Use of the Directed Graph-Fault Tree Approach for Safeguards Effectiveness Assessment

Engineering

Howard Lambert
Visiting Science Professional

May 1, 2019

LLNL-PRES-969616
This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

Lawrence Livermore National Laboratory

Safeguards Diversion Scenarios

- International Safeguards
  - Member state attempts to divert Special Nuclear Material (SNM) so that the International Atomic Agency (IAEA) does not detect a significant amount of SNM diversion in a timely manner
- Domestic Safeguards
  - An insider or group of insiders attempt to divert Special Nuclear Material so that DOE and/or USNRC does not detect a significant amount of SNM diversion in a timely manner
- Safety Analysis – includes unintentional acts excludes malevolent acts
- Safeguards and Security Analysis – includes Malevolent Acts
- Scope much different between Safety and Safeguards and Security Analysis

References on the Use of the Directed Graph Fault Tree Approach For Safeguards Effectiveness Assessment

- International Safeguards
  - H. A. Elayat, H. Lambert, W. J. O'Connell, L. Szytel, M. Dreicer Systems Analysis for Evaluation of Safeguards Effectiveness Lawrence Livermore National Laboratory UCRL-PRES-225238 April 2011
- Domestic Safeguards
  - H Lambert and J Lim,UCRL-79217, Lawrence Livermore National Laboratory, June 1977, Presented at the INMM conference, June 29,1997, Arlington, VA.
  - H. E. Lambert, J. J. Lim and F.M. Gilman, A Digraph-Fault Tree Methodology for the Assessment of Material Control Programs, NUREG/CR-0777, Lawrence Livermore National Laboratory, UCRL-52710. May 1979.

International Atomic energy Agency (IAEA) Safeguards vulnerabilities

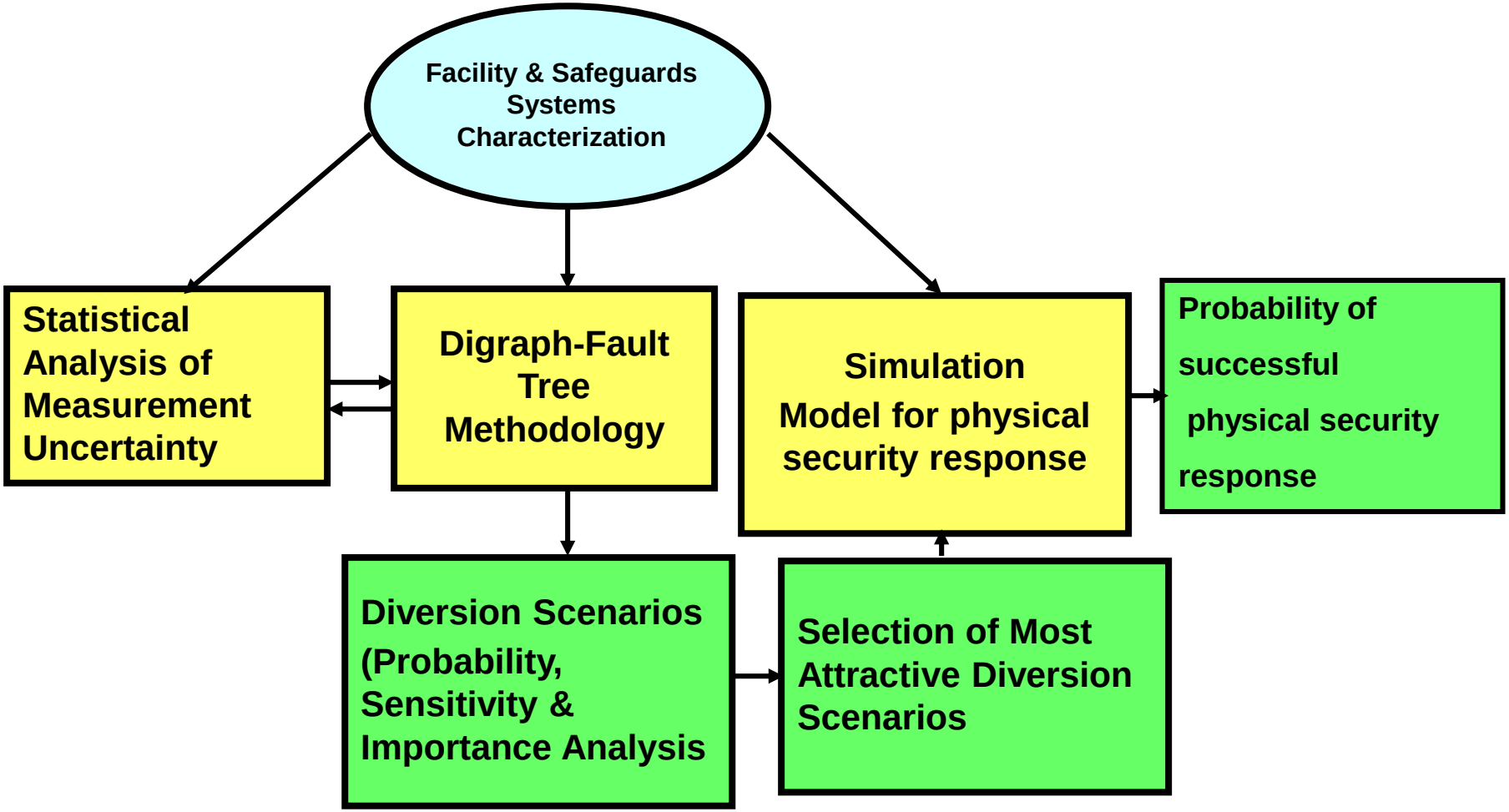
- "Ideal world" versus "real world"
- Ideal world consider equipment and instrumentation capabilities only
- Real world – consider vulnerabilities of the safeguards systems
  - Concealment activities (next slide)

Concealment Activities

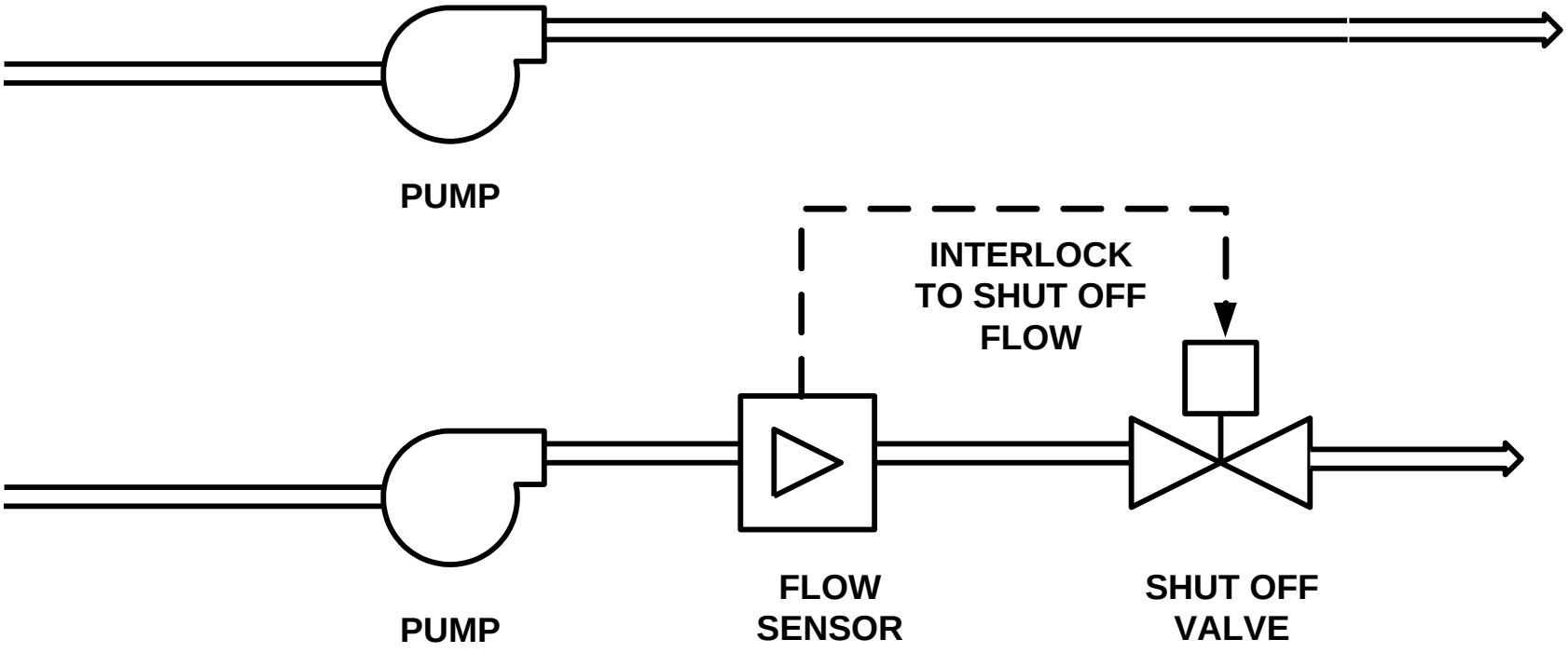
- Stimulus Variable Cancellation
  - Flow meter – by pass
  - Radiation detector – shield SNM
  - Measure Level in Tank – liquid substitution
- IAEA Material Accounting
  - Diversion into MUF (Large Measurement Uncertainty)
  - Defects (misdeclarations)
    - Gross (Sampling Scheme Misses Gross Defect)
    - Partial (Sampling Scheme Misses Partial Defect)
    - Biased (Sampling sheme Misses Biased Defect and/or Measurement system inaccurate)

