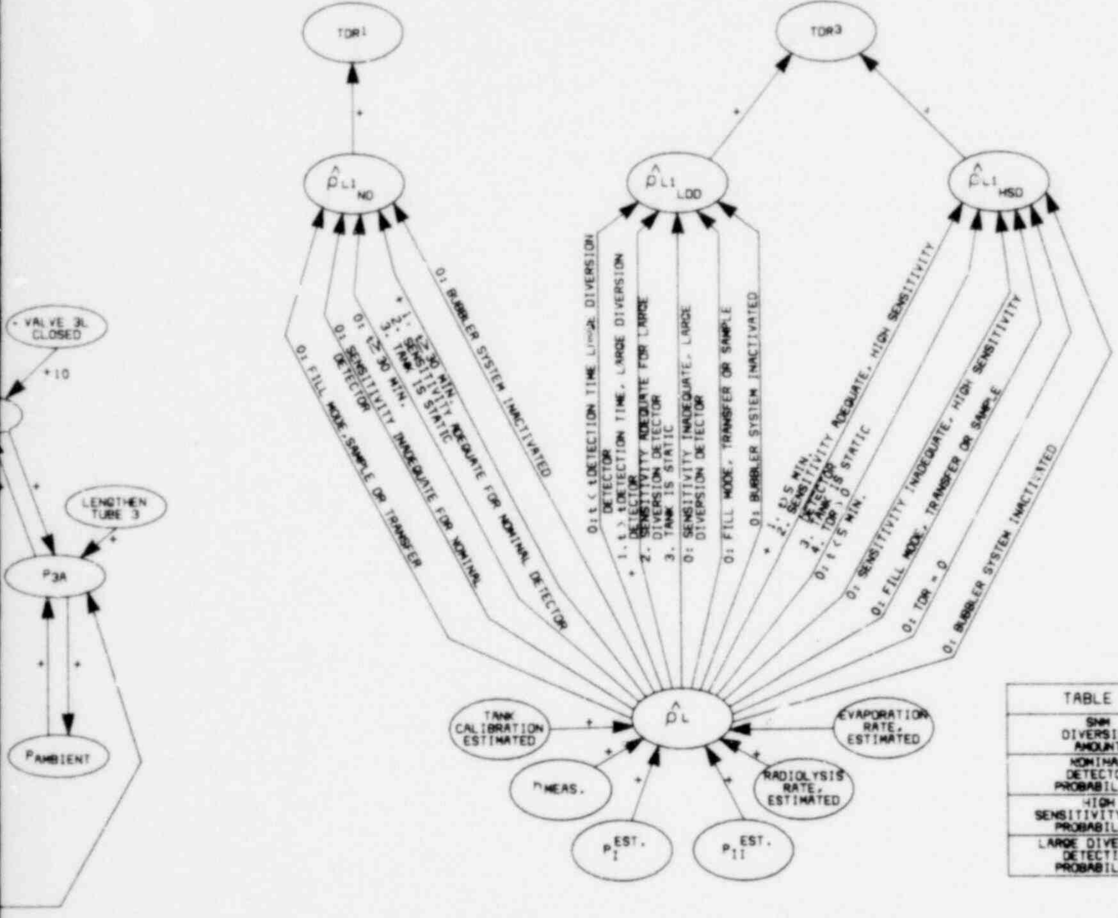

TDR1
TDR3
ρ̂L1 ND
ρ̂L1 LDD
ρ̂L1 HSD
0: BUBBLER SYSTEM INACTIVATED
+ 1: t≥ 30 MIN.
2: SENSITIVITY ADEQUATE FOR NOMINAL DETECTOR
3: TANK IS STATIC
0: t≤ 30 MIN.
0: SENSITIVITY INADEQUATE FOR NOMINAL DETECTOR
0: FILL MODE, SAMPLE OR TRANSFER
0: t < tDETECTION TIME LARGE DIVERSION DETECTOR
+ 1. t > tDETECTION TIME, LARGE DIVERSION DETECTOR
2. SENSITIVITY ADEQUATE FOR LARGE DIVERSION DETECTOR
3. TANK IS STATIC
0: SENSITIVITY INADEQUATE, LARGE DIVERSION DETECTOR
0: FILL MODE, TRANSFER OR SAMPLE
0: BUBBLER SYSTEM INACTIVATED
+ 1: t≥5 MIN.
2. SENSITIVITY ADEQUATE, HIGH SENSITIVITY DETECTOR
3: TANK IS STATIC
4. TDR > 0
0: t < 5 MIN.
0: SENSITIVITY INADEQUATE, HIGH SENSITIVITY
0: FILL MODE, TRANSFER OR SAMPLE
0: TDR = 0
0: BUBBLER SYSTEM INACTIVATED
ρ̂L
TANK CALIBRATION ESTIMATED
hMEAS.
PI EST.
PII EST.
RADIOLYSIS RATE, ESTIMATED
EVAPORATION RATE, ESTIMATED
VALVE 3L CLOSED
+10
+
LENGTHEN TUBE 3
P3A
PAMBIENT

TABLE OF DETECTION PROBABILITIES			
SNM DIVERSION AMOUNT	.5g	200g	5Kg
NOMINAL DETECTOR PROBABILITY	0	.99	1.00
HIGH SENSITIVITY DET. PROBABILITY	0	.99	1.00
LARGE DIVERSION DETECTION PROBABILITY	0	.75 (t>100 SEC.)	1.00 (10 SEC.)

UNIT MODEL DIGRAPH OF ESTIMATION DETECTORS

(PART OF SYSTEM DIGRAPH)

system digraph for SNM diversion at pump washcut line (706).
(Sheet 4 of 6)

1426 029

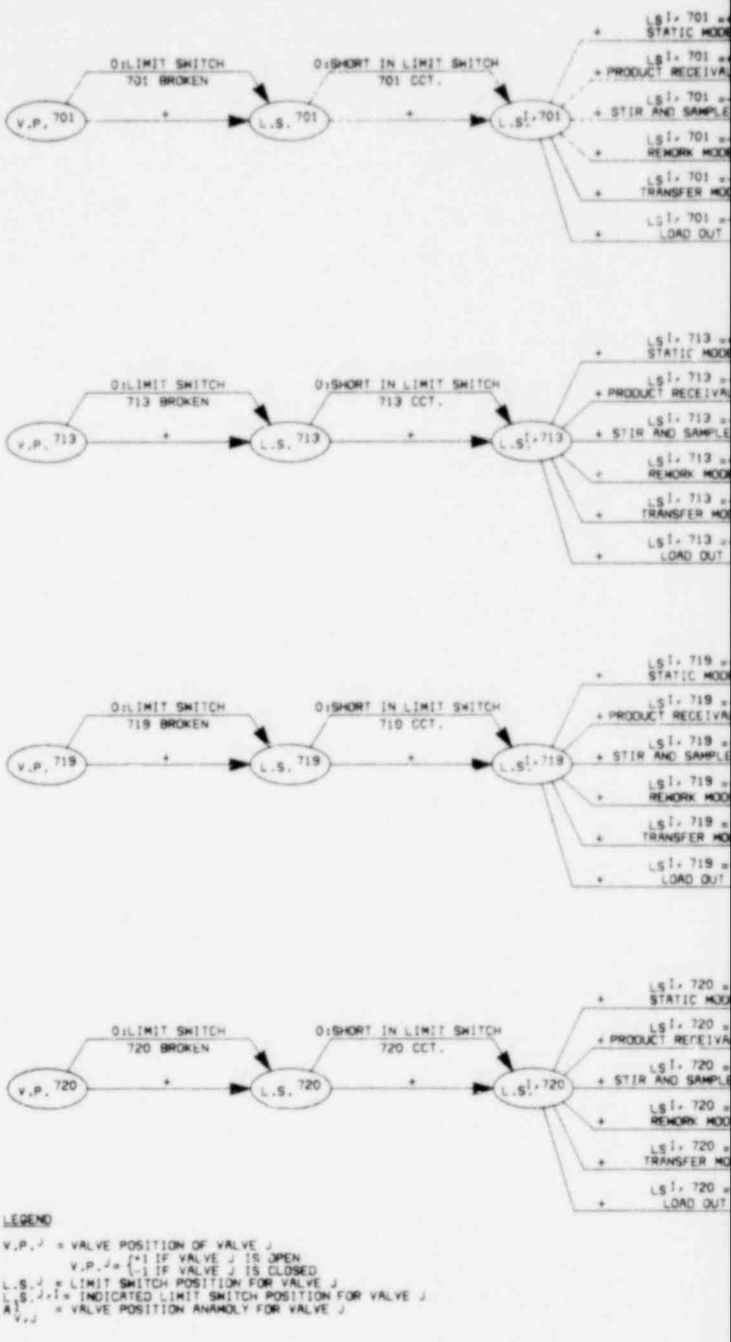
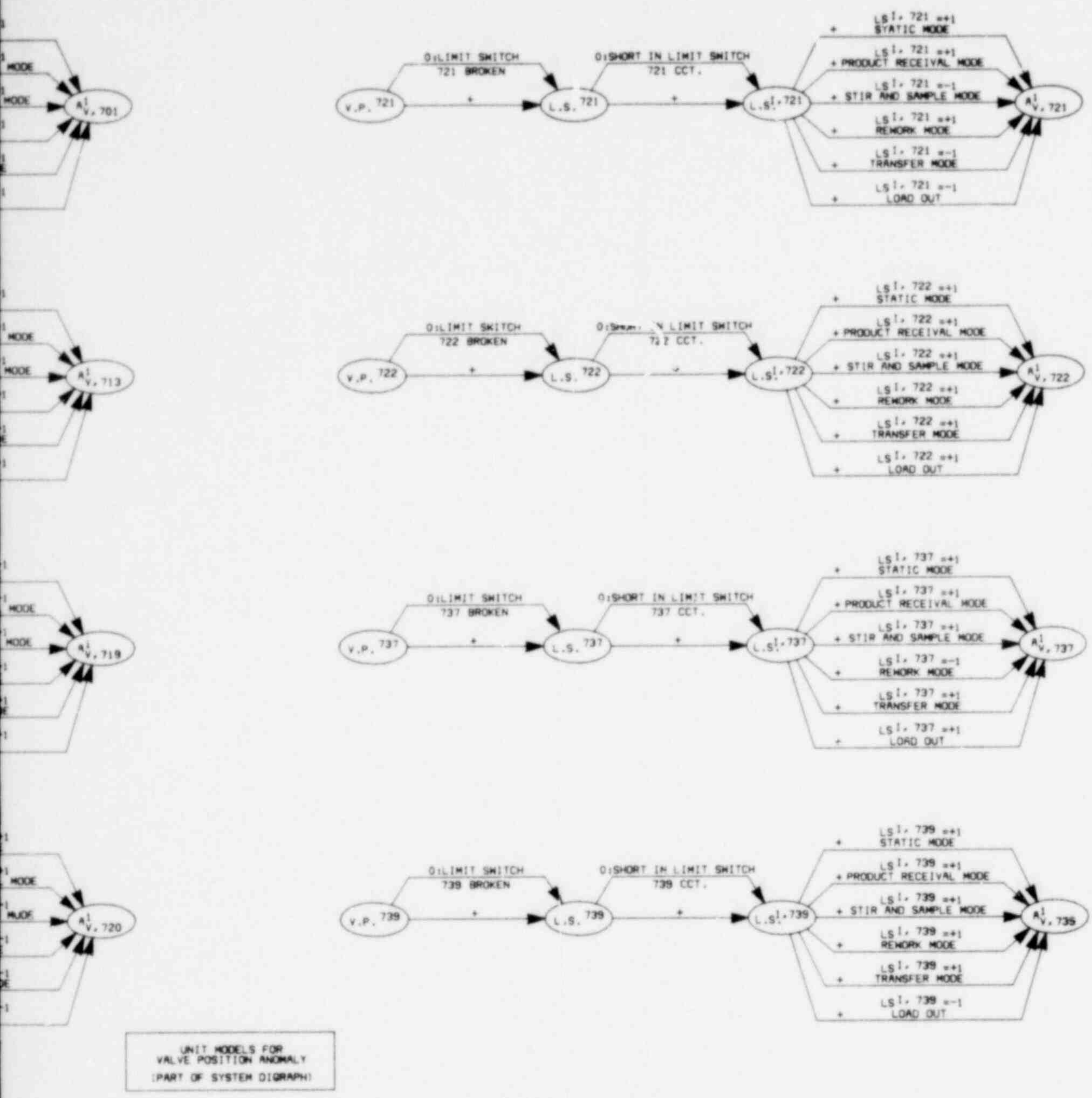


