TABLE-TOP
VULNERABILITY ANALYSIS
WORKSHOP

NOVEMBER 1994

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

TABLE-TOP VULNERABILITY ANALYSIS WORKSHOP AGENDA

1 Introduction

2 VA Process

3 VA Team

4 Threats

5 Targets

6 Outsider Threat Analysis (No Insider)

6A - VA Example

6B - VA Exercise

6C - Performance Testing

6D - Airborne Threat

7 Insider Threat Analysis

7A - VA Example

7B - VA Exercise

7C - Performance Testing

7D - Protracted Action

7E - Violent Insider

7F - Insider Assistance

8 Outsider Threat Analysis (with Insider)

8A - Non-Violent Insider Assistance

8B - Violent Insider Assistance

9 Performance Testing - Advanced Analysis

10 VA Quality

11 Summary

Test

TABLE-TOP VULNERABILITY ANALYSIS WORKSHOP

LEAD FACILITATORS

Lew Goldman and Larry Harris
Science Applications International Corporation
10260 Campus Point Drive (MS A1)
San Diego, CA 92121
Phones: (619) 458-2627 and (619) 458-2634

OUTSIDER THREAT PERFORMANCE TESTING

Garl Bultz
Science Applications International Corporation
USDOE Savannah River Site
Admin. Bldg. 703A, Road 1-A
P.O. Box A
Aiken, SC 20981
Phone: (803) 725-3063

Jack Pope
Science Applications International Corporation
20201 Century Blvd., Suite 300
Germantown, MD 20874
Phone: (301) 903-3286

INSIDER THREAT PERFORMANCE TESTING AND PERFORMANCE TESTING -- ADVANCED ANALYSIS

Joe Rivers
Science Applications International Corporation
20201 Century Blvd., Suite 300
Germantown, MD 20874
Phone: (301) 353-0172

Forward

This workshop was first funded in February 1993 by Battelle, Pacific Northwest Laboratories and was conducted for the DOE Rocky Flats Office in March 1993. The workshop was conducted for the DOE Savannah River Operations Office in April 1993. The vulnerability analysis (VA) method used for the workshop is a systems approach called VISA (Vulnerability of Integrated Security Analysis). This method resulted from a 1976 nationwide competition to develop a standard VA method to be used at U.S. licensed nuclear facilities. The VISA method was first presented by SAIC at the 1977 Institute of Nuclear Materials Management (INMM) annual meeting. Subsequently, the method was applied at high-risk facilities operated by DOD, DOE, NASA and other agencies. The method has been continually refined through the years by incorporating lessons learned from its application at many types of facilities and from ideas offered in published papers and reports and at professional conferences on other security evaluation methods. Follow-up SAIC papers describing these refinements and related topics were presented at INMM annual meetings in 1981, 1985, 1989 and 1992. The 1992 INMM paper, which is included in Section 12, describes a six-step VA process that is used for this workshop. The published SAIC papers include acknowledgments of the many contributors to the VISA method and references that give attribution to the work of several other developers of security evaluation methods.

Lewis Goldman and Lawrence Harris

1. Introduction

1. INTRODUCTION

PURPOSE OF
TABLE-TOP VULNERABILITY ANALYSIS WORKSHOP

To provide participants an understanding of the vulnerability analysis (VA) process and to prepare them to participate on VA teams to perform table-top VAs in roles consistent with their security training and experience. Participants should also gain a broad view of how many, diverse safeguards and security measures can work together to protect designated targets against design-basis threats. An understanding of the VA process is an essential prerequisite to effective and efficient use of any computer VA method.

GOALS FOR
TABLE-TOP VULNERABILITY ANALYSIS WORKSHOP

Introduction To describe the purpose and goals of the workshop and to provide an overview of the presentations and exercises planned.

VA Process To provide an understanding of the purpose and roles of vulnerability analyses (VAs) and a general understanding of the VA process.

VA Team To provide an understanding of criteria used for selecting VA team members and an approach for preparing team members to perform VAs.

Threats To describe the threat information required to perform VAs and to outline current DOE policy on threats.

GOALS FOR
TABLE-TOP VULNERABILITY ANALYSIS WORKSHOP

Targets To provide an approach for identifying SNM theft and sabotage targets that are to be protected against design-basis threats.

Facility and S&S System To describe the facility and safeguards and security (S&S) system information required to perform VAs and an approach for acquiring and organizing this information. Insider and outsider threats.

Vulnerabilities and Scenarios To provide approaches for identifying vulnerabilities associated with the protection of specific targets against design-basis threats and developing scenarios that adversaries could use to exploit these vulnerabilities. Insider and outsider threats.

System Effectiveness To provide an approach for evaluating the effectiveness of a S&S system to protect designated targets against design-basis threats. Insider and outsider threats.

GOALS FOR
TABLE-TOP VULNERABILITY ANALYSIS WORKSHOP

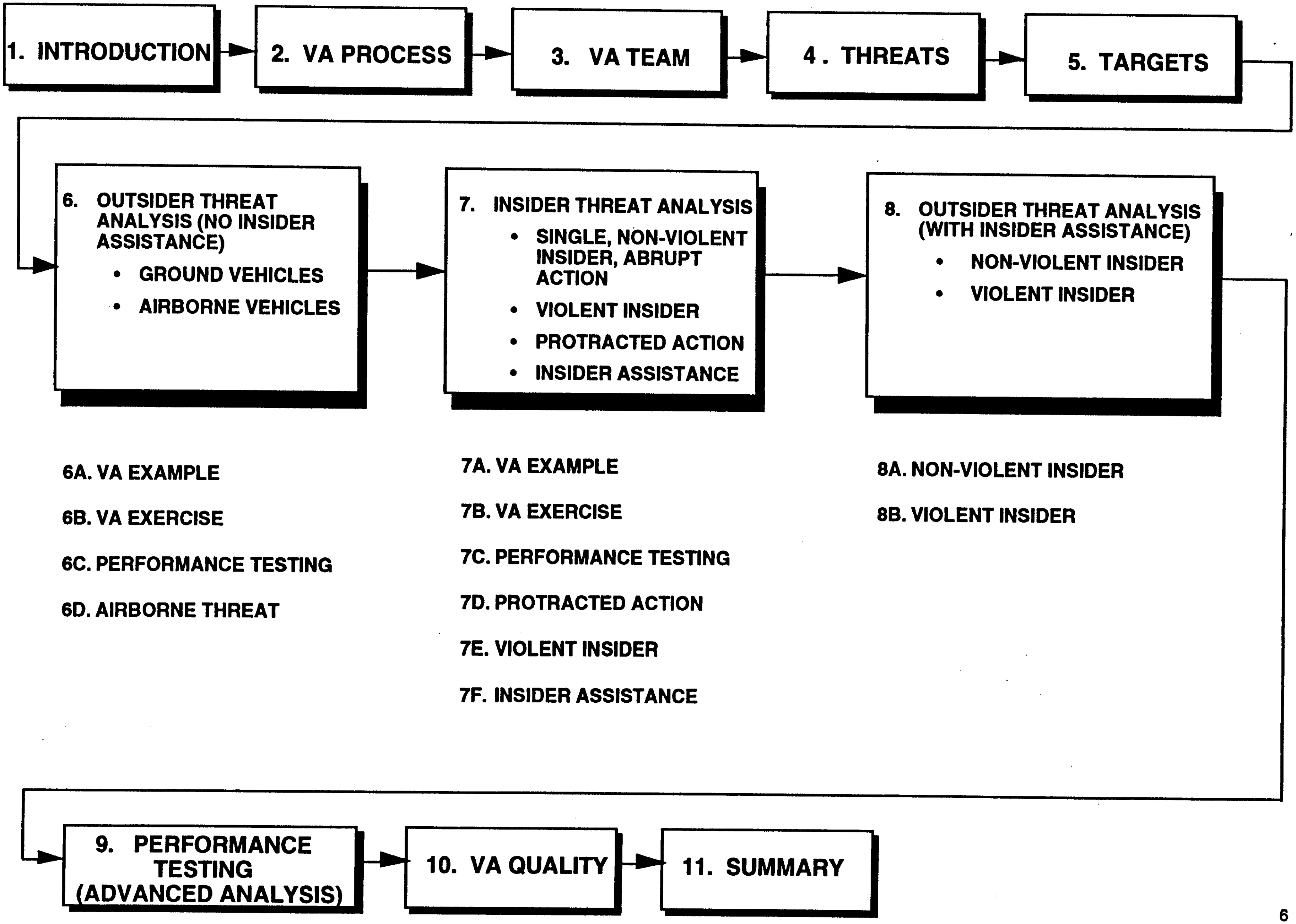
Performance Testing To provide an understanding of the various types of performance tests that can contribute to an evaluation of system effectiveness and to provide approaches for selecting such tests. Insider and outsider threats.

S&S System Change To provide an approach for identifying candidate S&S system changes and prioritizing them according to efficiency/cost-effectiveness criteria. Insider and outsider threats.

VA Quality To provide an approach for influencing the quality of VAs.

Summary To review key aspects of the VA process and its uses.

FLOWCHART FOR TABLE-TOP VA WORKSHOP



1. INTRODUCTION

2. VA PROCESS

3. VA TEAM

4. THREATS

5. TARGETS

6. OUTSIDER THREAT ANALYSIS (NO INSIDER ASSISTANCE)
   - GROUND VEHICLES
   - AIRBORNE VEHICLES

7. INSIDER THREAT ANALYSIS
   - SINGLE, NON-VIOLENT INSIDER, ABRUPT ACTION
   - VIOLENT INSIDER
   - PROTRACTED ACTION
   - INSIDER ASSISTANCE

8. OUTSIDER THREAT ANALYSIS (WITH INSIDER ASSISTANCE)
   - NON-VIOLENT INSIDER
   - VIOLENT INSIDER

6A. VA EXAMPLE

6B. VA EXERCISE

6C. PERFORMANCE TESTING

6D. AIRBORNE THREAT

7A. VA EXAMPLE

7B. VA EXERCISE

7C. PERFORMANCE TESTING

7D. PROTRACTED ACTION

7E. VIOLENT INSIDER

7F. INSIDER ASSISTANCE

8A. NON-VIOLENT INSIDER

8B. VIOLENT INSIDER

9. PERFORMANCE TESTING (ADVANCED ANALYSIS)

10. VA QUALITY

11. SUMMARY

2. VA Process

2. VA PROCESS

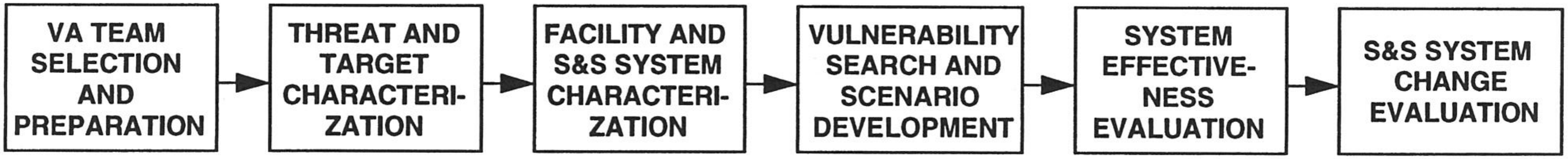
WHY PERFORM VULNERABILITY ANALYSES?

- VAs PROVIDE A “YARDSTICK” FOR DETERMINING HOW WELL A SYSTEM PERFORMANCE REQUIREMENT IS MET.

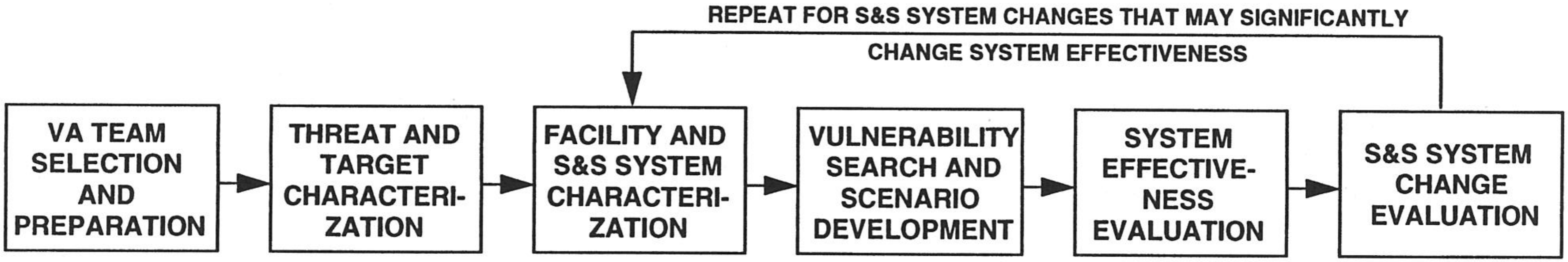
WHAT IS A "SYSTEM PERFORMANCE REQUIREMENT"?

- SECURITY REQUIREMENTS CAN BE CATEGORIZED AS FOLLOWS:
  - PRESCRIPTIVE REQUIREMENTS SPECIFY VARIOUS S&S MEASURES THAT NEED TO BE PROVIDED TO PROTECT DESIGNATED ASSETS.
  - COMPONENT AND SUBSYSTEM PERFORMANCE REQUIREMENTS SPECIFY HOW WELL INDIVIDUAL S&S MEASURES NEED TO FUNCTION.
  - SYSTEM PERFORMANCE REQUIREMENTS SPECIFY HOW WELL S&S MEASURES NEED TO FUNCTION TOGETHER (IN SOME SITUATIONS, VERY PROMPTLY) TO PROTECT DESIGNATED TARGETS AGAINST DESIGN-BASIS THREATS. THE MEASURE OF PERFORMANCE IS CALLED "SYSTEM EFFECTIVENESS."

FLOWCHART OF VA PROCESS

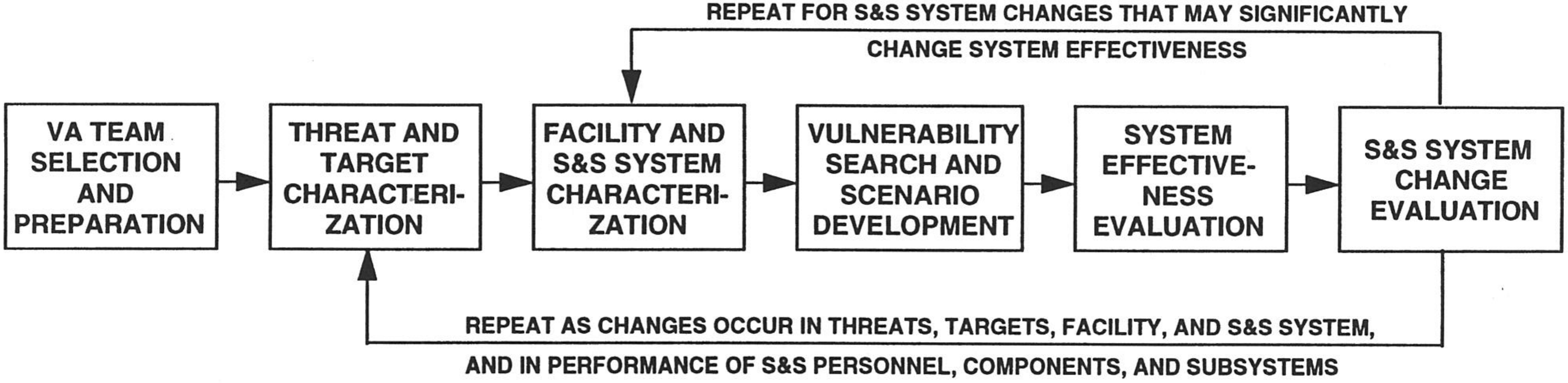

VA TEAM SELECTION AND PREPARATION
THREAT AND TARGET CHARACTERIZATION
FACILITY AND S&S SYSTEM CHARACTERIZATION
VULNERABILITY SEARCH AND SCENARIO DEVELOPMENT
SYSTEM EFFECTIVENESS EVALUATION
S&S SYSTEM CHANGE EVALUATION

FLOWCHART OF VA PROCESS



REPEAT FOR S&S SYSTEM CHANGES THAT MAY SIGNIFICANTLY CHANGE SYSTEM EFFECTIVENESS
VA TEAM SELECTION AND PREPARATION
THREAT AND TARGET CHARACTERIZATION
FACILITY AND S&S SYSTEM CHARACTERIZATION
VULNERABILITY SEARCH AND SCENARIO DEVELOPMENT
SYSTEM EFFECTIVENESS EVALUATION
S&S SYSTEM CHANGE EVALUATION

FLOWCHART OF VA PROCESS



REPEAT FOR S&S SYSTEM CHANGES THAT MAY SIGNIFICANTLY CHANGE SYSTEM EFFECTIVENESS

VA TEAM SELECTION AND PREPARATION

THREAT AND TARGET CHARACTERIZATION

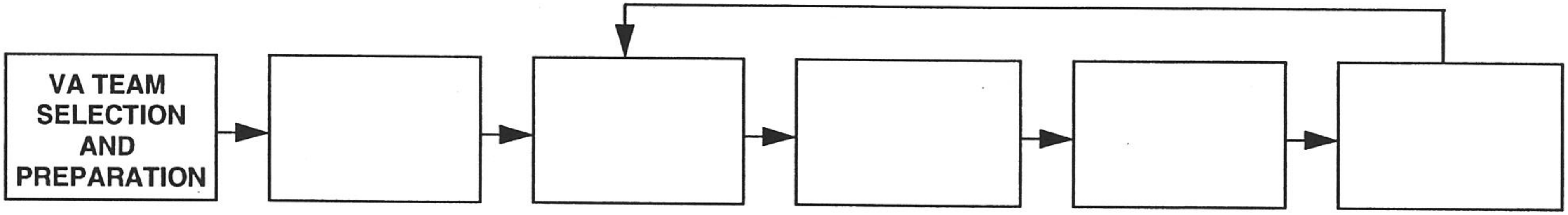
FACILITY AND S&S SYSTEM CHARACTERIZATION

VULNERABILITY SEARCH AND SCENARIO DEVELOPMENT

SYSTEM EFFECTIVENESS EVALUATION

S&S SYSTEM CHANGE EVALUATION

REPEAT AS CHANGES OCCUR IN THREATS, TARGETS, FACILITY, AND S&S SYSTEM, AND IN PERFORMANCE OF S&S PERSONNEL, COMPONENTS, AND SUBSYSTEMS



VA TEAM SELECTION AND PREPARATION

VA CORE TEAM

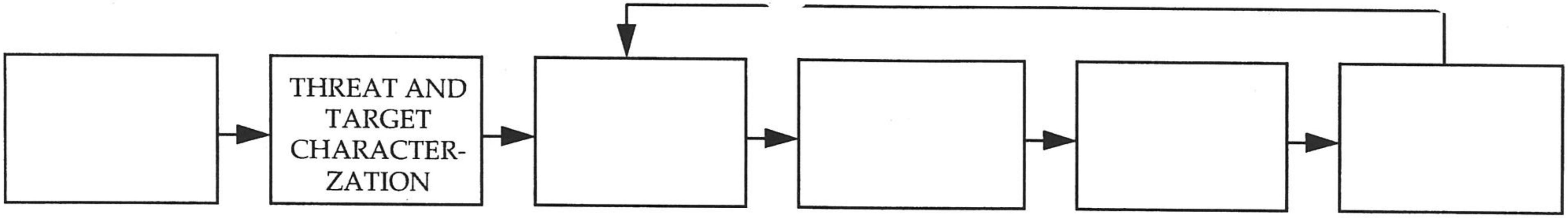
- VA SPECIALIST
- PERFORMANCE TESTING (PT) SPECIALIST
- PROTECTIVE FORCE (PF) SPECIALIST
- PHYSICAL SECURITY SYSTEMS (PSS) SPECIALIST
- MC&A SPECIALIST
- FACILITY OPERATION SPECIALIST

VA SUPPORT TEAM

- CAS/SAS SPECIALIST
- UTILITIES SPECIALIST
- MAINTENANCE SPECIALIST
- SHIPMENT AND TRANSPORTATION SPECIALIST
- BUDGET SPECIALIST
- SAFETY SPECIALIST
- FACILITY MANAGER
- PROGRAM MANAGER
- OTHER SPECIALISTS AND MANAGERS AS REQURED

- VA TEAM SELECTION
  - PURPOSE AND SCOPE OF VA
  - EXPERIENCE REQUIRED
  - TEAM DIVERSITY
  - TEAM FACILITATOR

- VA TEAM PREPARATION
  - PLANNING VA
  - ESTABLISHING VA REPORT FORMAT
  - ORIENTING VA TEAM TO FACILITY AND S&S SYSTEM



PRODUCT: LIST OF THREAT-TARGET PAIRS TO BE ANALYZED

- Design-basis threats

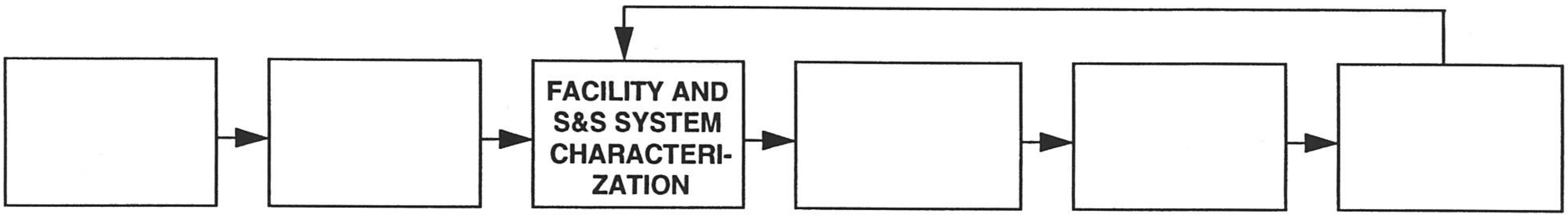
Adversary types

- ▲ Terrorists
- ▲ Criminals
- ▲ Psychotics
- ▲ Disgruntled employees
- ▲ Violent activist

Malevolent acts

- ▲ SNM theft
- ▲ Radiological/toxicological sabotage
- ▲ Industrial sabotage

- Key adversary attributes
  - ▲ Number of outsiders and/or insiders
  - ▲ Motivation
  - ▲ Willingness to kill and/or be killed
  - ▲ Knowledge and skills
  - ▲ Weapons, explosives, and tools
  - ▲ Vehicles (ground and/or airborne)
  - ▲ Communications
  - ▲ Access and S&S authority (insiders)
- Like targets can be grouped
  - ▲ Similar nuclear materials
  - ▲ Similar protection



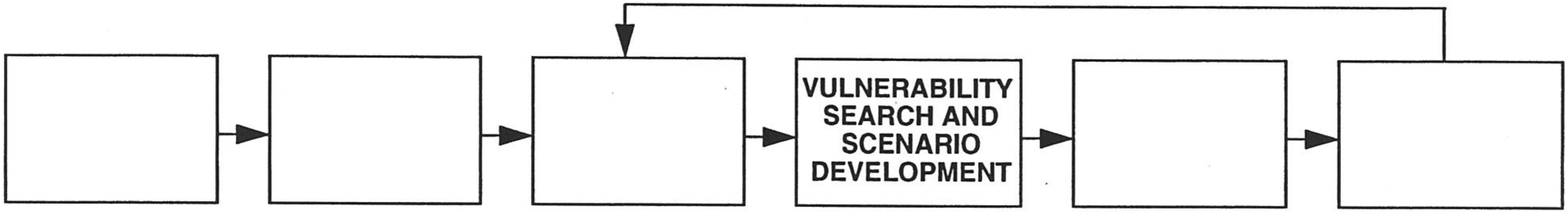
PRODUCT:

- DESCRIPTION OF SITE, FACILITY AND S&S SYSTEM.
- INFORMATION ON PERFORMANCE OF S&S PERSONNEL, COMPONENTS AND SUBSYSTEMS.

- **FACILITY AND S&S SYSTEM CHARACTERIZATION SHOULD REPRESENT A SNAPSHOT IN TIME WHICH IS CONSISTENT WITH PURPOSE OF VA.**
- **COLLECT INFORMATION RELEVANT TO PROTECTION OF KEY TARGETS AGAINST THREATS TO BE ADDRESSED.**

SOURCES OF FACILITY AND S&S SYSTEM INFORMATION

- AS-BUILT DRAWINGS OF SITE, FACILITY, S&S COMPONENTS, AND S&S SUBSYSTEMS.
- S&S PLANS:
  - SECURITY PLANS, PROCEDURES, AND RECORDS.
  - PROTECTIVE FORCE POST ORDERS AND EMERGENCY RESPONSE PLANS.
  - MC&A PLANS, PROCEDURES AND RECORDS.
  - STAFFING PLANS.
- TRAINING PLANS AND RECORDS.
- EQUIPMENT SPECIFICATIONS, OPERATING MANUALS, MAINTENANCE PLANS AND RECORDS.
- ALARM LOGS AND INCIDENT REPORTS.
- SURVEY AND INSPECTION REPORTS.
- TEAM MEMBER TOURS, INSPECTIONS AND INTERVIEWS.



PRODUCT:

- LIST OF VULNERABILITIES.
- ADVERSARY'S PLANS OFATTACK FOR MOST CREDIBLE SCENARIOS.

- PERFORM ANALYSIS FOR EACH COMBINATION OF THREAT AND TARGET.
- SEARCH FOR VULNERABILITIES THAT CAN BE EXPLOITED BY ADVERSARY.
- CONSIDER ALL REASONABLE ADVERSARY STRATEGIES, TACTICS, AND PATHS.
- CONSIDER ALL FACILITY CONDITIONS (OPERATING, SHUTDOWN, MAINTENANCE, EMERGENCY).
- DEVELOP CREDIBLE SCENARIOS THAT GIVE ADVERSARY BEST CHANCE FOR SUCCESS.