Red indicates failure modes

LLNL Integrated Safeguards System Analysis Tool (LISSAT)
Domestic Safeguards – 70's Barnwell Study

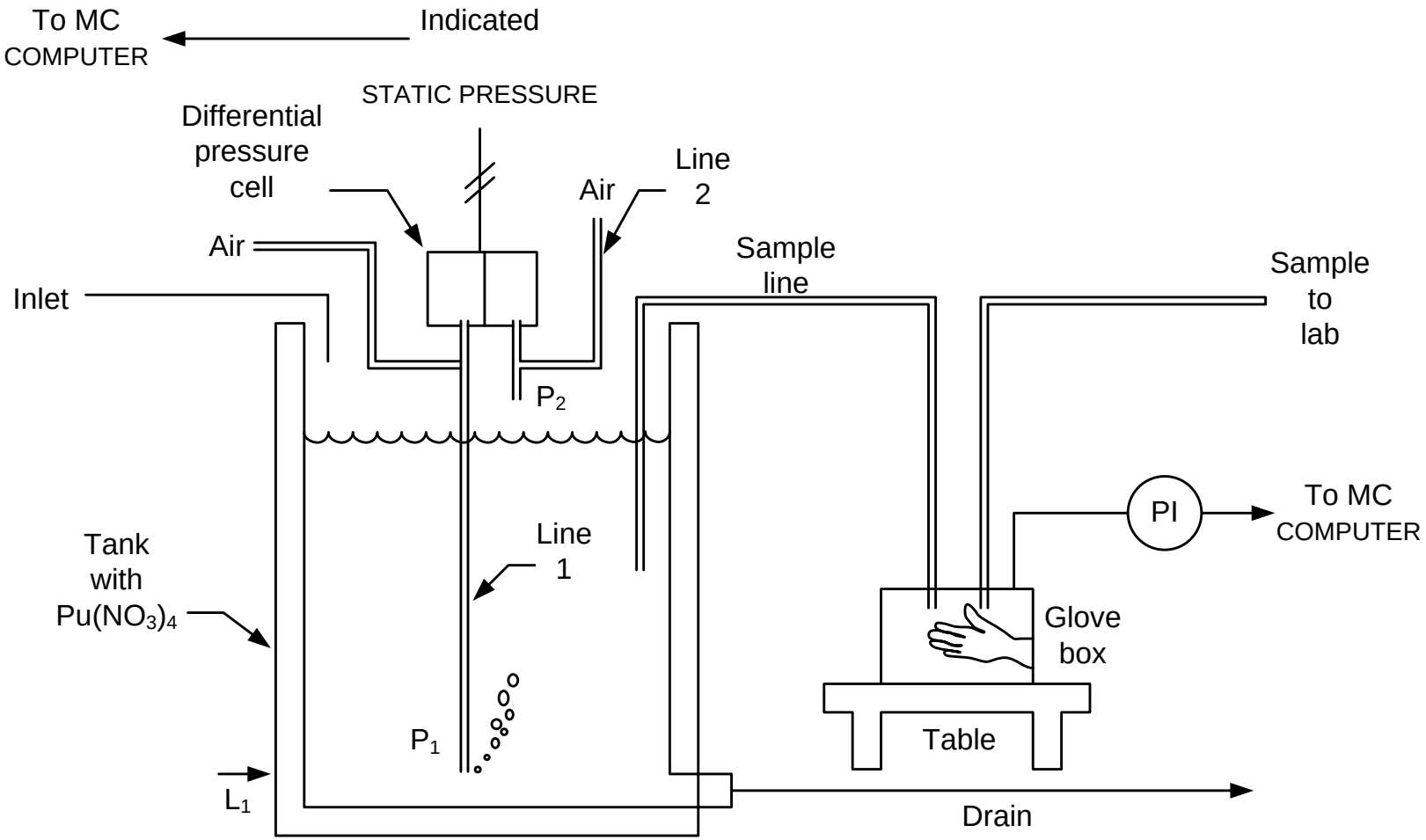


Pump System Analogy for Digraph-Fault Tree Methodology



1. What are the diversionary activities – e.g. removal of material, concealment
2. How are these activities detected?
3. How can detection fail so that diversion goes undetected?

PU Nitrate Storage Tank (UCRL-79217) (Domestic Safeguards Example)



Glovebox Description

- A glovebox is used to sample plutonium nitrate from the storage tank via a sample line. A technician transfers the sample through a pneumatic sample line to the laboratory for chemical analysis. The glove box is under a vacuum. It is assumed that the material control system will generate a security response when the following alarms are received

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

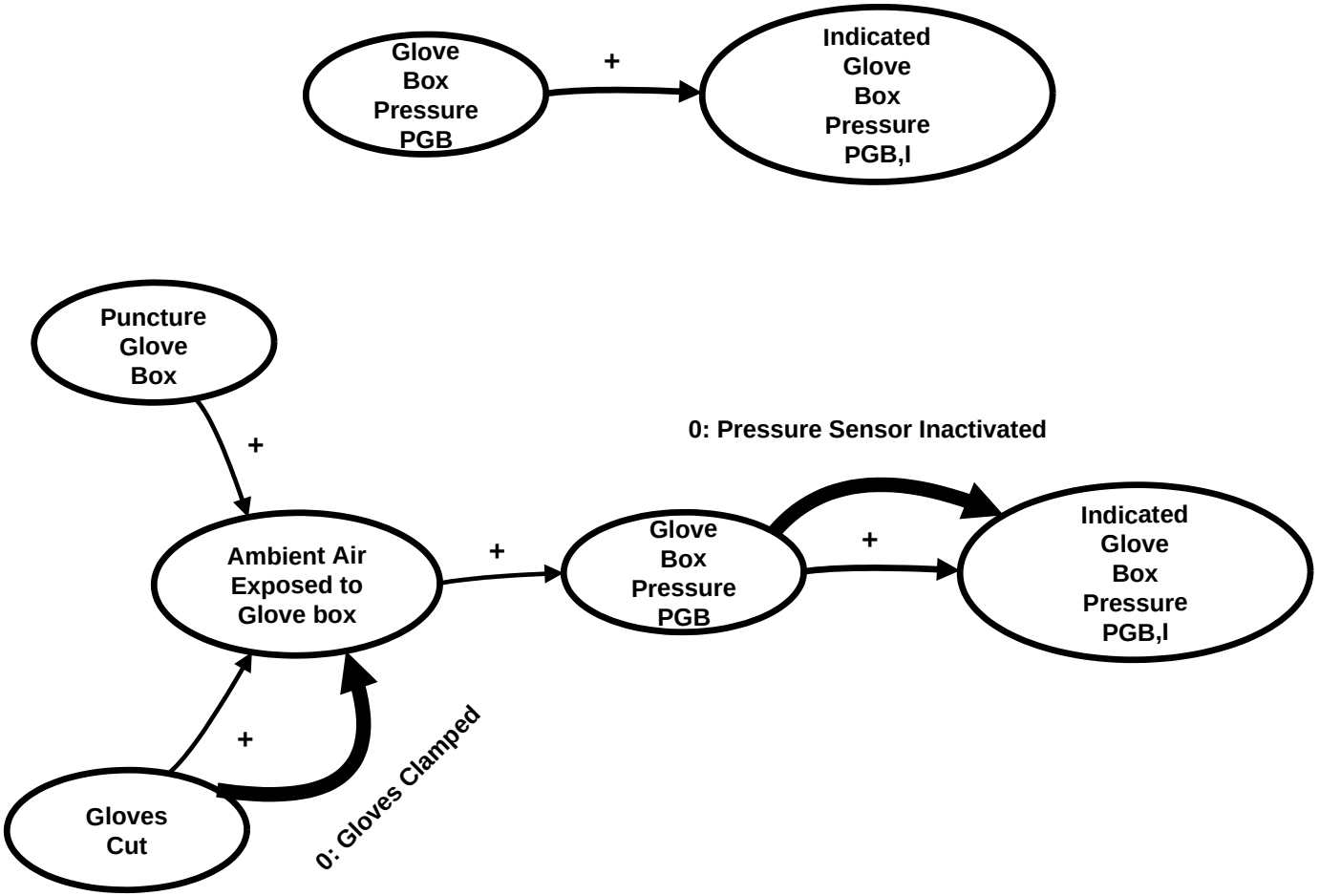
2. Change in level reading determined by a differential pressure cell measurement

In addition, Material Control (MC) system procedures require security to inspect the glovebox at random times intervals and apprehend any personnel diverting SNM.