FIG. C-1. Test Bed desigr


MODE
MODE
$A^1_{V,701}$
$A^1_{V,713}$
$A^1_{V,719}$
$A^1_{V,720}$
0:LIMIT SWITCH 721 BROKEN
0:SHORT IN LIMIT SWITCH 721 CCT.
V.P. 721
L.S. 721
L.S.I. 721
+
LS I, 721 =+1 STATIC MODE
LS I, 721 =+1 PRODUCT RECEIVAL MODE
LS I, 721 =-1 STIR AND SAMPLE MODE
LS I, 721 =+1 REWORK MODE
LS I, 721 =-1 TRANSFER MODE
LS I, 721 =-1 LOAD OUT
$A^1_{V,721}$
0:LIMIT SWITCH 722 BROKEN
0:SHORT IN LIMIT SWITCH 722 CCT.
V.P. 722
L.S. 722
L.S.I. 722
LS I, 722 =+1 STATIC MODE
LS I, 722 =+1 PRODUCT RECEIVAL MODE
LS I, 722 =+1 STIR AND SAMPLE MODE
LS I, 722 =+1 REWORK MODE
LS I, 722 =+1 TRANSFER MODE
LS I, 722 =+1 LOAD OUT
$A^1_{V,722}$
0:LIMIT SWITCH 737 BROKEN
0:SHORT IN LIMIT SWITCH 737 CCT.
V.P. 737
L.S. 737
L.S.I. 737
LS I, 737 =+1 STATIC MODE
LS I, 737 =+1 PRODUCT RECEIVAL MODE
LS I, 737 =+1 STIR AND SAMPLE MODE
LS I, 737 =-1 REWORK MODE
LS I, 737 =+1 TRANSFER MODE
LS I, 737 =+1 LOAD OUT
$A^1_{V,737}$
0:LIMIT SWITCH 739 BROKEN
0:SHORT IN LIMIT SWITCH 739 CCT.
V.P. 739
L.S. 739
L.S.I. 739
LS I, 739 =+1 STATIC MODE
LS I, 739 =+1 PRODUCT RECEIVAL MODE
LS I, 739 =+1 STIR AND SAMPLE MODE
LS I, 739 =+1 REWORK MODE
LS I, 739 =+1 TRANSFER MODE
LS I, 739 =-1 LOAD OUT
$A^1_{V,739}$
UNIT MODELS FOR
VALVE POSITION ANOMALY
(PART OF SYSTEM DIGRAPH)

system digraph for SNM diversion at pump washout line (706).
(Sheet 5 of 6)

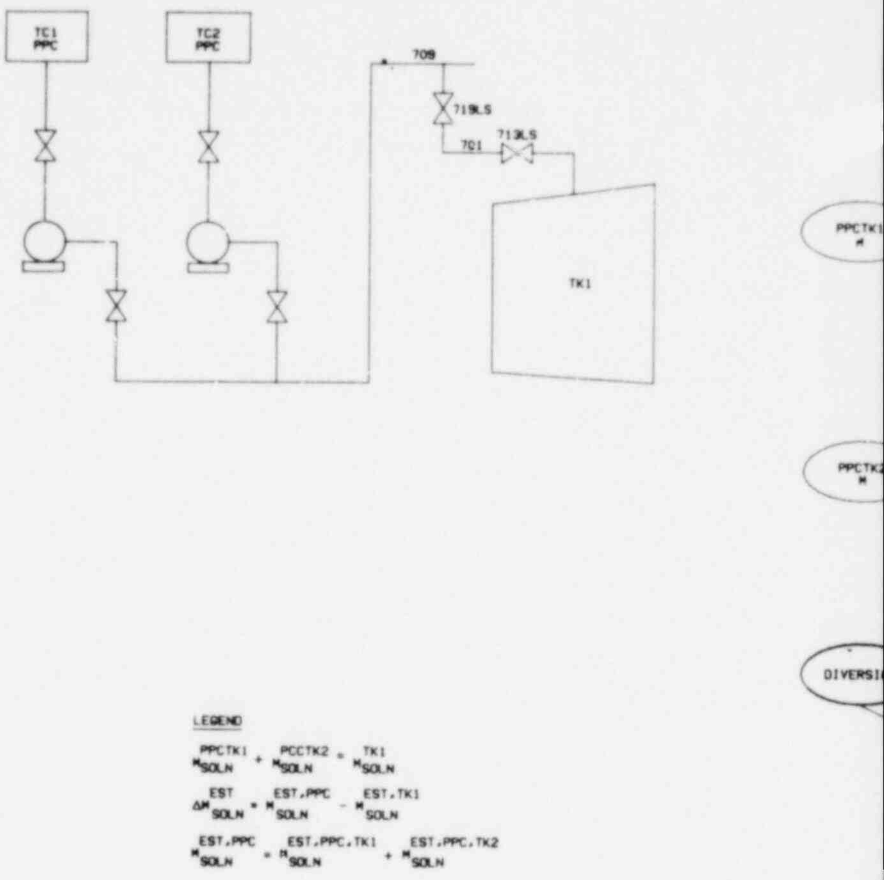
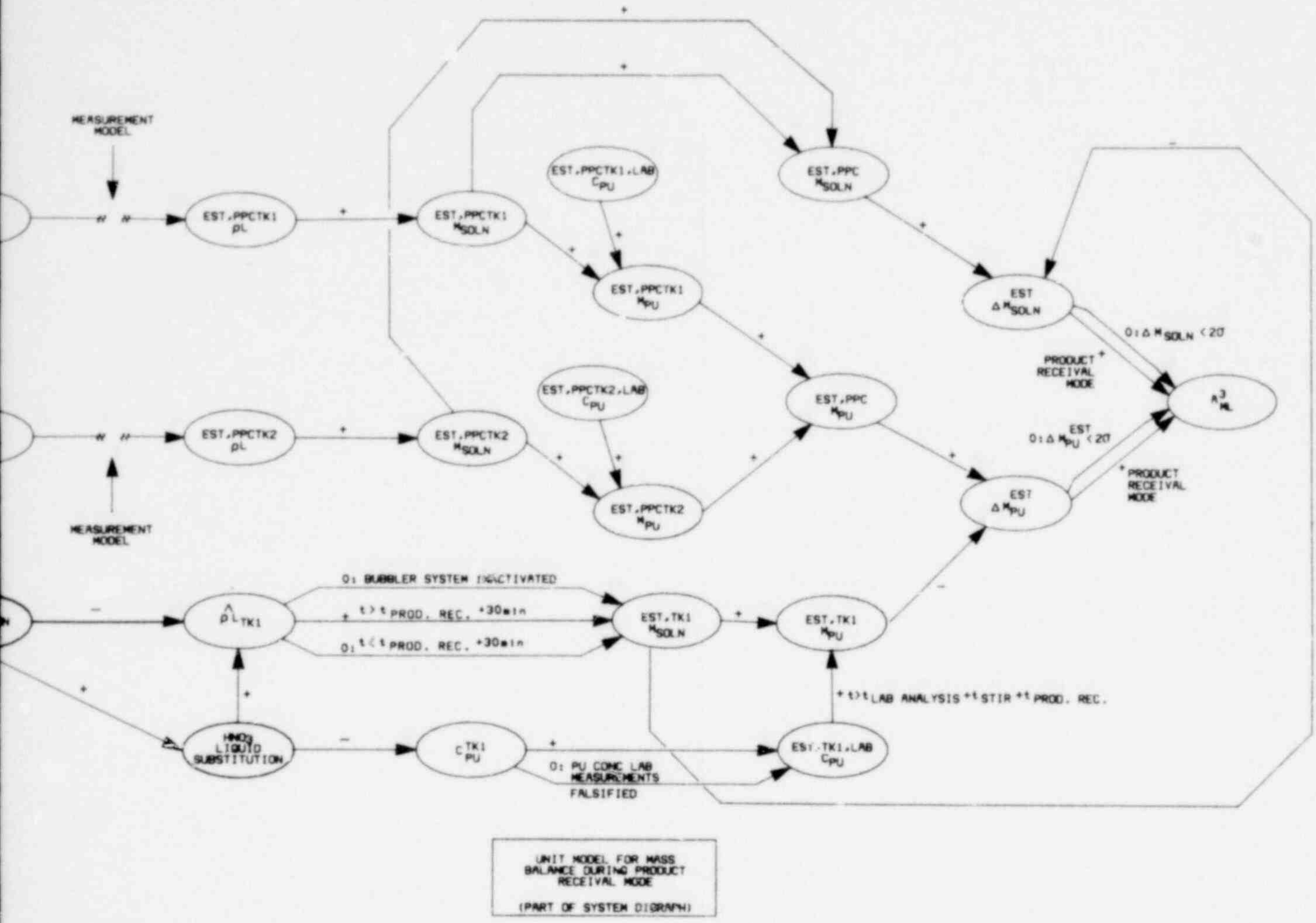

TC1
PPC
TC2
PPC
709
719LS
701
713LS
TK1
PPCTK1
M
PPCTK2
M
DIVERSI
LEGEND
$M^{PPCTK1}_{SOLN} + M^{PCCTK2}_{SOLN} = M^{TK1}_{SOLN}$
$\Delta M^{EST}_{SOLN} = M^{EST,PPC}_{SOLN} - M^{EST,TK1}_{SOLN}$
$M^{EST,PPC}_{SOLN} = M^{EST,PPC,TK1}_{SOLN} + M^{EST,PPC,TK2}_{SOLN}$

FIG. C-1. Test Bed design



system digraph for SNM diversion at pump washou. 'ine (706).
(Sheet 6 of 6)