VULNERABILITY SEARCH METHODS

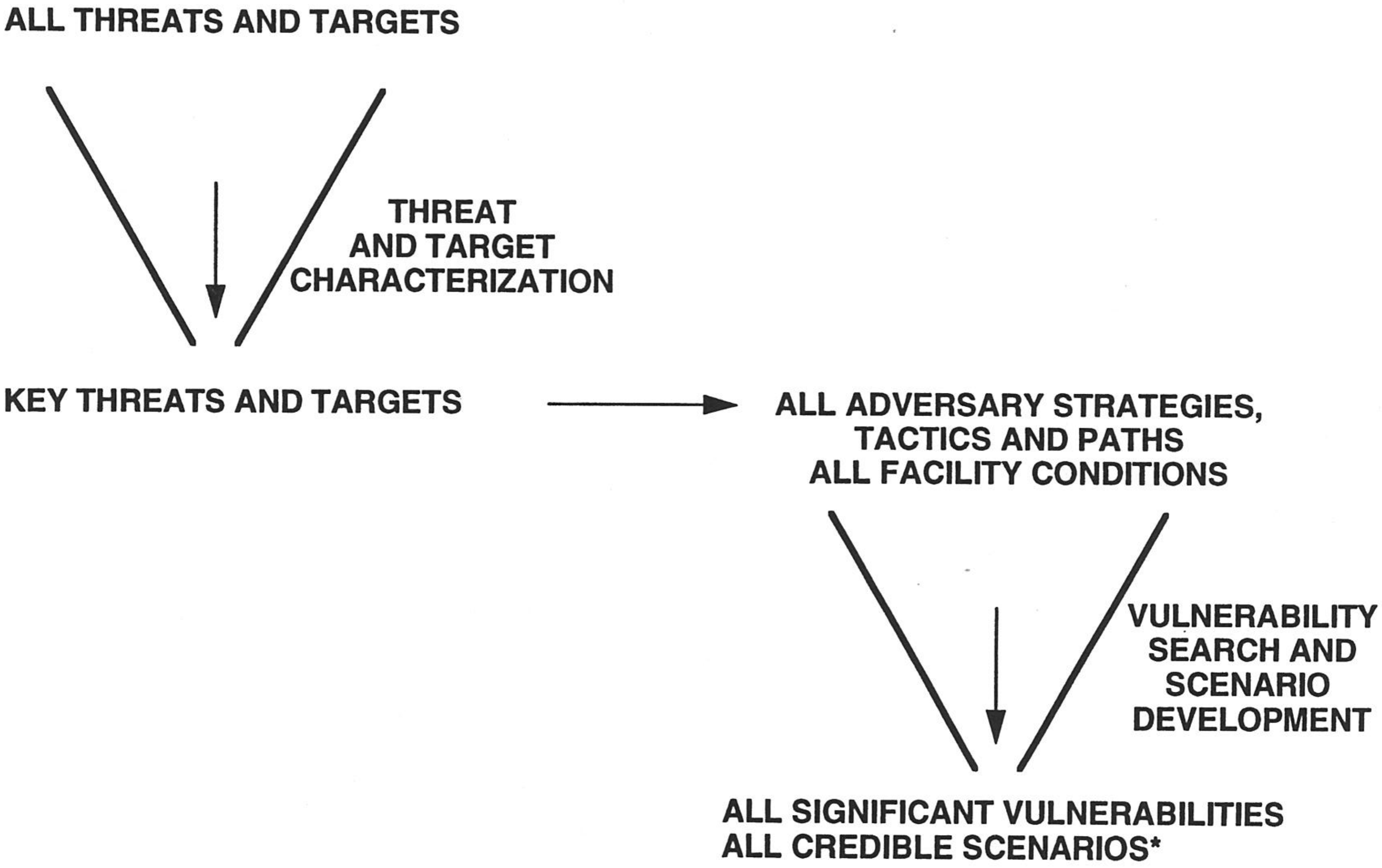
- OBSERVATION AND INSPECTION.
- ADVERSARY ROLE PLAYING.
- SCENARIO DEVELOPMENT.
- PERFORMANCE TESTING.
- ADVERSARY SEQUENCE DIAGRAM ANALYSIS.

ADVERSARY STRATEGIES, TACTICS AND PATHS

- STRATEGIES
  - COVERT (AND POSSIBLE USE OF COVERUP) OR COVERT, THEN OVERT (AND POSSIBLE USE OF SURPRISE)
  - ABRUPT OR PROTRACTED (ONE STAGE OR MULTIPLE STAGES)
  - INSIDER ASSISTANCE
- TACTICS
  - STEALTH
  - DECEIT
  - FORCE (VIOLENCE)
  - COMPROMISE AND/OR CIRCUMVENTION OF S&S MEASURES (MAY INCLUDE TAMPERING, COERSION, AMBUSH, DIVERSION, ETC.)
- PATHS
  - GROUND
  - UNDERGROUND
  - AIR

VULNERABILITY
SEARCH AND
SCENARIO
DEVELOPMENT

SCREENING INHERENT IN VA PROCESS



ALL THREATS AND TARGETS

THREAT
AND TARGET
CHARACTERIZATION

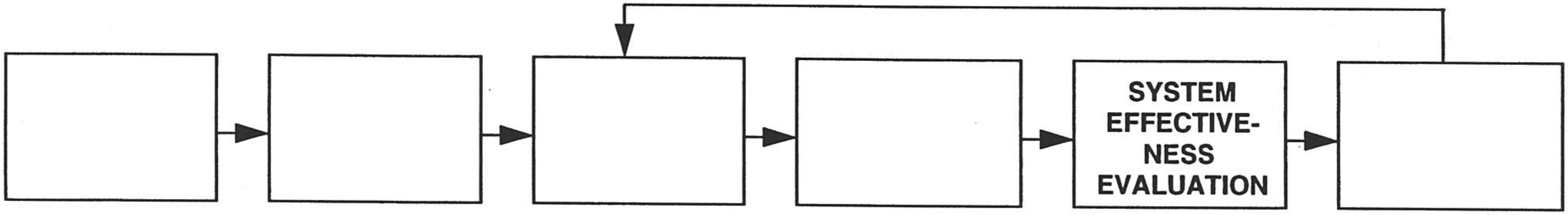
KEY THREATS AND TARGETS

ALL ADVERSARY STRATEGIES,
TACTICS AND PATHS
ALL FACILITY CONDITIONS

VULNERABILITY
SEARCH AND
SCENARIO
DEVELOPMENT

ALL SIGNIFICANT VULNERABILITIES
ALL CREDIBLE SCENARIOS*

* Credible scenarios are those that give adversary best chance for success.



PRODUCT:

LEVELS OF SYSTEM EFFECTIVENESS

- PERFORM EVALUATION FOR EACH CREDIBLE SCENARIO DEVELOPED.
- FOR COVERT SCENARIOS
  - DETERMINE EFFECTIVENESS OF TWO ESSENTIAL S&S SYSTEM CAPABILITIES:
    - DETECTION
    - ASSESSMENT
  - COMBINE RESULTS TO DETERMINE SYSTEM EFFECTIVENESS.
- FOR COVERT-OVERT SCENARIOS
  - ESTIMATE ADVERSARY TIME LINES AND RESPONSE FORCE TIME LINES.
  - DETERMINE EFFECTIVENESS OF FOUR ESSENTIAL S&S CAPABILITIES:
    - DETECTION
    - ASSESSMENT
    - ENGAGEMENT
    - NEUTRALIZATION
  - COMBINE RESULTS TO DETERMINE SYSTEM EFFECTIVENESS.

ESSENTIAL S&S SYSTEM CAPABILITIES

- DETECTION: PRODUCE AN ALARM
- ASSESSMENT: DECIDE IF RESPONSE FORCE SHOULD DEPLOY
- ENGAGEMENT: DEPLOY RESPONSE FORCE TO LOCATIONS WHERE ADVERSARIES CAN BE ENGAGED
- NEUTRALIZATION: STOP ADVERSARIES FROM ACHIEVING THEIR OBJECTIVE

APPLICABILITY OF S&S MEASURES TO FOUR ESSENTIAL S&S SYSTEM CAPABILITIES

S&S MEASURES	DETECTION	ASSESSMENT	ENGAGEMENT	NEUTRALIZATION
ACCESS CONTROLS	●			
MATERIAL CONTROLS	●			
INTRUSION DETECTION	●	●		
MATERIAL ACCOUNTING	●	●		
LIGHTING AND CCTV	●	●	●	●
SECURITY POSTS	●	●	●	●
COMMUNICATIONS	●	●	●	●
BARRIERS AND DELAYS	●	●	●	●
COMMAND AND CONTROL		●	●	●
RESPONSE FORCE			●	●
FIGHTING POSITIONS				●

DETECTION & ASSESSMENT & ENGAGEMENT = "INTERRUPTION" IN SAVI/ASSESS OUTSIDER THREAT MODULE

TWO-PARAMETER EQUATION FOR S&S SYSTEM EFFECTIVENESS (SE)

-- FOR TWO INDEPENDENT DETECTION OPPORTUNITIES --

$$SE = \underset{\substack{\text{CONTRIBUTION OF FIRST}\\ \text{DETECTION OPPORTUNITY}}}{\underline{PD1 \bullet PR1}} + \underset{\substack{\text{CONTRIBUTION OF SECOND}\\ \text{DETECTION OPPORTUNITY}}}{\underline{(1 - PD1)\ PD2 \bullet PR2}}$$

PD = PROBABILITY OF DETECTION AND CORRECT ALARM ASSESSMENT, GIVEN ADVERSARY ATTEMPT.

PR = PROBABILITY OF ENGAGEMENT AND NEUTRALIZATION, GIVEN DETECTION AND CORRECT ALARM ASSESSMENT.

TWO-PARAMETER EQUATION FOR SE

-- FOR THREE INDEPENDENT DETECTION OPPORTUNITIES --

$$SE = \underbrace{PD1 \bullet PR1}_{\substack{\text{CONTRIBUTION}\\ \text{OF FIRST}\\ \text{DETECTION}\\ \text{OPPORTUNITY}}} + \underbrace{(1\text{-}PD1)PD2 \bullet PR2}_{\substack{\text{CONTRIBUTION}\\ \text{OF SECOND}\\ \text{DETECTION}\\ \text{OPPORTUNITY}}} + \underbrace{(1 - PD1)(1\text{-}PD2)\ PD3 \bullet PR3}_{\substack{\text{CONTRIBUTION OF THIRD}\\ \text{DETECTION OPPORTUNITY}}}$$

FOUR-PARAMETER EQUATION FOR SE

-- FOR TWO INDEPENDENT DETECTION OPPORTUNITIES --

$$SE = \underbrace{PD1 \bullet PA1 \bullet PE1 \bullet PN1}_{\substack{\text{CONTRIBUTION OF FIRST} \\ \text{DETECTION OPPORTUNITY}}} + \underbrace{(1 - PD1 \bullet PA1)\ PD2 \bullet PA2 \bullet PE2 \bullet PN2}_{\substack{\text{CONTRIBUTION OF SECOND} \\ \text{DETECTION OPPORTUNITY}}}$$

PD = PROBABILITY OF DETECTION, GIVEN ADVERSARY ATTEMPT.

PA = PROBABILITY OF CORRECT ALARM ASSESSMENT, GIVEN DETECTION.

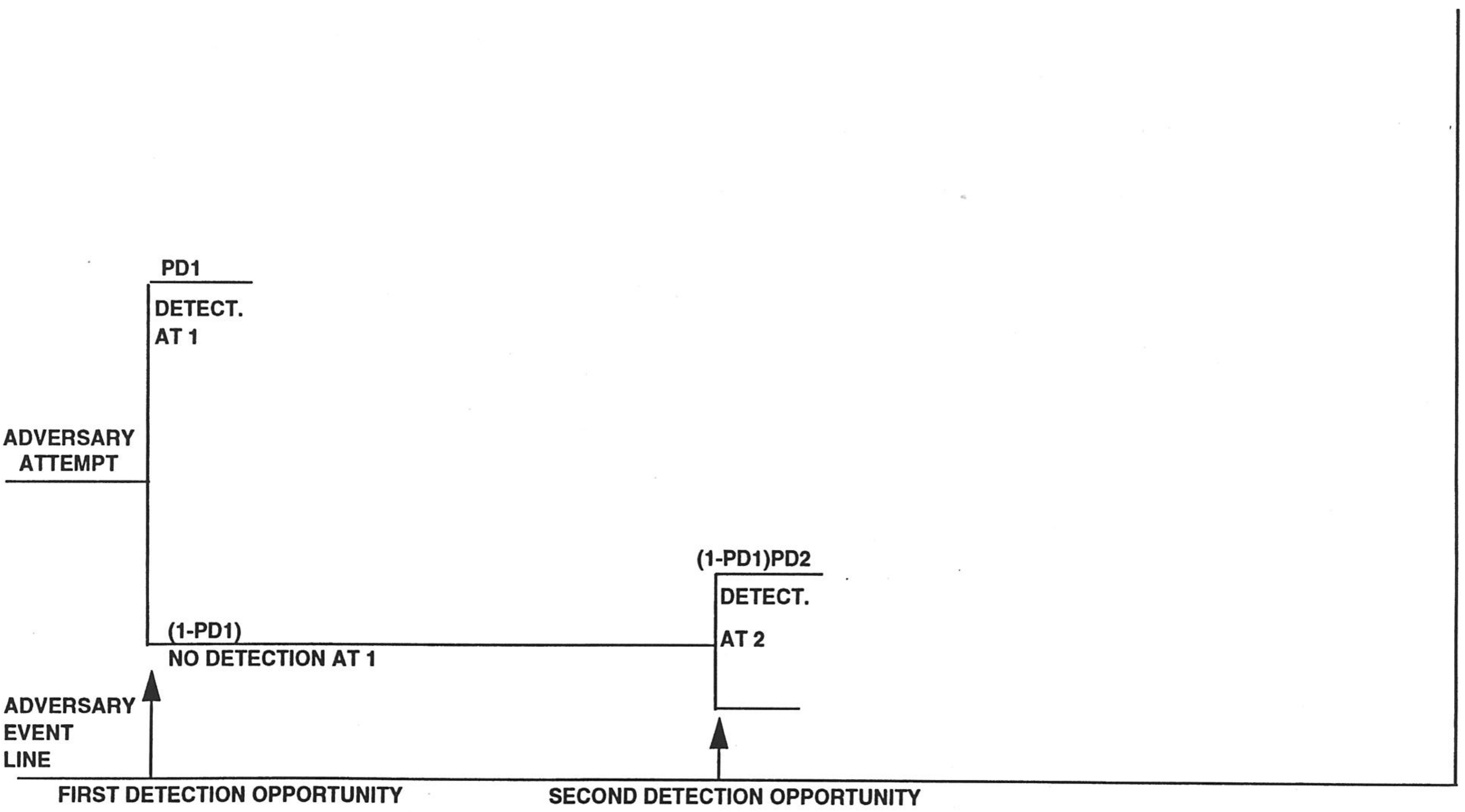
PE = PROBABILITY OF ENGAGEMENT, GIVEN CORRECT ALARM ASSESSMENT.

PN = PROBABILITY OF NEUTRALIZATION, GIVEN ENGAGEMENT.

SYSTEM EFFECTIVENESS EVALUATION

LOGIC TREE TO DETERMINE FOUR-PARAMETER EQUATION FOR SE

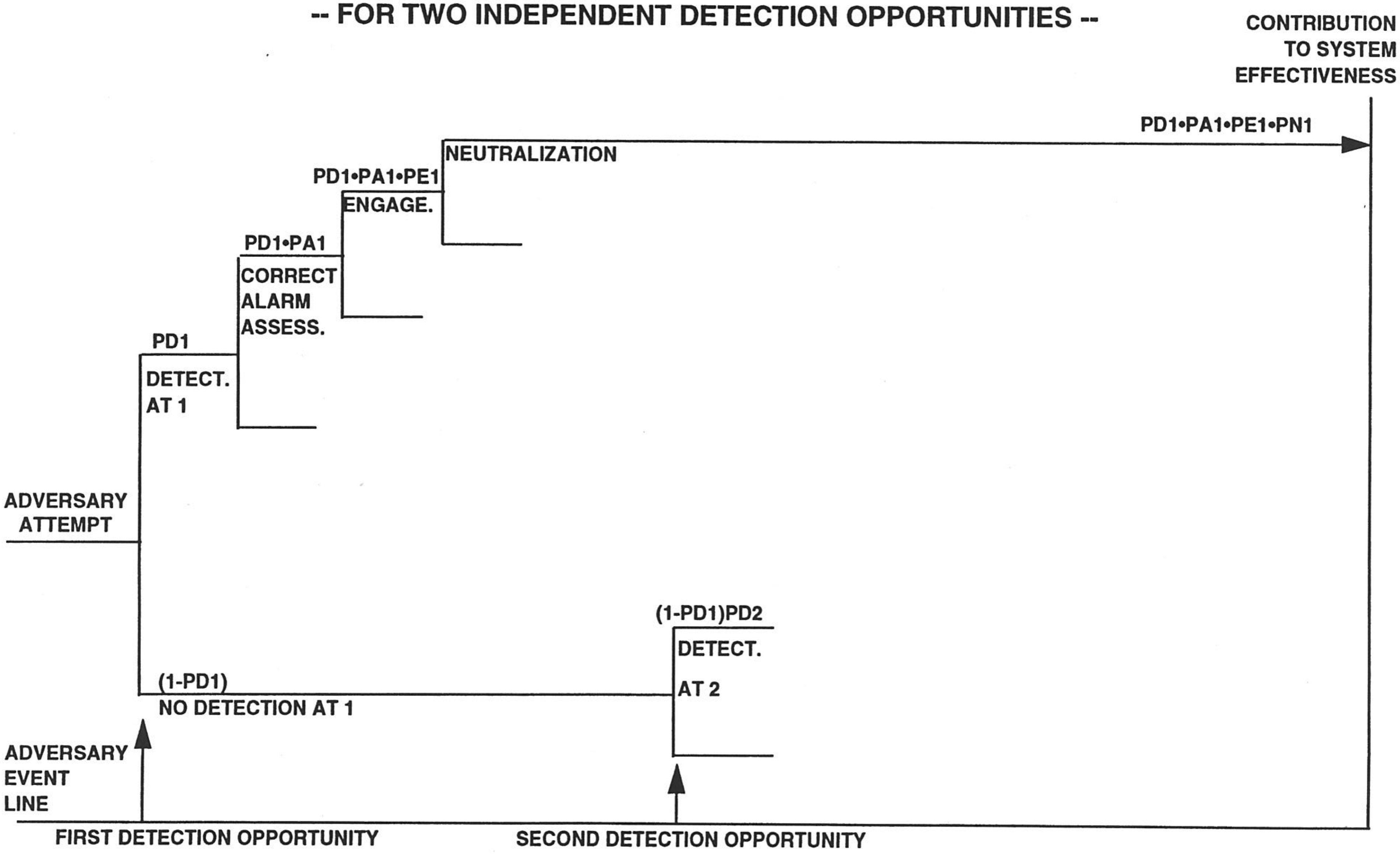
-- FOR TWO INDEPENDENT DETECTION OPPORTUNITIES --



SYSTEM
EFFECTIVE-
NESS
EVALUATION

LOGIC TREE TO DETERMINE FOUR-PARAMETER EQUATION FOR SE

-- FOR TWO INDEPENDENT DETECTION OPPORTUNITIES --



CONTRIBUTION TO SYSTEM EFFECTIVENESS

PD1•PA1•PE1•PN1

NEUTRALIZATION

PD1•PA1•PE1

ENGAGE.

PD1•PA1

CORRECT ALARM ASSESS.

PD1

DETECT. AT 1

ADVERSARY ATTEMPT

(1-PD1)PD2

DETECT. AT 2

(1-PD1)

NO DETECTION AT 1

ADVERSARY EVENT LINE

FIRST DETECTION OPPORTUNITY

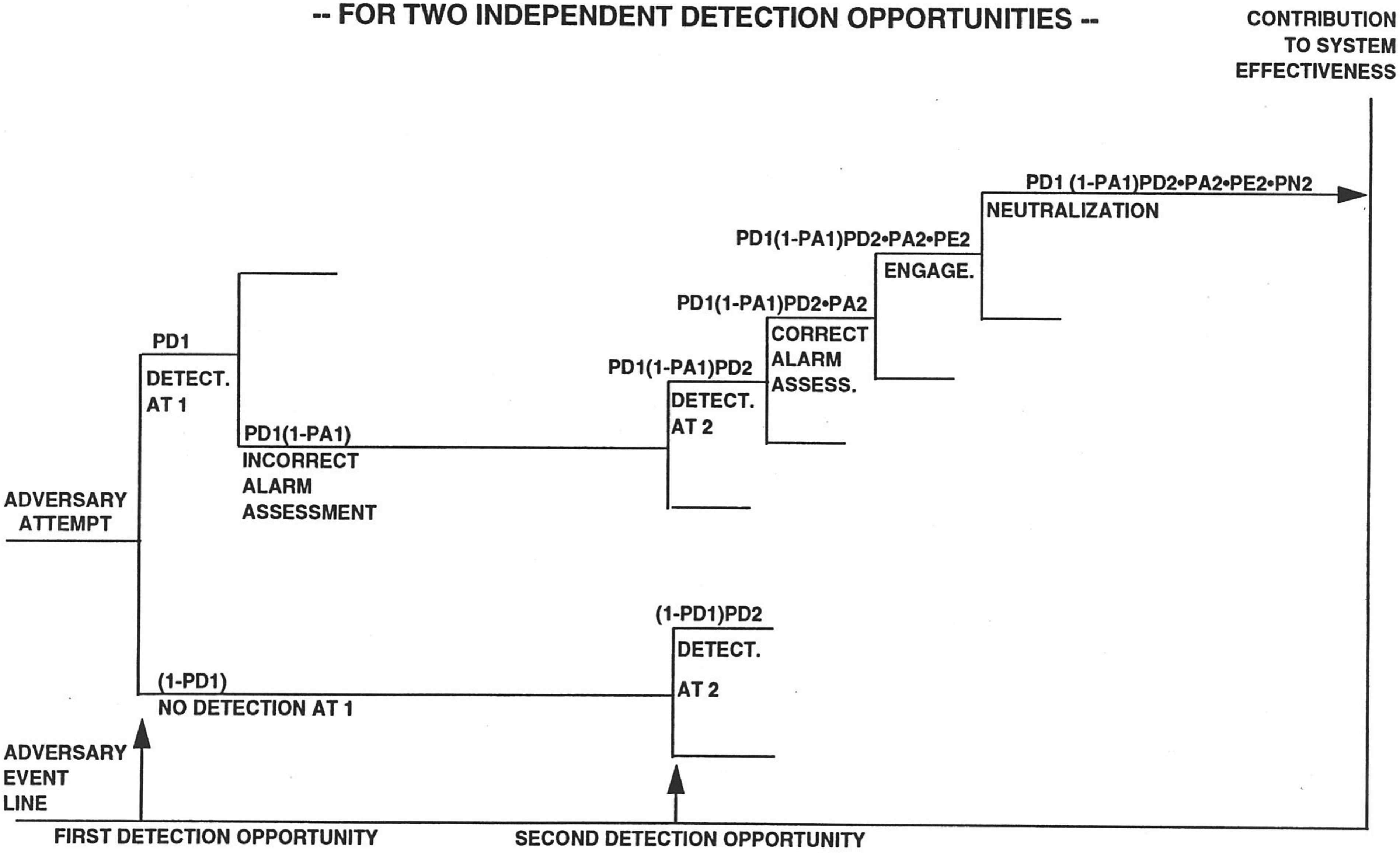
SECOND DETECTION OPPORTUNITY

$$SE = PD1 \bullet PA1 \bullet PE1 \bullet PN1$$

SYSTEM EFFECTIVENESS EVALUATION

LOGIC TREE TO DETERMINE FOUR-PARAMETER EQUATION FOR SE

-- FOR TWO INDEPENDENT DETECTION OPPORTUNITIES --



CONTRIBUTION TO SYSTEM EFFECTIVENESS

ADVERSARY ATTEMPT

PD1

DETECT. AT 1

PD1(1-PA1)

INCORRECT ALARM ASSESSMENT

PD1(1-PA1)PD2

DETECT. AT 2

PD1(1-PA1)PD2•PA2

CORRECT ALARM ASSESS.

PD1(1-PA1)PD2•PA2•PE2

ENGAGE.

PD1 (1-PA1)PD2•PA2•PE2•PN2

NEUTRALIZATION

(1-PD1)

NO DETECTION AT 1

(1-PD1)PD2

DETECT.