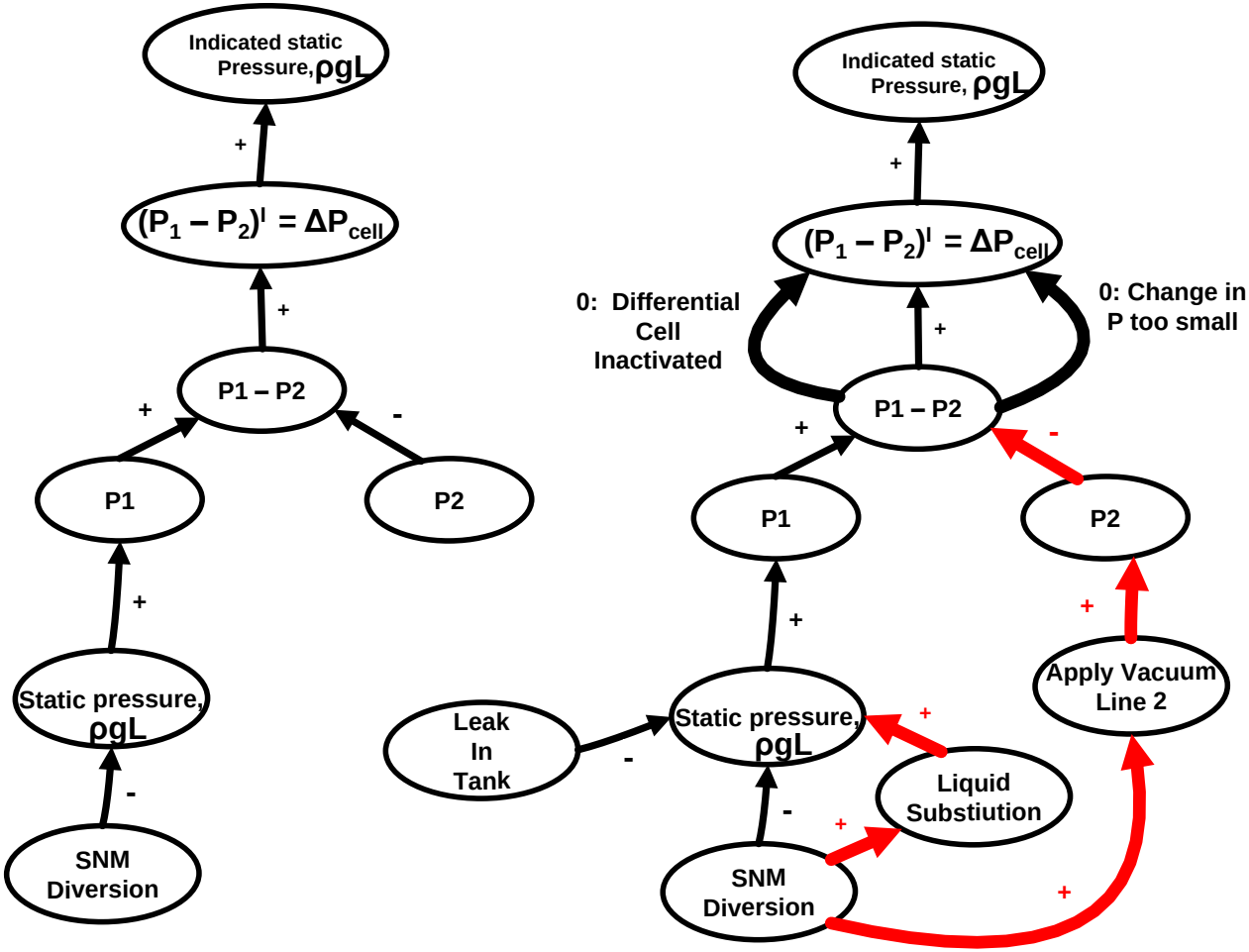
Digraph-Fault Tree Analysis

- Successful Diversion of liquid Plutonium Nitrate from Glovebox
- Generate Unit Model Digraphs
- Merge unit Model Digraphs into System Digraph
- Generate Fault Tree from System Digraph
- Generate diversion scenarios from fault tree

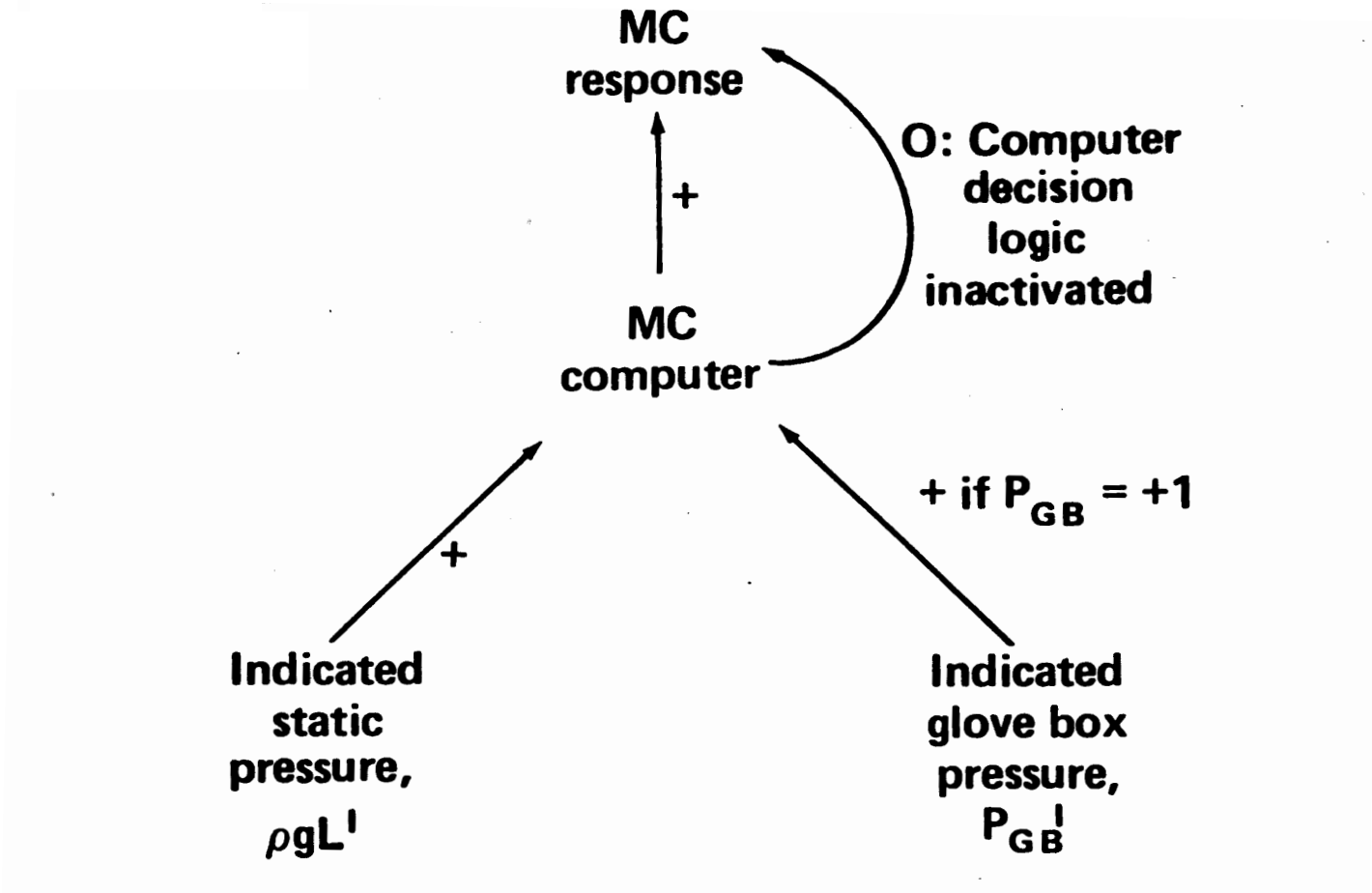
Unit Model Digraph of Glove Box with Pressure Sensor



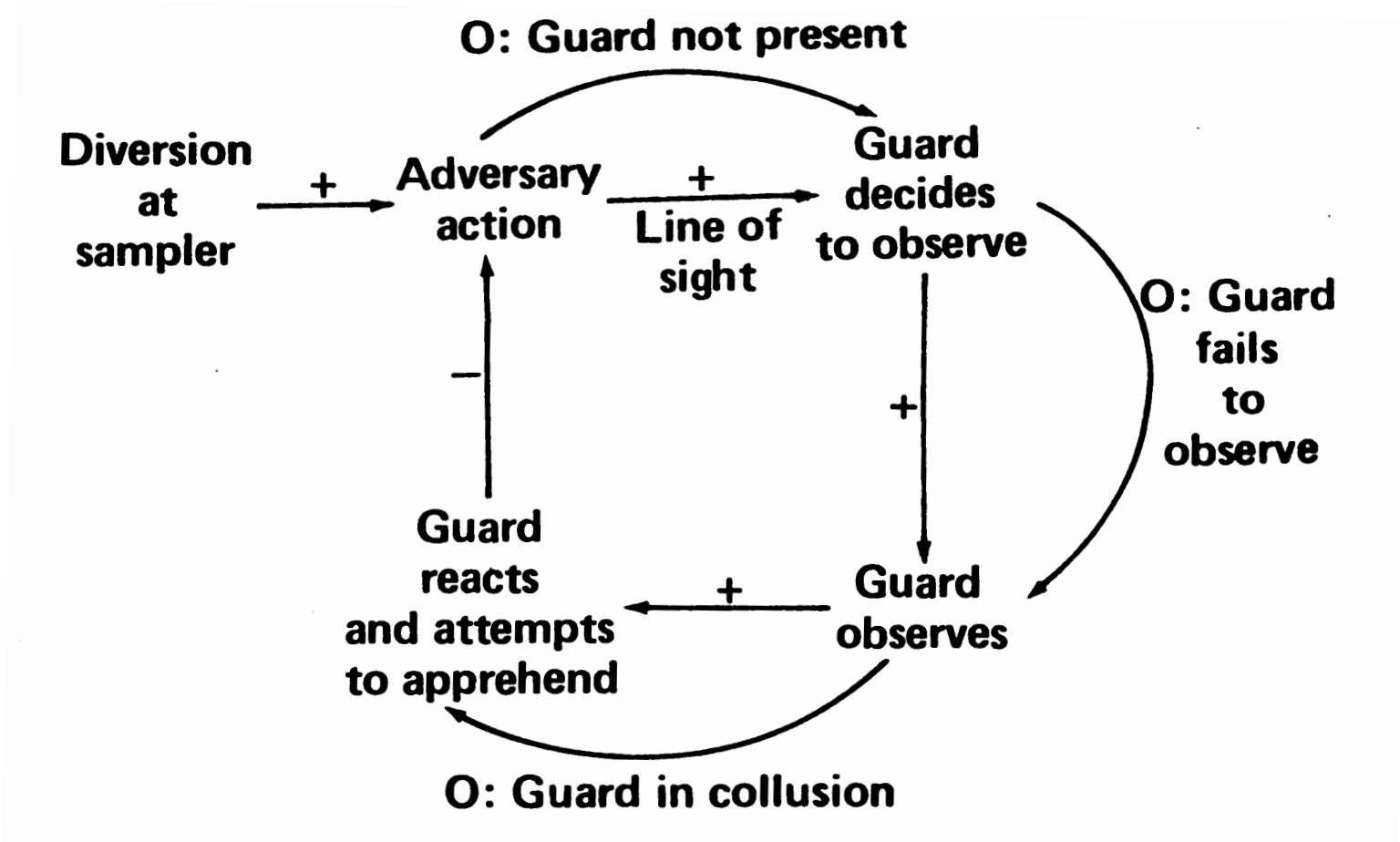
Unit Model Digraph of Storage Tank with Differential Pressure Cell (Red Indicates Stimulus Variable Cancellation by Adversary)