Appendix D

FAULT TREE FOR THE TEST BED ASSESSMENT

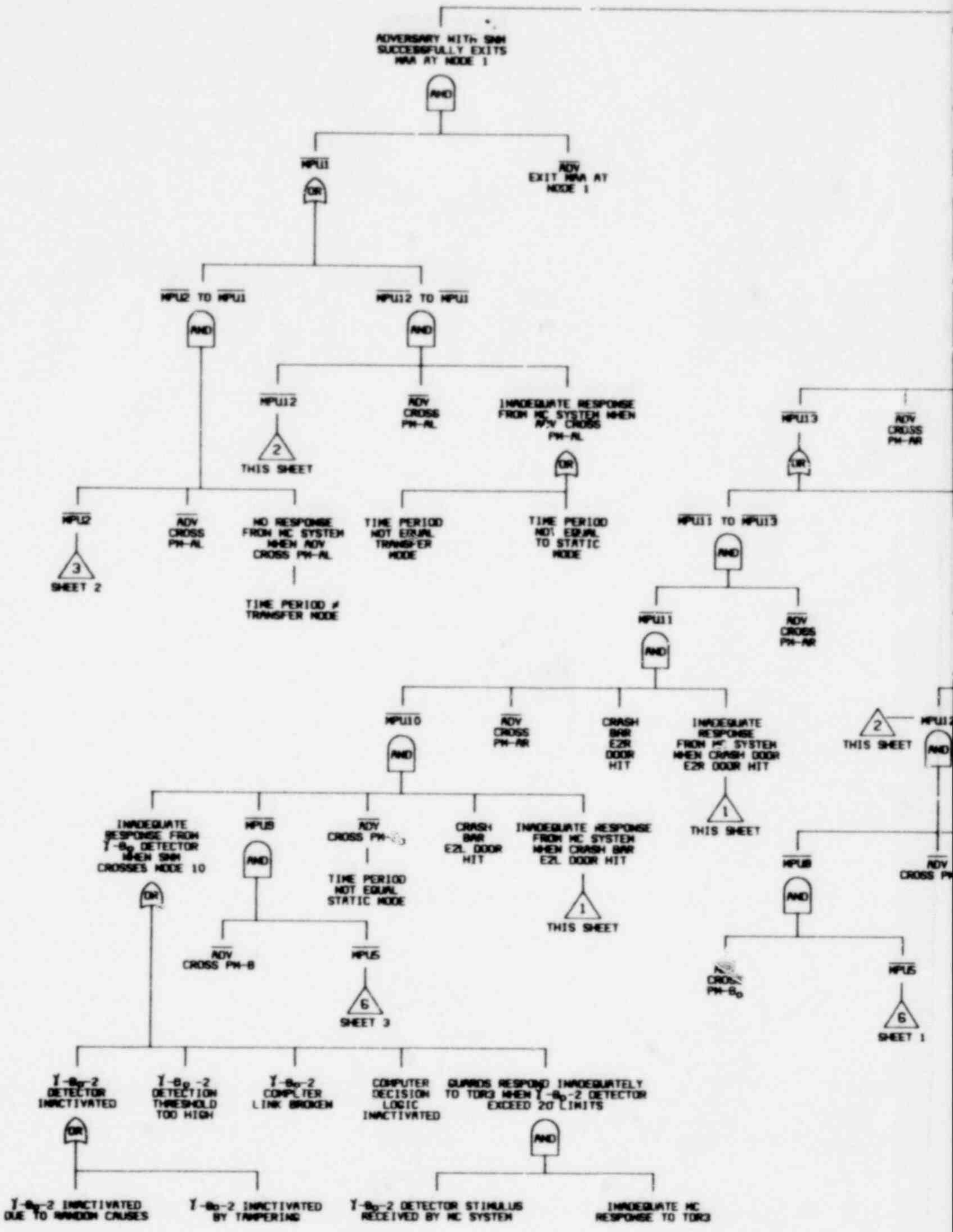
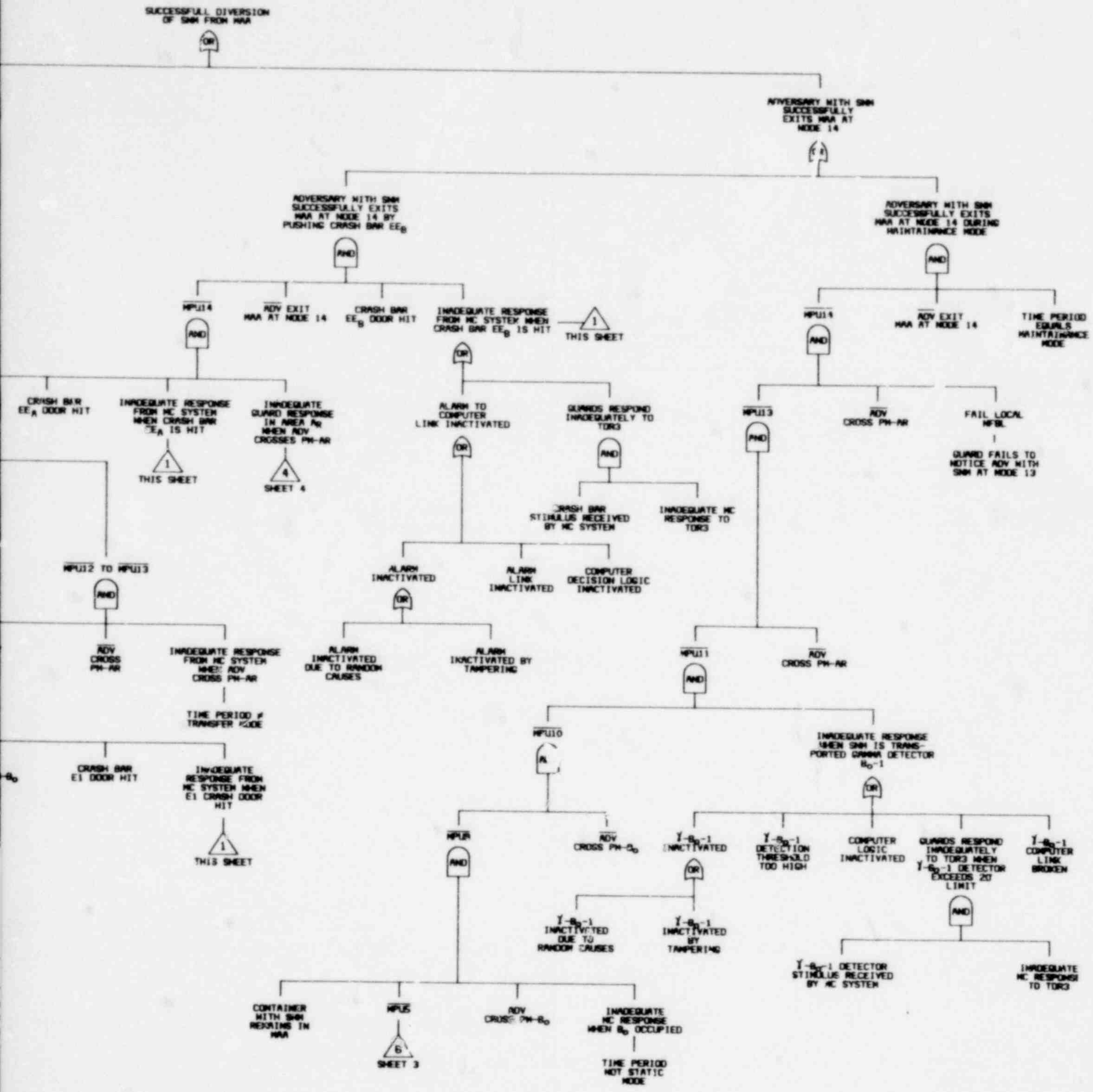

ADVERSARY WITH SNM SUCCESSFULLY EXITS MAA AT NODE 1
AND
$\overline{\text{MPU1}}$
OR
$\overline{\text{ADV}}$ EXIT MAA AT NODE 1
$\overline{\text{MPU2}}$ TO $\overline{\text{MPU1}}$
AND
$\overline{\text{MPU12}}$ TO $\overline{\text{MPU1}}$
AND
$\overline{\text{MPU12}}$
2
THIS SHEET
$\overline{\text{ADV}}$ CROSS PM-AL
INADEQUATE RESPONSE FROM MC SYSTEM WHEN ADV CROSS PM-AL
OR
TIME PERIOD NOT EQUAL TRANSFER MODE
TIME PERIOD NOT EQUAL TO STATIC MODE
$\overline{\text{MPU2}}$
3
SHEET 2
$\overline{\text{ADV}}$ CROSS PM-AL
NO RESPONSE FROM MC SYSTEM WHEN ADV CROSS PM-AL
TIME PERIOD ≠ TRANSFER MODE
$\overline{\text{MPU13}}$
OR
$\overline{\text{ADV}}$ CROSS PM-AR
$\overline{\text{MPU11}}$ TO $\overline{\text{MPU13}}$
AND
$\overline{\text{MPU11}}$
AND
$\overline{\text{ADV}}$ CROSS PM-AR
$\overline{\text{MPU10}}$
AND
$\overline{\text{ADV}}$ CROSS PM-AR
CRASH BAR E2R DOOR HIT
INADEQUATE RESPONSE FROM MC SYSTEM WHEN CRASH DOOR E2R DOOR HIT
1
THIS SHEET
2
THIS SHEET
$\overline{\text{MPU12}}$
AND
INADEQUATE RESPONSE FROM γ-θ_D DETECTOR WHEN SNM CROSSES NODE 10
OR
$\overline{\text{MPU8}}$
AND
$\overline{\text{ADV}}$ CROSS PM-θ_D
TIME PERIOD NOT EQUAL STATIC MODE
CRASH BAR E2L DOOR HIT
INADEQUATE RESPONSE FROM MC SYSTEM WHEN CRASH BAR E2L DOOR HIT
1
THIS SHEET
$\overline{\text{ADV}}$ CROSS PM-B
$\overline{\text{MPU5}}$
6
SHEET 3
$\overline{\text{MPU8}}$
AND
$\overline{\text{ADV}}$ CROSS PM-θ_D
$\overline{\text{MPU5}}$
6
SHEET 1
$\overline{\text{ADV}}$ CROSS PM
γ-θ_D-2 DETECTOR INACTIVATED
OR
γ-θ_D-2 DETECTION THRESHOLD TOO HIGH
γ-θ_D-2 COMPUTER LINK BROKEN
COMPUTER DECISION LOGIC INACTIVATED
GUARDS RESPOND INADEQUATELY TO TDR3 WHEN γ-θ_D-2 DETECTOR EXCEED 2σ LIMITS
AND
γ-θ_D-2 INACTIVATED DUE TO RANDOM CAUSES
γ-θ_D-2 INACTIVATED BY TAMPERING
γ-θ_D-2 DETECTOR STIMULUS RECEIVED BY MC SYSTEM
INADEQUATE MC RESPONSE TO TDR3

FIG. D-1. Test Bed design fault


SUCCESSFULL DIVERSION OF SNM FROM MAA
OR
ADVERSARY WITH SNM SUCCESSFULLY EXITS MAA AT NODE 14
OR
ADVERSARY WITH SNM SUCCESSFULLY EXITS MAA AT NODE 14 BY PUSHING CRASH BAR EE_B
AND
ADVERSARY WITH SNM SUCCESSFULLY EXITS MAA AT NODE 14 DURING MAINTAINANCE MODE
AND
$\overline{\text{MPU14}}$
AND
$\overline{\text{ADV}}$ EXIT MAA AT NODE 14
CRASH BAR EE_B DOOR HIT
INADEQUATE RESPONSE FROM MC SYSTEM WHEN CRASH BAR EE_B IS HIT
1
THIS SHEET
OR
CRASH BAR EE_A DOOR HIT
INADEQUATE RESPONSE FROM MC SYSTEM WHEN CRASH BAR EE_A IS HIT
1
THIS SHEET
INADEQUATE GUARD RESPONSE IN AREA A_R WHEN ADV CROSSES PH-AR
4
SHEET 4
ALARM TO COMPUTER LINK INACTIVATED
OR
GUARDS RESPOND INADEQUATELY TO TDR3
AND
CRASH BAR STIMULUS RECEIVED BY MC SYSTEM
INADEQUATE MC RESPONSE TO TDR3
ALARM INACTIVATED
OR
ALARM LINK INACTIVATED
COMPUTER DECISION LOGIC INACTIVATED
ALARM INACTIVATED DUE TO RANDOM CAUSES
ALARM INACTIVATED BY TAMPERING
$\overline{\text{MPU12}}$ TO $\overline{\text{MPU13}}$
AND
$\overline{\text{ADV}}$ CROSS PH-AR
INADEQUATE RESPONSE FROM MC SYSTEM WHEN ADV CROSS PH-AR
TIME PERIOD ≠ TRANSFER MODE
-θ_D
CRASH BAR E1 DOOR HIT
INADEQUATE RESPONSE FROM MC SYSTEM WHEN E1 CRASH DOOR HIT
1
THIS SHEET
$\overline{\text{MPU14}}$
AND
$\overline{\text{ADV}}$ EXIT MAA AT NODE 14
TIME PERIOD EQUALS MAINTAINANCE MODE
$\overline{\text{MPU13}}$
AND
$\overline{\text{ADV}}$ CROSS PH-AR
FAIL LOCAL NFBL
GUARD FAILS TO NOTICE ADV WITH SNM AT NODE 13
$\overline{\text{MPU11}}$
AND
$\overline{\text{ADV}}$ CROSS PH-AR
$\overline{\text{MPU10}}$
A
INADEQUATE RESPONSE WHEN SNM IS TRANSPORTED GAMMA DETECTOR θ_D-1
OR
$\overline{\text{MPU9}}$
AND
$\overline{\text{ADV}}$ CROSS PH-θ_D
γ-θ_D-1 INACTIVATED
OR
γ-θ_D-1 DETECTION THRESHOLD TOO HIGH
COMPUTER LOGIC INACTIVATED
GUARDS RESPOND INADEQUATELY TO TDR3 WHEN γ-θ_D-1 DETECTOR EXCEEDS 2σ LIMIT
AND
γ-θ_D-1 COMPUTER LINK BROKEN
γ-θ_D-1 INACTIVATED DUE TO RANDOM CAUSES
γ-θ_D-1 INACTIVATED BY TAMPERING
γ-θ_D-1 DETECTOR STIMULUS RECEIVED BY MC SYSTEM
INADEQUATE MC RESPONSE TO TDR3
CONTAINER WITH SNM REMAINS IN MAA
$\overline{\text{MPU5}}$
6
SHEET 3
ADV CROSS PH-θ_D
INADEQUATE MC RESPONSE WHEN θ_D OCCUPIED
TIME PERIOD NOT STATIC MODE

tree for SNM diversion at pump washout line (706).
(Sheet 1 of 5)