AT 2

ADVERSARY EVENT LINE

FIRST DETECTION OPPORTUNITY

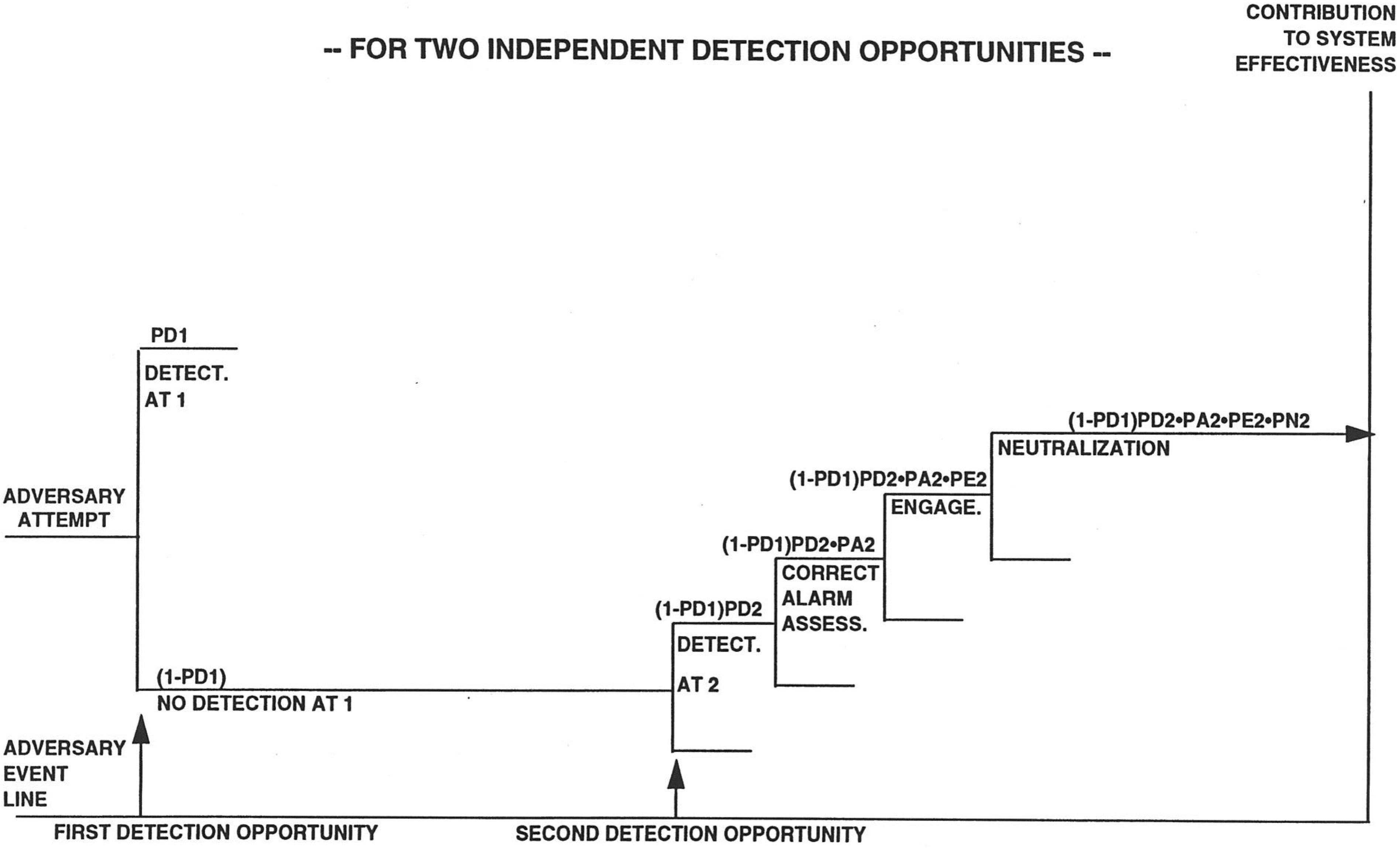
SECOND DETECTION OPPORTUNITY

$$SE = PD1 \bullet PA1 \bullet PE1 \bullet PN1 + PD1\,(1-PA1)\,PD2 \bullet PA2 \bullet PE2 \bullet PN2$$

SYSTEM EFFECTIVENESS EVALUATION

LOGIC TREE TO DETERMINE FOUR-PARAMETER EQUATION FOR SE

-- FOR TWO INDEPENDENT DETECTION OPPORTUNITIES --

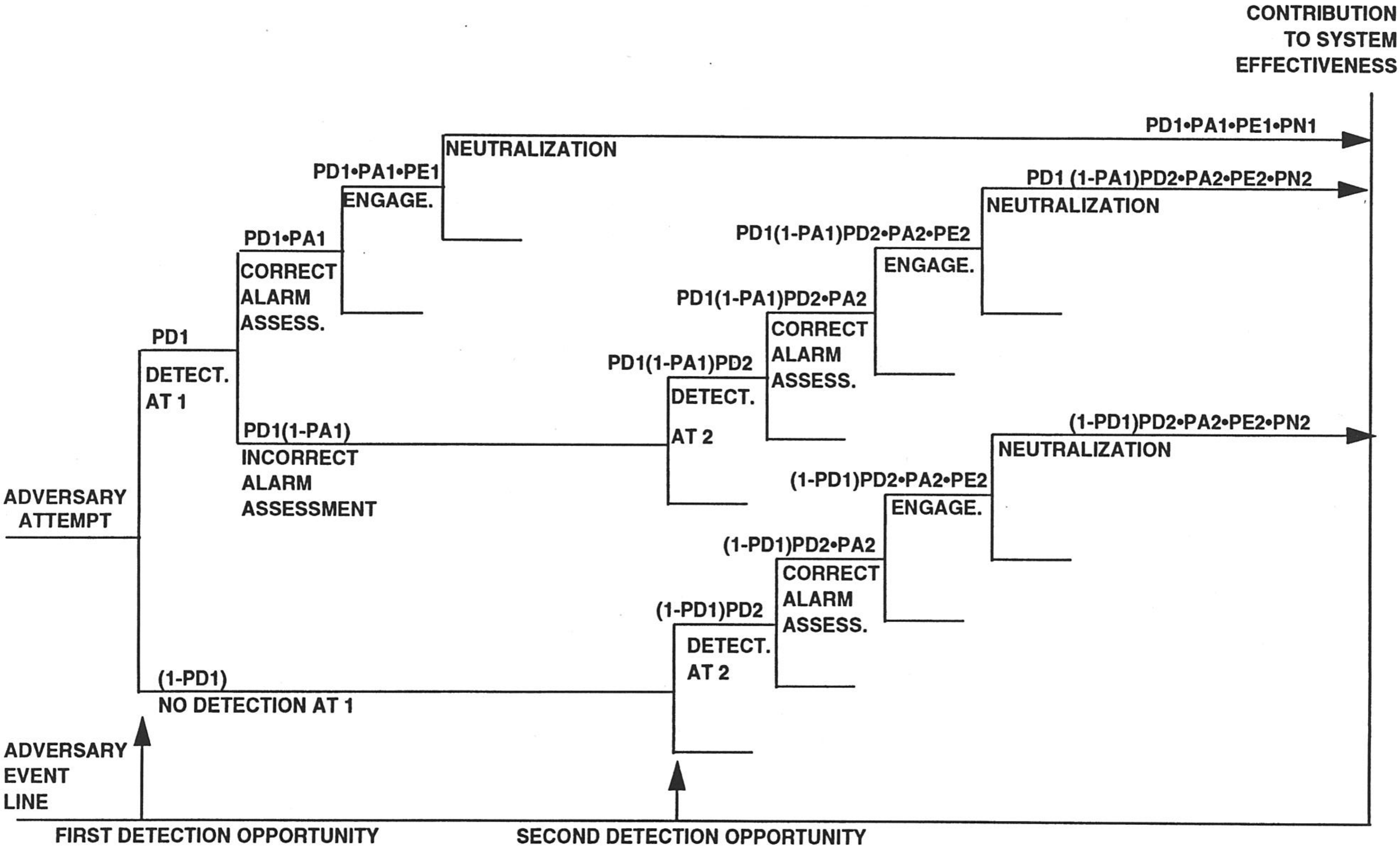


SE = PD1 • PA1 • PE1 • PN1 + PD1 (1-PA1) PD2 • PA2 • PE2 • PN2 + (1-PD1) PD2 • PA2 • PE2 • PN2

SYSTEM EFFECTIVENESS EVALUATION

LOGIC TREE TO DETERMINE FOUR-PARAMETER EQUATION FOR SE

-- FOR TWO INDEPENDENT DETECTION OPPORTUNITIES --



$$SE = PD1 \bullet PA1 \bullet PE1 \bullet PN1 + PD1\ (1\text{-}PA1)\ PD2 \bullet PA2 \bullet PE2 \bullet PN2 + (1\text{-}PD1)\ PD2 \bullet PA2 \bullet PE2 \bullet PN2$$

$$SE = PD1 \bullet PA1 \bullet PE1 \bullet PN1 + (1\text{-}\ PD1 \bullet PA1)\ PD2 \bullet PA2 \bullet PE2 \bullet PN2$$

FOUR-PARAMETER EQUATION FOR SE

-- FOR THREE INDEPENDENT DETECTION OPPORTUNITIES --

$$SE = \underbrace{PD1 \bullet PA1 \bullet PE1 \bullet PN1}_{\substack{\text{CONTRIBUTION OF FIRST}\\ \text{DETECTION OPPORTUNITY}}} + \underbrace{(1 - PD1 \bullet PA1)\ PD2 \bullet PA2 \bullet PE2 \bullet PN2}_{\substack{\text{CONTRIBUTION OF SECOND}\\ \text{DETECTION OPPORTUNITY}}}$$

$$+ \underbrace{(1 - PD1 \bullet PA1)(1 - PD2 \bullet PA2)\ PD3 \bullet PA3 \bullet PE3 \bullet PN3}_{\substack{\text{CONTRIBUTION OF THIRD}\\ \text{DETECTION OPPORTUNITY}}}$$

ASSUMPTIONS INHERENT IN EQUATION FOR SE

- ADVERSARY ACTIONS, WITHOUT SECURITY INTERVENTION, ALWAYS SUCCEED.
- DETECTION EVENTS ARE INDEPENDENT.

GENERAL TYPES OF PERFORMANCE TESTS

- PERFORMANCE TEST (PT) = ANY OBSERVATION, EXERCISE OR TEST THAT PROVIDES A MEASURE OF HOW A S&S PERSON, COMPONENT, SUBSYSTEM OR SYSTEM ACTUALLY PERFORMS HIS, HER, OR ITS INTENDED FUNCTION(S).
- STANDARD PT = ANY PT TO MEASURE PERFORMANCE RELATIVE TO AN ESTABLISHED OR DOCUMENTED STANDARD (E.G., BALL DRAG TESTS THROUGH AN INTRUSION DETECTION SENSOR FIELD).
- STRESS PT = ANY PT PERFORMED UNDER CONDITIONS OF A CREDIBLE SCENARIO (E.G., ADVERSARY IS ATTEMPTING TO AVOID DETECTION BY CIRCUMVENTING OR COMPROMISING INTRUSION DETECTION SYSTEM).

STANDARD PERFORMANCE TESTS FOR S&S EQUIPMENT

- OPERABILITY TEST (ALSO CALLED FUNCTIONAL TEST)
  - A TEST TO DETERMINE IF EQUIPMENT IS OPERATING OR FUNCTIONING.
  - FOR EXAMPLE, FOR A BALANCED MAGNETIC SWITCH, AN OPERABILITY TEST WOULD DETERMINE IF OPENING THE DOOR FOR ENTRY OR EXIT RESULTS IN AN ALARM.
- SENSITIVITY TEST (ALSO CALLED EFFECTIVENESS TEST)
  - A TEST TO DETERMINE IF EQUIPMENT IS OPERATING OR FUNCTIONING ABOVE SOME THRESHOLD OR OVER ITS INTENDED RANGE.
  - FOR EXAMPLE, FOR A BALANCED MAGNETIC SWITCH, A SENSITIVITY TEST FOR INTRUSION DETECTION WOULD DETERMINE IFA 1-INCH OR MORE OPENING MOVEMENT OF A DOOR RESULTS IN AN ALARM.

STANDARD PERFORMANCE TESTS FOR S&S PERSONNEL

- PROCEDURAL TEST
  - A TEST TO DETERMINE IF A SECURITY POLICE OFFICER (SPO) OR OTHER S&S PERSON FOLLOWS DOCUMENTED PROCEDURES SUCH AS PACKAGE OR VEHICLE SEARCHES AT ENTRY PORTALS. THE EFFECTIVENESS OF THE PROCEDURE, ITS DOCUMENTATION, TRAINING TO IMPLEMENT IT AND SUPERVISION TO ENSURE IT IS FOLLOWED MAY ALSO BE EVALUATED.
- SKILL TEST
  - A TEST TO DETERMINE IF A SPO OR OTHER S&S PERSON MEETS OR EXCEEDS MINIMUM SKILL CRITERIA SUCH AS THOSE FOR FIREARMS PROFICIENCY OR PHYSICAL FITNESS.

STRESS PERFORMANCE TESTS FOR S&S EQUIPMENT

- EQUIPMENT DEFEAT TEST (EDT)
  - A TEST TO DETERMINE IF S&S EQUIPMENT CAN BE COMPROMISED OR CIRCUMVENTED BY AN ADVERSARY.
  - TEST FOCUSES ON S&S EQUIPMENT WHOSE DEFEAT COULD RESULT IN LOSS OF ONE OR MORE ESSENTIAL S&S SYSTEM CAPABILITIES (DETECTION, ASSESSMENT, ENGAGEMENT, NEUTRALIZATION) UNDER CONDITONS OF A CREDIBLE SCENARIO.

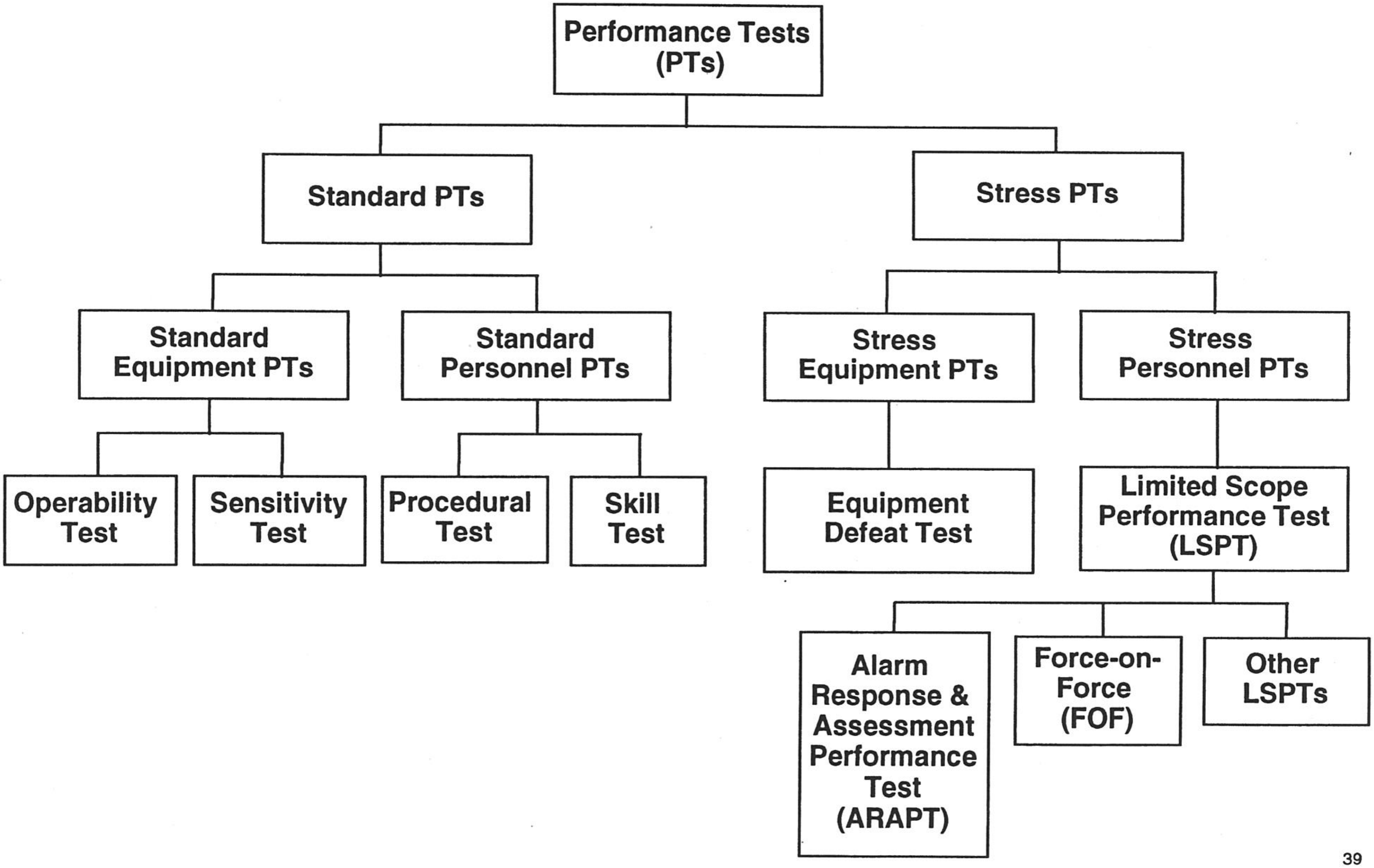
STRESS PERFORMANCE TESTS FOR S&S PERSONNEL

- **LIMITED SCOPE PERFORMANCE TEST (LSPT)**
  - PREPLANNED AND SCHEDULED EXERCISES CONDUCTED EITHER ANNOUNCED OR UNANNOUNCED, TO DETERMINE LEVEL OF SKILL OR CAPABILITY OF PROTECTIVE FORCE OR OTHER S&S PERSONNEL IN A SPECIFIC AREA OF OPERATION OR PROCEDURE.
- **LSPTs FOR PROTECTIVE FORCE**
  - ALARM RESPONSE AND ASSESSMENT PERFORMANCE TEST (ARAPT)

    UNANNOUNCED TESTS TO EVALUATE ON-DUTY PROTECTIVE FORCE RESPONSE TO ALARMS. FOR TEST SCENARIOS THAT ARE CONSISTENT WITH THE APPLICABLE DESIGN-BASIS THREATS AND THE SITE S&S SYSTEM.
  - FORCE-ON-FORCE (FOF) EXERCISE

    PREPLANNED, SCHEDULED EXERCISE SCENARIOS DESIGNED TO EVALUATE THE EFFECTIVENESS OF THE SITE S&S SYSTEM, INCLUDING THE PROTECTIVE FORCE IN RESPONDING TO A SIMULATED ATTACK ON A SPECIFIC TARGET.

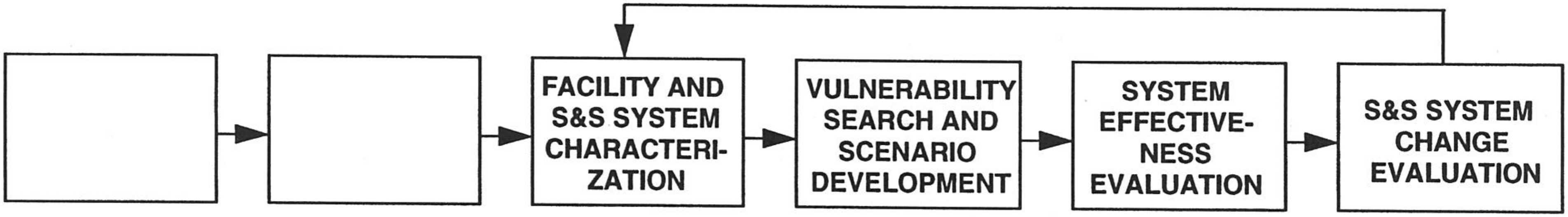
TYPES OF PERFORMANCE TESTS THAT SUPPORT VAs



- Performance Tests (PTs)
  - Standard PTs
    - Standard Equipment PTs
      - Operability Test
      - Sensitivity Test
    - Standard Personnel PTs
      - Procedural Test
      - Skill Test
  - Stress PTs
    - Stress Equipment PTs
      - Equipment Defeat Test
    - Stress Personnel PTs
      - Limited Scope Performance Test (LSPT)
        - Alarm Response & Assessment Performance Test (ARAPT)
        - Force-on-Force (FOF)
        - Other LSPTs

PERFORMANCE TESTS TO DETERMINE PROBABILITY VALUES

TYPE OF	STANDARD PT		STRESS PT	
PROBABILITY	EQUIPMENT	PERSONNEL	EQUIPMENT	PERSONNEL
PD	OPERABILITY, SENSITIVITY	PROCEDURAL	EDT	LSPT
PA	OPERABILITY, SENSITIVITY	PROCEDURAL	EDT	LSPT
PD•PA				LSPT
PE		PROCEDURAL, SKILL	EDT	LSPT (ARAPT)
PN		PROCEDURAL, SKILL		LSPT (FOF)
PE•PN				LSPT (FOF)
PD•PA•PE•PN				LSPT (FOF)



FACILITY AND S&S SYSTEM CHARACTERIZATION

VULNERABILITY SEARCH AND SCENARIO DEVELOPMENT

SYSTEM EFFECTIVENESS EVALUATION

S&S SYSTEM CHANGE EVALUATION

<u>PRODUCT</u>:

- DESCRIPTION OF CANDIDATE S&S CHANGES.
- INFORMATION ON PERFORMANCE OF S&S CHANGES.

<u>PRODUCT:</u>

- LIST OF VULNERABILITIES FOR CHANGED S&S SYSTEM.
- ADVERSARY'S PLANS OF ATTACK FOR MOST CREDIBLE SCENARIOS.

<u>PRODUCT</u>:

- LEVELS OF SYSTEM EFFECTIVENESS FOR CHANGED S&S SYSTEM.

<u>PRODUCT</u>:

- PRIORITIZED LIST OF S&S CHANGES.

- ESTABLISH GOAL FOR S&S SYSTEM CHANGE:
  - IMPROVE SYSTEM EFFECTIVENESS
  - REDUCE SYSTEM COSTS
  - IMPROVE EFFICIENCY
- IDENTIFY COMPLEMENTARY SETS OF S&S SYSTEM CHANGES:
  - FACILITY
  - EQUIPMENT
  - PERSONNEL
  - PROCEDURES
- DETERMINE CHANGE IN SYSTEM EFFECTIVENESS AND COST FOR EACH SET.
- PRIORITIZE EACH SET OF S&S SYSTEM CHANGES BASED ON GOAL AND ON CHANGES IN SYSTEM EFFECTIVENESS, COST AND OTHER RELEVANT FACTORS.

USES FOR VULNERABILITY ANALYSES

	M&O CONTRACTOR	DOE FIELD OFFICE	DOE HEADQUARTERS
SSSP PREPARATION	PERFORM	REVIEW	REVIEW
S&S SYSTEM DESIGN	PERFORM	REVIEW	REVIEW
PROTECTIVE FORCE RESPONSE PLAN DEVELOPMENT	PERFORM	REVIEW	REVIEW
S&S SYSTEM CHANGE EVALUATION	PERFORM	PERFORM	PERFORM
S&S SELF-ASSESSMENTS	PERFORM	REVIEW	REVIEW
S&S SURVEYS/INSPECTIONS		PERFORM	PERFORM
S&S INDEPENDENT ASSESSMENTS	PERFORM	PERFORM	PERFORM
S&S TRAINING	PERFORM	PERFORM	PERFORM

LEVELS OF EFFORT FOR VULNERABILITY ANALYSES

LEVEL OF EFFORT FOR VA	NUMBER OF THREATS	NUMBER OF TARGETS	VA CORE TEAM	VA SUPPORT TEAM	FACILITY INSPECTION	STANDARD PERF. TESTS	STRESS PERF. TESTS	DOCUMENTATION	DURATION
MINIMUM	1	1	2-3 SPECIAL-ISTS	NONE	DOCUMENT REVIEWS	AS AVAILABLE	AS AVAILABLE	SUMMARY REPORT	1-3 DAYS
	2-4	1-3	3-5 SPECIALISTS	1-5 PEOPLE	DOCUMENT REVIEWS AND WALK-THROUGHS	AS AVAILABLE	AS AVAILABLE	10-30 PAGE REPORT	1-3 WEEKS
	≥4	3-4	4-6 SPECIALISTS	5-10 PEOPLE	DOCUMENT REVIEWS AND EXTENSIVE OBSERVATIONS	AS AVAILABLE	DETECTION, ALARM ASSESSMENT, ENGAGEMENT	DETAILED REPORT	1-3 MONTHS
MAXIMUM	≥6	4-6	5-7 SPECIALISTS	5-10 PEOPLE	DOCUMENT REVIEWS & EXTENSIVE OBSERVIATIONS	SUPPLEMENT AS APPROPRIATE	DETECTION, ALARM ASSESSMENT, ENGAGEMENT, NEUTRALIZATION	DETAILED REPORT	3-6 MONTHS

STRENGTHS AND WEAKNESSES OF TABLE-TOP VA METHOD

STRENGTHS

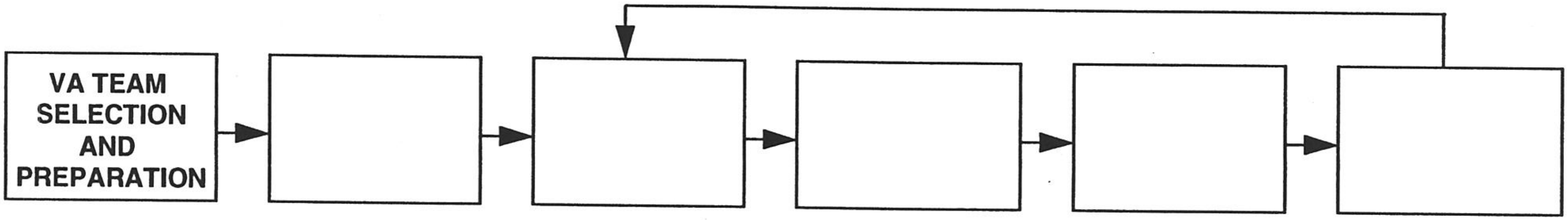
- FLEXIBLE
  - TREATS ALL TYPES OF THREATS AND TARGETS.
  - TREATS ALL TYPES OF FACILITIES AND S&S SYSTEMS.
  - TREATS ALL TYPES OF ADVERSARY STRATEGIES, TACTICS AND PATHS.
  - ADAPTABLE TO MANY USES AND LEVELS OF EFFORT.
  - ANALYSIS CAN BE QUANTITATIVE OR QUALITATIVE.
  - PERFORMANCE DATA CAN BE ESTIMATED OR MEASURED.
- EFFICIENT
  - FOCUSES ON KEY PERFORMANCE DATA.
  - DIRECTLY INTEGRATES RESULTS OF PERFORMANCE TESTS INTO VA PROCESS.
- EASY TO USE
  - COMMON SENSE APPROACH.
  - VA PROCESS AND RESULTS ARE TRANSPARENT

WEAKNESSES

- QUALITY OF RESULTS DEPENDS ON TRAINING, EXPERIENCE, INTEGRITY, AND EFFORT OF THOSE WHO PERFORM AND REVIEW VAs AND PTs

3. VA Team

3. VA TEAM



VA CORE TEAM

- VA SPECIALIST
- PERFORMANCE TESTING (PT) SPECIALIST
- PROTECTIVE FORCE (PF) SPECIALIST
- PHYSICAL SECURITY SYSTEMS (PSS) SPECIALIST
- MC&A SPECIALIST
- FACILITY OPERATION SPECIALIST

VA SUPPORT TEAM

- CAS/SAS SPECIALIST
- UTILITIES SPECIALIST
- MAINTENANCE SPECIALIST
- SHIPMENT AND TRANSPORTATION SPECIALIST
- BUDGET SPECIALIST
- SAFETY SPECIALIST
- FACILITY MANAGER
- PROGRAM MANAGER
- OTHER SPECIALISTS AND MANAGERS AS REQURED

- VA TEAM SELECTION
  - PURPOSE AND SCOPE OF VA
  - EXPERIENCE REQUIRED
  - TEAM DIVERSITY
  - TEAM FACILITATOR

- VA TEAM PREPARATION
  - PLANNING VA
  - ESTABLISHING VA REPORT FORMAT
  - ORIENTING VA TEAM TO FACILITY AND S&S SYSTEM

VA TEAM SELECTION

- CONSIDERATIONS IN ESTABLISHING SELECTION CRITERIA
  - PURPOSE OR USE OF VA (E.G., S&S SYSTEM CHANGE EVALUATION)
  - SCOPE OR LEVEL OF VA (E.G., MINIMUM LEVEL)
- ELEMENTS OF SELECTION CRITERIA
  - NUMBER OF PERSONS REQUIRED
  - TYPES AND LEVELS OF EXPERIENCE REQUIRED
- TEAM MEMBER SELECTION
  - SELECTION CRITERIA
  - EXPERIENCE PROFILES OF AVAILABLE STAFF
  - TEAM DIVERSITY
- TEAM FACILITATOR

EXPERIENCE PROFILE FOR VA TEAM MEMBER

TECHNICAL AREA	OUTSIDER THREAT EXPERIENCE				INSIDER THREAT EXPERIENCE			
	NONE	SOME	MOD.	EXTENSIVE	NONE	SOME	MOD.	EXTENSIVE
1. VULNERABILITY ANALYSIS								
2. PERFORMANCE TESTING								

	TOTAL EXPERIENCE				LOCAL SITE EXPERIENCE			
	NONE	SOME	MOD.	EXTENSIVE	NONE	SOME	MOD.	EXTENSIVE
3. PROTECTIVE FORCE								
4. PHYSICAL SECURITY								
5. MC&A								
6. FACILITY OPERATIONS								
7. OTHER RELEVANT EXPERIENCE								
______________								
______________								

TEAM DIVERSITY

- FOR SOME PARTS OF VA PROCESS, ANALYSIS CAN BE BASED ON ESTABLISHED PROCEDURES AND MEASURED DATA.