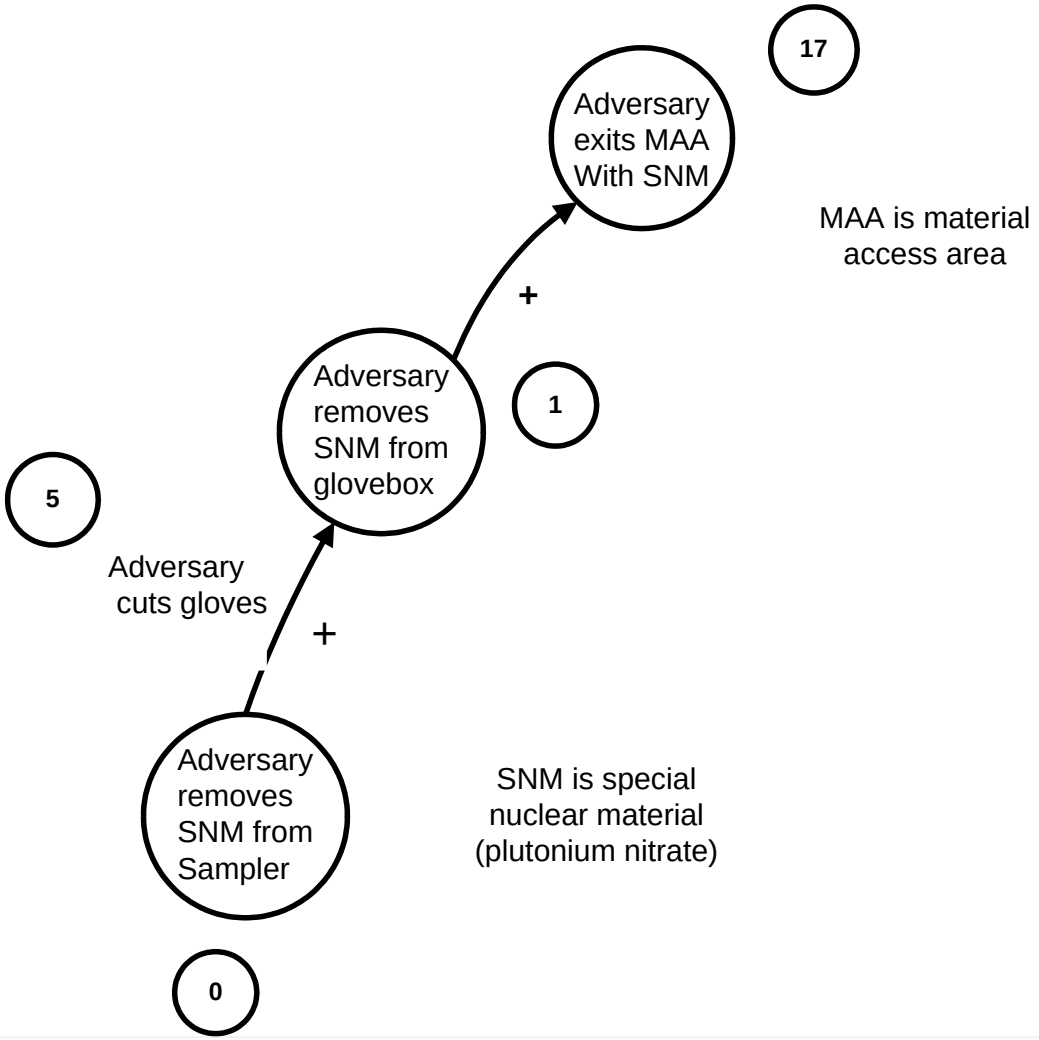
Unit Model Digraph of MC Computer Logic Decision Logic