1426 03

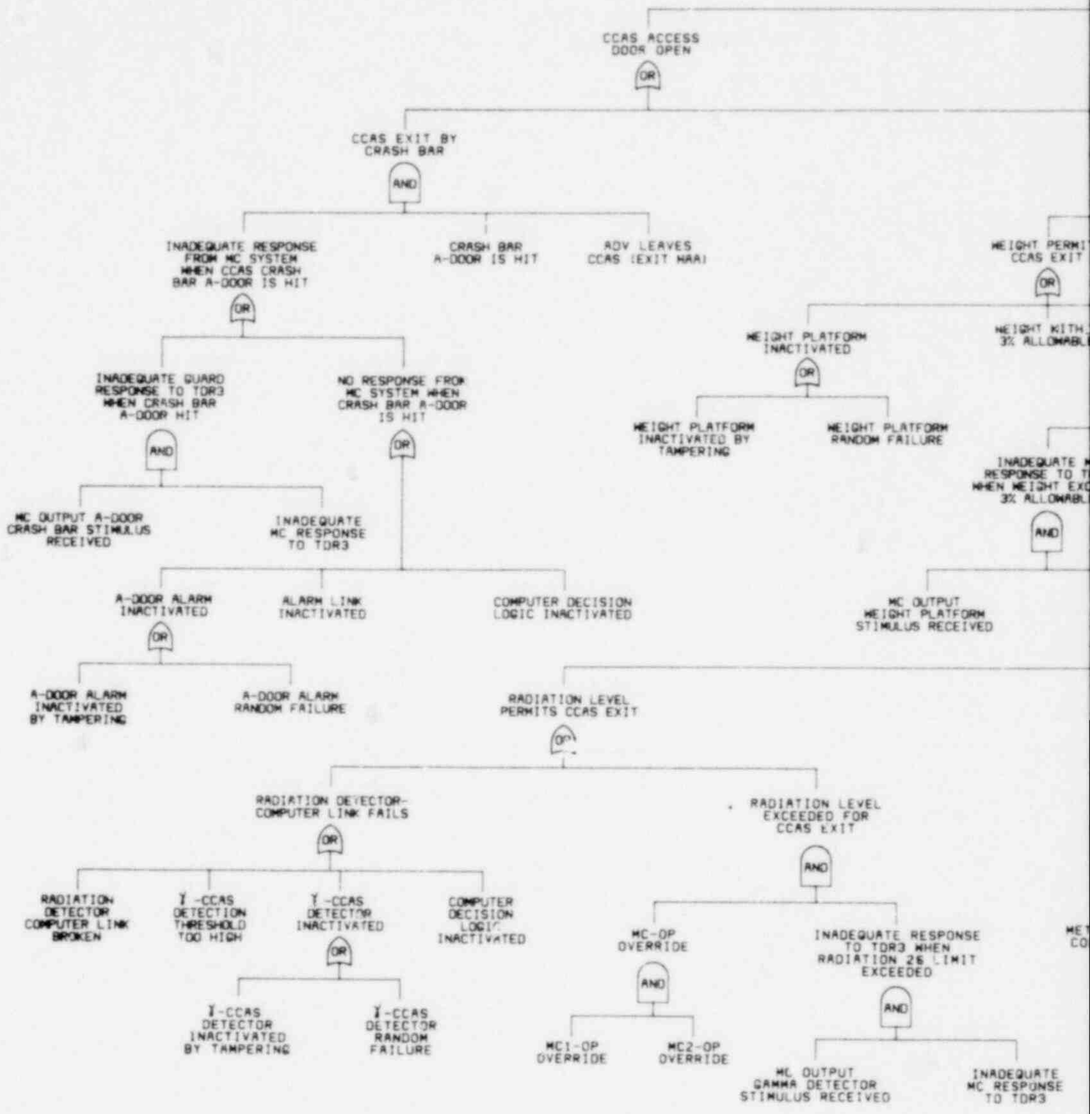
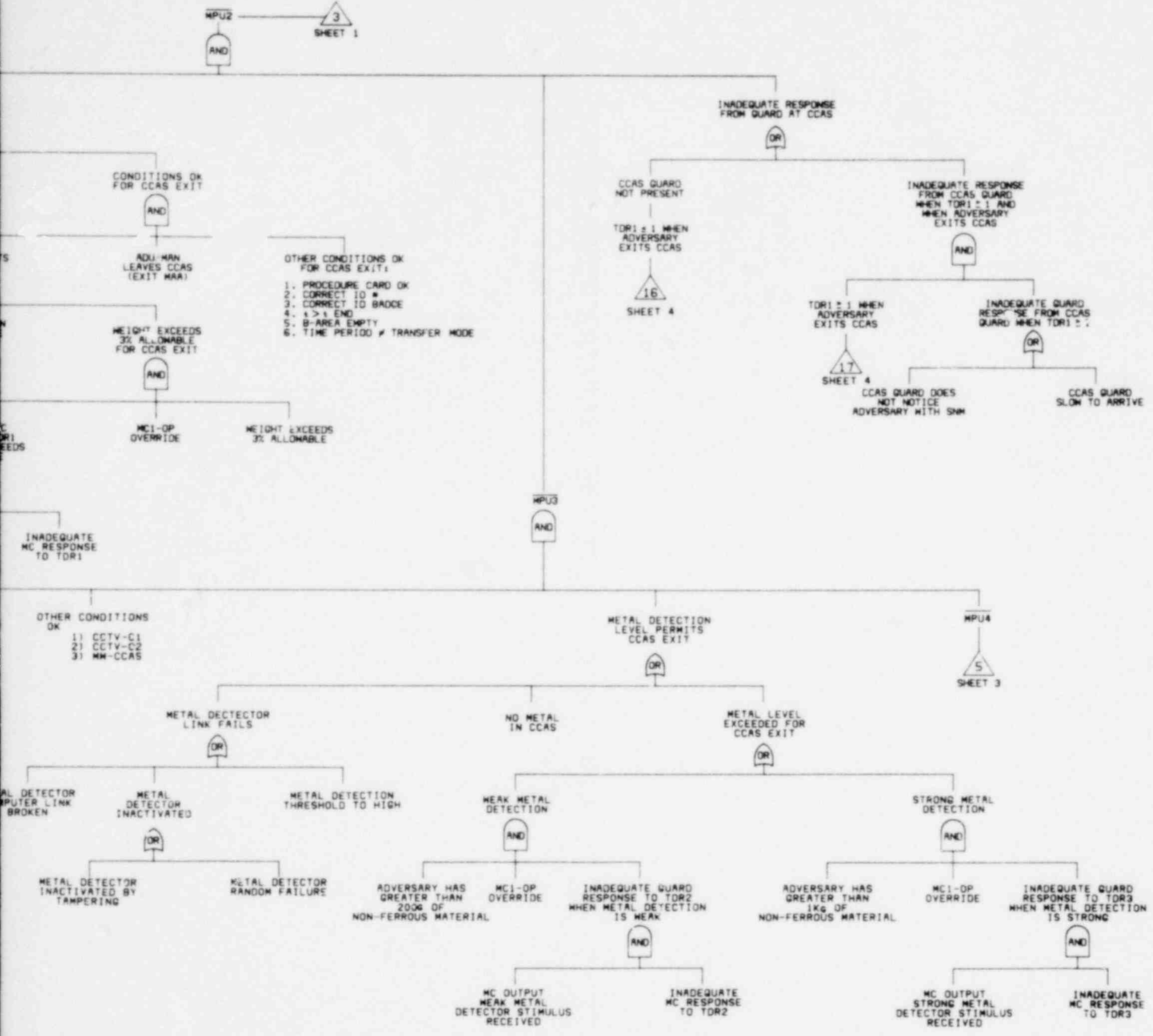

CCAS ACCESS DOOR OPEN
OR
CCAS EXIT BY CRASH BAR
AND
INADEQUATE RESPONSE FROM MC SYSTEM WHEN CCAS CRASH BAR A-DOOR IS HIT
OR
CRASH BAR A-DOOR IS HIT
ADV LEAVES CCAS (EXIT NAA)
INADEQUATE GUARD RESPONSE TO TDR3 WHEN CRASH BAR A-DOOR HIT
AND
NO RESPONSE FROM MC SYSTEM WHEN CRASH BAR A-DOOR IS HIT
OR
MC OUTPUT A-DOOR CRASH BAR STIMULUS RECEIVED
INADEQUATE MC RESPONSE TO TDR3
A-DOOR ALARM INACTIVATED
OR
ALARM LINK INACTIVATED
COMPUTER DECISION LOGIC INACTIVATED
A-DOOR ALARM INACTIVATED BY TAMPERING
A-DOOR ALARM RANDOM FAILURE
WEIGHT PERMI
CCAS EXIT
OR
WEIGHT PLATFORM INACTIVATED
OR
WEIGHT WITH
3% ALLOWABL
WEIGHT PLATFORM INACTIVATED BY TAMPERING
WEIGHT PLATFORM RANDOM FAILURE
INADEQUATE
RESPONSE TO T
WHEN WEIGHT EXC
3% ALLOWABL
AND
MC OUTPUT WEIGHT PLATFORM STIMULUS RECEIVED
RADIATION LEVEL PERMITS CCAS EXIT
OR
RADIATION DETECTOR-COMPUTER LINK FAILS
OR
RADIATION LEVEL EXCEEDED FOR CCAS EXIT
AND
RADIATION DETECTOR COMPUTER LINK BROKEN
γ-CCAS DETECTION THRESHOLD TOO HIGH
γ-CCAS DETECTOR INACTIVATED
OR
COMPUTER DECISION LOGIC INACTIVATED
γ-CCAS DETECTOR INACTIVATED BY TAMPERING
γ-CCAS DETECTOR RANDOM FAILURE
MC-OP OVERRIDE
AND
MC1-OP OVERRIDE
MC2-OP OVERRIDE
INADEQUATE RESPONSE TO TDR3 WHEN RADIATION 2δ LIMIT EXCEEDED
AND
MC OUTPUT GAMMA DETECTOR STIMULUS RECEIVED
INADEQUATE MC RESPONSE TO TDR3
ME
CO

FIG. D-1. Test Bed design f

1426 037


MPU2
3
SHEET 1
AND
INADEQUATE RESPONSE FROM GUARD AT CCAS
OR
CONDITIONS OK FOR CCAS EXIT
AND
S
ADU-MAN LEAVES CCAS (EXIT MAA)
OTHER CONDITIONS OK FOR CCAS EXIT:
1. PROCEDURE CARD OK
2. CORRECT ID #
3. CORRECT ID BADGE
4. t > t END
5. B-AREA EMPTY
6. TIME PERIOD ≠ TRANSFER MODE
CCAS GUARD NOT PRESENT
TDR1 ≤ 1 WHEN ADVERSARY EXITS CCAS
16
SHEET 4
INADEQUATE RESPONSE FROM CCAS GUARD WHEN TDR1 ≥ 1 AND WHEN ADVERSARY EXITS CCAS
AND
TDR1 ≥ 1 WHEN ADVERSARY EXITS CCAS
17
SHEET 4
INADEQUATE GUARD RESPONSE FROM CCAS GUARD WHEN TDR1 ≥ 1
OR
CCAS GUARD DOES NOT NOTICE ADVERSARY WITH SNM
CCAS GUARD SLOW TO ARRIVE
N
WEIGHT EXCEEDS 3% ALLOWABLE FOR CCAS EXIT
AND
C
RI
EEDS
MC1-OP OVERRIDE
WEIGHT EXCEEDS 3% ALLOWABLE
INADEQUATE MC RESPONSE TO TDR1
MPU3
AND
OTHER CONDITIONS OK
1) CCTV-C1
2) CCTV-C2
3) MM-CCAS
METAL DETECTION LEVEL PERMITS CCAS EXIT
OR
MPU4
5
SHEET 3
METAL DECTECTOR LINK FAILS
OR
NO METAL IN CCAS
METAL LEVEL EXCEEDED FOR CCAS EXIT
OR
AL DETECTOR
PUTER LINK
BROKEN
METAL DETECTOR INACTIVATED
OR
METAL DETECTION THRESHOLD TO HIGH
METAL DETECTOR INACTIVATED BY TAMPERING
METAL DETECTOR RANDOM FAILURE
WEAK METAL DETECTION
AND
ADVERSARY HAS GREATER THAN 200G OF NON-FERROUS MATERIAL
MC1-OP OVERRIDE
INADEQUATE GUARD RESPONSE TO TDR2 WHEN METAL DETECTION IS WEAK
AND
MC OUTPUT WEAK METAL DETECTOR STIMULUS RECEIVED
INADEQUATE MC RESPONSE TO TDR2
STRONG METAL DETECTION
AND
ADVERSARY HAS GREATER THAN 1KG OF NON-FERROUS MATERIAL
MC1-OP OVERRIDE
INADEQUATE GUARD RESPONSE TO TDR3 WHEN METAL DETECTION IS STRONG
AND
MC OUTPUT STRONG METAL DETECTOR STIMULUS RECEIVED
INADEQUATE MC RESPONSE TO TDR3

ault tree for SNM diversion at pump washout line (706).
(Sheet 2 of 5)