- HOWEVER, FOR OTHER PARTS OF VA PROCESS, PARTICULARLY THOSE PARTS INVOLVING PREDICTION OF HUMAN BEHAVIOR, ANALYSIS HAS TO BE BASED ON JUDGEMENT OF TEAM MEMBERS.

- HENCE, QUALITY OF VAs DEPENDS ON SOUNDNESS OF TEAM'S COLLECTIVE JUDGEMENT.

- EXPERIENCE HAS SHOWN A TEAM'S COLLECTIVE JUDGEMENT IS LIKELY TO BE MOST SOUND WHEN ITS TEAM MEMBERS HAVE DIVERSITY IN TRAINING AND EXPERIENCE.

VA PLANNING

- SCHEDULE
- ASSIGNMENTS
  - PREPARATION
  - ANALYSIS
  - PERFORMANCE TESTS
  - DOCUMENTATION

FORMAT FOR DOCUMENTING VAs

- EXECUTIVE SUMMARY
- INTRODUCTION
- APPROACH
- VA TEAM
- THREATS AND TARGETS
    - LIST OF THREAT-TARGET PAIRS TO BE ANALYZED
- FACILITY AND S&S SYSTEM
    - DESCRIPTION OF SITE, FACILITY AND S&S SYSTEM
    - INFORMATION ON PERFORMANCE OF S&S PERSONNEL, COMPONENTS AND SUBSYSTEMS.
- VULNERABILITIES AND SCENARIOS (FOR EACH THREAT-TARGET PAIR)
    - LIST OF VULNERABILITIES
    - ADVERSARY'S PLANS OF ATTACK FOR MOST-CREDIBLE SCENARIOS
- SYSTEM EFFECTIVENESS EVALUATION (FOR EACH THREAT-TARGET PAIR)
    - LEVELS OF SYSTEM EFFECTIVENESS
- S&S SYSTEM EFFICIENCY EVALUATION (FOR EACH THREAT-TARGET PAIR)
    - PRIORITIZED LIST OF S&S SYSTEM CHANGES
- SUMMARY

VA TEAM ORIENTATION

- ORIENTATION EFFORT DEPENDS ON PURPOSE AND SCOPE OF VA

- ORIENTATION MAY INCLUDE:

  - DOCUMENT REVIEW

  - FACILITY WALK-THROUGH

  - INTERVIEWS WITH MANAGEMENT, TECHNICAL AND OPERATIONAL STAFF

  - OTHER WORK TO CHARACTERIZE FACILITY AND S&S SYSTEM

4. THREATS

TYPES OF THREATS

Type	Description	Use
Historical Threat (Product of Historians)	Record of malevolent acts including targets, adversary tactics and equipment used, and, in some cases, identity of adversaries.	Record of malevolent acts provides insight on adversary motivations, tactics and capabilities.
Threat Estimate (Product of Intelligence Analysts)	Current information collected and analyzed by intelligence specialists about potential adversaries and their plans.	May provide basis for pre-emptive action against potential adversaries or for security alert at one or more facilities
Design-Basis Threat (Product of Policy Makers)	Description of malevolent acts and adversaries that safeguards and security system is to protect against.	Together with system effectiveness requirement, provides system performance requirement.

5. TARGETS

TARGET ANALYSIS

- IDENTIFY ALL SECURITY INTERESTS
  - SNM TARGETS
  - SABOTAGE TARGETS

TARGET ANALYSIS (CONTINUED)

- CHARACTERIZE MATERIAL IN THESE LOCATIONS
  - TYPE
  - SIZE
  - WEIGHT
  - QUANTITY
- IDENTIFY (LIST) TARGETS THAT MATCH ADVERSARY'S GOAL
  - THEFT
  - SABOTAGE
  - OTHER

TARGETS

- GROUP LIKE TARGETS
  - SIMILAR ATTRACTIVENESS
  - SIMILAR PROTECTION
  - SIMILAR CONSEQUENCES
- DOE POLICY (BASED ON CONDITIONAL RISK LEVELS)

- DOE POLICY IDENTIFIES A RISK EQUATION

WHERE:

RISK $= F_{ATTACK} \text{ X } P_{FAILURE} \text{ X } CONSEQUENCES_{EVENT}$

F_{ATTACK} = FREQUENCY OF ATTACK

$P_{FAILURE}$ = PROBABILITY OF SYSTEM FAILURE

CONDITIONAL RISK

- LIKE CONDITIONAL PROBABILITY, CONDITIONAL RISK (CR) IS DEFINED AS THE RISK, GIVEN AN ADVERSARY ATTEMPT IS MADE.

$$CR = P_{FAILURE} \times CONSEQUENCES_{EVENT}$$

CONSEQUENCE OF EVENT

- DOE defines the consequence of an event for SSSP purposes in the SSSP preparation guide and format and content review guides. The consequence values given have been normalized to one for the most serious consequence expected to result from each type of event.

- April 1993 DOE guides increased some consequence values for SNM theft events.

PROBABILITY OF SYSTEM FAILURE

- **THE P_F IS RELATED TO SYSTEM EFFECTIVENESS**

  WHERE:

  P_F = 1.0 - SYSTEM EFFECTIVENESS (SE)

- **SINCE CONSEQUENCE IS DEFINED, THE 'SE' IS THE ONLY VARIABLE A SITE CAN USE TO MITIGATE CONDITIONAL RISK IN THE SSSP PROCESS.**

DOE POLICY ON SYSTEM EFFECTIVENESS REQUIREMENTS

- SYSTEM EFFECTIVENESS (SE) REQUIREMENTS FOR PROTECTION OF SNM THEFT AND SABOTAGE TARGETS AGAINST DESIGN-BASIS THREATS ARE PRESCRIBED BY THE FOLLOWING FORMULA.

$$SE = 1 - {}^{CR}/_{C}$$

WHERE CR (CONDITIONAL RISK) = __________ FOR SATISFACTORY PROTECTION (LOW CONDITIONAL RISK)

__________ FOR MARGINAL PROTECTION (MODERATE CONDITIONAL RISK)

__________ FOR UNSATISFACTORY PROTECTION (HIGH CONDITIONAL RISK)

AND C (CONSEQUENCE) =

0.7* FOR CAT. I QUANTITY SNM (PURE PRODUCT SUCH AS PU METAL)

0.6 FOR CAT. I QUANTITY SNM (SIMPLE COMPOUNDS SUCH AS PU OXIDE)

0.5 FOR CAT. I QUANTITY SNM (HIGH GRADE MATERIAL SUCH AS PU NITRATE)

* SEE DOE CONSEQUENCE TABLES FOR OTHER SNM QUANTITIES AND FOR SABOTAGE TARGETS.

DOE REQUIREMENTS FOR SYSTEM EFFECTIVENESS*

	SYSTEM EFFECTIVENESS		
CATEGORY I QUANTITY OF SNM	SATISFACTORY PROTECTION	MARGINAL PROTECTION	UNSATISFACTORY PROTECTION
PU METAL	_____TO 1.00	_____TO _____	0 TO_____
PU OXIDE (POWDER)	_____TO 1.00	_____TO _____	0 TO_____
PU NITRATE (LIQUID)	_____TO 1.00	_____TO _____	0 TO_____

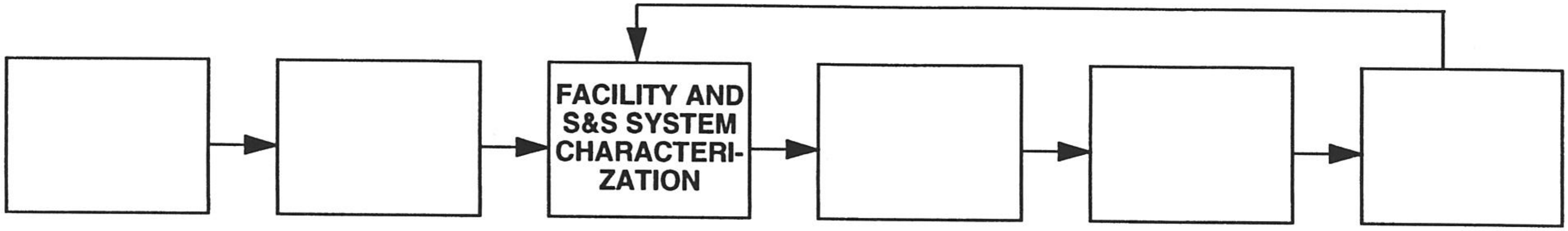
* DOE CONSEQUENCE TABLES ADDRESS OTHER SNM QUANTITIES AND SABOTAGE

6. Outsider Threat (No insider)

6. OUTSIDER THREAT ANALYSIS (NO INSIDER ASSISTANCE)

TYPES OF OUTSIDER THREAT ANALYSES

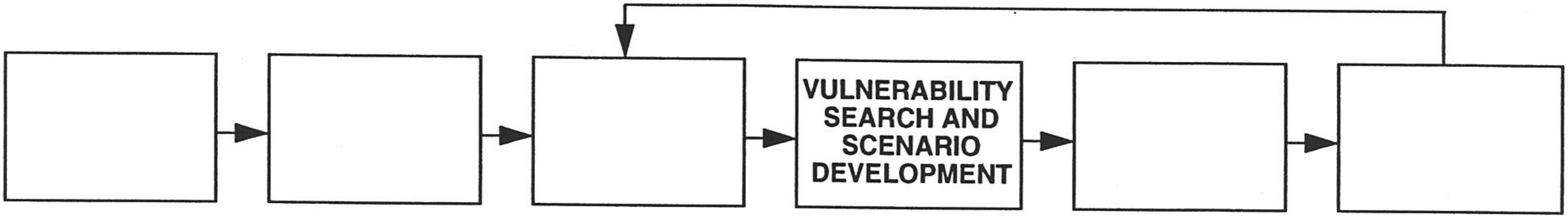
	VEHICLES AVAILABLE		INSIDER ASSISTANCE	
NO.	GROUND	AIRBORNE	NON-VIOLENT	VIOLENT
1	X			
2	X	X		
3	X		X	
4	X	X	X	
5	X			X
6	X	X		X



PRODUCT:

- DESCRIPTION OF SITE, FACILITY AND S&S SYSTEM
- INFORMATION ON PERFORMANCE OF S&S PERSONNEL, COMPONENTS AND SUBSYSTEMS

- CHARACTERIZATION SHOULD REPRESENT A SNAPSHOT IN TIME.
- MARK UP SITE DRAWING AND BUILDING DRAWING TO SHOW LOCATIONS OF KEY TARGETS AND KEY S&S MEASURES RELEVANT TO PROTECTION AGAINST OUTSIDER THREATS.
  - BARRIERS, INTRUSION SENSORS, CCTV AND ACCESS CONTROLS
  - SECURITY POSTS AND FIGHTING POSITIONS
  - ALARM STATIONS
- REVIEW EMERGENCY RESPONSE PLANS, TACTICAL COMMUNICATIONS AND LIGHTING.
- COLLECT OTHER INFORMATION, INCLUDING PERFORMANCE DATA, AS NEEDED.



PRODUCT:

- LIST OF VULNERABILITIES.
- ADVERSARY'S PLANS OFATTACK FOR MOST CREDIBLE SCENARIOS.

- PERFORM ANALYSIS FOR EACH COMBINATION OF TARGET AND OUTSIDER THREAT.
- SEARCH FOR VULNERABILITIES THAT CAN BE EXPLOITED BY ADVERSARY.
- CONSIDER ALL REASONABLE ADVERSARY STRATEGIES, TACTICS, AND PATHS.
- CONSIDER ALL FACILITY CONDITIONS (OPERATING, SHUTDOWN, MAINTENANCE, EMERGENCY).
- DEVELOP CREDIBLE SCENARIOS THAT GIVE ADVERSARY BEST CHANCE FOR SUCCESS.

VULNERABILITY SEARCH METHODS

- OBSERVATION AND INSPECTION.
- ADVERSARY ROLE PLAYING.
- SCENARIO DEVELOPMENT.
- PERFORMANCE TESTING.
- ADVERSARY SEQUENCE DIAGRAM ANALYSIS.

ADVERSARY STRATEGIES, TACTICS AND PATHS

- STRATEGIES
  - COVERT OR
    COVERT, THEN OVERT (AND POSSIBLE USE OF SURPRISE)
  - ABRUPT OR PROTRACTED
    (ONE STAGE OR MULTIPLE STAGES)
  - INSIDER ASSISTANCE
- TACTICS
  - STEALTH
  - DECEIT
  - FORCE (VIOLENCE)
  - COMPROMISE AND/OR CIRCUMVENTION OF S&S MEASURES (MAY INCLUDE TAMPERING, COERSION, AMBUSH, OR DIVERSION)
- PATHS
  - GROUND
  - UNDERGROUND
  - AIR

LOOK FOR EXPLOITABLE WEAKNESSES IN SECURITY MEASURES

- PA AND MAA PERIMETERS
  - BARRIERS AND DELAYS
  - ENTRY CONTROLS
  - INTRUSION DETECTION
  - LIGHTING AND CCTV
  - SECURITY POSTS
  - COMMUNICATIONS
- VAULTS AND PROCESSING AREAS
  - BARRIERS AND DELAYS
  - ENTRY CONTROLS
  - INTRUSION DETECTION
  - LIGHTING AND CCTV
- SITEWIDE AND WITHIN PA
  - SECURITY POSTS
  - LIGHTING AND CCTV
  - COMMUNICATIONS
  - COMMAND AND CONTROL
  - RESPONSE FORCE
  - FIGHTING POSITIONS

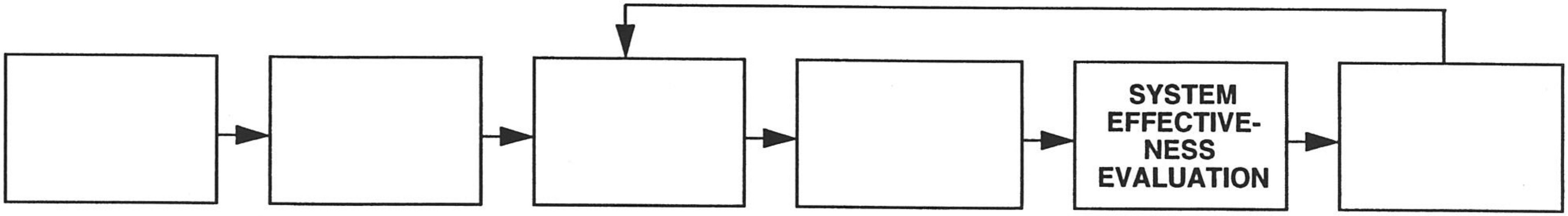
CONSIDER ALL ELEMENTS OF SECURITY MEASURES

- FACILITIES
- EQUIPMENT
- PERSONNEL
- PROCEDURES

SCENARIO DEVELOPMENT

-- ADVERSARY'S PLAN OF ATTACK --

- MOST SERIOUS VULNERABILITIES EXPLOITED.
- BEST CHANCE FOR ADVERSARY SUCCESS SOUGHT.
- ADVERSARY PREFERS SIMPLE STRATEGY, SIMPLE TACTICS AND EASY PATHS.
- IF COMPLEX ADVERSARY ACTIONS ARE REQUIRED, ADVERSARY SHOULD HAVE SUFFICIENT BACKUP AVAILABLE TO ENSURE SUCCESS FOR EACH ESSENTIAL ACTION.
- TIME OF ATTACK AND WEATHER CONDITIONS SET.
- EVENT AND TIME LINES ESTIMATED.



<u>PRODUCT</u>:

LEVELS OF SYSTEM EFFECTIVENESS

- PERFORM EVALUATION FOR EACH CREDIBLE SCENARIO DEVELOPED.
- ESTIMATE LOCATIONS OF SECURITY POLICE OFFICERS AT TIME OF ATTACK.
- DETERMINE MOST LIKELY PATHS AND TIME LINES FOR DEPLOYMENT OF RESPONSE FORCE.
- FOR EACH SIGNIFICANT DETECTION OPPORTUNITY:
  - ESTIMATE PD, PA, PE, AND PN
  - DETERMINE SE
- IDENTIFY CRITICAL PROBABILITIES THAT WARRANT ADDITIONAL WORK TO IMPROVE THEIR ACCURACY.
- DEVELOP AND IMPLEMENT PERFORMANCE TEST PLANS, AS NEEDED, TO IMPROVE ACCURACY OF CRITICAL PROBABILITIES.

ESSENTIAL S&S SYSTEM CAPABILITIES

- DETECTION: PRODUCE AN ALARM.
- ASSESSMENT: DECIDE IF RESPONSE FORCE SHOULD DEPLOY.
- ENGAGEMENT: DEPLOY RESPONSE FORCE TO LOCATIONS WHERE ADVERSARIES CAN BE ENGAGED.
- NEUTRALIZATION: STOP ADVERSARIES FROM ACHIEVING THEIR OBJECTIVE.

APPLICABILITY OF S&S MEASURES TO FOUR ESSENTIAL S&S SYSTEM CAPABILITIES

S&S MEASURES	DETECTION	ASSESSMENT	ENGAGEMENT	NEUTRALIZATION
ACCESS CONTROLS	●			
MATERIAL CONTROLS	●			
INTRUSION DETECTION	●	●		
MATERIAL ACCOUNTING	●	●		
LIGHTING AND CCTV	●	●	●	●
SECURITY POSTS	●	●	●	●
COMMUNICATIONS	●	●	●	●
BARRIERS AND DELAYS	●	●	●	●
COMMAND AND CONTROL		●	●	●
RESPONSE FORCE			●	●
FIGHTING POSITIONS				●

DETECTION & ASSESSMENT & ENGAGEMENT = "INTERRUPTION" IN SAVI/ASSESS OUTSIDER THREAT MODULE

FOUR-PARAMETER EQUATION FOR SE

-- FOR TWO INDEPENDENT DETECTION OPPORTUNITIES --

$$SE = \underbrace{PD1 \bullet PA1 \bullet PE1 \bullet PN1}_{\text{CONTRIBUTION OF FIRST DETECTION OPPORTUNITY}} + \underbrace{(1 - PD1 \bullet PA1)\ PD2 \bullet PA2 \bullet PE2 \bullet PN2}_{\text{CONTRIBUTION OF SECOND DETECTION OPPORTUNITY}}$$

PD = PROBABILITY OF DETECTION, GIVEN ADVERSARY ATTEMPT.

PA = PROBABILITY OF CORRECT ALARM ASSESSMENT, GIVEN DETECTION.

PE = PROBABILITY OF ENGAGEMENT, GIVEN CORRECT ALARM ASSESSMENT.

PN = PROBABILITY OF NEUTRALIZATION, GIVEN ENGAGEMENT.

DETECTION EVALUATION

- DETECTION OPPORTUNITIES
  - ACCESS CONTROL DETECTION OF UNAUTHORIZED ENTRY OR CONTRABAND.
  - INTRUSION DETECTION SENSORS ON PERIMETER FENCE LINE OR IN BUILDINGS.
  - SURVEILLANCE BY SECURITY PERSONNEL ON PATROL, IN TOWER, OR USING CCTV.
- DETECTION AVOIDANCE.
- SCENARIO CONDITIONS.
- INITIAL PD VALUES: EXPERT JUDGEMENT, ASSESS DEFAULT VALUES OR DETECTION HANDBOOKS.
- IMPROVED PD VALUES: PERFORMANCE TESTS.

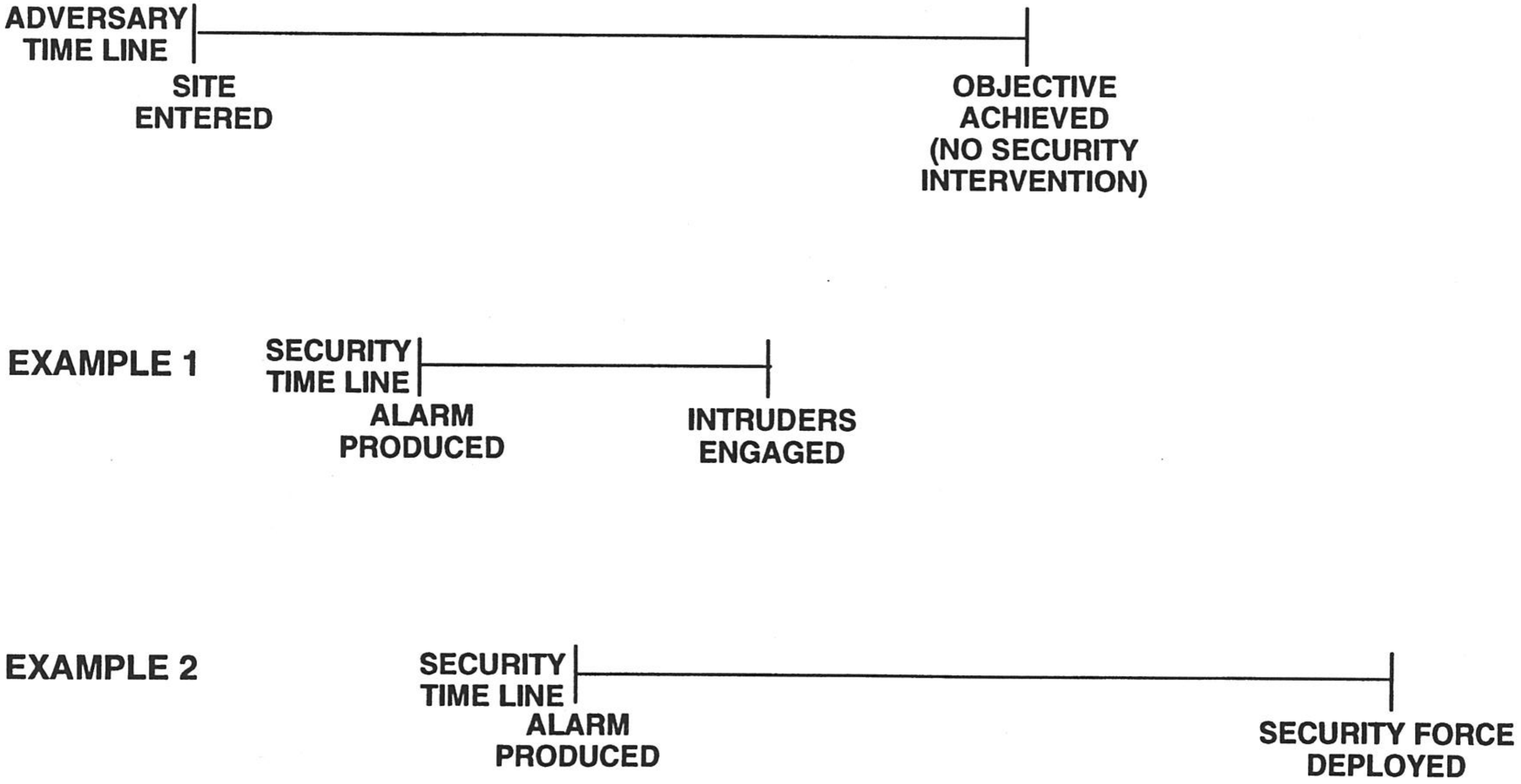
ASSESSMENT EVALUATION

- AUTOMATIC ASSESSMENT
  - SURVEILLANCE ALARM
  - DURESS ALARM
  - OTHER ALARMS
- OTHER ASSESSMENTS
  - CCTV
  - DIRECT OBSERVATION
- CRITERIA
  - VALIDITY
  - TIME REQUIRED
- ASSESSMENT AVOIDANCE
- SCENARIO CONDITIONS
- INITIAL PA VALUES: EXPERT JUDGEMENT
- IMPROVED PA VALUES: PERFORMANCE TESTS

ENGAGEMENT EVALUATION

- ADVERSARY'S TIME LINE
  - EACH SIGNIFICANT DETECTION OPPORTUNITY
  - EVENTS AFTER DETECTION
  - DELAY TIMES: EXPERT JUDGEMENT, ASSESS DEFAULT VALUES, BARRIER HANDBOOK, OR TESTS
- SECURITY FORCE'S EXPECTED RESPONSE
  - INITIAL LOCATIONS
  - PREDICTED ACTIONS
- SECURITY FORCE TIME LINE
  - TIME ANALYSIS
  - PERFORMANCE TESTS
- COMPARISON OF TIME LINES

EXAMPLE TIME LINES



ADVERSARY TIME LINE

SITE ENTERED

OBJECTIVE ACHIEVED (NO SECURITY INTERVENTION)

EXAMPLE 1

SECURITY TIME LINE

ALARM PRODUCED

INTRUDERS ENGAGED

EXAMPLE 2

SECURITY TIME LINE

ALARM PRODUCED

SECURITY FORCE DEPLOYED

NEUTRALIZATION EVALUATION

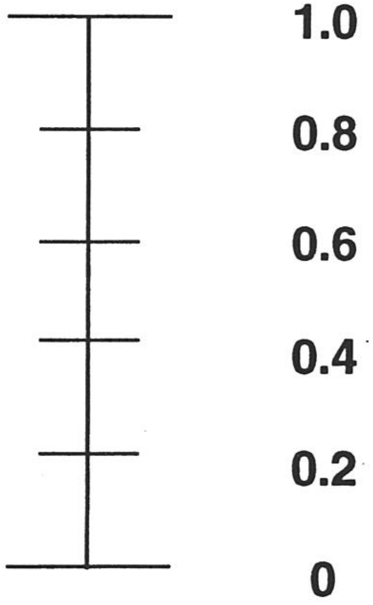
- ENGAGEMENT CONDITIONS
  - NUMBER OF ADVERSARIES
  - NUMBER OF DEFENDERS
- USE OF DEADLY FORCE
  - POLICY
  - TRAINING
- ENGAGEMENT OUTCOME
  - COMPUTER MODEL: BATLE
  - FORCE-ON-FORCE EXERCISES

BATLE COMPUTER MODEL ESTIMATES

RATIO OF ADVERSARIES TO DEFENDERS	LIKELIHOOD OF SECURITY FORCE WIN
<1.5	VERY HIGH
1.5 TO 1.9	HIGH
1.9 TO 2.3	MODERATE
2.3 TO 3.1	LOW
>3.1	VERY LOW

SYSTEM EFFECTIVENESS SCALE

QUANTITATIVE OR NUMERICAL



1.0

0.8

0.6

0.4

0.2

0

QUALITATIVE OR DESCRIPTIVE

VERY HIGH

HIGH

MODERATE

LOW

VERY LOW

DETECTION VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary ______________ Act ________________________ Target ________________________ Date _______________ Worksheet No. _______________

Adversary Event Line

	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6 Movement in Area	1.7	1.8				
ENTRY	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7 Movement in Area	2.8	2.9			
	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10 Movement in Area	3.11	3.12
ACQUISITION	Target*	4.1 Normal Access	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9			
	MAA	5.1 Thru Personnel Portal	5.2 Thru S/R** Portal	5.3 Thru Emergency Exit	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10 Movement in Area	5.11	5.12
REMOVAL	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7 Movement in Area	6.8	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6 Movement in Area	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.