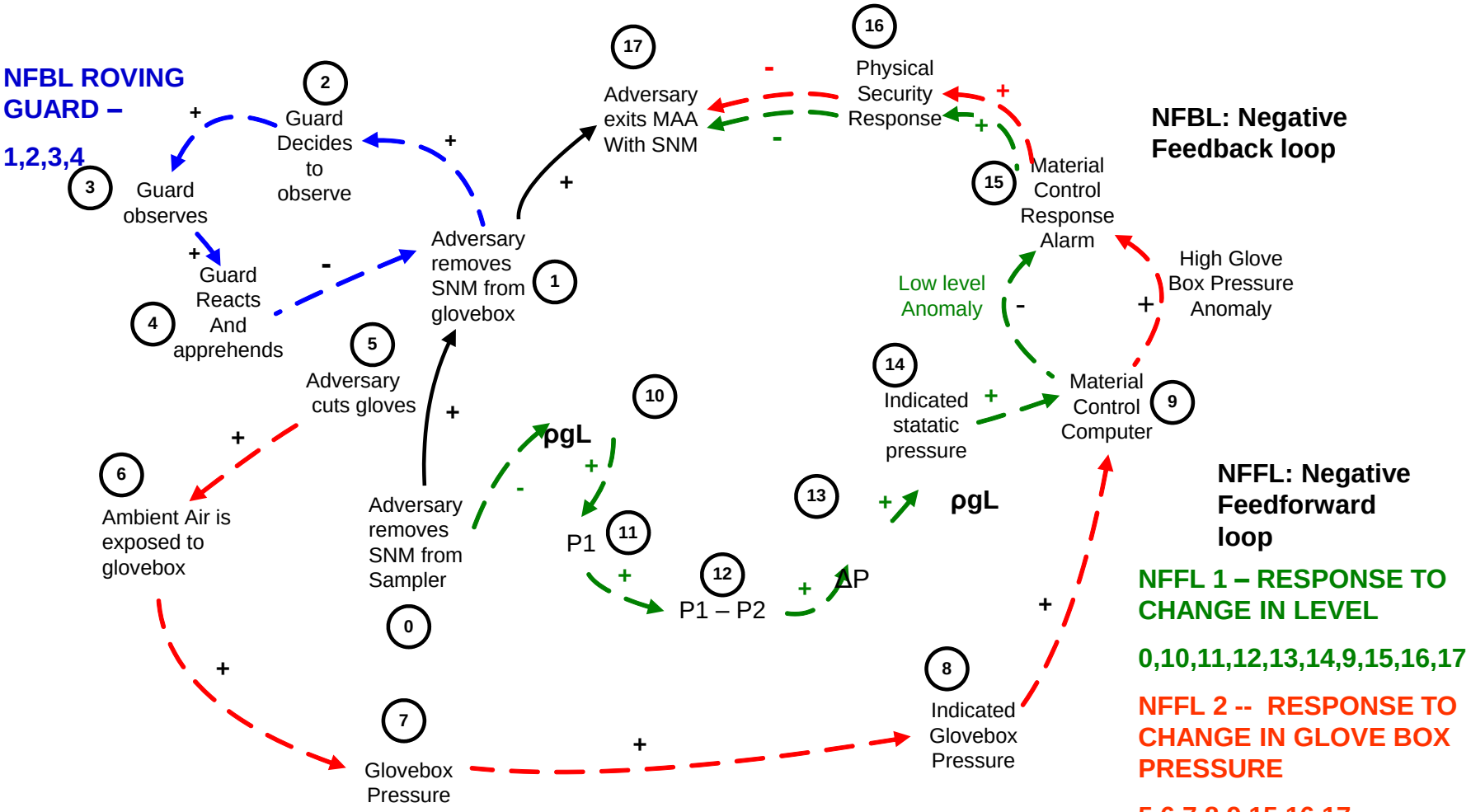
Unit Model Digraph of Roving Guard



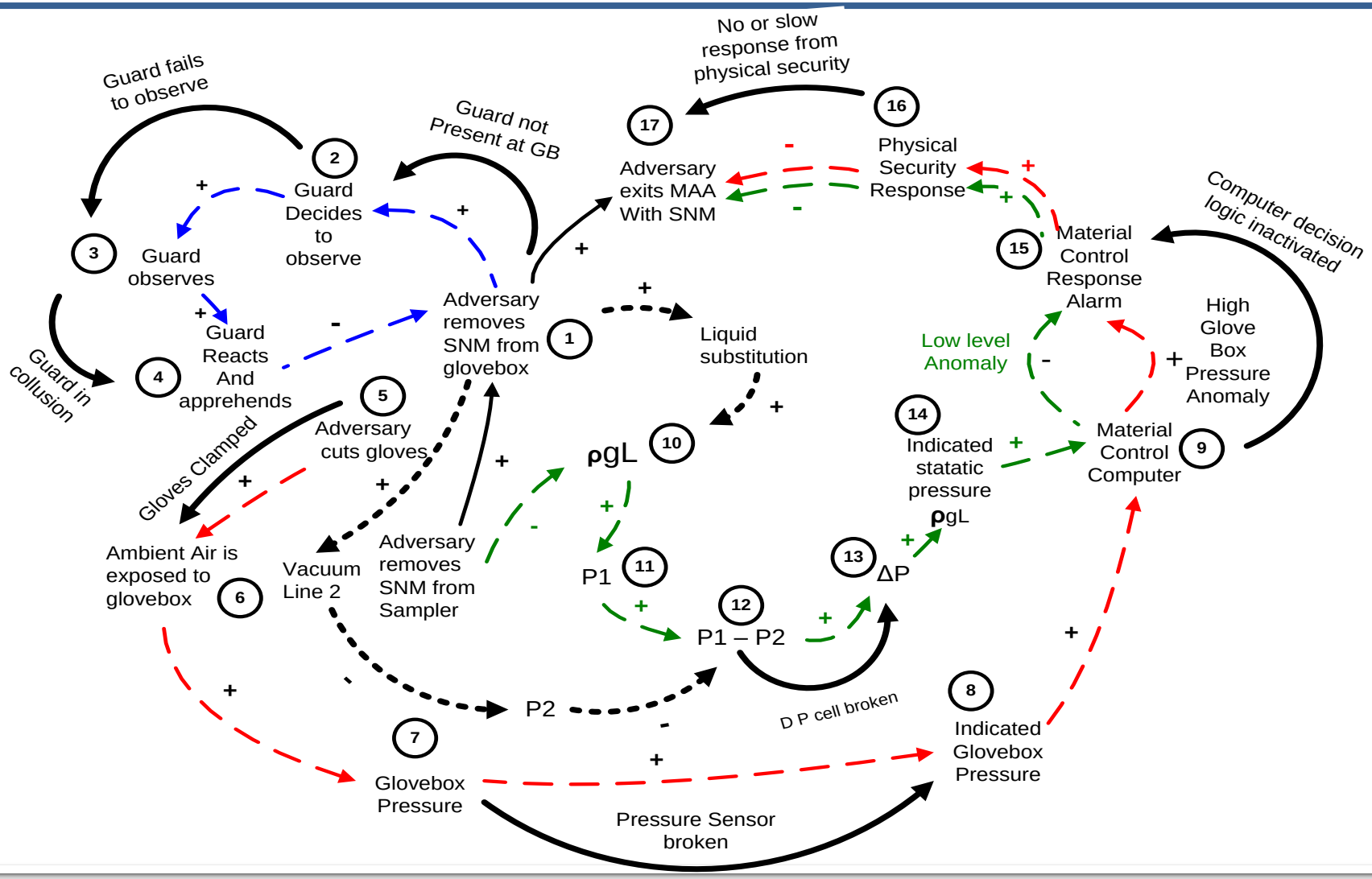
Digraph – Removal of SNM



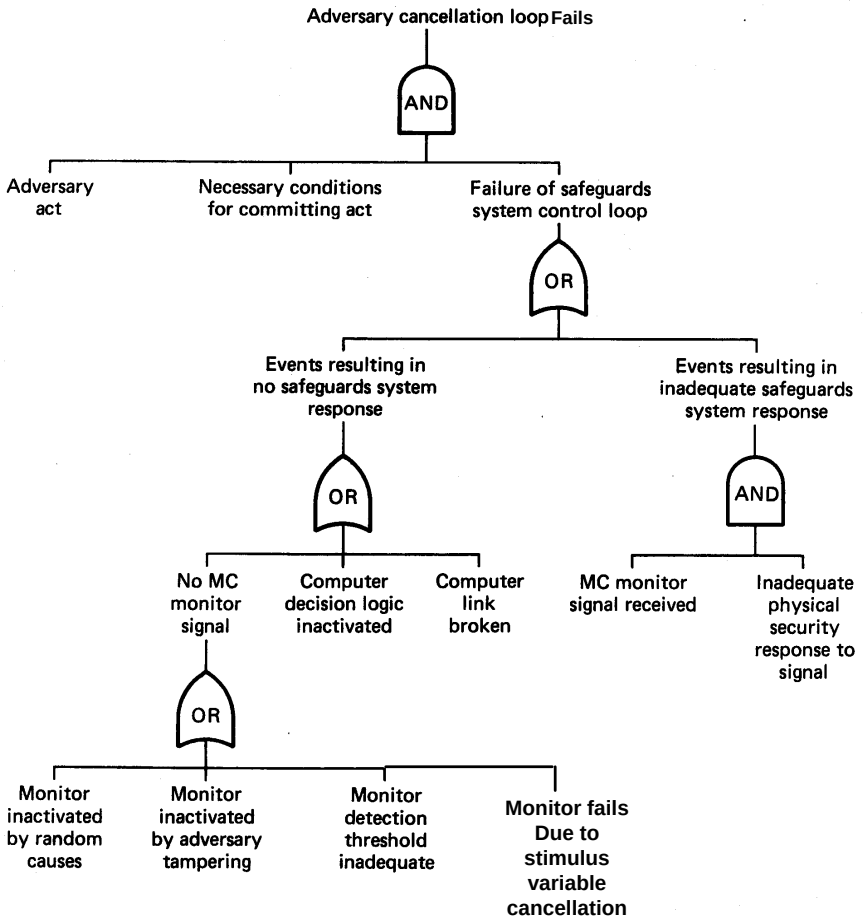
System Digraph with Detection Loops



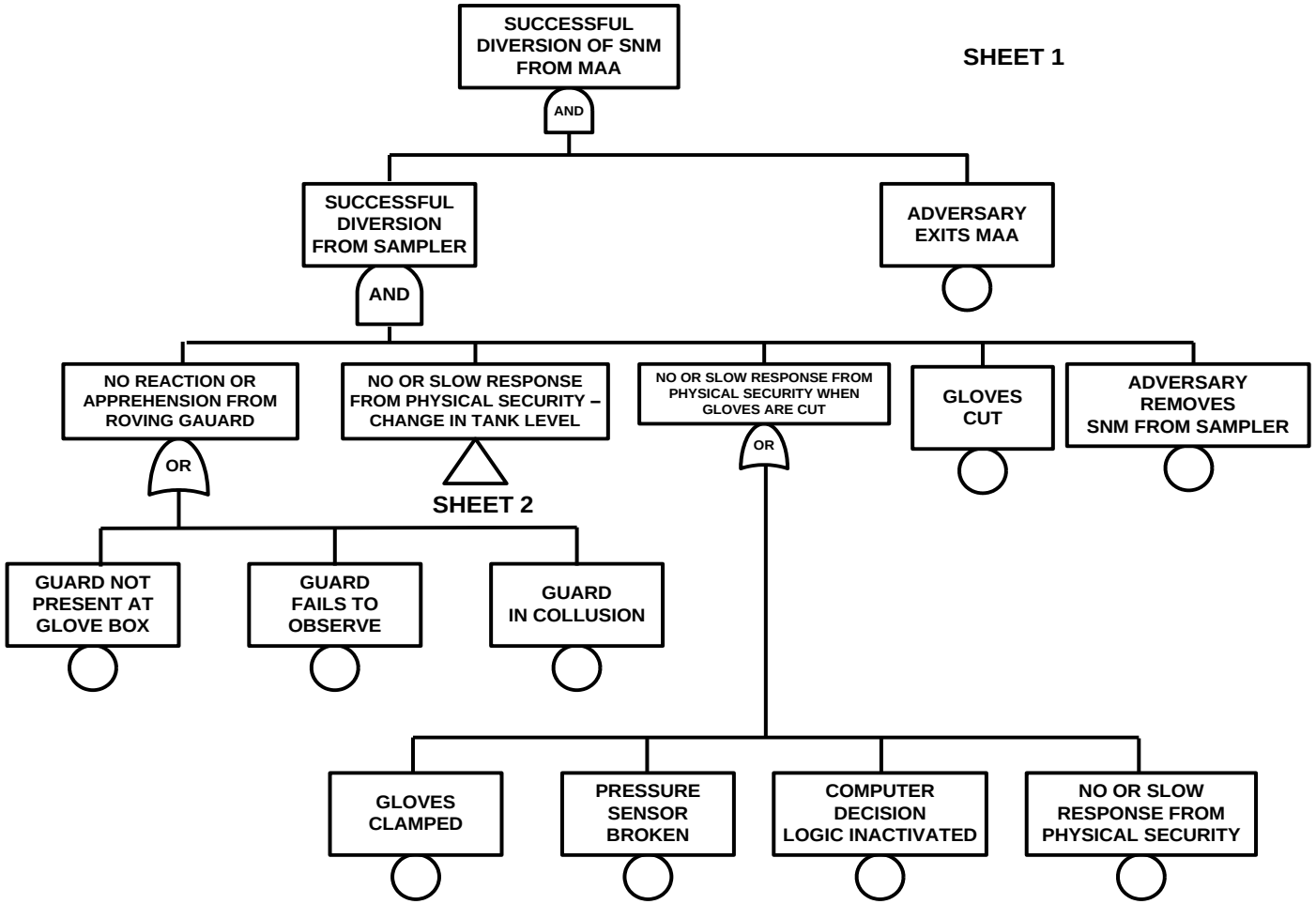
System Digraph with Detection Cancellation Loops