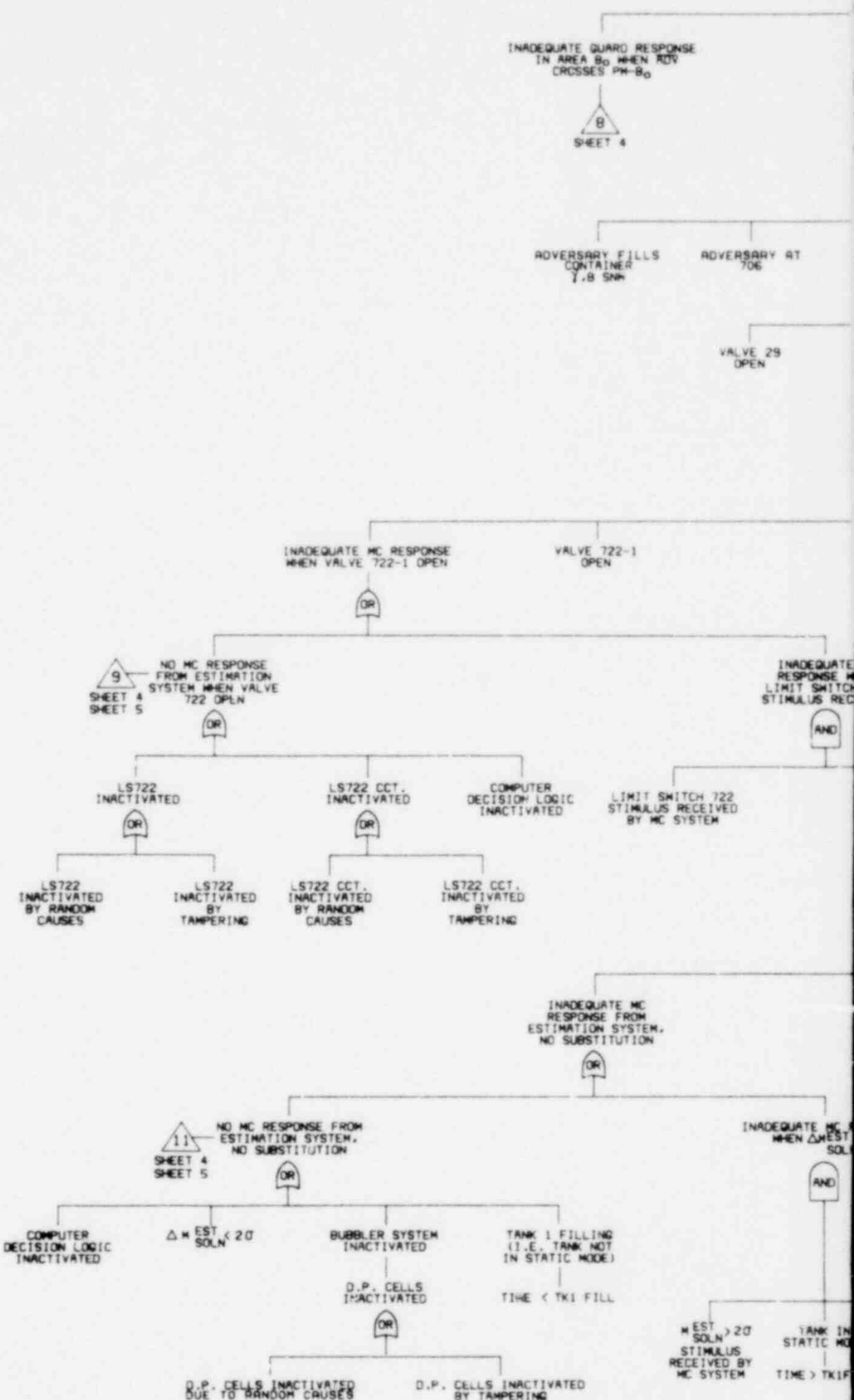
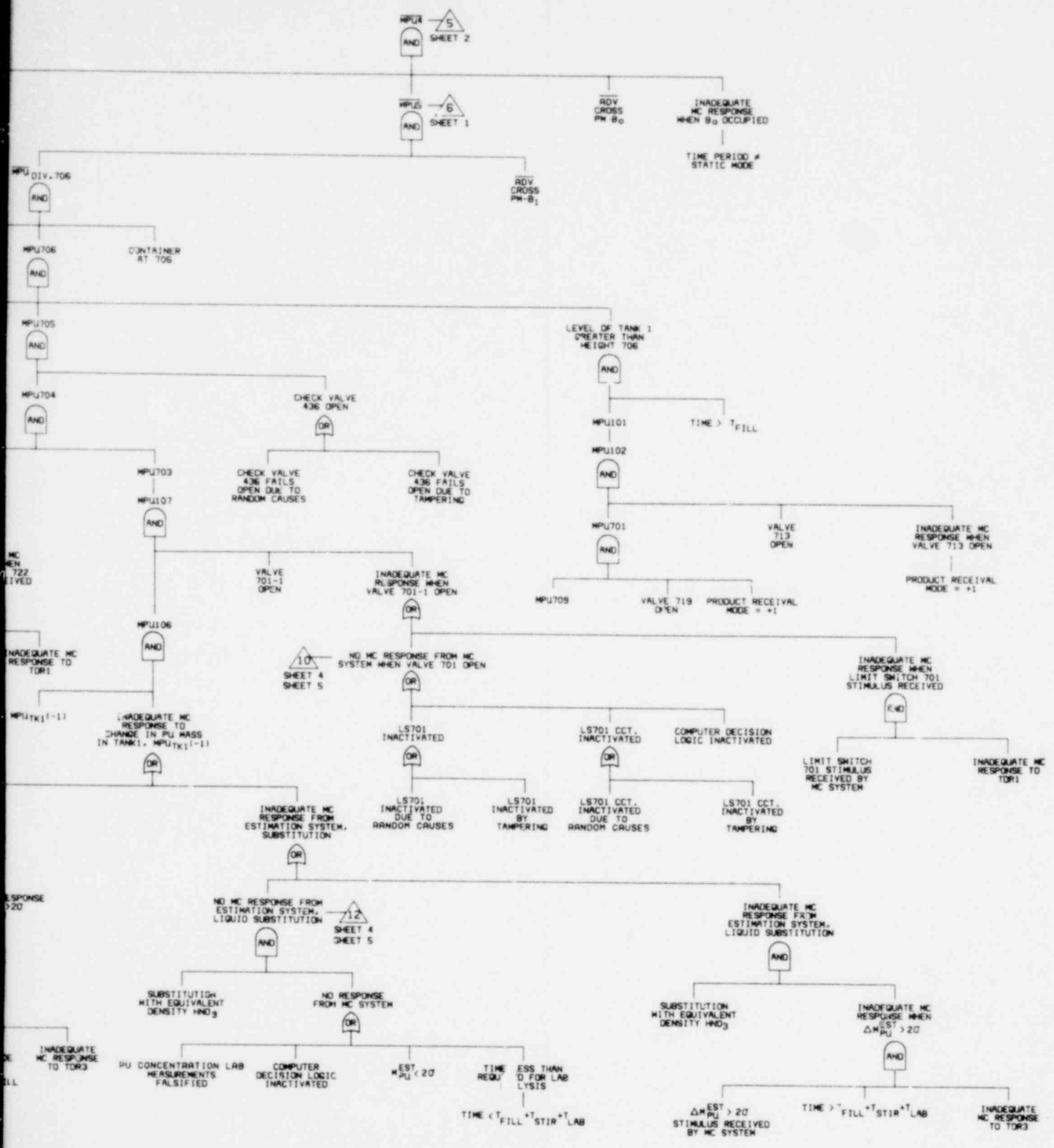

INADEQUATE GUARD RESPONSE IN AREA B_0 WHEN ADV CROSSES PM-B_0
8
SHEET 4
ADVERSARY FILLS CONTAINER ?.8 SNM
ADVERSARY AT 706
VALVE 29 OPEN
INADEQUATE MC RESPONSE WHEN VALVE 722-1 OPEN
OR
VALVE 722-1 OPEN
9
SHEET 4
SHEET 5
NO MC RESPONSE FROM ESTIMATION SYSTEM WHEN VALVE 722 OPLN
OR
INADEQUATE RESPONSE W LIMIT SWITCH STIMULUS REC
AND
LS722 INACTIVATED
OR
LS722 CCT. INACTIVATED
OR
COMPUTER DECISION LOGIC INACTIVATED
LIMIT SWITCH 722 STIMULUS RECEIVED BY MC SYSTEM
LS722 INACTIVATED BY RANDOM CAUSES
LS722 INACTIVATED BY TAMPERING
LS722 CCT. INACTIVATED BY RANDOM CAUSES
LS722 CCT. INACTIVATED BY TAMPERING
INADEQUATE MC RESPONSE FROM ESTIMATION SYSTEM, NO SUBSTITUTION
OR
11
SHEET 4
SHEET 5
NO MC RESPONSE FROM ESTIMATION SYSTEM, NO SUBSTITUTION
OR
INADEQUATE MC WHEN ΔM EST SOL
AND
COMPUTER DECISION LOGIC INACTIVATED
Δ M EST SOLN < 2σ
BUBBLER SYSTEM INACTIVATED
TANK 1 FILLING (I.E. TANK NOT IN STATIC MODE)
D.P. CELLS INACTIVATED
OR
TIME < TK1 FILL
M EST SOLN > 2σ STIMULUS RECEIVED BY MC SYSTEM
TANK IN STATIC MO
TIME > TK1F
D.P. CELLS INACTIVATED DUE TO RANDOM CAUSES
D.P. CELLS INACTIVATED BY TAMPERING