** S/R = Shipper/Receiver

VULNERABILITY DESCRIPTIONS FOR WORKSHEET NO. ____________

Vulnerability Number	Vulnerability Description

Provide descriptions for vulnerability levels VH, H, M and others where appropriate.

DELAY VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary ____________ Act ______________________ Target ______________________ Date _____________ Worksheet No. _____________

Adversary Event Line

ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7	2.8	2.9			
ACQUISITION	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10	3.11	3.12
	Target*	4.1 Normal Access	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9	4.10		
	MAA	5.1 Thru Personnel Portal	5.2 Thru S/R** Portal	5.3 Thru Emergency Exit	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10	5.11	5.12
REMOVAL	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7	6.8	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.
** S/R = Shipper/Receiver

ALARM ASSESSMENT VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER ADVERSARIES

Adversary ______________ Act ______________ Target ______________ Date ______________ Worksheet No. ________

Type of Alarm Assessment							
CCTV Response To Alarm	1.1 Defeat Camera	1.2 Defeat Com. to CAS/SAS	1.3 Use Deceit	1.4 Use Stealth	1.5 Report False Alarm	1.6	1.7
SPO Response To Alarm	2.1 Neutralize SPO	2.2 Defeat Com. to CAS/SAS	2.3 Use Deceit	2.4 Use Stealth	2.5 Report False Alarm	2.6	2.7
Routine SPO Patrol	3.1 Neutralize SPO	3.2 Defeat Com. to CAS/SAS	3.3 Use Deceit	3.4 Use Stealth	3.5 Report False Alarm	3.6	3.7
Multiple Alarms	4.1 Report False Alarm	4.2	4.3				
Duress Alarm	5.1Report False Alarm	5.2	5.3				

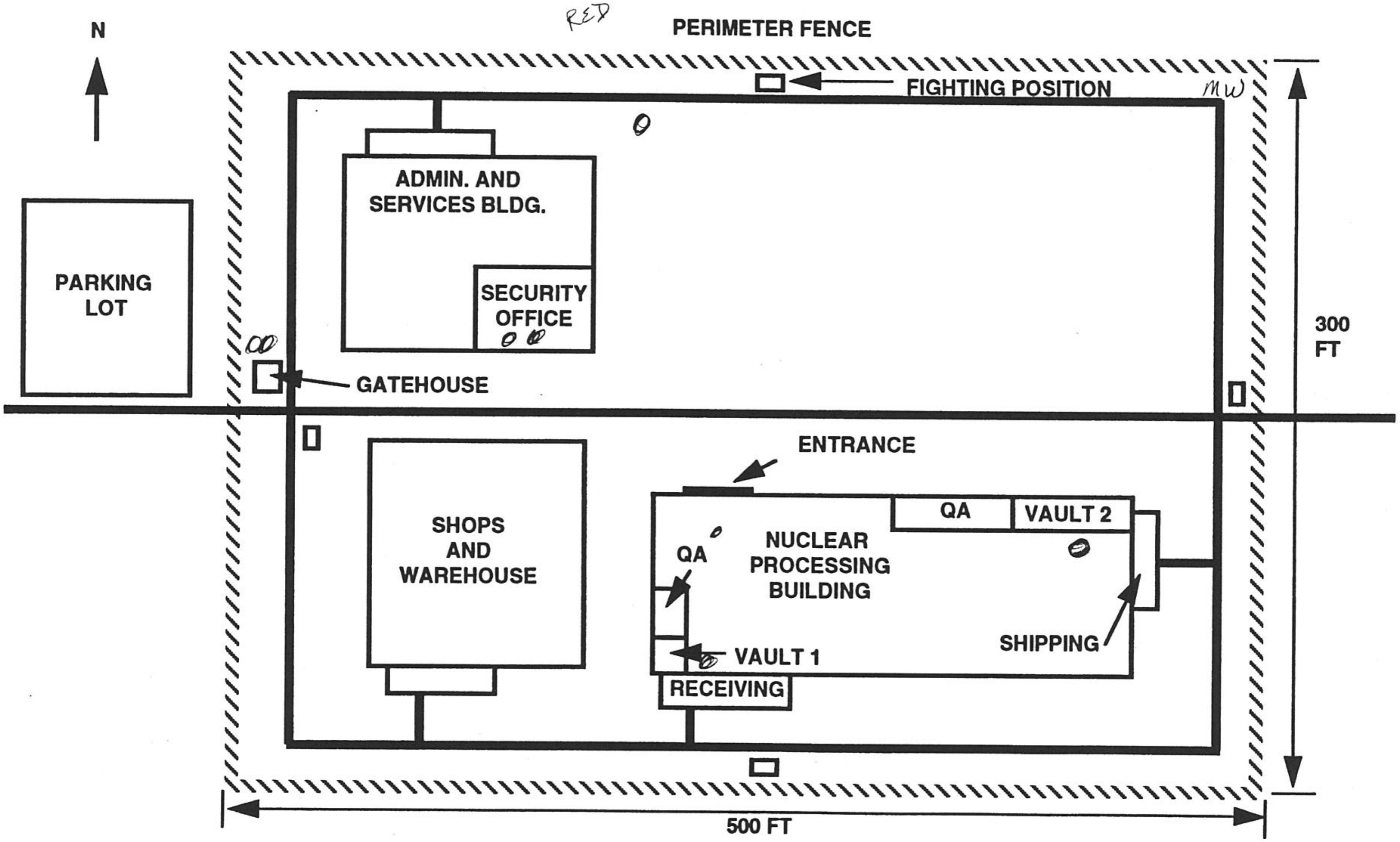
Abbreviations

Com. = Communication
SPO = Special Police Officer
CAS = Central Alarm Station
SAS = Secondary Alarm Station

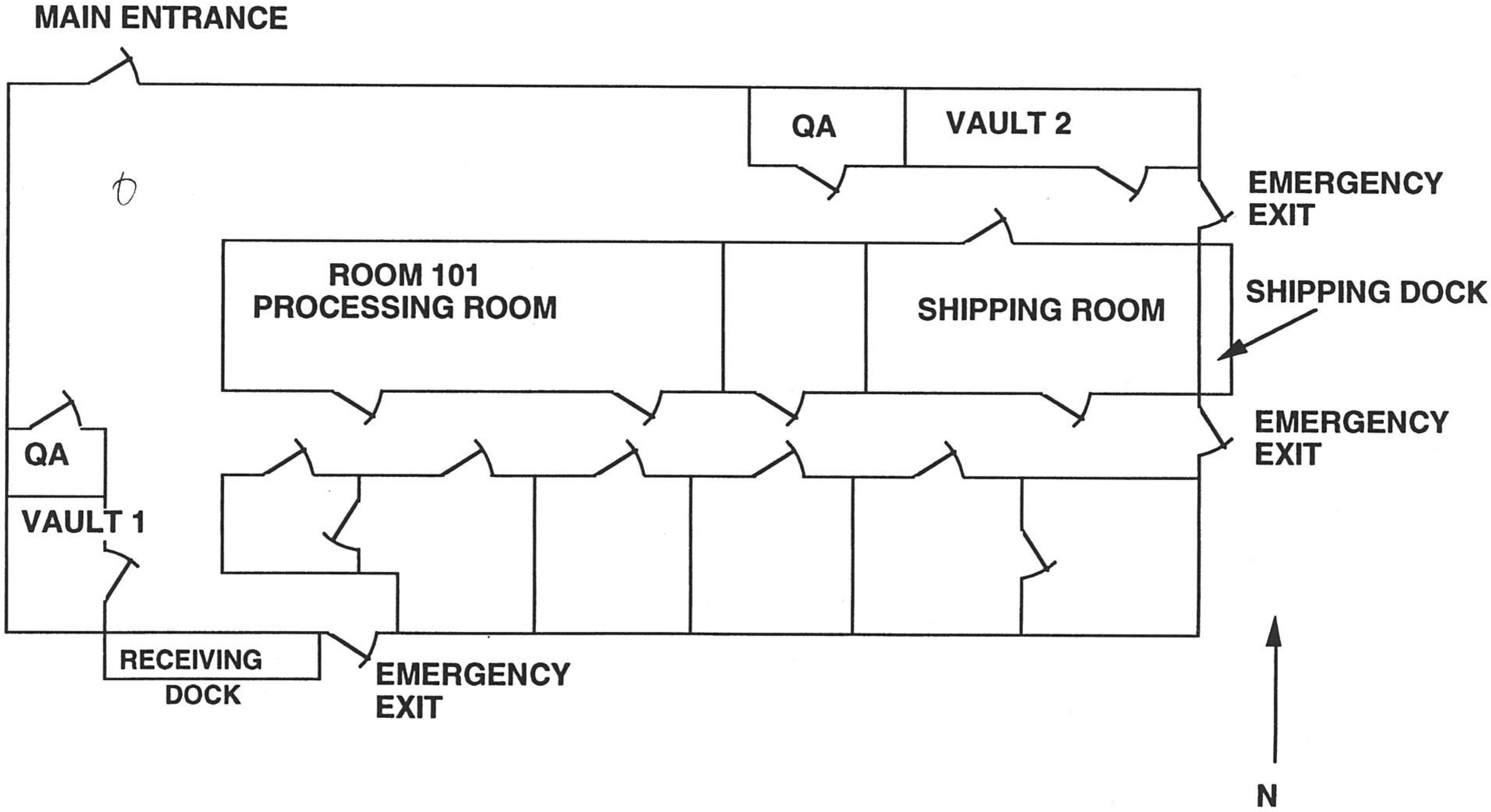
6.a. VA Example

6A. VA EXAMPLE

EXAMPLE NUCLEAR PROCESSING PLANT (SNM)



NUCLEAR PROCESSING BUILDING



NUCLEAR PROCESSING PLANT I

Layout of the Site

This is a layout of the example site. The processing plant is enclosed by a single chain-link fence that forms the perimeter boundary. The Processing Building is located in the southeast corner of the plant.

To the northwest of the processing building is the security office with the central alarm station (CAS), which serves as our security control center. Four security police officers (SPOs) staff the CAS 24 hours/day.

Layout of the Processing Building

This is our main processing building where ingots are cast into weapons components. The walls of the building form the boundary of the Material Access Area (MAA). Inside the building there are offices, a processing area, the special nuclear material vaults where raw materials and products are stored, shipping and receiving docks, and two nondestructive assay laboratories. Significant quantities of SNM are routinely tested overnight in the product QA laboratory. Authorized access to the processing building is through the gatehouse on the west side of the site.

Site Perimeter

The perimeter is surrounded by a single 8-foot-high chainlink fence topped with three strands of barbed wire. The fence fabric is not anchored to the ground. A roving SPO patrols the PA boundary 24 hours/day. The perimeter area is lighted but does not have CCTV.

Fence disturbance sensors are mounted on the perimeter fence. If the fence is disturbed by someone climbing or cutting the fence, an alarm annunciates in the CAS and SAS.

Entrance to the Site

Two SPOs staff the gatehouse portal and vehicle gate 24 hours/day. One monitors alarms and handles communications while the other is responsible for processing pedestrians and vehicles through the portals. The gatehouse also contains the secondary alarm station (SAS) and a duress alarm that annunciates in the CAS.

To enter the perimeter through the pedestrian portal, each person must present a picture badge. The officer checks the validity of the picture badge and has each person enter his or her personal identification number (PIN). Visitors are given badges marked "Visitor" and require an authorized escort at all times within the plant area.

A SPO visually inspects all packages carried into the plant area for contraband and unauthorized items. The pedestrian must walk through a metal detector before entering the perimeter. The metal detector annunciates locally. Upon exit, there is a random search of the personal effects of 5% of all personnel leaving the plant area.

Vehicles enter the plant area through a vehicle trap. Only vehicles with special permits are allowed inside the plant area. At the vehicle gate, the SPO checks the permit. Drivers and passengers must leave their vehicle and follow access control procedures through the pedestrian portal. The SPO quickly performs a visual check of the vehicle's interior for contraband. If no contraband is detected, the SPO opens the gate to let the vehicle through.

Upon exit, the driver and passengers get out of their vehicle and proceed through the pedestrian portal, then drive out after the SPO opens the gate. There is a random search of 10% of the vehicles leaving the plant area.

Processing Building

The walls and roof of the building are constructed of 1-foot thick concrete reinforced with rebar. All ventilation and ductwork is protected with 3/8-inch rebar on 6-inch centers. Wall thickness around the vault is 18 inches of concrete with rebar reinforcement.

All exterior doors are standard metal doors and are equipped with balanced magnetic switches. A SPO is on duty at the building entrance when the plant is operating (7 am to 5 pm weekdays). A duress alarm at the entrance annunciates in the CAS and SAS.

EXAMPLE THREAT-TARGET COMBINATION

THREAT - FOUR TERRORISTS TO STEAL A CATEGORY I QUANTITY OF SNM

TARGET - SNM IN SHIPPING QA LAB

EXAMPLE SECURITY SYSTEM

PERIMETER FENCE	• SINGLE CHAINLINK, LIGHTED, NO CCTV, NO FENCE ANCHORS
ALARMS	• FENCE DISTURBANCE SENSORS ON PERIMETER FENCE
	• BALANCE MAGNETIC SWITCHES ON PROCESSING BUILDING DOORS
	• DURESS ALARM AT GATEHOUSE AND PROCESSING BUILDING ENTRANCE
SECURITY POST	• SECURITY OFFICE (4 SECURITY POLICE OFFICERS), ALSO CENTRAL ALARM STATION
	• GATEHOUSE (2 SECURITY POLICE OFFICERS), ALSO SECONDARY ALARM STATION
	• PROCESSING BUILDING (1 SECURITY POLICE OFFICER AT ENTRANCE 7 AM TO 5 PM WEEKDAYS)
	• PATROL (1 SECURITY POLICE OFFICER)
ACCESS CONTROLS	• GATEHOUSE AND PROCESSING BUILDING ENTRANCE
RESPONSE PLAN	• ONE SPO DEPLOYS TO EACH OF 4 FIGHTING POSITIONS
COMMUNICATIONS	• PORTABLE FM + 2 BASE STATIONS
WEAPONS	• 8 PISTOLS + 7 SEMIAUTOMATIC RIFLES + 1 SHOTGUN

SYSTEM EFFECTIVENESS EVALUATION
-- PROBABILITY WORKSHEET --

ADVERSARY ____________________ ACT ________________ TARGET ____________________

SCENARIO NO. ________________ CASE ____

ADVERSARY EVENT LINE	SITE	ENTRY PA	MAA	ACQUISITION	MAA	REMOVAL PA	SITE
ADVERSARY TIME LINE	________	□	________	________	________	________	□ ________ MINUTES
PD	________	________	________	________	________	________	________
PA	________	________	________	________	________	________	________
PE	________	________	________	________	________	________	________
PN	________	________	________	________	________	________	________
PMIN	________	________	________	________	________	________	________

SE ____

$$SE = PD1 \bullet PA1 \bullet PE1 \bullet PN1 + (1 - PD1 \bullet PA1)\, PD2 \bullet PA2 \bullet PE2 \bullet PN2$$

DETECTION VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary ____________ Act ____________________ Target ____________________ Date ____________ Worksheet No. ____________

	Adversary Event Line												
ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6 Movement in Area	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal X	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7 Movement in Area	2.8	2.9			
ACQUISITION	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10 Movement in Area	3.11	3.12
	Target*	4.1 Normal Access	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9			
	MAA	5.1 Thru Personnel Portal	5.2 Thru S/R** Portal	5.3 Thru Emergency Exit	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10 Movement in Area	5.11	5.12
REMOVAL	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7 Movement in Area	6.8	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6 Movement in Area	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.
** S/R = Shipper/Receiver

VULNERABILITY DESCRIPTIONS FOR WORKSHEET NO. ____________

Vulnerability Number	Vulnerability Description

Provide descriptions for vulnerability levels VH, H, M and others where appropriate.

DELAY VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary ________ Act ________ Target ________ Date ________ Worksheet No. ________

Adversary Event Line

ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7	2.8	2.9			
ACQUISITION	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10	3.11	3.12
	Target*	4.1 Normal Access	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9	4.10		
	MAA	5.1 Thru Personnel Portal	5.2 Thru S/R** Portal	5.3 Thru Emergency Exit	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10	5.11	5.12
REMOVAL	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7	6.8	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.
** S/R = Shipper/Receiver

ALARM ASSESSMENT VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER ADVERSARIES

Adversary ______________ Act ______________ Target ______________ Date ____________ Worksheet No. ________

Type of Alarm Assessment							
CCTV Response To Alarm	1.1 Defeat Camera	1.2 Defeat Com. to CAS/SAS	1.3 Use Deceit	1.4 Use Stealth	1.5 Report False Alarm	1.6	1.7
SPO Response To Alarm	2.1 Neutralize SPO	2.2 Defeat Com. to CAS/SAS	2.3 Use Deceit	2.4 Use Stealth	2.5 Report False Alarm	2.6	2.7
Routine SPO Patrol	3.1 Neutralize SPO	3.2 Defeat Com. to CAS/SAS	3.3 Use Deceit	3.4 Use Stealth	3.5 Report False Alarm	3.6	3.7
Multiple Alarms	4.1 Report False Alarm	4.2	4.3				
Duress Alarm	5.1Report False Alarm	5.2	5.3				

Abbreviations

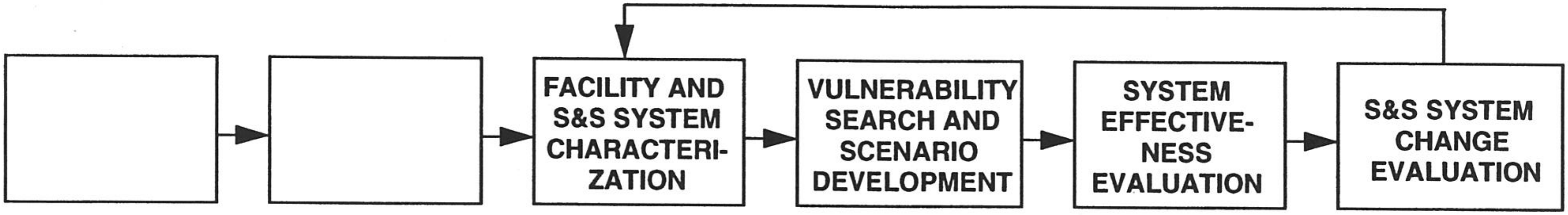
Com.	=	Communication
SPO	=	Special Police Officer
CAS	=	Central Alarm Station
SAS	=	Secondary Alarm Station

6.b. VA Exercise

6B. VA EXERCISE

VA EXERCISE

- UPGRADE S&S SYSTEM
- PERFORM VA FOR UPGRADED S&S SYSTEM



FACILITY AND S&S SYSTEM CHARACTERIZATION

VULNERABILITY SEARCH AND SCENARIO DEVELOPMENT

SYSTEM EFFECTIVENESS EVALUATION

S&S SYSTEM CHANGE EVALUATION

<u>PRODUCT</u>:

- DESCRIPTION OF CANDIDATE S&S CHANGES.
- INFORMATION ON PERFORMANCE OF S&S CHANGES.

<u>PRODUCT:</u>

- LIST OF VULNERABILITIES FOR CHANGED S&S SYSTEM.
- ADVERSARY'S PLANS OF ATTACK FOR MOST CREDIBLE SCENARIOS.

<u>PRODUCT</u>:

- LEVELS OF SYSTEM EFFECTIVENESS FOR CHANGED S&S SYSTEM.

<u>PRODUCT</u>:

- PRIORITIZED LIST OF S&S CHANGES.

- ESTABLISH GOAL FOR S&S SYSTEM CHANGE:
  - IMPROVE SYSTEM EFFECTIVENESS
  - REDUCE SYSTEM COSTS
  - IMPROVE EFFICIENCY
- IDENTIFY COMPLEMENTARY SETS OF S&S SYSTEM CHANGES:
  - FACILITY
  - EQUIPMENT
  - PERSONNEL
  - PROCEDURES
- DETERMINE CHANGE IN SYSTEM EFFECTIVENESS AND COST FOR EACH SET.
- PRIORITIZE EACH SET OF S&S SYSTEM CHANGES BASED ON GOAL AND ON CHANGES IN SYSTEM EFFECTIVENESS, COST AND OTHER RELEVANT FACTORS.

6.c. Performance
Testing

6C. PERFORMANCE TESTING

OUTSIDER THREAT PERFORMANCE TESTING

-- EXAMPLES OF TESTS TO DETERMINE PD --

- PERIMETER INTRUSION DETECTION SYSTEM
  - OPERABILITY TESTS
  - SENSITIVITY TESTS
  - EQUIPMENT DEFEAT TESTS
- ENTRY CONTROL FACILITY
  - OPERABILITY TESTS
  - SENSITIVITY TESTS
  - LIMITED SCOPE PERFORMANCE TESTS

OUTSIDER THREAT PERFORMANCE TESTING

-- EXAMPLES OF TESTS TO DETERMINE PA --

- ASSESSMENT SYSTEMS
  - OPERABILITY TESTS
  - SENSITIVITY TESTS
  - EQUIPMENT DEFEAT TESTS
- PERSONNEL
  - PROCEDURAL TESTS
  - LIMITED SCOPE PERFORMANCE TESTS

OUTSIDER THREAT PERFORMANCE TESTING

-- EXAMPLES OF TESTS TO DETERMINE PE --

- DEPLOYMENT INITIATION
  - PROCEDURAL TESTS
  - COMMUNICATION TIME TESTS
- RESPONSE TIME
  - SKILL TESTS
  - ALARM RESPONSE AND ASSESSMENT PERFORMANCE TESTS

OUTSIDER THREAT PERFORMANCE TESTING

-- EXAMPLES OF TESTS TO DETERMINE PN --

- FIREARMS PROFICIENCY
- FORCE-ON-FORCE EXERCISES

6D. AIRBORNE THREAT

AIRBORNE THREAT

- HELICOPTERS
  - INCOMING TO FACILITY
  - OUTGOING FROM FACILITY
  - RELIABILITY FOR ADVERSARIES
  - USE OF DEADLY FORCE BY SPOs
    - POLICY
    - TRAINING
- OTHER AIRBORNE VEHICLE

7. INSIDER THREAT ANALYSIS

INSIDER THREAT VULNERABILITY ANALYSIS
OUTSIDER VS INSIDER THREATS

Outsiders

- More people in adversary group
- More likely to use violence
- Greater firepower
- One or several types of outsiders

Insiders

- Additional tactics
  - Misuse of authorized access to targets
  - Misuse of S&S authority To reduce effectiveness of protective measures
  - Carry out of theft or sabotage in stages over period of time or under different conditions
  - Coverup of theft
- Many types of insiders with different capabilities to misuse access and S&S authority

INSIDER THREAT VULNERABILITY ANALYSIS
OUTSIDER VS INSIDER
FACILITY CHARACTERIZATION

Outsiders

- Focus on perimeter and entry controls
- Focus on building externals
- Focus on response plans and tactical communications

Insiders

- Focus on building internals
- Operational understanding
- MC&A operations
- Systems details
- SNM removal detection

Facility will look different through the eyes of the insider.