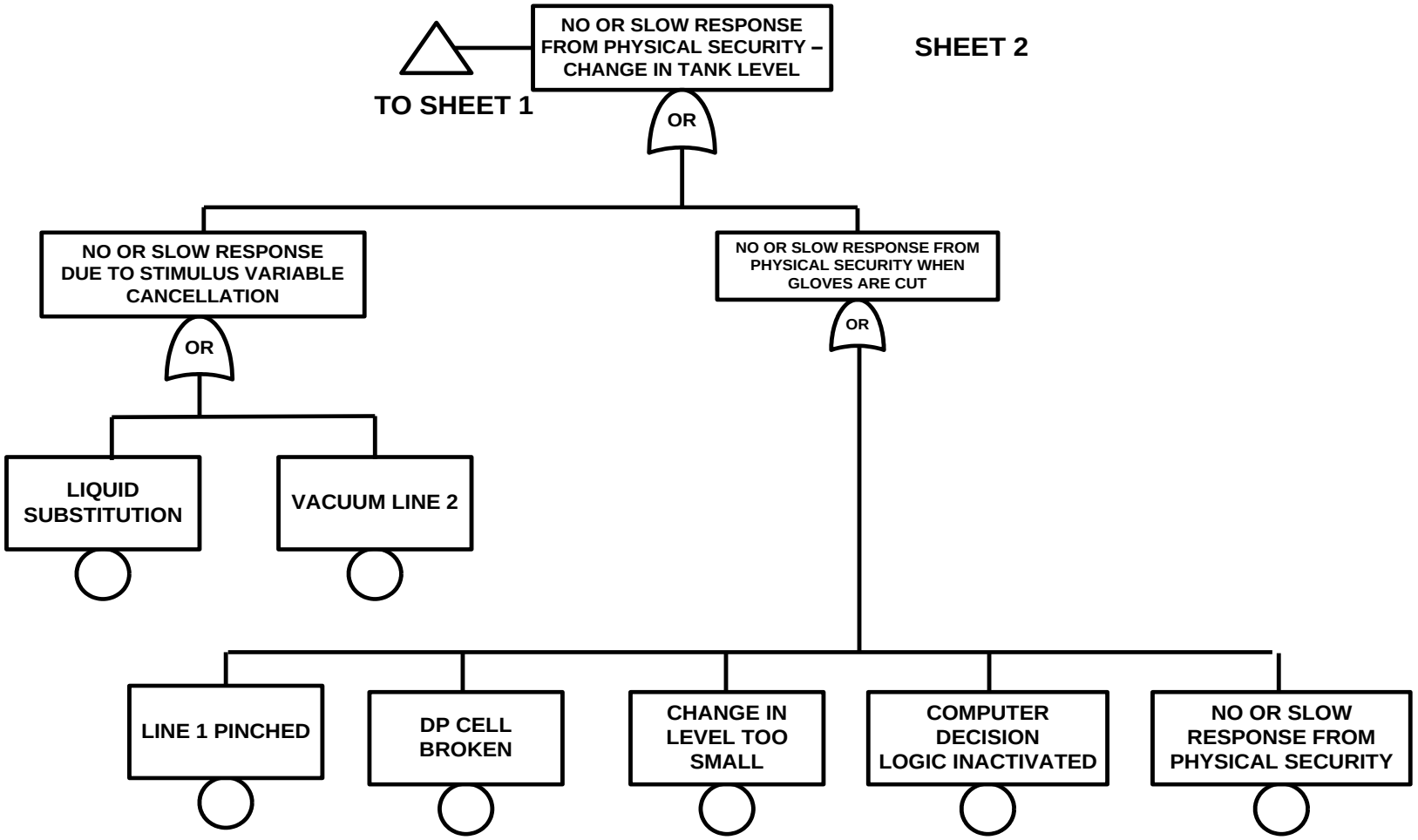
Fault Tree Operator for Adversary Cancellation Failure



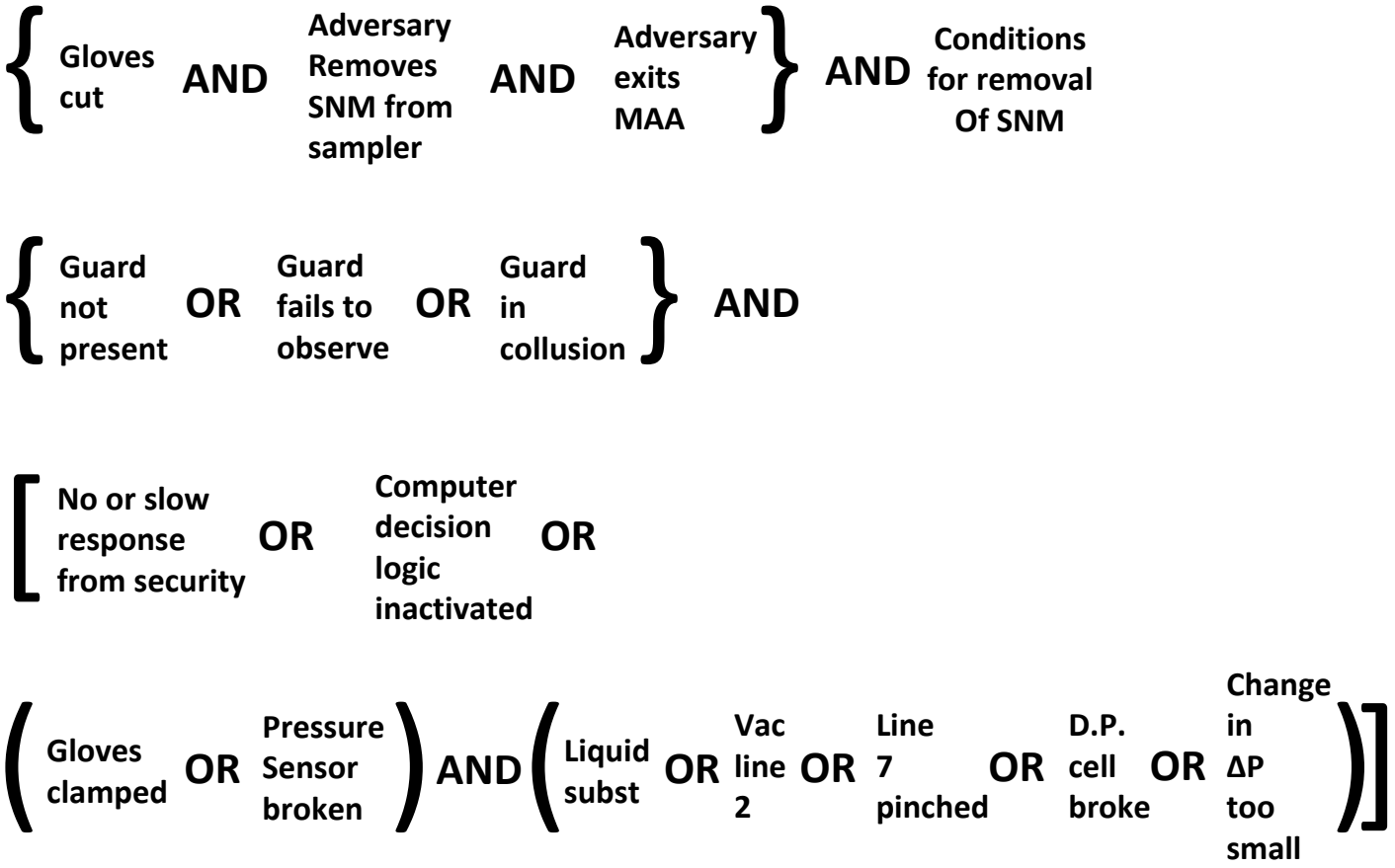
Fault Tree for Successful Diversion from Storage Tank