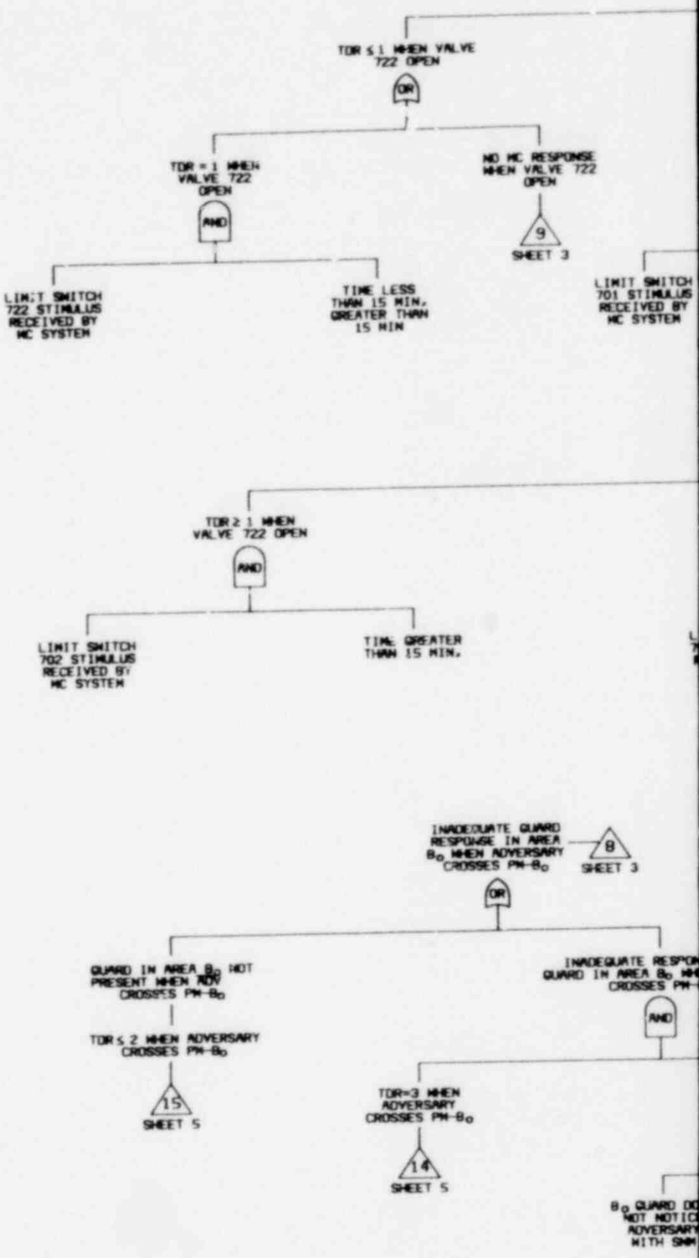
FIG. D-1. Test Bed de



$\overline{MPU4}$
5
SHEET 2
$\overline{MPU5}$
6
SHEET 1
$\overline{ADV}$ CROSS PM B_0
INADEQUATE MC RESPONSE WHEN B_0 OCCUPIED
TIME PERIOD ≠ STATIC MODE
$\overline{MPU}$ DIV.706
$\overline{ADV}$ CROSS PM-B_1
MPU706
CONTAINER AT 706
MPU705
LEVEL OF TANK 1 GREATER THAN HEIGHT 706
MPU704
CHECK VALVE 436 OPEN
MPU101
TIME > T_{FILL}
MPU102
CHECK VALVE 436 FAILS OPEN DUE TO RANDOM CAUSES
CHECK VALVE 436 FAILS OPEN DUE TO TAMPERING
MPU703
MPU107
MPU701
VALVE 713 OPEN
INADEQUATE MC RESPONSE WHEN VALVE 713 OPEN
PRODUCT RECEIVAL MODE = +1
MC
EN
722
IVED
VALVE 701-1 OPEN
INADEQUATE MC RESPONSE WHEN VALVE 701-1 OPEN
MPU709
VALVE 719 OPEN
PRODUCT RECEIVAL MODE = +1
MPU106
INADEQUATE MC RESPONSE TO TOR1
10
SHEET 4
SHEET 5
NO MC RESPONSE FROM MC SYSTEM WHEN VALVE 701 OPEN
INADEQUATE MC RESPONSE WHEN LIMIT SWITCH 701 STIMULUS RECEIVED
$MPU_{TK1}(-1)$
INADEQUATE MC RESPONSE TO CHANGE IN PU MASS IN TANK1, $MPU_{TK1}(-1)$
LS701 INACTIVATED
LS701 CCT. INACTIVATED
COMPUTER DECISION LOGIC INACTIVATED
LIMIT SWITCH 701 STIMULUS RECEIVED BY MC SYSTEM
INADEQUATE MC RESPONSE TO TOR1
INADEQUATE MC RESPONSE FROM ESTIMATION SYSTEM, SUBSTITUTION
LS701 INACTIVATED DUE TO RANDOM CAUSES
LS701 INACTIVATED BY TAMPERING
LS701 CCT. INACTIVATED DUE TO RANDOM CAUSES
LS701 CCT. INACTIVATED BY TAMPERING
ESPONSE
>2σ
NO MC RESPONSE FROM ESTIMATION SYSTEM, LIQUID SUBSTITUTION
12
SHEET 4
SHEET 5
INADEQUATE MC RESPONSE FROM ESTIMATION SYSTEM, LIQUID SUBSTITUTION
SUBSTITUTION WITH EQUIVALENT DENSITY HNO_3
NO RESPONSE FROM MC SYSTEM
SUBSTITUTION WITH EQUIVALENT DENSITY HNO_3
INADEQUATE MC RESPONSE WHEN $\Delta M_{PU}^{EST} > 2\sigma$
DE
ILL
INADEQUATE MC RESPONSE TO TOR3
PU CONCENTRATION LAB MEASUREMENTS FALSIFIED
COMPUTER DECISION LOGIC INACTIVATED
$M_{PU}^{EST} < 2\sigma$
TIME ESS THAN REQU D FOR LAB LYSIS
TIME < $T_{FILL}+T_{STIR}+T_{LAB}$
$\Delta M_{PU}^{EST} > 2\sigma$ STIMULUS RECEIVED BY MC SYSTEM
TIME > $T_{FILL}+T_{STIR}+T_{LAB}$
INADEQUATE MC RESPONSE TO TOR3

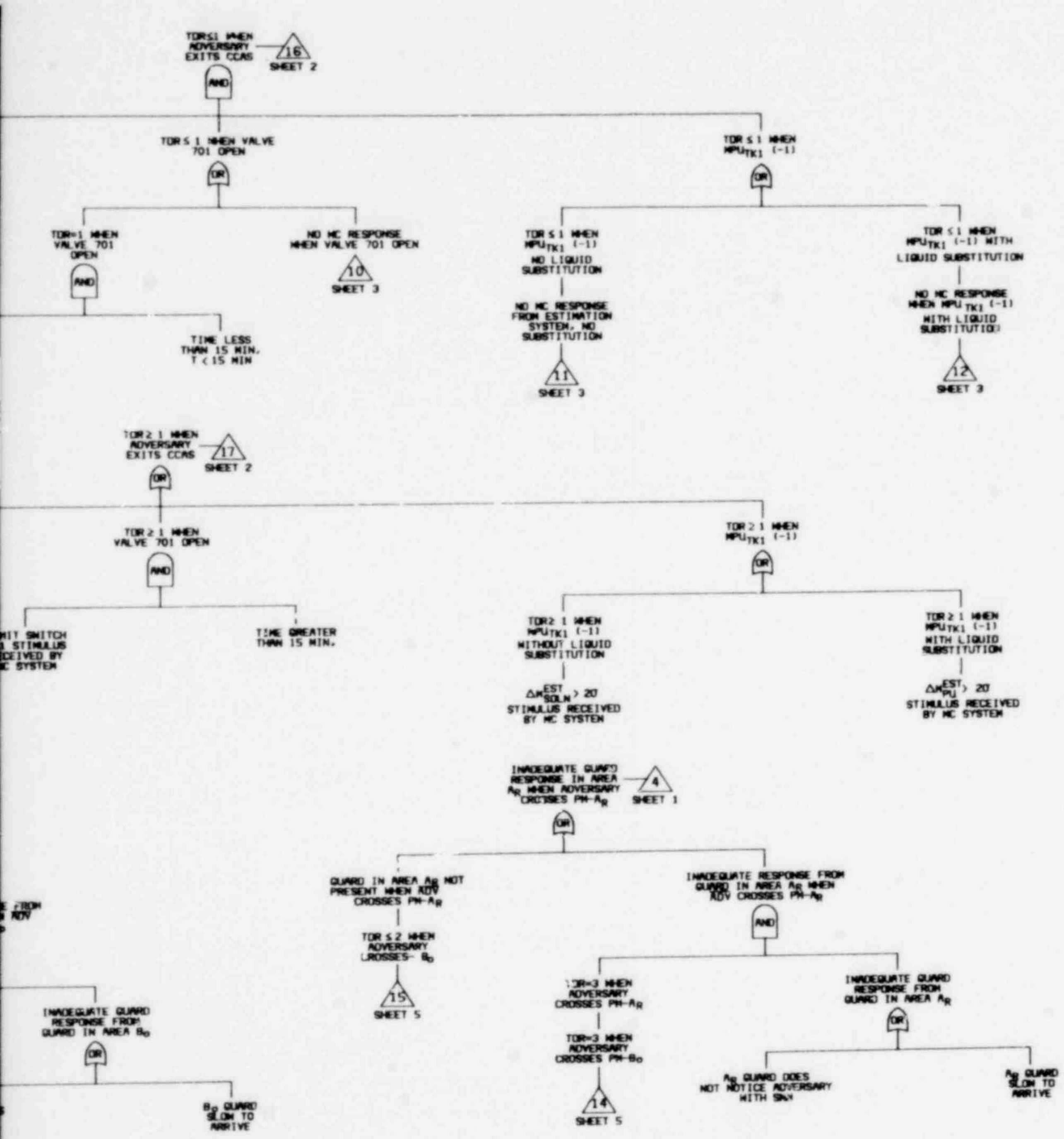
sign fault tree for SNM diversion at pump washout line (706).
(Sheet 3 of ;)

1426 040



TDR ≤ 1 WHEN VALVE 722 OPEN
OR
TDR = 1 WHEN VALVE 722 OPEN
AND
LIMIT SWITCH 722 STIMULUS RECEIVED BY MC SYSTEM
TIME LESS THAN 15 MIN, GREATER THAN 15 MIN
NO MC RESPONSE WHEN VALVE 722 OPEN
9
SHEET 3
LIMIT SWITCH 701 STIMULUS RECEIVED BY MC SYSTEM
TDR ≥ 1 WHEN VALVE 722 OPEN
AND
LIMIT SWITCH 702 STIMULUS RECEIVED BY MC SYSTEM
TIME GREATER THAN 15 MIN.
INADEQUATE GUARD RESPONSE IN AREA B₀ WHEN ADVERSARY CROSSES PM-B₀
8
SHEET 3
OR
GUARD IN AREA B₀ NOT PRESENT WHEN ADV CROSSES PM-B₀
TDR ≤ 2 WHEN ADVERSARY CROSSES PM-B₀
15
SHEET 5
INADEQUATE RESPON GUARD IN AREA B₀ WH CROSSES PM-
AND
TDR=3 WHEN ADVERSARY CROSSES PM-B₀
14
SHEET 5
B₀ GUARD DO NOT NOTIC ADVERSARY WITH SNM

FIG. D-1. Test Bed c



TDR≤1 WHEN ADVERSARY EXITS CCAS
16
SHEET 2
AND
TDR ≤ 1 WHEN VALVE 701 OPEN
OR
TDR=1 WHEN VALVE 701 OPEN
AND
NO MC RESPONSE WHEN VALVE 701 OPEN
10
SHEET 3
TIME LESS THAN 15 MIN. T < 15 MIN
TDR ≤ 1 WHEN MPU_{TK1} (-1)
OR
TDR ≤ 1 WHEN MPU_{TK1} (-1) NO LIQUID SUBSTITUTION
NO MC RESPONSE FROM ESTIMATION SYSTEM, NO SUBSTITUTION
11
SHEET 3
TDR ≤ 1 WHEN MPU_{TK1} (-1) WITH LIQUID SUBSTITUTION
NO MC RESPONSE WHEN MPU_{TK1} (-1) WITH LIQUID SUBSTITUTIO
12
SHEET 3
TDR ≥ 1 WHEN ADVERSARY EXITS CCAS
17
SHEET 2
OR
TDR ≥ 1 WHEN VALVE 701 OPEN
AND
MIT SWITCH STIMULUS CEIVED BY C SYSTEM
TIME GREATER THAN 15 MIN.
TDR ≥ 1 WHEN MPU_{TK1} (-1)
OR
TDR≥ 1 WHEN MPU_{TK1} (-1) WITHOUT LIQUID SUBSTITUTION
$\Delta M^{EST}_{SOLN} > 2\sigma$ STIMULUS RECEIVED BY MC SYSTEM
TDR ≥ 1 WHEN MPU_{TK1} (-1) WITH LIQUID SUBSTITUTION
$\Delta M^{EST}_{PU} > 2\sigma$ STIMULUS RECEIVED BY MC SYSTEM
INADEQUATE GUARD RESPONSE IN AREA A_R WHEN ADVERSARY CROSSES PH-A_R
4
SHEET 1
OR
GUARD IN AREA A_R NOT PRESENT WHEN ADV CROSSES PH-A_R
TDR ≤ 2 WHEN ADVERSARY CROSSES- B_D
15
SHEET 5
INADEQUATE RESPONSE FROM GUARD IN AREA A_R WHEN ADV CROSSES PH-A_R
AND
TDR=3 WHEN ADVERSARY CROSSES PH-A_R
TDR=3 WHEN ADVERSARY CROSSES PH-B_D
14
SHEET 5
INADEQUATE GUARD RESPONSE FROM GUARD IN AREA A_R
OR
A_R GUARD DOES NOT NOTICE ADVERSARY WITH SNM
A_R GUARD SLOW TO ARRIVE
E FROM ADV
INADEQUATE GUARD RESPONSE FROM GUARD IN AREA B_D
OR
B_D GUARD SLOW TO ARRIVE

esign fault tree for SNM diversion at pump washout line (706).