INSIDER THREAT VULNERABILITY ANALYSIS

INSIDER TACTICS

Covert tactics

- More plausible
- Non-violent
- Tactics emphasize
  - Misuse of authorized access
  - Misuse of S&S authority
  - Stealth
  - Deceit
  - Staging
  - Coverup (theft)
- Detection capability is essential for effective protection

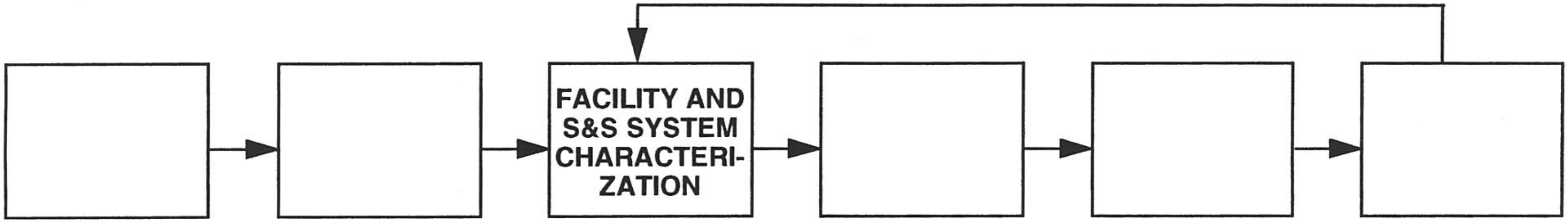
Covert-overt tactics

- Less plausible
- May be violent
- Covert tactics used as long as possible
- Overt tactics used when necessary
- Four protection capabilities are essential for effective protection

7.a. VA Example

7A. VA EXAMPLE

INSIDER THREAT VULNERABILITY ANALYSIS



PRODUCT:

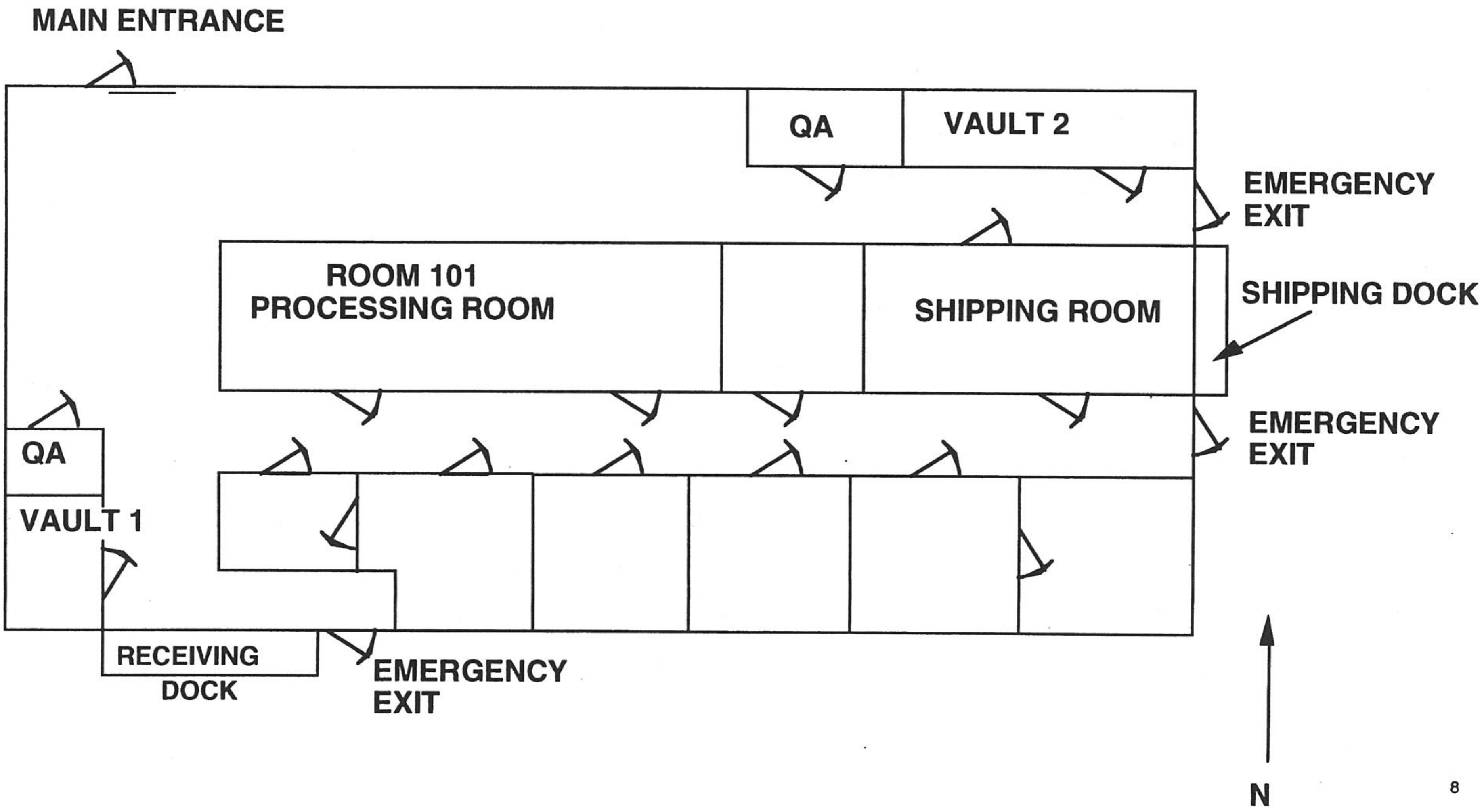
- **DESCRIPTION OF SITE, FACILITY AND S&S SYSTEM**
- INFORMATION ON PERFORMANCE OF S&S PERSONNEL, COMPONENTS AND SUBSYSTEMS

- **Characterization should represent a snapshot in time.**
- **Mark up site and building drawings to show locations of key targets and key S&S measures relevant to protection against insider threats.**
  - ▲ **Barriers, intrusion sensors, CCTV and access controls**
  - ▲ **SNM detection equipment**
  - ▲ **Alarm locations**
- **Review building operational plans and procedures.**

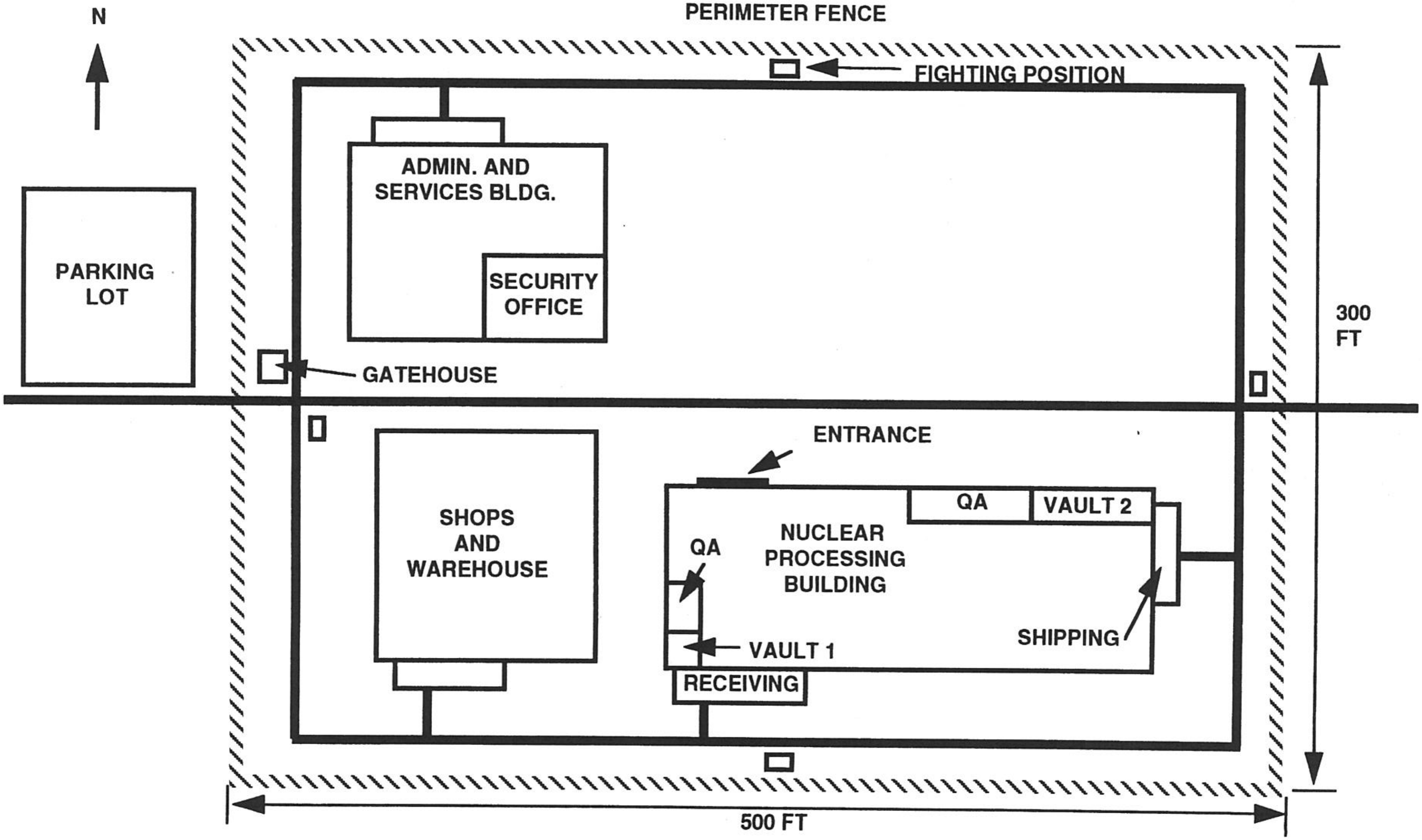
SOURCES OF FACILITY AND S&S SYSTEM INFORMATION

- As-built drawings of site, facility, S&S components, and S&S subsystems.
- S&S plans:
  - ▲ Security plans, procedures, and records.
  - ▲ Protective force post orders and emergency response plans.
  - ▲ MC&A plans, procedures and records.
  - ▲ Staffing plans.
- Training plans and records.
- Equipment specifications, operating manuals, maintenance plans and records.
- Survey and inspection reports.
- Team member tours, inspections and interviews.

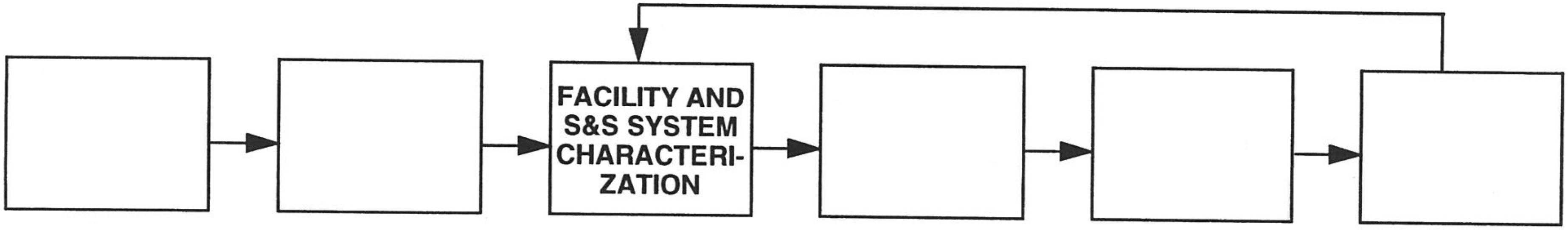
NUCLEAR PROCESSING BUILDING



EXAMPLE NUCLEAR PROCESSING PLANT (SNM)



INSIDER THREAT VULNERABILITY ANALYSIS



PRODUCT:

- DESCRIPTION OF SITE, FACILITY AND S&S SYSTEM
- **INFORMATION ON PERFORMANCE OF S&S PERSONNEL, COMPONENTS AND SUBSYSTEMS**

- **Identify authorized access and S&S authority for each category of site employee.**
- **Collect other information, including performance data, as needed**

DEVELOP POTENTIAL ADVERSARY LIST

- Define all personnel types to assure characterization of all potential adversaries
- List all important personnel (vault access, hands-on SNM, combinations, SNM detectors, criticality detectors)
- Combine personnel with:
  - Same authorized access
  - Same authority over protection measures
  - Similar knowledge
  - Similar safeguards performance

EXAMPLE GROUP ATTRIBUTES

- Hands-on access to SNM
- Access to MC&A records and computers system
- Prepares, participates in, or authorizes transfer of SNM
- Maintains and calibrates vault alarms, SNM, or metal detectors
- Tests alarms (SNM, health physics, etc.)
- Controls searches, assesses alarms, staffs security posts
- Supervisory authority

EXAMINE EACH GROUPS ATTRIBUTES:

- Vault custodians may have vault combinations
- Alarm technicians have access to and opportunities to defeat or tamper with alarms
- 'SPOs' may be exempt from searches or may control the SNM alarm
- Operators may have hands-on access to SNM but no control of SNM detectors
- CAS operators may be able to reset alarms

DOCUMENT EACH GROUPS ATTRIBUTES

- ●Access to critical areas
- ●Special authority or privileges
- ●Combinations/keys held or acquired
- ●Special knowledge

Note: adversary attributes may change based on facility conditions.

Example:

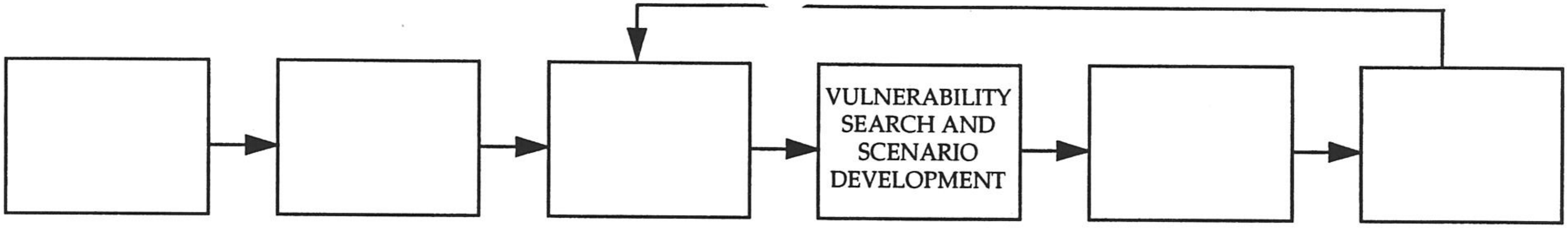
Security police officer:

- ▲ Has no hands-on to SNM
- ▲ Controls the access point to MAA as part of a two-person team
- ▲ Carries weapon with access past search points
- ▲ Provides alarm assessment
- ▲ May be part of a responding unit
- ▲ Works on all shifts, etc.

ADVERSARY LIST

GROUP	ACCESS	AUTHORITY
Vault Custodian	PA; MAA; Vault; A Combination	Vault Alarm; Shipping
Operator	PA; MAA; Vault	

- Prioritize groups with robust authority and/or access.
- Focus initial analysis on the strong groups depending on threat/target combination and facility condition



PRODUCT:

- LIST OF VULNERABILITIES
- ADVERSARY'S PLANS OF ATTACK FOR MOST CREDIBLE SCENARIOS

VULNERABILITY SEARCH

- Threat-target combinations
- Exploitable weaknesses
- All adversary options
  - ▲ Strategies
  - ▲ Tactics
  - ▲ Paths
- All facility conditions (operating, shutdown, maintenance, emergency).

INSIDER THREAT VULNERABILITY ANALYSIS

- ● Develop credible scenarios that give adversary best chance for success
  - ▲ Assume adversary seeks to exploit most serious vulnerabilities
- ● KISS
  - ▲ Simple strategies
  - ▲ Simple tactics
  - ▲ Easy paths

TYPES OF INSIDER THREAT ANALYSES

	SINGLE INSIDER		ADVERSARY ACTION		INSIDER
NO.	NON-VIOLENT	VIOLENT	ABRUPT	PROTRACTED	ASSISTANCE
1	X		X		
2		X	X		
3	X			X	
4	X		X		X
5		X	X		X
6	X			X	X

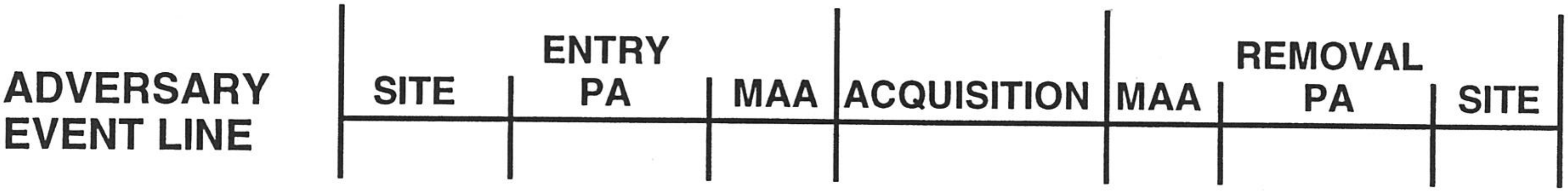
INSIDER THREAT VULNERABILITY ANALYSIS

ANALYSIS FOR EACH THREAT - TARGET COMBINATION.

Examine:

- Non-violent
    - Single
    - Multiple
- Violent
    - Single
    - Multiple
- Criminal
    - Passive assistance
    - Active assistance
    - Violent assistance

SCENARIO DEVELOPMENT



ADVERSARY EVENT LINE

SITE | ENTRY PA | MAA | ACQUISITION | MAA | REMOVAL PA | SITE

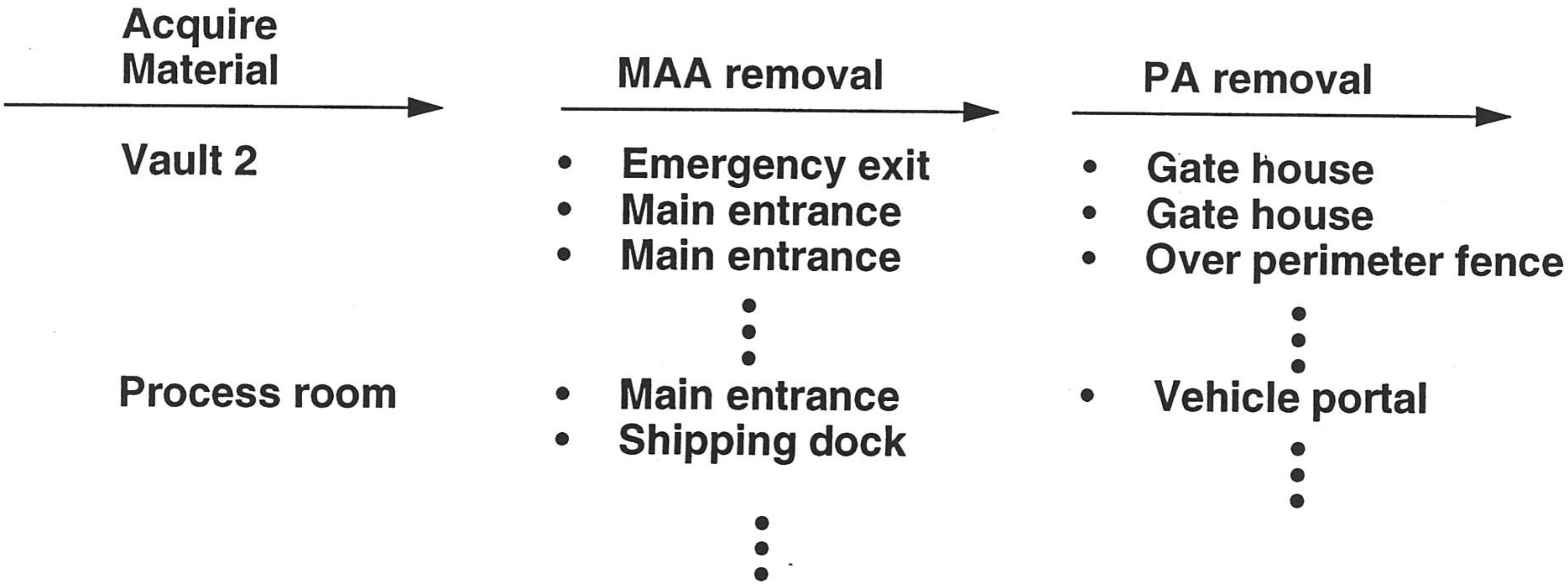
For insider, entry is usually a given so delete entry segments as appropriate.

SCENARIO DEVELOPMENT

- Theft scenarios are separated into segments
  - ▲ Gain access to target
  - ▲ Acquire material
  - ▲ MAA removal
  - ▲ Move material off-site
- For a scenario to be successful, the adversary must complete entrance and exit with materials

SCENARIO DEVELOPMENT

- Each segment provides the adversary with many alternatives.
- Adversary will choose best strategy for success at each segment.



Acquire Material

Vault 2

Process room

MAA removal

- Emergency exit
- Main entrance
- Main entrance

⋮

- Main entrance
- Shipping dock

⋮

PA removal

- Gate house
- Gate house
- Over perimeter fence

⋮

- Vehicle portal

⋮

IDENTIFY VULNERABILITIES AT EACH SAFEGUARD

- Understand functions and operation
- “Adversary perspective”of security equipment and procedures
- Utilize interviews and expert knowledge
- Subject matter experts

---- UNDERSTAND DETAIL ---

INSIDER TACTICS

- Insiders exploit their knowledge
  - Safeguards and security procedures
  - Facility operations
  - Material control
- Insiders are opportunists
  - Choice of time and strategy
  - Usually have access to critical areas
- Insiders abuse authority
  - Alarm monitoring
  - Response
  - Material handling

INSIDER TACTICS

- Defeat detection, exploit access/authority
  - ▲ Tamper with S&S components
  - ▲ Shield material
  - ▲ Collude
  - ▲ Falsify records
  - ▲ Hide material in non-SNM shipment for later retrieval
  - ▲ Create emergency
  - ▲ Pass through duct, window, wall or tunnel

INSIDER TACTICS

- Disable, confuse, or delay response or assessment
  - ▲ Plant false data (MC&A)
  - ▲ Misuse authority (SI, vault custodian)
  - ▲ Take advantage of human nature
  - ▲ Collude
  - ▲ Abrupt vs protracted (theft)

INSIDER TACTICS

- Defeat delay
  - ▲ Wait for appropriate time
  - ▲ Utilize access

- For each personnel group based on access and authority identify tactics to complete theft using the best chance of success.

DETECTION VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary Custodian Act Theft Target Vault Date ______ Worksheet No. A

Adversary Event Line

ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6 Movement in Area	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7 Movement in Area	2.8	2.9			
ACQUISITION	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10 Movement in Area	3.11	3.12
	Target*	4.1 Normal Access VL	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9			
REMOVAL	MAA	5.1 Thru Personnel Portal M	5.2 Thru S/R** Portal H	5.3 Thru Emergency Exit M	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10 Movement in Area	5.11	5.12
	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7 Movement in Area	6.8 Shipping L	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6 Movement in Area	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.

** S/R = Shipper/Receiver

VULNERABILITY DESCRIPTIONS FOR WORKSHEET NO. A

Vulnerability Number	Vulnerability Description
4.1	Custodian has normal access; no detection
5.1	Ability to disable the detection devices or conceal material from detection
5.3	A. Deceit on tripping BMS on MAA boundary
	B. Cause an MAA evacuation
6.8	A. Conceal theft by piggybacking unauthorized material in an authorized shipment
	B. Falsely authorize a shipment

Provide descriptions for vulnerability levels VH, H, M and others where appropriate.

DETECTION VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary Operator Act Theft Target Vault Date ________ Worksheet No. B

Adversary Event Line													
ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6 Movement in Area	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7 Movement in Area	2.8	2.9			
ACQUISITION	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10 Movement in Area	3.11	3.12
	Target*	4.1 Normal Access Ⓜ	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9			
	MAA	5.1 Thru Personnel Portal H	5.2 Thru S/R** Portal Ⓛ	5.3 Thru Emergency Exit M	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10 Movement in Area	5.11	5.12
REMOVAL	PA	6.1 Thru Fence H	6.2 Over Fence H	6.3 Under Fence --	6.4 Thru Personnel Portal H	6.5 Over Personnel Portal --	6.6 Thru Vehicle Portal --	6.7 Movement in Area	6.8	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6 Movement in Area	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.
** S/R = Shipper/Receiver

VULNERABILITY DESCRIPTIONS FOR WORKSHEET NO. B

Vulnerability Number	Vulnerability Description
4.1	Remove material in violation of two-person rule
5.1	Disable the SNM search portal
5.2	Defeat rollup door on shipping dock
5.3	Cause and evacuation
6.1	Pass material through the fence
6.2	Toss material over the fence
6.3	Conceal material on person exiting the PA

Provide descriptions for vulnerability levels VH, H, M and others where appropriate.

DETECTION VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES (Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary SPO Act Theft Target Vault Date ______ Worksheet No. C

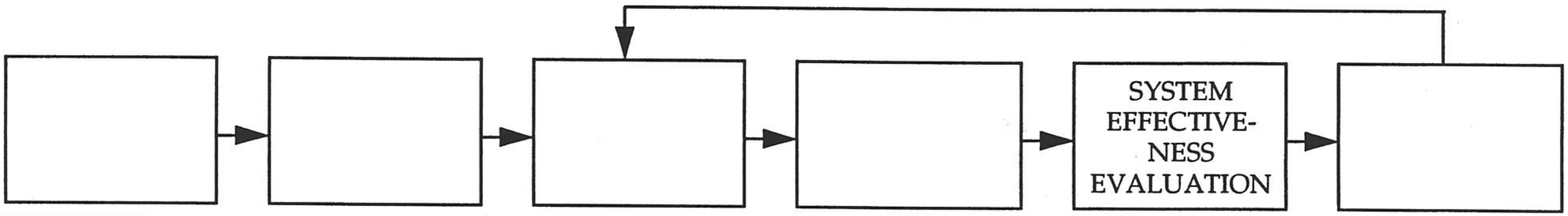
Adversary Event Line													
ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6 Movement in Area	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7 Movement in Area	2.8	2.9			
	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10 Movement in Area	3.11	3.12
ACQUISITION	Target*	4.1 Normal Access	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9			
			Ⓗ										
REMOVAL	MAA	5.1 Thru Personnel Portal	5.2 Thru S/R** Portal	5.3 Thru Emergency Exit	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10 Movement in Area	5.11	5.12
		Ⓛ	H	Ⓛ									
	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7 Movement in Area	6.8	6.9			
		H	H	--	H								
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6 Movement in Area	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.
** S/R = Shipper/Receiver

VULNERABILITY DESCRIPTIONS FOR WORKSHEET NO. C

Vulnerability Number	Vulnerability Description
4.2	Gain material during a vault inspection
5.1	Misuse access/authority to cross portal; reset alarm
5.3	Misuse access/authority to circumvent BMS alarm on the emergency exit
6.1	Pass material through the fence; tower observation; fence sensors
6.2	Toss material over fence; tower observation
6.3	

Provide descriptions for vulnerability levels VH, H, M and others where appropriate.



PRODUCT:

LEVELS OF SYSTEM EFFECTIVENESS

Covert threat rule:

- Active insider (non-violent) will stop when confronted

  SE = PD • PA

  SE = PD1 • PA1 + (1 - PD1 • PA1) PD2 • PA2

For covert scenarios:

- Determine effectiveness of two essential capabilities using performance testing as much as practical.
  - ▲ Detection
  - ▲ Assessment
- Combine results for essential capabilities.