Fault Tree For Successful Diversion From Storage Tank



Adversary Event Sets



36 Event Sets

814,000 FOR TEST BED STUDIED IN NUREG/CR-0777

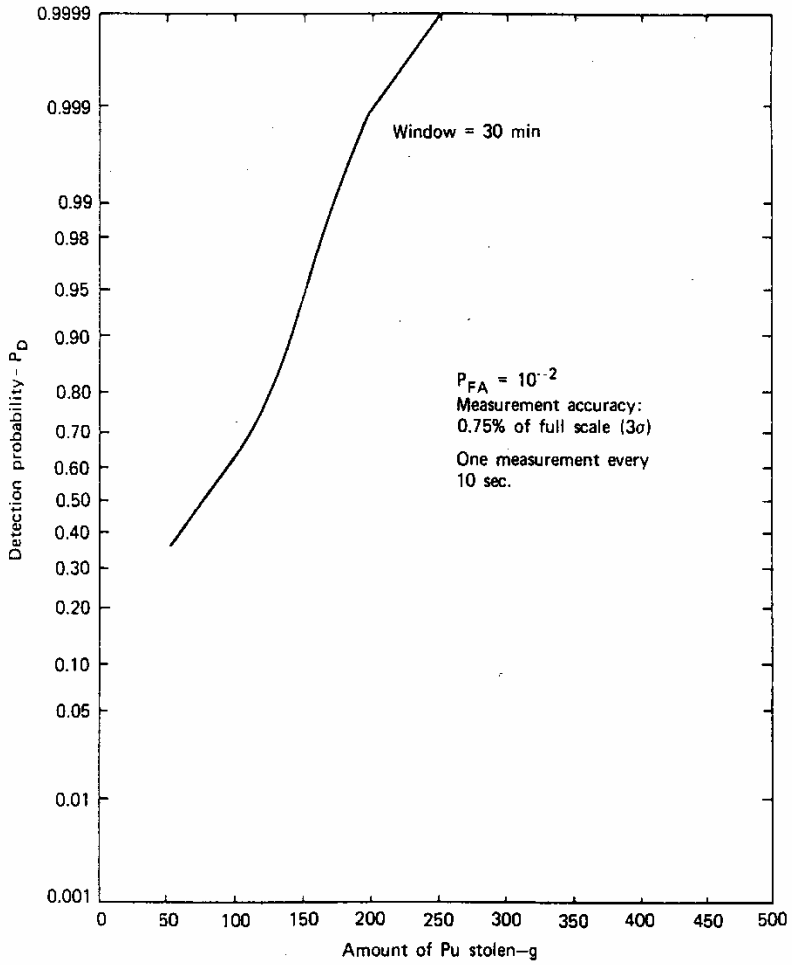
Sample Diversion Path

REFERENCE TABLE FOR MIN CUT SETS (TOTAL 36)

ORDER	1	2	3	4	5	6
NO. OF MIN CUT SETS	0	0	0	0	6	30

MIN CUT SET NO	ORDER	8-DIGIT NAME	FULL BASIC EVENT DESCRIPTION
1	5	BE1	GLOVES CUT
		BE2	ADVERSARY REMOVES SNM FROM SAMPLER
		BE3	ADVERSARY EXITS MAA
		BE6	GUARD IN COLLUSION
		BE7	NO OR SLOW RESPONSE FROM SECURITY

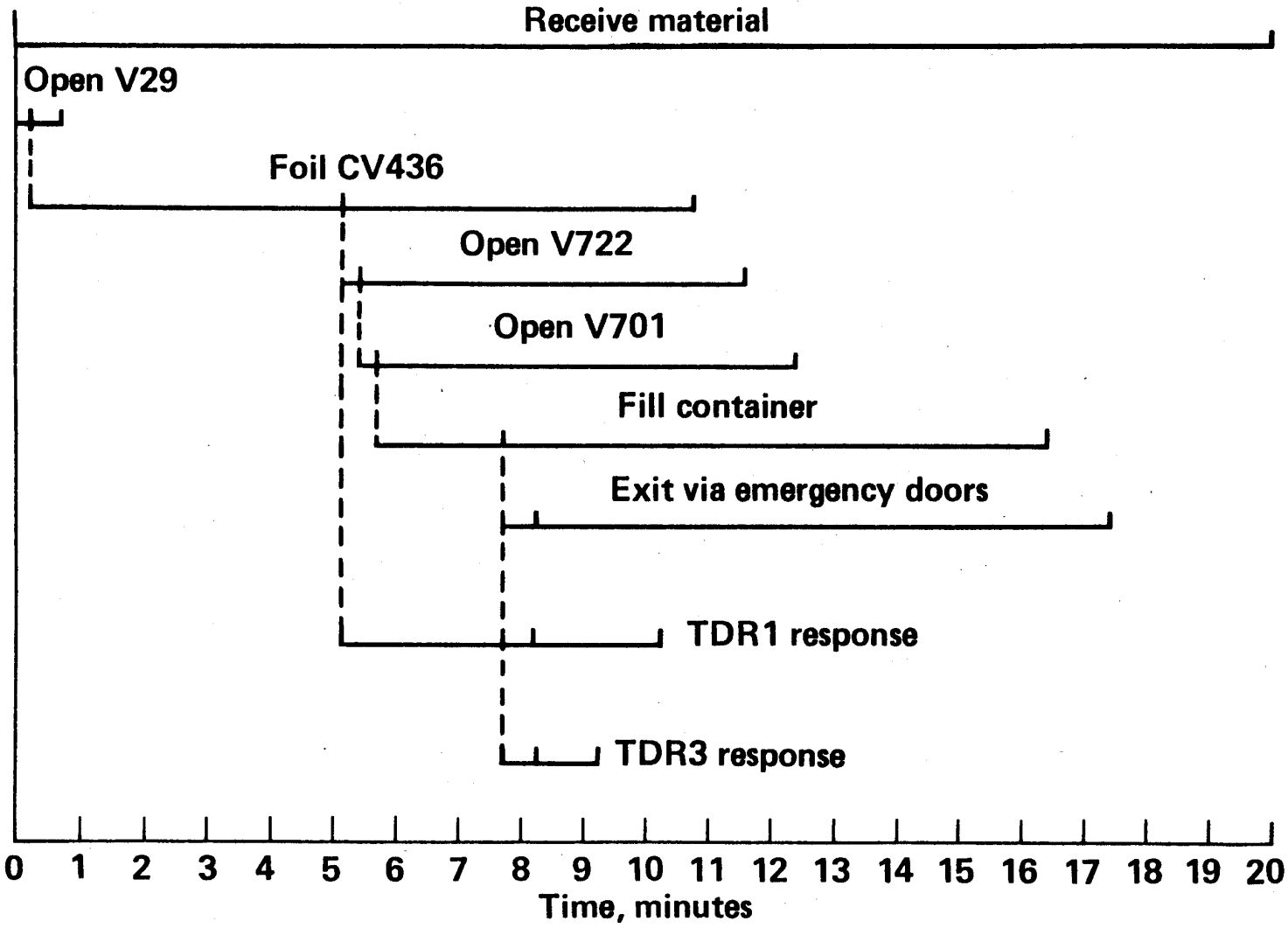
Detector Performance – Level Measurement



Safeguards System Reaction Rules (TDRs)

NATURE OF THE SITUATION	THEFT DANGER RATING (TDR)	RESPONSE
DIVERSION	TDR-3	ADEQUATE SECURITY REPONSE
POSSIBILITY OF DIVERSION	TDR-2	ADEQUATE SECURITY REPONSE
ANOMALY REQUIRING INVESTIGATION	TDR-1	INFORMATION GATHERING

Timing of Adversary Action and Physical Security Response



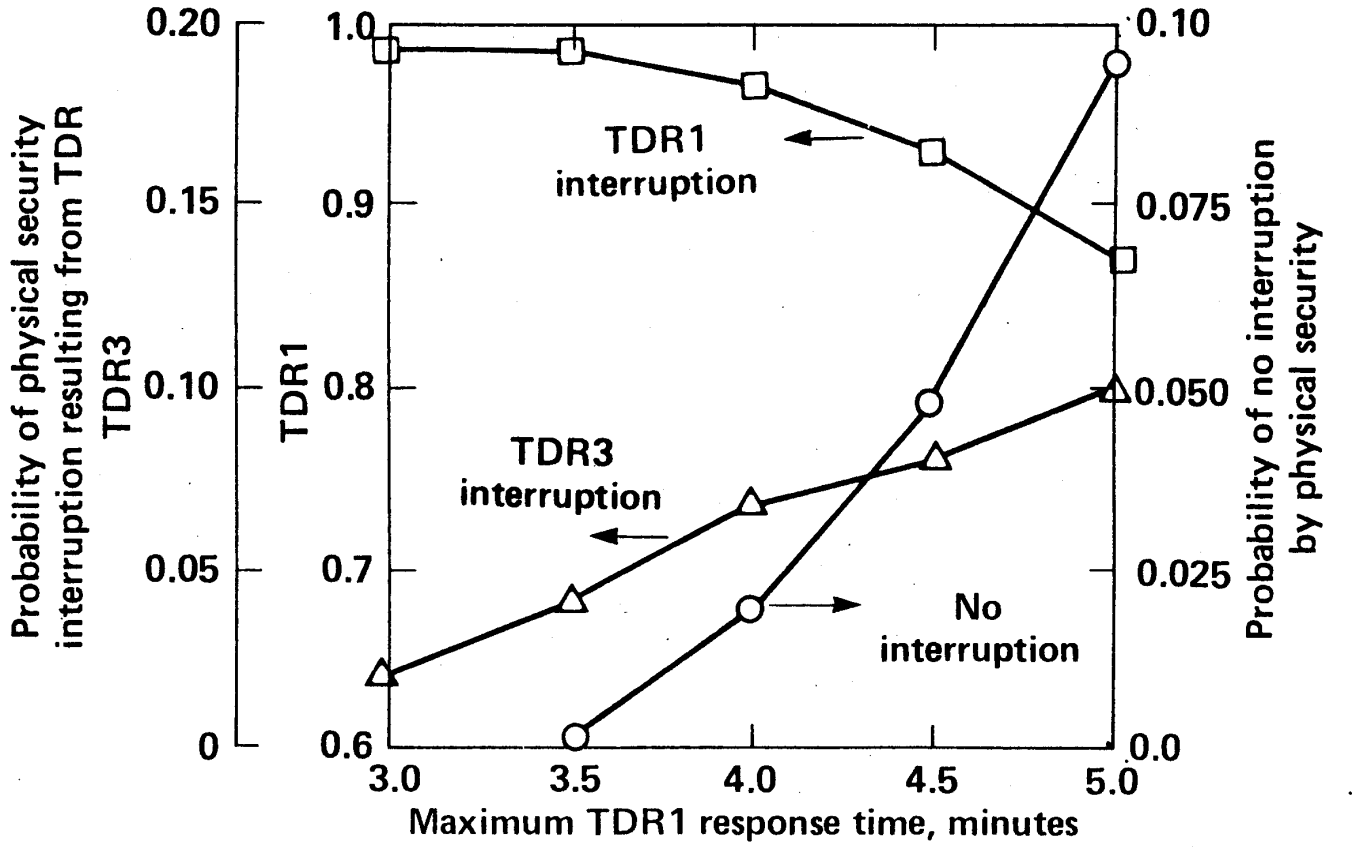
SIMULATION APPLICATION

- Probability of physical security interrupting an adversary within the Material Access Area (MAA), after TDR1 and TDR3 alarms was obtained from a simulation model – Material Control System Simulation (MCSS) software