(Sheet 4 of 5)

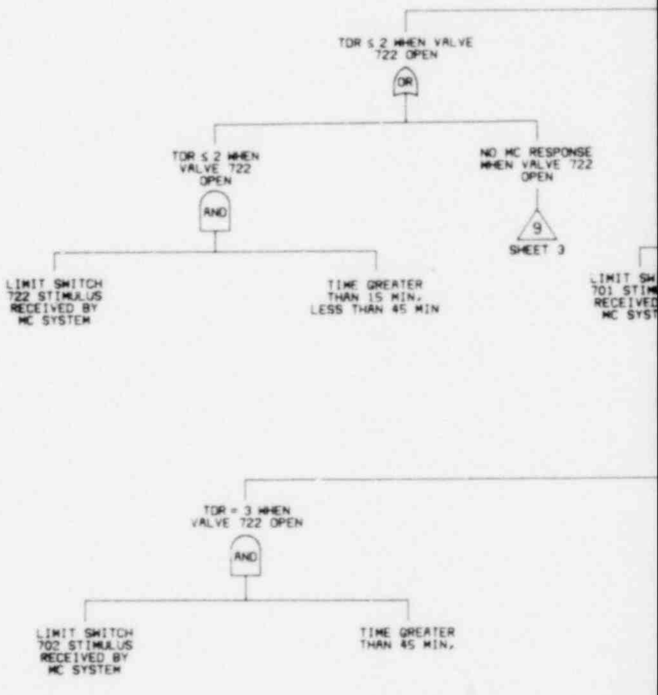
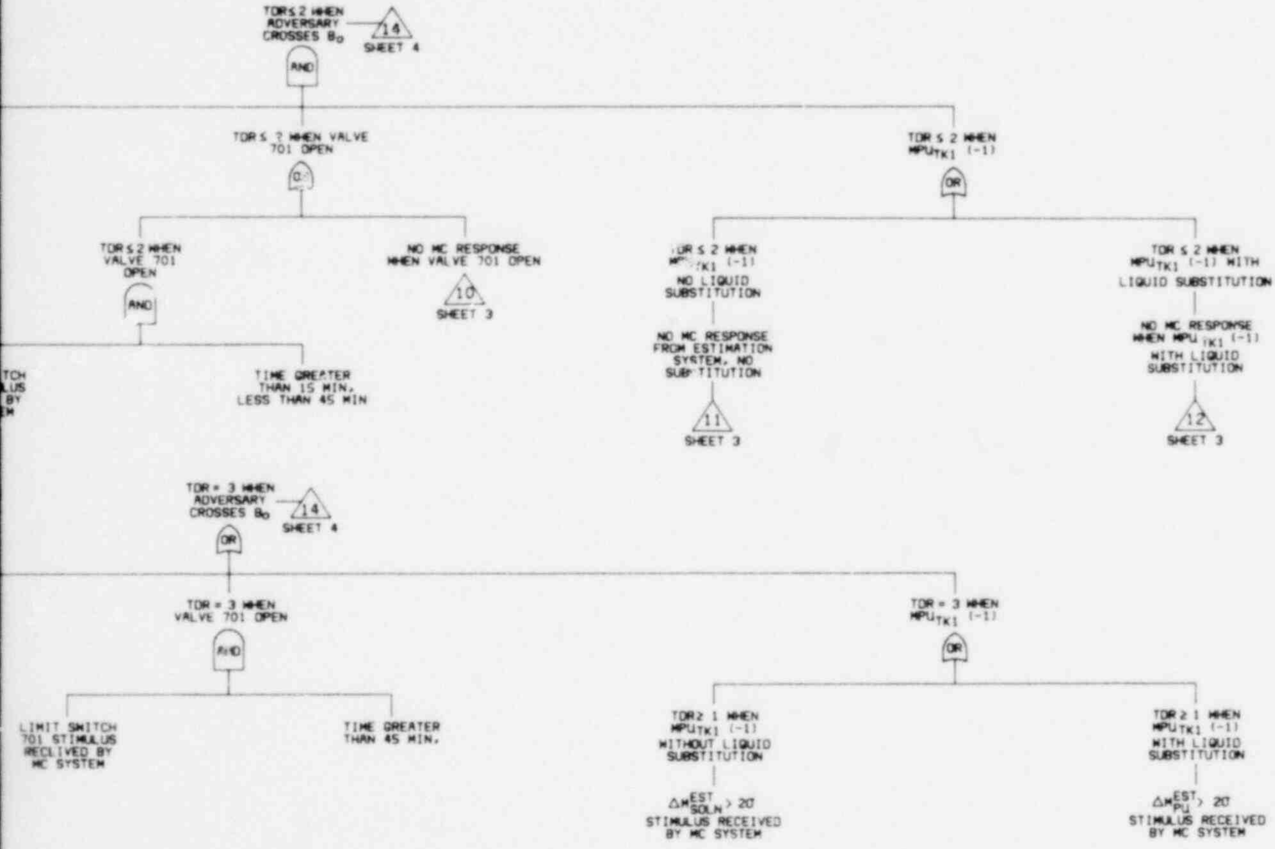

TDR ≤ 2 WHEN VALVE 722 OPEN
OR
TDR ≤ 2 WHEN VALVE 722 OPEN
AND
NO MC RESPONSE WHEN VALVE 722 OPEN
9
SHEET 3
LIMIT SWITCH 722 STIMULUS RECEIVED BY MC SYSTEM
TIME GREATER THAN 15 MIN. LESS THAN 45 MIN
LIMIT SW 701 STIM RECEIVED MC SYST
TDR = 3 WHEN VALVE 722 OPEN
AND
LIMIT SWITCH 702 STIMULUS RECEIVED BY MC SYSTEM
TIME GREATER THAN 45 MIN.

FIG. D-1. Test Bed des


TDR≤2 WHEN ADVERSARY CROSSES B₀
14
SHEET 4
AND
TDR ≤ ? WHEN VALVE 701 OPEN
OR
TDR≤2 WHEN VALVE 701 OPEN
AND
NO MC RESPONSE WHEN VALVE 701 OPEN
10
SHEET 3
TCH
LUS
BY
EM
TIME GREATER THAN 15 MIN, LESS THAN 45 MIN
TDR ≤ 2 WHEN MPU TK1 (-1)
OR
TDR ≤ 2 WHEN MPU TK1 (-1) NO LIQUID SUBSTITUTION
NO MC RESPONSE FROM ESTIMATION SYSTEM, NO SUBSTITUTION
11
SHEET 3
TDR ≤ 2 WHEN MPU TK1 (-1) WITH LIQUID SUBSTITUTION
NO MC RESPONSE WHEN MPU TK1 (-1) WITH LIQUID SUBSTITUTION
12
SHEET 3
TDR = 3 WHEN ADVERSARY CROSSES B₀
14
SHEET 4
OR
TDR = 3 WHEN VALVE 701 OPEN
AND
LIMIT SWITCH 701 STIMULUS RECLIVED BY MC SYSTEM
TIME GREATER THAN 45 MIN.
TDR = 3 WHEN MPU TK1 (-1)
OR
TDR≥ 1 WHEN MPU TK1 (-1) WITHOUT LIQUID SUBSTITUTION
ΔM EST SOLN > 2σ STIMULUS RECEIVED BY MC SYSTEM
TDR ≥ 1 WHEN MPU TK1 (-1) WITH LIQUID SUBSTITUTION
ΔM EST PU > 2σ STIMULUS RECEIVED BY MC SYSTEM

ign fault tree for SNM diversion at pump washout line (706).
(Sheet 5 of 5)

1426 044

Appendix E

TABLE OF BASIC EVENT DEFINITIONS AND PROBABILITIES FOR THE FAULT TREE

TABLE E-1. Basic event definitions and probabilities for the fault tree.

Alphanumeric designator	Basic event description	Basic event probability
AA-DHIT	Adversary hits crash bar A-door	1
ACCAS	Adversary at CCAS (Exit MAA)	1
ADV1KGMT	Adversary has greater than 1 Kg of nonferrous metal	0 if no shielding 1 if shielding
ADV200GT	Adversary has greater than 200 g of nonferrous material	0 if no shielding 1 if shielding
AFILLCON	Adversary fills container with SNM	1
ALARMIR	Alarm inactivated due to random causes	4×10^{-6}
ALARMIT	Alarm inactivated due to tampering	0.8
ALARMLX	Alarm link inactivated	1.3×10^{-5}
ALCCAS	Adversary leaves CCAS (Exit MAA)	1
ANODE14	Adversary at node 14	1
ANODE1	Adversary exits MAA at node 1	1
ANODE706	Adversary at node 706	1
APM-AL	Adversary crosses PM-AL	1
APM-AR	Adversary crosses PM-AR	1
APM-B0	Adversary crosses PM-B_0	1
APM-B1	Adversary crosses PM-B1	1
ASUBHNO	Adversary substitutes with equivalent density HNO_3	0 if no substitution 1 if substitution
CBEEAHIT	Crash bar EE_A door hit	1
CBEEHIT	Crash bar EE_B door hit	1
CBE1HIT	Crash bar E1 door hit	1
CBE2LHIT	Crash bar E2L door hit	1
CBE2RHIT	Crash bar E2R door hit	1

1426 046

E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
CCASOK	Other conditions OK for CCAS exit	1 (insider)
CDALRMIR	A-door alarm inactivated due to random causes	4×10^{-6}
CDALRMIT	A-door alarm inactivated due to tampering	0.8
CDALRMLX	Alarm link inactivated	1.3×10^{-5}
CDLI	Computer decision logic inactivated	1×10^{-3}
CONAT706	Container at node 706	1
CSNMRMAA	Container with SNM remains in MAA	1
CV436IR	Check valve 436 fails open due to random causes	3.9×10^{-2}
CV436IT	Check valve 436 fails open due to tampering	0.1
DPCELLIR	D.P. cells inactivated due to random causes	4×10^{-6}
DPCELLIT	D.P. cell inactivated due to tampering	1
GAMB01HI	γ Detector 1 in area B_0 detection threshold too high	0 if α = 0.5 g and no shielding 0 if α = 200 g and no shielding 0 if α = 5 Kg and no shielding 0.98 if α = 0.5 g and shielding 0 if α = 200 g and shielding 0 if α = 5 Kg and shielding
GAMB01IR	Inactivated due to random causes	6×10^{-5}

Table E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
GAMB01IT	Inactivated due to tampering	0.05
GAMB01LX	Computer link broken	1.3×10^{-5}
GAMB02HI	γ detector 2 in area B_0 detection threshold too high	0.7 if α = 0.5 g and no shielding 0 if α = 200 g and no shielding 0 if α = 5 Kg and no shielding 0.98 if α = 0.5 g and shielding 0.6 if α = 200 g and shielding 0 if α = 5 Kg and shielding
GAMB02IR	Inactivated due to random causes	6×10^{-5}
GAMB02IT	Inactivated due to tampering	0.05
GAMB02LX	Computer link inactivated due to random causes	1.3×10^{-5}
GARFAIL	A_R guard does not notice with SNM	0.01[a]
GARSLOW	A_r guard slow to arrive	0.1[b]
GBOFAIL	B_0 guard does not notice adversary with SNM	0.01[a]
GBSLOW	B_0 guard slow to arrive	0.1[b]
GCCASF	CCAS guard does not notice adversary with SNM	0.01[a]
GCCASLOW	CCAS guard slow to arrive	0.1[b]
GFAIL13	Guard fails to notice adversary with SNM at node 13	0.01[a]

[a] Assumed.
[b] From MCSS.