INSIDER THREAT VULNERABILITY ASSESSMENT

Covert-overt rule:

- Violent insider will stop when neutralized
- Will remain covert until detected then go overt

$$SE = PD \bullet PA \bullet PE \bullet PN$$

$$SE = PD1 \bullet PA1 \bullet PE1 \bullet PN1 + PD(1 - PD1 \bullet PA1)\, PD2 \bullet PA2 \bullet PE2 \bullet PN2$$

For covert-overt scenarios

- Estimate adversary timelines and protection response times
- Determine effectiveness of four essential capabilities using performance testing as much as practical.
  - ▲ Detection
  - ▲ Assessment
  - ▲ Engagement
  - ▲ Neutralization
- Combine results for essential capabilities.

INSIDER THREAT VULNERABILITY ASSESSMENT

- Eliminate personnel groups with obvious non-credible scenarios for specific target and threat; i.e., those groups which cannot complete an action.

  Example: non-violent abrupt-theft.

  ▲ SPO cannot gain SNM from vault but may be able to remove from processing room.

  ▲ No group can access material with vault closed.

- Each adversary group may have different acquistion strategies.
- Examine those strategies with the best chance of success.

DETECTION VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary ____________ Act ______________________ Target ______________________ Date ______________ Worksheet No. ______________

Adversary Event Line

ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6 Movement in Area	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7 Movement in Area	2.8	2.9			
ACQUISITION	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10 Movement in Area	3.11	3.12
	Target*	4.1 Normal Access	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9			
	MAA	5.1 Thru Personnel Portal	5.2 Thru S/R** Portal	5.3 Thru Emergency Exit	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10 Movement in Area	5.11	5.12
REMOVAL	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7 Movement in Area	6.8	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6 Movement in Area	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.
** S/R = Shipper/Receiver

VULNERABILITY DESCRIPTIONS FOR WORKSHEET NO. ____________

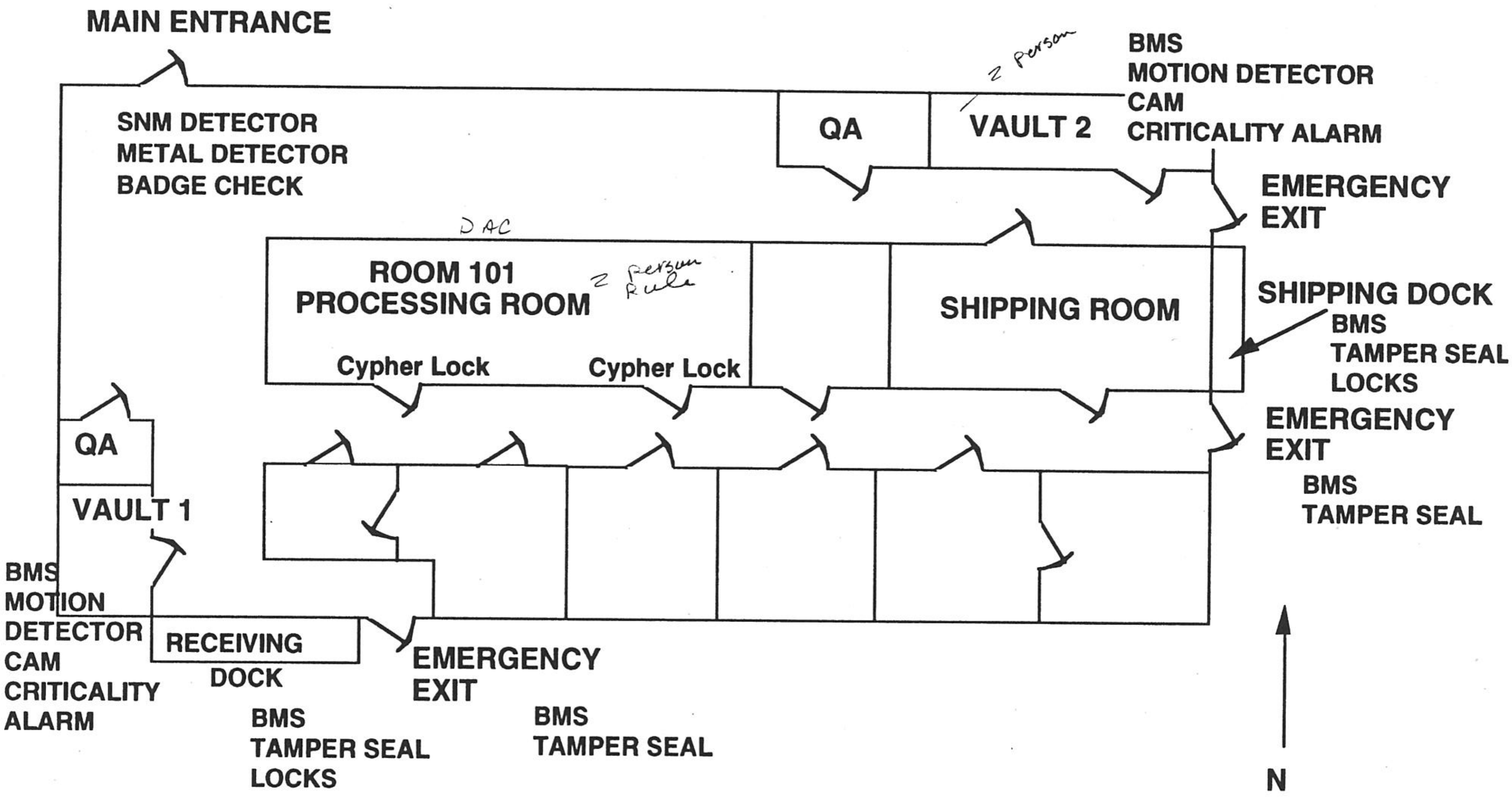
Vulnerability Number	Vulnerability Description

Provide descriptions for vulnerability levels VH, H, M and others where appropriate.

ADVERSARY LIST

GROUP	ACCESS	AUTHORITY
Vault Custodian	PA/MAA/Vault/ A Combo	Vault alarm/Shipping
Operator	PA/MAA/Vault/ B Comb.	vault/Processing/Shipping
Supervisor	PA/MAA/Vault/ A comb/Production schedule	vault/shipping/Process
HP	PA/MAA/vault Processing	Admin Alarm / waste remov Shipping
Maintenance	PA/MAA/vault Processing	security alarm/vault
NDA	PA/MAA/vault? processing?	processing/shipping?
SPO	PA/MAA/vault Processing	alarms/shipping
Cas	PA	alarms

NUCLEAR PROCESSING BUILDING



MAIN ENTRANCE

SNM DETECTOR
METAL DETECTOR
BADGE CHECK

QA

2 person

VAULT 2

BMS
MOTION DETECTOR
CAM
CRITICALITY ALARM

EMERGENCY EXIT

DAC

ROOM 101
PROCESSING ROOM

2 person Rule

Cypher Lock

Cypher Lock

SHIPPING ROOM

SHIPPING DOCK
BMS
TAMPER SEAL
LOCKS

EMERGENCY EXIT
BMS
TAMPER SEAL

QA

VAULT 1

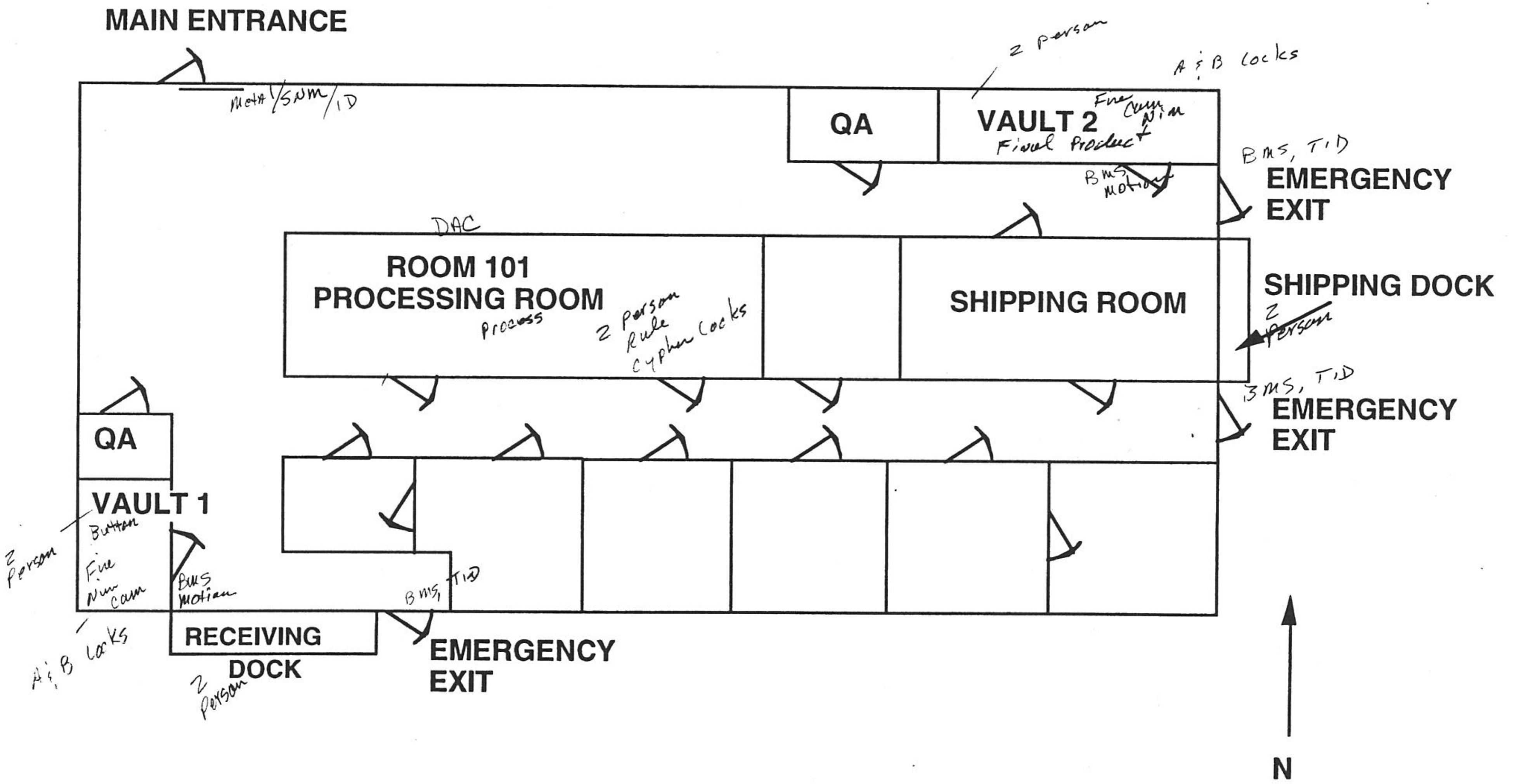
BMS
MOTION
DETECTOR
CAM
CRITICALITY
ALARM

RECEIVING DOCK
BMS
TAMPER SEAL
LOCKS

EMERGENCY EXIT
BMS
TAMPER SEAL

N

NUCLEAR PROCESSING BUILDING



SCENARIO/PROBABILITY WORKSHEET SUMMARY

THREAT: Non-Violent Insider

STRATEGY: Theft

ADVERSARY	TARGET	SCENARIO (Vulnerability No.)*			PD			
		ACQ.	MAA	PA	PD1	PD2	PD3	PD
Custodian	SNM Vault	4.1	5.1	6.8	VL	M	L	M
SPO	SNM Vault	4.2	5.1,5.3	6.1	H	L	H	H
Operator	SNM Vault	4.1	5.2	6.0	M	L	H	H

PD = PD1 + (1-PD1)PD2 + (1-PD1)(1-PD2)PD3

* Found on the Vulnerability Search Worksheets

INSIDER SUMMARY SHEET

THREAT:

SYSTEM STRENGTHS	SYSTEM WEAKNESSES

CHANGE IDENTIFICATION

- Based on goal of change
  - Improve system effectiveness
  - Reduce costs
  - Efficiency
- All types of changes
  - Facilities
  - Personnel
  - Equipment
  - Procedures
- Candidate changes
- Change costs
- Change sets
  - Complementary changes
  - Achievement of change goal

COST-BENEFIT EVALUATION

- Change set evaluation
  - System effectiveness
  - Cost
- Benefit evaluation
  - Achievement of change goal
  - Target importance
- Cost-benefit ratio

7B. VA EXERCISE

NUCLEAR PROCESSING PLANT II

Layout of the Site

This is a layout of the example site. The processing plant is enclosed by a single chain-link fence that forms the perimeter boundary. The Processing Building is located in the southeast corner of the plant.

To the northwest of the processing building is the security office with the central alarm station (CAS), which serves as our security control center. Four security police officers staff the CAS. To get to the processing building, one must walk through the gatehouse, which provides our access control point. There are two security police officers staffing the gatehouse.

Layout of Site Perimeter

The perimeter is surrounded by a single fence. A roving security officer patrols the PA boundary 24 hours/day. The area is lighted but does not have CCTV coverage.

On the west side of the perimeter, there is a pedestrian portal and a vehicle gate.

One 8-foot-high chainlink fence topped with 3 strands of barbed wire surround the perimeter.

A fence disturbance sensor is mounted on the perimeter fence. If the fence is disturbed by someone climbing or cutting the fence, an alarm annunciates in the CAS.

Entrance to the Site

Two security officers staff the gatehouse portal and vehicle gate 24 hours/day. One monitors alarms and handles communications while the other is responsible for processing pedestrians and vehicles through the portals.

To enter the perimeter through the pedestrian portal, each person must present his or her picture badge. The officer checks the validity of the picture badge and has each person enter his or her personal identification number (PIN). Visitors are given badges marked "Visitor" and require an authorized escort at all times within the plant area.

The security officer visually inspects all packages carried into the plant area for contraband and unauthorized items. The pedestrian must walk through a metal detector before entering the perimeter. The metal detector annunciates locally. Upon exit, there is a random search of the personal effects of 5% of all personnel leaving the plant area.

Vehicles enter the plant area through a vehicle trap. Only vehicles with special permits are allowed inside the plant area. At the vehicle gate the security officer checks the permit. Drivers and passengers must leave their vehicle and follow access control procedures through the pedestrian portal. The officer quickly performs a visual check of the vehicle's interior for contraband. He or she then opens the gate to let the vehicle through.

Upon exit, the driver and passengers get out of their vehicle and proceed through the pedestrian portal, then drive out after the security officer opens the gate. There is a random search of 10% of the vehicles leaving the plant area.

Layout of the Processing Building

This is our main processing building where ingots are cast into weapons components. The walls of the building form the boundary of the Material Access Area (MAA). Inside the building there are offices, a processing area, the special nuclear material vaults where raw materials and products are stored, shipping and receiving docks, and a nondestructive assay (QA) lab.

Process Building

Just inside the entrance to the processing building is the portal to the Building MAA. This portal is staffed by security police officer.

Employees must enter the building through the MAA portal.

Here a security officer controls access to the MAA. The officer checks that each person has proper authorization to enter the building. There are detectors for metal and SNM in the portal.

The processing area where SNM buttons are manufactured into components is located in Room 101 of the processing building.

SNM buttons are brought into the processing area from the SNM vault (Vault 1). Here the buttons are melted down and cast into appropriate components. Processing operations are done in gloveboxes and under hoods.

SNM buttons and completed products are stored in the SNM vault (Vault 2). Inside each vault, there are four rows of shelves (floor to ceiling), with three aisles between them. Each location on each shelf is labeled with a location number.

Description of the Processing Building

The walls and roof of the building are constructed of 1-foot thick concrete reinforced with rebar. All ventilation and ductwork is protected with 3/8-inch rebar on 6-inch centers. Wall thickness around the vault is 18 inches of concrete with rebar reinforcement.

The normal means of entering and leaving the building is the MAA portal. There are three other ways out of the MAA: the shipping dock, the receiving dock, and emergency exits.

Upon entering the processing building, personnel first pass through a metal detector. Next they must present a picture badge to the security officer at the post and then go through an SNM monitor.

If the metal detector alarms, the person must go back and walk through it again. If he or she is carrying metal that is causing the alarm, the metal items must be handed to the officer and the person again walks through the detector.

Once through the metal detector, the person must present his or her badge to the security officer. The officer checks that the badge is valid for the site and for the processing building.

Those with a "visitor" badge must be accompanied by someone authorized to enter the building.

After the badge check, a person passes through the SNM monitor and the double doors into the building. To leave the MAA, the person must pass through the SNM and metal detectors without causing an alarm. He or she must also show the security officer his or her badge.

The SNM and metal detectors annunciate locally -- at the security officer's post only. The officer can reset the alarms from within the post. If either detector is down, the officer uses a handheld monitor.

A security police officer is on duty at the MAA portal 10 hours per day (7:00 AM to 5:00 PM). After hours, the portal and building are closed and locked. If access to the building is required during off hours, the person requesting access must arrange for a security officer to let them in. He then verifies ID and performs a manual search of the requestor upon entry and exit. Officers change shifts every 4 hours. When it is time for a shift change, an officer arrives at the post from outside the building. The officer going off duty leaves the building. Although both officers walk through the metal detector, they are not required to remove their guns and other metals objects that may set off the metal detector.

A duress alarm at the entrance annunciates in the CAS and SAS.

During off-shift hours, the security police officer patrolling the PA boundary inspects the interior of the process building.

Opening and Securing the Vaults

The vault can be opened only under the two-person rule. On the vault door, there are two locks: a combination lock and a padlock. The vault custodian and processing supervisor have access to the combination of one of the locks. Their names appear on the "A" access list. At the beginning of each shift, two operators are assigned keys to the padlock by the head of production. The operators scheduled to have keys appear on the "B" access list.

Each week, a security police officer tests the vault door alarm. The security police officer first calls the CAS to inform them of the test, two authorized people unlock the vault door, the security officer slowly opens the door and verifies over radio that the CAS receives an alarm.

Before opening the door, either the supervisor or the vault custodian calls the CAS and identifies him or herself to the security officer. He or she then informs the officer that the vault door is to be opened. The officer in the CAS then switches the vault door alarm and vault motion-detection alarms into "access" mode.

The vault custodian unlocks the combination lock, and an operator unlocks the padlock.

To secure the vault upon leaving, the vault custodian or supervisor calls the CAS and requests the vault be placed in "secure" position. This reactivates the door alarm and the motion-detection system. After securing the vault door, the supervisor or vault custodian calls the CAS to inform them that the vault has been secured. A signal at the CAS indicates that the vault door has been closed and the alarms reactivated.

All work in the vault is done under the two-person rule with at least one "A"-list person present at all times. Once the vault has been opened by the operator and the vault custodian or supervisor, other classifications of employees may also work in the vault as long as two people are always present.

Each item in the vault is assigned to a specific shelf location in the vault. This is true whether the item is a SNM button or component inside a sealed can.

Other people have access to the vault besides the vault custodian, operators, and supervisors. For example, the health physics people go into the vault periodically to change the filters of the CAM alarm system, to test the criticality alarm, and monitor the area for contamination. The health physics people change the CAM alarm system filters each week, and each month they test the criticality alarm.

Maintenance workers must be accompanied by a vault custodian or supervisor. After maintenance is completed on any safeguards equipment, the equipment must be tested by a security officer before it is placed back in service.

Alarm with Alarm Tests

There are 5 types of alarms in the vaults; the alarm on the vault door, the motion-detection system, criticality alarm, continuous air monitoring (CAM) alarm, and the fire alarm.

The vault door is equipped with a balanced magnetic switch the same as those on the building emergency exits. If the door is opened without authorization, an alarm is triggered in the Central Alarm Station and a security police officer is dispatched to investigate.

After testing the door alarm, the security police officer enters the vault to test the series of electronic motion detectors covering the aisles in the vault.

Once inside the vault, the officer closes the vault door until it is only slightly ajar and stands still until the motion detector system is reset. He or she then moves slowly until the CAS receives a motion detection alarm. The vault custodian and an operator observe the SPO from within the vault as this test is conducted.

The criticality alarm, when activated, is a Klaxon sound. This alarm causes evacuation of the processing building until re-entry is authorized by health physics personnel. Evacuation drills are held three or four times a year, and they are announced a week in advance.

Once a month, the health physics representative brings a radioactive source into the vault and holds it up to the criticality alarm to test the alarm. The CAS and process building personnel are notified in advance, and the building is not evacuated.

The CAM alarm warns of any airborne contamination. Upon alarm, only the immediate area is evacuated until health physics personnel declare it is safe to re-enter the area. A health physics person changes the filters on the contamination alarm system weekly. He or she also checks the calibration of the system via the gauge readings.

A fire alarm can be activated by a hand-pull box on the wall, a phone call to the fire department, or by the automatic fire detection and suppression system. In the event of an alarm, instructions are given over the public address system. In the event of an alarm, instructions are given over the public address system. No Klaxon or siren sounds. The building is evacuated only if there is widespread danger. Otherwise, only the immediate area is evacuated.

Emergency Evacuation Alarms

When an emergency alarm sounds, all personnel are instructed to exit the building as quickly as possible through the nearest emergency exit.

After any unscheduled evacuations, all personnel in the Assembly Areas are monitored for SNM or radiological contamination by health physics personnel before being allowed back into the building. After an evacuation, personnel must reenter the building via the MAA portal. Inventory?

Shipping, Receiving, and Processing

When SNM buttons arrive at the processing building from other buildings or offsite, they are brought in through the receiving dock and are taken directly to the SNM storage vault (Vault 1). When required for processing, the SNM buttons are taken to the gloveboxes in the processing area.

Manufactured components are transferred to the other SNM vault (Vault 2) for storage. When there are enough components to make up a shipment, the components are taken out of the vault and leave the building through the shipping dock door.

Incoming SNM shipments to the building are transported under the two-person rule from the receiving dock to the vault (Vault 1).

In the vault, the item number of each item is recorded on a tag that is taped to each plastic bag. When an item is placed on a shelf, the item number and shelf location is noted on the vault inventory list.

No material can be stored overnight in the processing area. Therefore, the quantity of material in the processing area is limited to what is needed for a single shift. At the beginning of their shift, operators in the processing area make up a list of the items they'll need during the day based on the supervisor's production schedule. The supervisor must approve the list.

The shipping dock is where all SNM material leaves the building. Transfer through the shipping room include: outgoing supplies equipment and outgoing waste, and product. Shipments occur approximately every other day.

When waste or equipment is to be removed from the building, it is taken to the health physics station in the shipping room. Generally, waste is stored in drums.

The health physics technician monitors drums and equipment for radioactivity, then places a health physics paper seal on them.

The monitored drums are stored in the shipping room until the area is almost full. When ready to ship material, the dock clerk calls transportation and security. The shipping door is alarmed and double-locked; therefore, when a shipment is made, security must be notified and a security officer unlocks the door from the outside while the vault custodian unlocks the door from the inside.

Loading dock clerks load the waste or equipment onto the truck in the presence of the officer. Waste and equipment are removed separately. Waste goes to the burial ground and equipment to the location requested by the authorizing shipper.

All SNM transfer from the facility go through the warehouse building. When SNM is to be moved into or out of the processing building, an intrasite truck is dispatched from the warehouse building. The intrasite truck backs up to the shipping dock, and a security patrol car is parked at a right angle in front of the truck.

On incoming or outgoing shipments, the vault custodian verifies each drum number against the shipping document to make sure that the drum numbers match the list. Two operators are chosen by the vault custodian to move material onto or off the intrasite truck.

After loading or unloading the intrasite truck, the roll-up door is closed and double-locked. The vault custodian calls the CAS to report that the shipping door has been secured.

Removing Items from Vault

Accompanied by the "A" list person, the operator loads the requested items on a cart.

When all the items are loaded, both people in the vault sign the material list. The items are taken to the processing area under the two-person rule (usually two operators).

The same procedures are used at the end of the shift to transfer finished components to the vault.

Personnel Types and Numbers

The following of personnel have regular access to the processing building:

Personnel Type	Number
Vault custodian	3
Supervisor	3
Operator	20
Health physics	5
Maintenance	5
Security officer	15
NDA technician	3
Loading dock clerk	4

The vault custodian and supervisor personnel groups include their alternates who have the same authority as the regular custodian or supervisor.

There are 20 operators who work mainly in the processing area but on any given day only two operators have the key to the vault door. All operators have access to the key at one time or another.

Emergency Exits

There are three emergency exits out the process building. The locations are illustrated on the building layout. Each emergency exit is equipped with a balanced magnetic switch (BMS) door alarm. When the door is opened, the two components of the switch are separated, and the alarm sounds in the CAS.

A wire tamper-indicating seal is placed on the outside of each emergency exit. The integrity of each seal is checked by a roving security officer on a daily basis. If the door alarm is triggered, a broken seal serves as an indication that the door has been opened.

The two components of the BMS are attached to aluminum plates that are fastened to the door and the frame with machine screws.

When the door alarm sounds, the CAS dispatches an officer to check the emergency exit. The officer checks the seal to determine whether or not the door has been opened. If the seal is broken, the security officer radios for additional help and replaces the seal.

Each week, a security officer tests the emergency exit alarms. Before testing an alarm, the officer radios to inform the CAS.

The officer opens the emergency exit door, breaking the seal. The CAS informs the officer whether or not the alarm sounded. The officer then places another seal on the door.

If the door alarm malfunctions, an officer is posted at the door until it has been repaired. After any maintenance on door alarms, the alarms are retested by security.

Processing Room and NDA Lab Procedures/Access

Access is controlled by cypher locks. All personnel with responsibilities in the processing room or NDA lab are provided with the appropriate combinations. When SNM is present in either room, there is an administrative two-person rule. Two people are required to be in the room, but do not have to maintain constant visual and verbal contact.