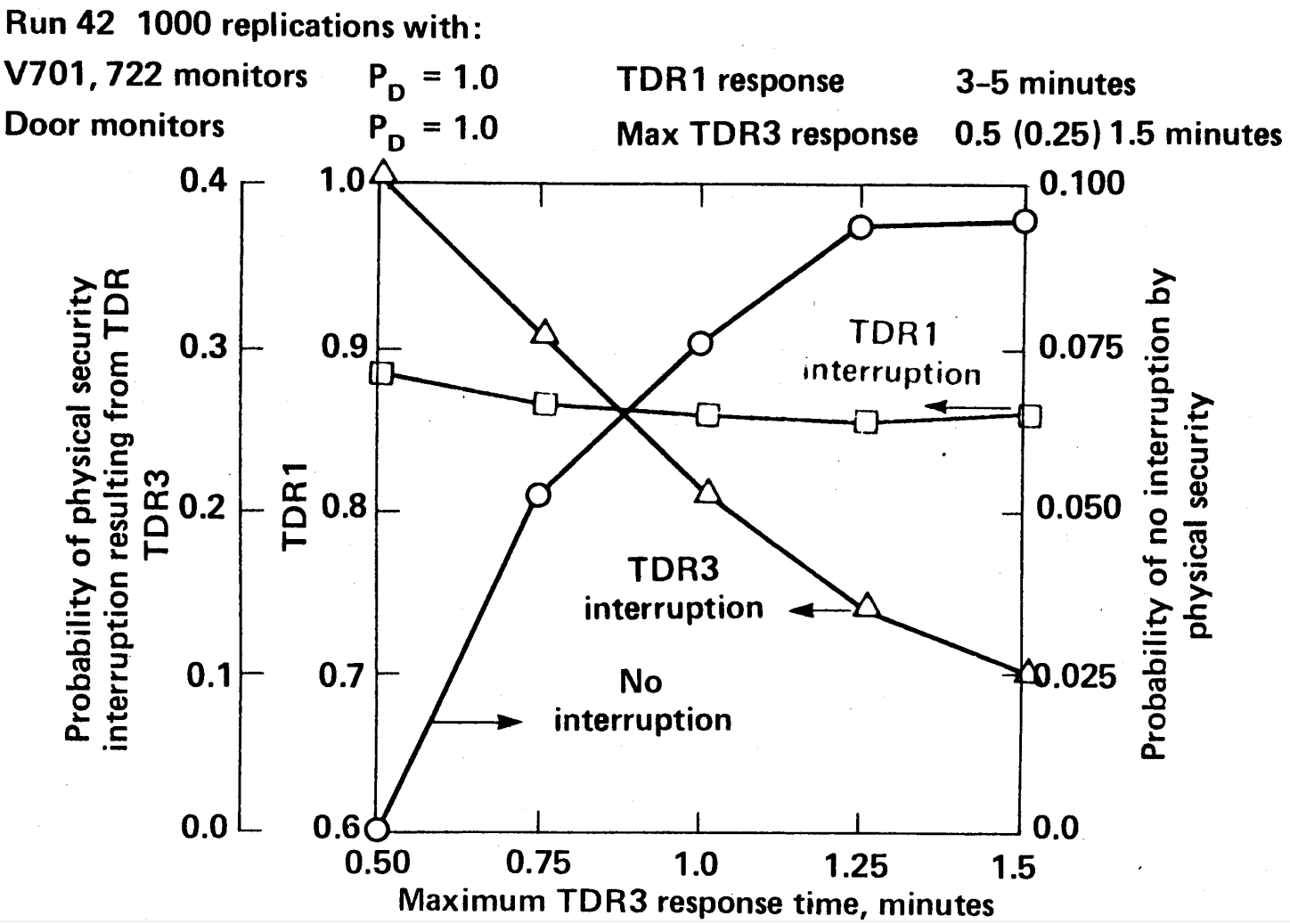
Results For Maximum TDR 1 Response Time

Run 41 1000 replications with:

V701, 722 monitors	P_D = 1.0	TDR 1 response	3.0 (0.5) 5.0 minutes
Door monitors	P_D = 1.0	TDR 3 response	0.5–1.5 minutes



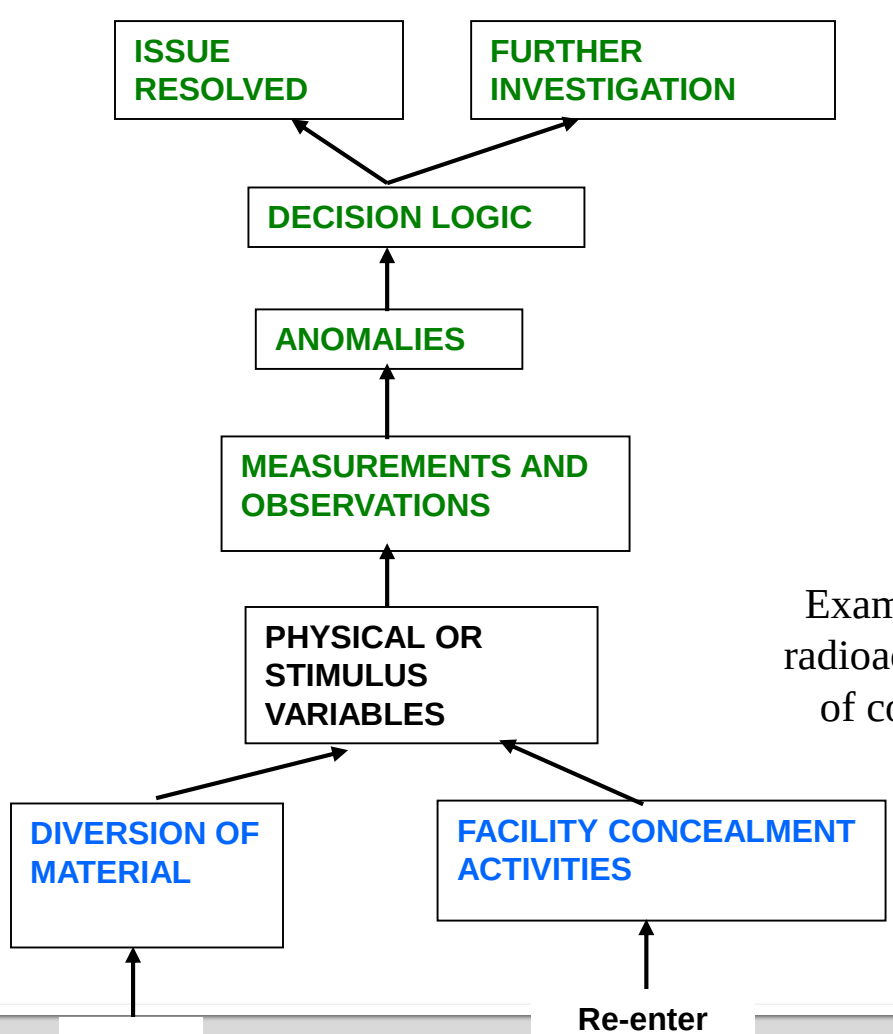
Results For Maximum TDR 3 Response Time



RESULTS FOR MAXIUM TDR1 RESPONSE TIME

TDR 1 RESPONSE	3-5 MINUTES
TDR 3 RESPONSE	0.5-1.5 MINUTES
PROBABILITY OF NO INTERRUPTION	0.095
PROBABILITY OF INTERRUPTION WITHIN MAA RESULTING FROM PHYSICAL SECURITY RESPONSE TO TDR1 ALARM	0.880
PROBABILITY OF INTERRUPTION WITHIN MAA RESULTING FROM PHYSICAL SECURITY RESPONSE TO TDR 3 ALARM	0.101

Flow of Information Regarding Detection Paths in the Digraph (International Safeguards)



IAEA ACTIONS

Examples, flow, concentration, mass, radioactive emissions, number and type of containers, facility configuration

Clandestine actions in facility

Applications of Directed Graph Fault Tree Approach for Safeguards Effectiveness Assessment

- **Provides a *structured systematic approach to incorporate all root causes for each diversion scenario* including operator misdeclarations**
- **Help *quantify the change in the probability of detection of diversion* due to the introduction or use of:**
  - **Material accounting, surveillance cameras, detectors…**
  - **New safeguards measures/tools**
  - **New technology**
  - **Changes in plant designs**
  - **Increasing Physical Security Response Times**
- **Help analyze cost-effectiveness of options**