Table E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
LABFALSE	Pu lab concentration measurements falsified	0.7
LS701CIR[c]	LS 701 circuit inactivated due to random causes	1.3×10^{-5}
LS701CIT	LS 701 circuit inactivated due to tampering	1
LS701IR	LS 701 inactivated due to tampering	4.8×10^{-5}
LS701IT	LS 701 inactivated due to tampering	0.5
LS722CIR	LS 722 circuit inactivated due to random causes	1.3×10^{-5}
LS722CIT	LS 722 circuit inactivated due to tampering	1
LS722IR	LS 722 inactivated due to random causes	4.8×10^{-5}
LS722IT	LS 722 inactivated due to tampering	0.5
MC1-OPO	MC1-operator override permitting CCAS exit	1×10^{-2}
MC2-OPO	MC2-operator override permitting CCAS exit	1×10^{-2}
MDCCASHI	Metal detector detection threshold too high	1 if α = 0.5 g and no shielding 1 if α = 200 g and no shielding 1 if α = 5 Kg and no shielding 0 if α = 0.5 g and shielding 0 if α = 200 g and shielding 0 if α = 5 Kg and shielding

[c] LS denotes limit switch.

Table E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
MDCCASIR	Metal detector random failure	2×10^{-6}
MDCCASIT	Metal detector inactivated due to tampering	0.01
MDCCASLX	Metal detector computer link broken	1.3×10^{-5}
MPU709	Mass flow at node 709	1
NOMCCAS	No metal in CCAS	1 if α = 0.5 g and no shielding
		1 if α = 200 g and no shielding
		1 if α = 5 Kg and no shielding
		0 if α = 0.5 g and shielding
		0 if α = 200 g and shielding
		0 if α = 5 Kg and shielding
NORETDR1	Inadequate guard response to TDR 1	10^{-1}[b]
NORETDR2	Inadequate guard response to TDR 2	10^{-2}[a]
NORETDR3	Inadequate guard response to TDR 3	10^{-3}[a]
PRMODE	Time period equal to product receival mode	
RDCCASHI	γ CCAS detection threshold too high	0 if α = 0.5 g and no shielding
		0 if α = 200 g and no shielding

[a] Assumed.
[b] From MCSS.

Table E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
		0 if α = 5 Kg and no shielding 0.98 if α = 0.5 g and shielding 0 if α = 200 g and shielding 0 if α = 5 Kg and shielding
RDCCASIR	γ CCAS detector inactivated due to random causes	4×10^{-6}
RDCCASIT	γ CCAS detector inactivated due to tampering	0.1
RDCCASLX	Radiation computer link broken	1.3×10^{-5}
SENSLOWM	Estimate of difference in solution mass, $\Delta M^{EST}_{SOLN} < 2\sigma$ (σ= 237 g solution Note $P(\Delta M^{EST}_{SOLN} < 2\sigma) = 1$ if liquid substitution occurs	1 if α = 0.5 g and no shielding 7×10^{-3} if α = 200 g and no shielding 0 if α = 5 Kg and no shielding 1 if α = 0.5 g and shielding 7×10^{-3} if α = 200 g and shielding 0 if α = 5 Kg and shielding
SENSLOWP	Estimate of difference in Pu mass, $\Delta M^{EST}_{Pu} < 2\sigma$ (σ = 0.21%) Note P $(\nabla M^{EST}_{Pu} < 2\sigma)$ = 1 if no liquid substitution occurs	1 if α = 0.5 g and no shielding

Table E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
		1 if α = 200 g and no shielding
		0 if α = 5 Kg and no shielding
		1 if α = 0.5 g and shielding
		1 if α = 200 g and shielding
		0 if α = 5 Kg and shielding
SRCB	Crash bar stimulus received due to MC system	1
SRCDALARM	A-door crash bar stimulus received by MC system	1
SRGAMB01	γ-B_0-1 detector stimulus received due to MC system	1 if α = 0.5 g and no shielding
		1 if α = 200 g and no shielding
		1 if α = 5 Kg and no shielding
		0.02 if α = 0.5 g and shielding
		1 if α = 200 g and shielding
		1 if α = 5 Kg and shielding
SRGAMB02	γ-B_0-1 detector stimulus received due to MC system	0.3 if α = 0.5 g and no shielding
		1 if α = 200 g and no shielding
		1 if α = 5 Kg and no shielding
		0.02 if α = 0.5 g and shielding

Table E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
		0.4 if α = 200 g and shielding 1 if α = 5 Kg and shielding
SRLS701	Limit switch 701 stimulus received due to MC system	1
SRLS722	Limit switch 722 stimulus received due to MC system	1
SRMDS	Strong metal detector stimulus received by MC system	0 if α = 0.5 g and no shielding 0 if α = 200 g and no shielding 0 if α = 5 Kg and no shielding 1 if α = 0.5 g and shielding 1 if α = 200 g and shielding 1 if α = 5 Kg and shielding
SRMDW	Weak metal detector stimulus received by MC system	0 if α = 0.5 g and no shielding 0 if α = 200 g and no shielding 0 if α = 5 Kg and no shielding 1 if α = 0.5 g and shielding 1 if α = 200 g and shielding 1 if α = 5 Kg and shielding

Table E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
SRMSOLN	Estimate of difference in solution mass, $M^{EST}_{SOLN} < 2\sigma$ stimulus received[d]	0 if α = 0.5 g and no shielding 0.993 if α = 200 g and no shielding 1 if α = 5 Kg and no shielding 0 if α = 0.5 g and shielding 0.933 if α = 200 g and shielding 1 if α = 5 Kg and shielding
SRPUEST	Estimate of difference in PU concentration, $\Delta M^{EST}_{Pu} < 2\sigma$ stimulus received[e]	0 if α = 0.5 g and no shielding 0 if α = 200 g and no shielding 1 if α = 5 Kg and no shielding 0 if α = 0.5 g and shielding 0 if α = 200 g and shielding 1 if α = 5 Kg and shielding
SRRDCCAS	CCAS gamma detector stimulus received by MC system	1 if α = 0.5 g and no shielding

[d] No liquid solution.
[e] Liquid substitution.

Table E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
		1 if α = 200 g and no shielding 1 if α = 5 Kg and no shielding 0.02 if α = 0.5 g and shielding 1 if α = 200 g and shielding 1 if α = 5 Kg and shielding
SRWEIGHT	Weight platform stimulus received by MC system	0 if α = 0.5 g and no shielding 0 if α = 200 g and no shielding 1 if α = 5 Kg and no shielding 0 if α = 0.5 g and shielding 1 if α = 200 g and shielding 1 if α = 5 Kg and shielding
TDR1-G	Alarm state exists TDR1	
TDR2-G	Alarm state exists TDR2	
TDR3-G	Alarm state exists TDR3	
TGTLAB	Time greater than duration required for laboratory analysis	
TGTRPROMD	Time greater than duration of product receival mode	

Table E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
TGTTKFIL	Time greater than duration required to fill Tank 1	
TK1FILL	Tank 1 filled	
TLEVEL-1	Tank 1 level	
TLTLAB	Time less than required for laboratory analysis	
TPEQMM	Time period equal to maintenance mode	
TPNESM	Time period not equal to static mode	
TPNETM	Time period not equal to transfer mode	
T701GT15	Time greater than 15 min since LS 701 stimulus produced	
T701GT45	Time greater than 45 min since LS 701 stimulus produced	
T701LT15	Time less than 15 min since LS 701 stimulus produced	
T7011545	Time between 15 min and 45 min since LS 701 stimulus produced	
T722GT15	Time greater than 15 min since LS 722 stimulus produced	
T722GT45	Time between 15 min and 45 min since LS 701 stimulus produced	
T722LT15	Time less than 15 min since LS 722 stimulus produced	
TGT45	Time greater than 45 min since stimulus produced	
V290	Valve 29 open	1
V7010	Valve 701 open	1

Table E-1 (continued)

Alphanumeric designator	Basic event description	Basic event probability
V7130	Valve 713 open	1
V7190	Valve 719 open	1
V7220	Valve 722 open	1
WEGT3	Weight difference greater than 3% allowable difference	0 if α = 0.5 g and no shielding 0 if α = 200 g and no shielding 1 if α = 5 Kg and no shielding 0 if α = 0.5 g and shielding 1 if α = 200 g and shielding 1 if α = 5 Kg and shielding
WEIGHTIR	Weight platform inactivated due to random failure	5×10^{-5}
WEIGHTIT	Weight platform failure inactivated due to tampering	0.02
WEIGHTOK	Weight within 3% allowable difference	1 if α 0.5 g and no shielding 1 if α = 200 g and no shielding 0 if α = 5 Kg and no shielding 1 if α = 0.5 g and shielding 0 if α = 200 g and shielding 0 if α = 5 Kg and shielding

References

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

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

3. F. M. Gilman, M. H. Dittmore, J. J. Lim, Wood River Junction Vulnerability Analysis: Phase I Report, MC 79-197, Lawrence Livermore Laboratory, to be published as a NUREG Report (1979).

4. I. J. Sacks, A. A. Parziale, T. R. Rice, S. L. Derby, The Structured Assessment Analysis of Facility X, Volume 1 - Executive Summary, MC 79-12-D, Lawrence Livermore Laboratory, to be published as a NUREG Report (1979).

5. L. D. Chapman, et al., Physical Protection of Nuclear Material in Transit, Quarterly Progress Report (October - December 1978), Report SAND 790535/Report NUREG -CRO 694.

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

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

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

9. 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.

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

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

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

13. G. A. Morris, PIPE: A Computer Code for Piping Network Analysis, Lawrence Livermore Laboratory, Report UCRL-52441 (1978).*

*Available through the National Technical Information Service, Springfield, Virginia 22151.

References (continued)

14. Z. W. Birnbaum, "On the Importance of Different Components and a Multicomponent System," in Multivariate Analysis-II, P. R. Krishnaiah, Editor, Academic Press, New York (1969).

15. R. B. Hollstien, A Material Control System Simulator, Lawrence Livermore Laboratory, Report UCRL-80815 (1978).*

16. W. E. Vesely, "Reliability Quantitication Techniques Used in the Rasmussen Study," in Reliability and Fault Tree Analysis, R. E. Barlow, J. B. Fussell and N. D. Singpurwalla, Editors, SIAM (1975).

17. H. W. Lewis, et al., Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission, U.S. Nuclear Regulatory Commission, Report NUREG/Cr-0400, (1978).

NRC FORM 335
(7-77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG/CR-0777
UCRL-52710

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
A Digraph-Fault Tree Methodology for the Assessment of Material Control Systems

5. DATE REPORT COMPLETED
MONTH May 21 | YEAR 1979

DATE REPORT ISSUED
MONTH November 1 | YEAR 1979

6. *(Leave blank)*

7. AUTHOR(S)
H.E. Lambert, J.J. Lim, F.M. Gilman

8. *(Leave blank)*

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
LLL/NRC
P.O. Box 808
Livermore, CA 94550

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.
FIN A0115

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
U.S. Nuclear Regulatory Commission
Div. of Safeguards, Fuel Cycle, & Environmental Research
Washington, D.C. 20555

13. TYPE OF REPORT
Technical Report

PERIOD COVERED *(Inclusive dates)*

14. *(Leave blank)*

15. SUPPLEMENTARY NOTES

16. ABSTRACT *(200 words or less)*

The Lawrence Livermore Laboratory, under contract to the United States Nuclear Regulatory Commission, is developing a procedure to assess the effectiveness of material control and accounting systems at nuclear fuel cycle facilities. The purpose of a material control and accounting system is to prevent the theft of special nuclear material such as plutonium or highly enriched uranium. This report presents the use of a directed graph and fault tree analysis methodology in the assessment procedure. This methodology is demonstrated by assessing a simulated material control system design, the Test Bed.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
Unclassified

20. SECURITY CLASS *(This page)*
Unclassified

21. NO. OF PAGES

22. PRICE
$

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

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
U.S. NUCLEAR REGULATORY
COMMISSION

U.S. MAIL

Document Control Desk
P016

120555031837 2 ANRS
US NRC
SECY PUBLIC DOCUMENT ROOM
BRANCH CHIEF
HST LOBBY
WASHINGTON DC 20555