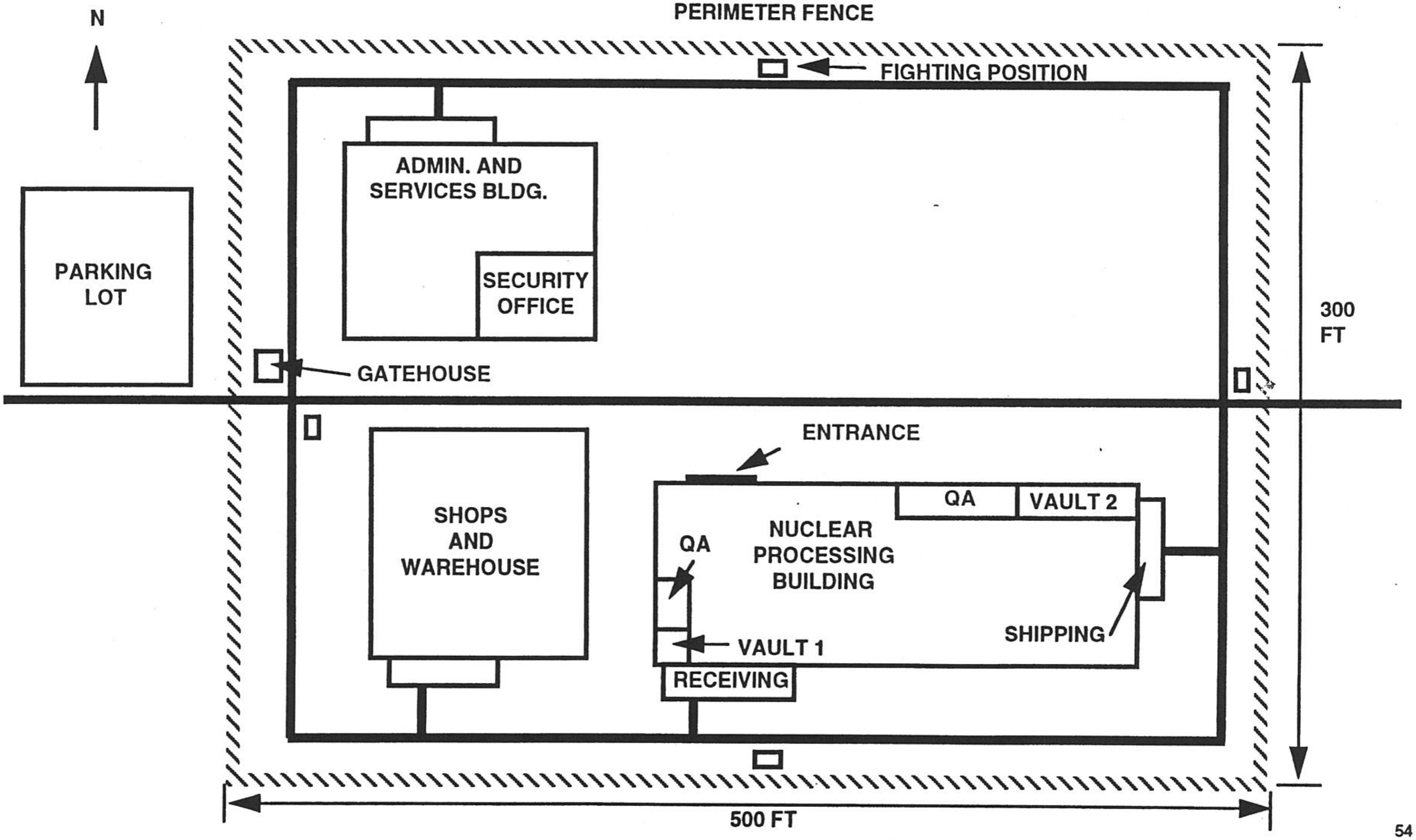
Significant quantities of SNM are routinely tested overnight in the laboratory.

When a measurement is recorded in the NDA lab, two people are required to acknowledge the value that is recorded.

When material is bagged in or out of the glove boxes in the processing room, two operators and a health physics person are required to be present.

There is a Daily Administrative Check (DAC) of the processing room at the end of the production operations to provide assurance that no SNM will remain in the room after the end of the shift.

EXAMPLE NUCLEAR PROCESSING PLANT (SNM)



DETECTION VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary ____________ Act ______________________ Target ______________________ Date ____________ Worksheet No. ____________

Adversary Event Line

ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6 Movement in Area	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7 Movement in Area	2.8	2.9			
ACQUISITION	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10 Movement in Area	3.11	3.12
	Target*	4.1 Normal Access	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9			
	MAA	5.1 Thru Personnel Portal	5.2 Thru S/R** Portal	5.3 Thru Emergency Exit	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10 Movement in Area	5.11	5.12
REMOVAL	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7 Movement in Area	6.8	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6 Movement in Area	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.
** S/R = Shipper/Receiver

VULNERABILITY DESCRIPTIONS FOR WORKSHEET NO. ____________

Vulnerability Number	Vulnerability Description

Provide descriptions for vulnerability levels VH, H, M and others where appropriate.

SCENARIO/PROBABILITY WORKSHEET SUMMARY

THREAT:

STRATEGY:

ADVERSARY	TARGET	SCENARIO (Vulnerability No.)*			PD			
		ACQ.	MAA	PA	PD1	PD2	PD3	PD

PD = PD1 + (1-PD1)PD2 + (1-PD1)(1-PD2)PD3

* Found on the Vulnerability Search Worksheets

INSIDER SUMMARY SHEET

THREAT:

SYSTEM STRENGTHS	SYSTEM WEAKNESSES

7C. PERFORMANCE TESTING

PERFORMANCE TESTS

- Which safeguards detection elements should be tested?

- How should they be tested?

WHICH ELEMENTS TO TEST

- Initial PD values assigned based on expert judgement/available data
- Select for testing if
  - ▲Greater than .10, And
  - ▲Either provides detection capability for credible scenarios, or
- Forces adversary to seek other strategies

HOW SHOULD DETECTION ELEMENTS BE TESTED?

● Consistent with assumptions of vulnerability assessment

  ▲ Test detection capabilities assuming adversary's attempts to defeat/circumvent the element

  ▲ Tests should minimize biases

IMPROVING ESTIMATES BY PERFORMANCE TESTS

- Establish quantitative detection probability
- Improve estimate of detection probability
- Substantiate suspected weaknesses or strengths of safeguards detection elements
- Enable evaluators to better understand interrelationships of multiple detection elements

DIFFICULTIES IN DEVELOPING/ EXECUTING PERFORMANCE TESTS

- Detection elements may be complex systems
  - ▲People/machine interfaces
- Strong dependence on procedures
  - ▲Training effectiveness
  - ▲Human errors
  - ▲Individual personalities
- Opportunism of the adversary
- Cost of test vs. benefit of validation
- Impact on operations
- Keeping an unannounced test a secret

COMPLEX PEOPLE/MACHINE SYSTEMS

- Test the entire system
- Test functionality of equipment
- Test adversary's capability of eliminating or reducing the sensitivity of the equipment
- Test procedures
- Test knowledge of operators
- Test ability of adversary to circumvent or talk his/her way around system

QUANTIFICATION

- Expert judgement
- Performance testing
- Combination of expert judgement and performance testing
  - ▲Weighted average
  - ▲Bayesian analysis

EXPERT JUDGEMENT

- Commonly used to quantify difficult to measure values
- Heavily used in the past
- Results highly dependent on the panel of experts
- May be more useful in establishing qualitative detection capabilities

PERFORMANCE TESTS

- Must realistically test the system to be beneficial
- Small number of tests provides minimal information
- Large number of tests required to precisely estimate detection probabilities
- Can be useful in identifying/confirming strengths/weaknesses in detection elements

CONFIDENCE BASED ON LIMITED TESTING

SAMPLE SIZE	SYSTEM SUCCESSES	CONFIDENCE INTERVALS		
		≥ 90%	≥ 95%	≥ 99%
1	0	.000<p<.950	.000<p<.975	.000<p<.995
2	0	.000<p<.776	.000<p<.842	.000<p<.929
2	1	.025<p<.975	.013<p<.987	.002<p<.998
3	0	.000<p<.632	.000<p<.708	.000<p<.829
3	1	.017<p<.865	.008<p<.906	.002<p<.959
4	0	.000<p<.527	.000<p<.602	.000<p<.734
4	1	.013<p<.751	.006<p<.806	.001<p<.889

TESTING REQUIREMENTS TO GAIN STRONG CONFIDENCE

PD < .25	=	More than 100 tests
.25 < PD <.4	=	About 80 tests
.4 < PD <.6	=	From 20 t0 50 tests
.6 < PD < .75	=	About 80 tests
PD > .75	=	More than 100 tests

7D. PROTRACTED ACTION

ABRUPT VS. PROTRACTED THEFT

Target acquisition

- Abrupt
  - Single acquisition
  - Rapid acquisition of multiple targets
- Protracted
  - Single acquisition with intent to stash (item must be separable)
  - Gradual acquisition over time

Removal

- Abrupt
  - Single removal attempt
- Protracted
  - Multiple removals over extended Period

7.e. Violent Insider

7E. VIOLENT INSIDER

VIOLENT INSIDER

- Insider in any potential adversary group.
- Estimate adversary time lines and protection response time.
- System effectiveness uses the four essential capabilities.
    - Detection
    - Assessment
    - Engagement
    - Neutralization
- Neutralization may be trivial.
- $SE = PD \cdot PA \cdot PE \cdot PN$ (1 detection point)

  $$SE = PD1 \cdot PA1 \cdot PE1 \cdot PN1 + (1 - PD1 \cdot PA1)\, PD2 \cdot PA2 \cdot PE2 \cdot PN2$$

  (2 detection points)

7.f. Inside Assistance

7F. INSIDER ASSISTANCE

8. Outsider Threat Analysis
(with Insider)

INSIDER ASSISTANCE (COLLUSION)

- Examine potential adversary list for complimentary pairs.
- For collusion look for strong pairs (e.g. those with access to SNM paired with those with authority over alarm systems and/or response).
- Examine scenario/probability worksheet to find potential adversaries when combined can complete a scenario; i.e., SPO and health physics.
- Analysis may be violent or non-violent.
- Complete for all adversary pairs.

8. OUTSIDER THREAT ANALYSIS (WITH INSIDER ASSISTANCE)

INSIDER ASSISTANCE TO OUTSIDER THREATS

- NON-VIOLENT INSIDER
- VIOLENT INSIDER

8.a. Non-Violent Insider
Assistance

8A. NON-VIOLENT INSIDER ASSISTANCE

NON-VIOLENT INSIDER ASSISTANCE TO OUTSIDER THREATS

- PRINCIPAL ADVERSARY TACTIC IS TO COMPROMISE S&S MEASURE THAT CAUSES AN ESSENTIAL S&S SYSTEM CAPABILITY (DETECTION, ASSESSMENT, ENGAGEMENT, NEUTRALIZATION) TO FAIL UNDER SCENARIO CONDITIONS.
- BASED ON EACH INSIDER'S AUTHORIZED ACCESS AND S&S AUTHORITY, S&S MEASURES NEED TO BE EXAMINED FOR SUSCEPTIBILITY TO COMPROMISE.
- KEY S&S MEASURES TO EXAMINE FOR SUSCEPTIBILITY TO COMPROMISE:
  - ACCESS CONTROLS
  - INTRUSION DETECTION
  - COMMUNICATIONS
  - BARRIERS AND DELAYS
  - COMMAND AND CONTROL

8B. VIOLENT INSIDER ASSISTANCE

VIOLENT INSIDER ASSISTANCE TO OUTSIDER THREATS

- IN ADDITION TO POSSIBILITY OF COMPROMISING S&S MEASURES, VIOLENT INSIDER USES FORCE IN PROVIDING ASSISTANCE TO OUTSIDERS.
- EXAMPLES OF VIOLENT INSIDER ASSISTANCE TO CONSIDER:
  - SPO USE OF FIREARM TO ENFORCE WILL ON OTHER EMPLOYEES.
  - EMPLOYEE DISABLES ANOTHER EMPLOYEE TO PREVENT INTERVENTION OR TO DELAY DETECTION OR ASSESSMENT.
  - EMPLOYEE SEIZURE OF SNM AND QUICK ESCAPE THROUGH EMERGENCY EXITS OR OTHER PORTALS (GRAB AND RUN).

9. PERFORMANCE TESTING -- ADVANCED ANALYSIS

BAYESIAN APPROACH

- COMBINES EXPERT JUDGEMENT AND PERFORMANCE TESTS
- PROVIDES ABILITY TO IMPROVE PD ESTIMATES OVER TIME

EXAMPLE OF USING BAYESIAN ANALYSIS TO ADJUST DETECTION PROBABILITIES BASED ON THREE PERFORMANCE TESTS

-- ADJUSTED PD VALUES FOR INIITAL ESTIMATE OF PD = .50 --

NUMBER OF	LEVEL OF CONFIDENCE IN INITIAL ESTIMATE OF PD		
SUCCESSES	VERY LOW	MODERATE	VERY HIGH
0	.20	.38	.49
1	.40	.46	.50
2	.60	.54	.50
3	.80	.62	.51

EXAMPLE OF USING BAYESIAN ANALYSIS TO ADJUST DETECTION PROBABILITIES BASED ON THREE PERFORMANCE TESTS

-- ADJUSTED PD VALUES FOR INIITAL ESTIMATE OF PD = .25 --

NUMBER OF	LEVEL OF CONFIDENCE IN INITIAL ESTIMATE OF PD		
SUCCESSES	VERY LOW	MODERATE	VERY HIGH
0	.10	.19	.24
1	.30	.27	.25
2	.50	.35	.26
3	.70	.44	.27

EXAMPLE OF USING BAYESIAN ANALYSIS TO ADJUST DETECTION PROBABILITIES BASED ON THREE PERFORMANCE TESTS

-- ADJUSTED PD VALUES FOR INIITAL ESTIMATE OF PD = .75 --

NUMBER OF	LEVEL OF CONFIDENCE IN INITIAL ESTIMATE OF PD		
SUCCESSES	VERY LOW	MODERATE	VERY HIGH
0	.30	.56	.73
1	.50	.65	.74
2	.70	.73	.75
3	.90	.81	.76

DYNAMIC ANALYSIS WORKSHEET

Element Name: Date:

Initial P: .5 Initial A: 1 Initial B: 1

Date:

N (# of Tests): 3 X (# of Successes): 3

Adjust A to A' = (A + X): 4
Adjust B to B'= (B + N - X): 1
Adjust P to P'= [A'/(A' + B')]: .8

Date:

Replace A with A' -- A: 4
Replace B with B' -- B: 1
Replace P with P' -- P: .8
N (# of Tests): 3 X (# of Successes): 3

Adjust A to A' = (A + X): 7
Adjust B to B'= (B + N - X): 1
Adjust P to P'= [A'/(A' + B')]: .875

Date:

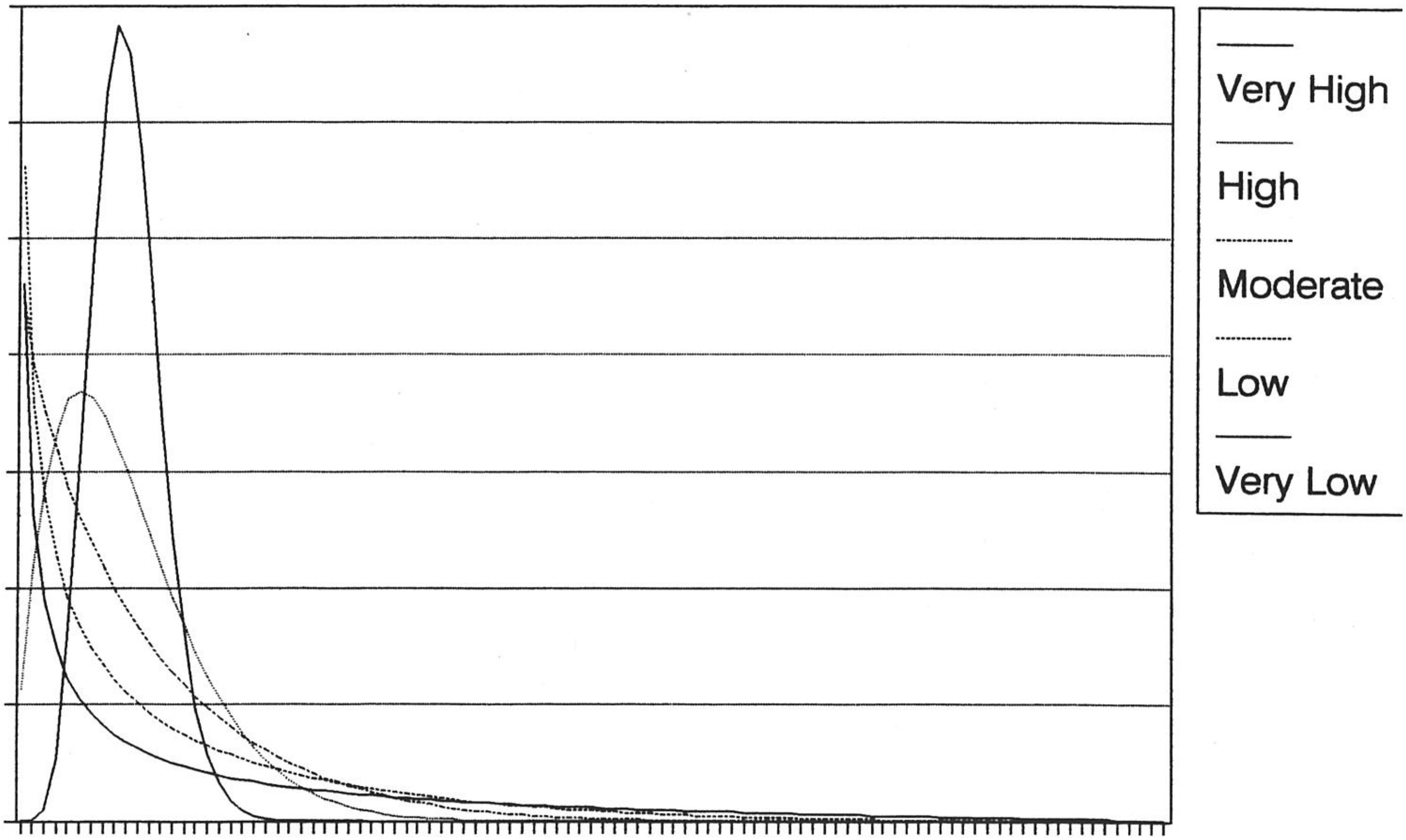
Replace A with A' -- A:
Replace B with B' -- B:
Replace P with P' -- P:
N (# of Tests): X (# of Successes):

Adjust A to A' = (A + X):
Adjust B to B'= (B + N - X):
Adjust P to P'= [A'/(A' + B')]:

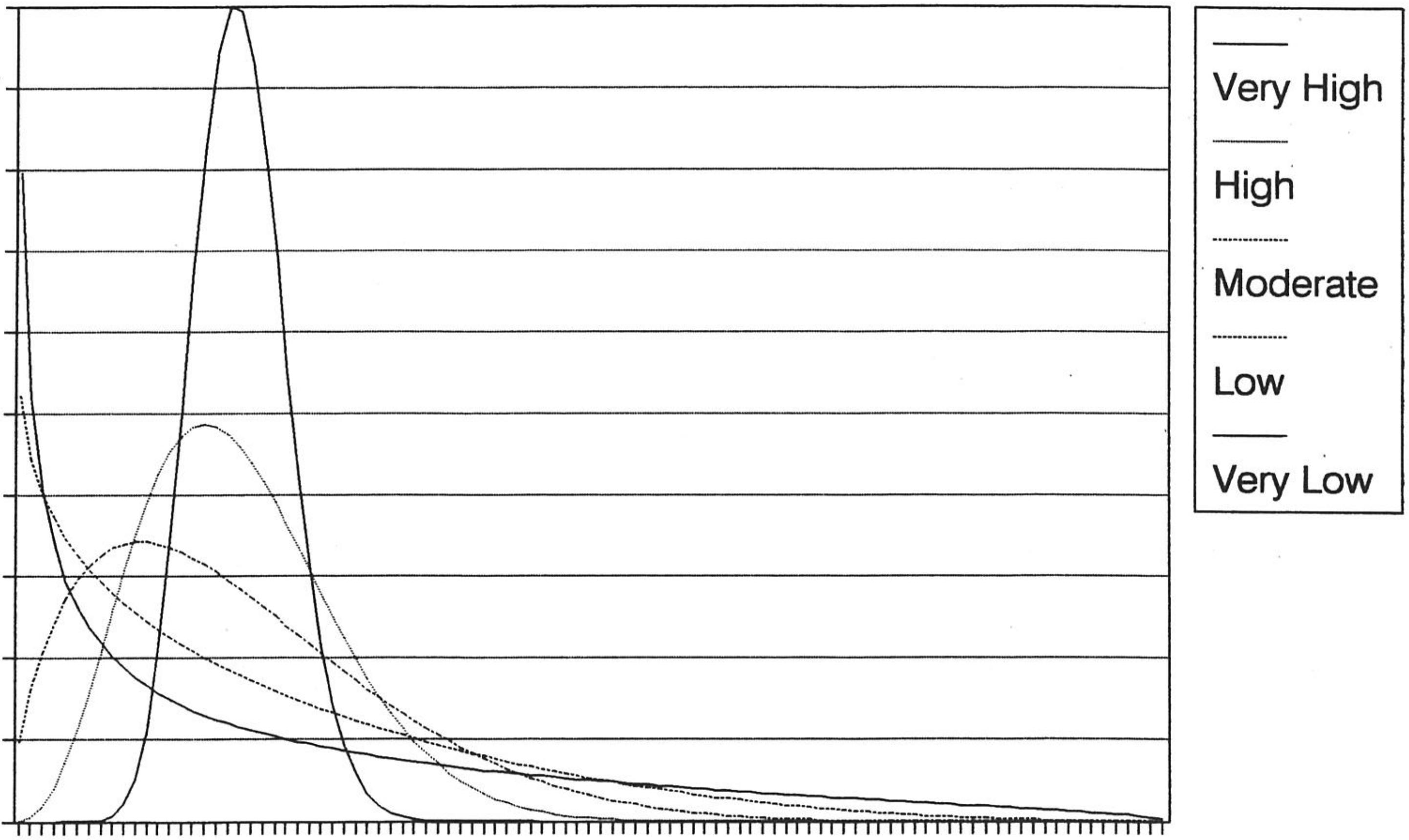
DYNAMIC ANALYSIS STARTING POINTS

Conf	Very Low		Low		Moderate		High		Very High	
Init Vals	A	B	A	B	A	B	A	B	A	B
P										
0.10	0.2	1.8	0.4	3.6	0.9	8.1	2.2	19.8	10	90
0.20	0.4	1.6	0.8	3.2	1.8	7.2	4.4	17.6	20	80
0.25	0.5	1.5	1	3	2.25	6.75	5.5	16.5	25	75
0.33	0.33	0.67	1.33	2.67	3	6	7.3	14.7	33.3	66.7
0.40	0.8	1.2	1.6	2.4	3.6	5.4	8.8	13.2	40	60
0.50	1	1	2	2	4.5	4.5	11	11	50	50
0.60	1.2	0.8	2.4	1.6	5.4	3.6	13.2	8.8	60	40
0.67	0.67	0.33	2.67	1.33	6	3	14.7	7.3	66.7	33.3
0.75	1.5	0.5	3	1	6.75	2.25	16.5	5.5	75	25
0.80	1.6	0.4	3.2	0.8	7.2	1.8	17.6	4.4	80	20
0.90	1.8	0.2	3.6	0.4	8.1	0.9	19.8	2.2	90	10

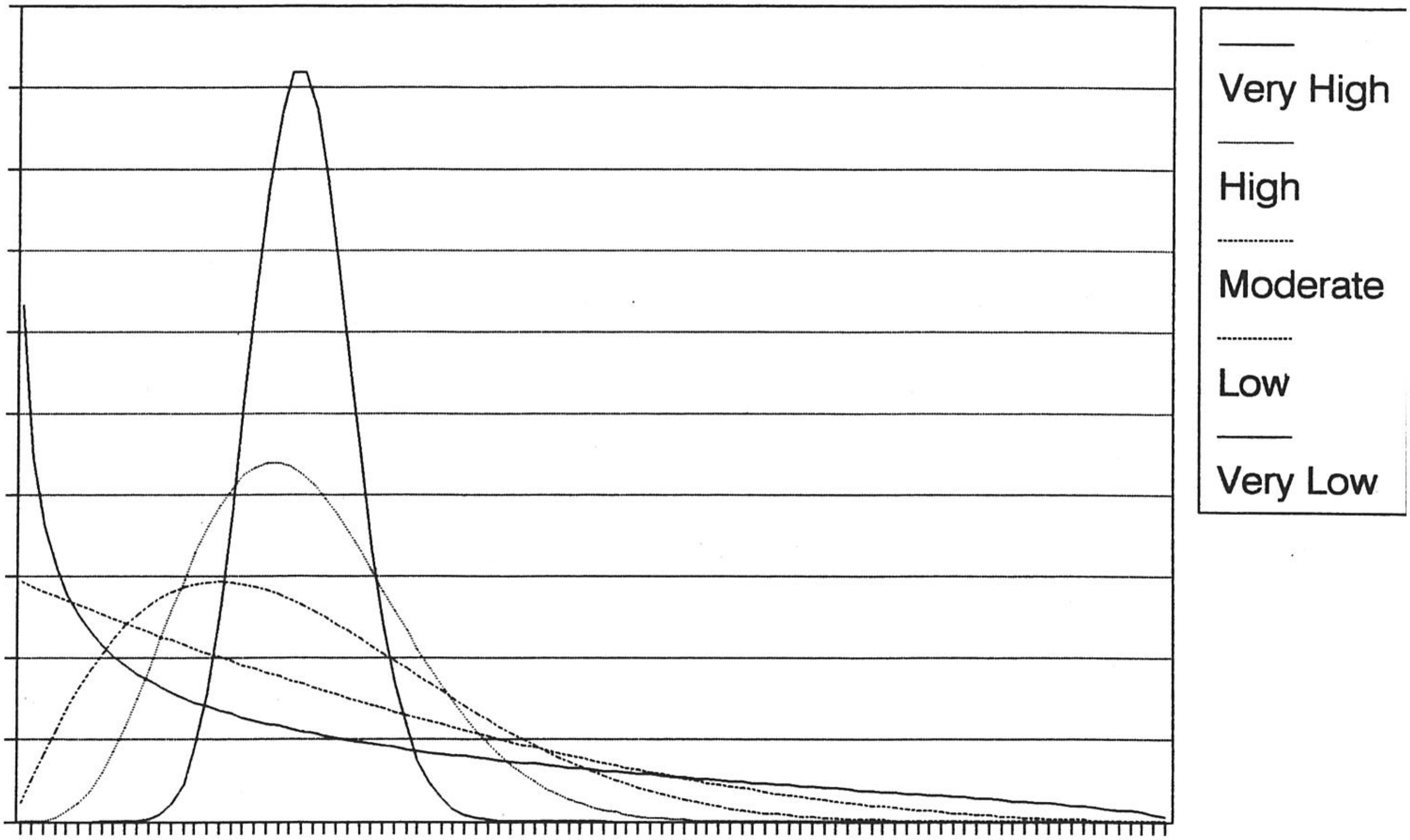
Initial Probability Functions for P = 0.10



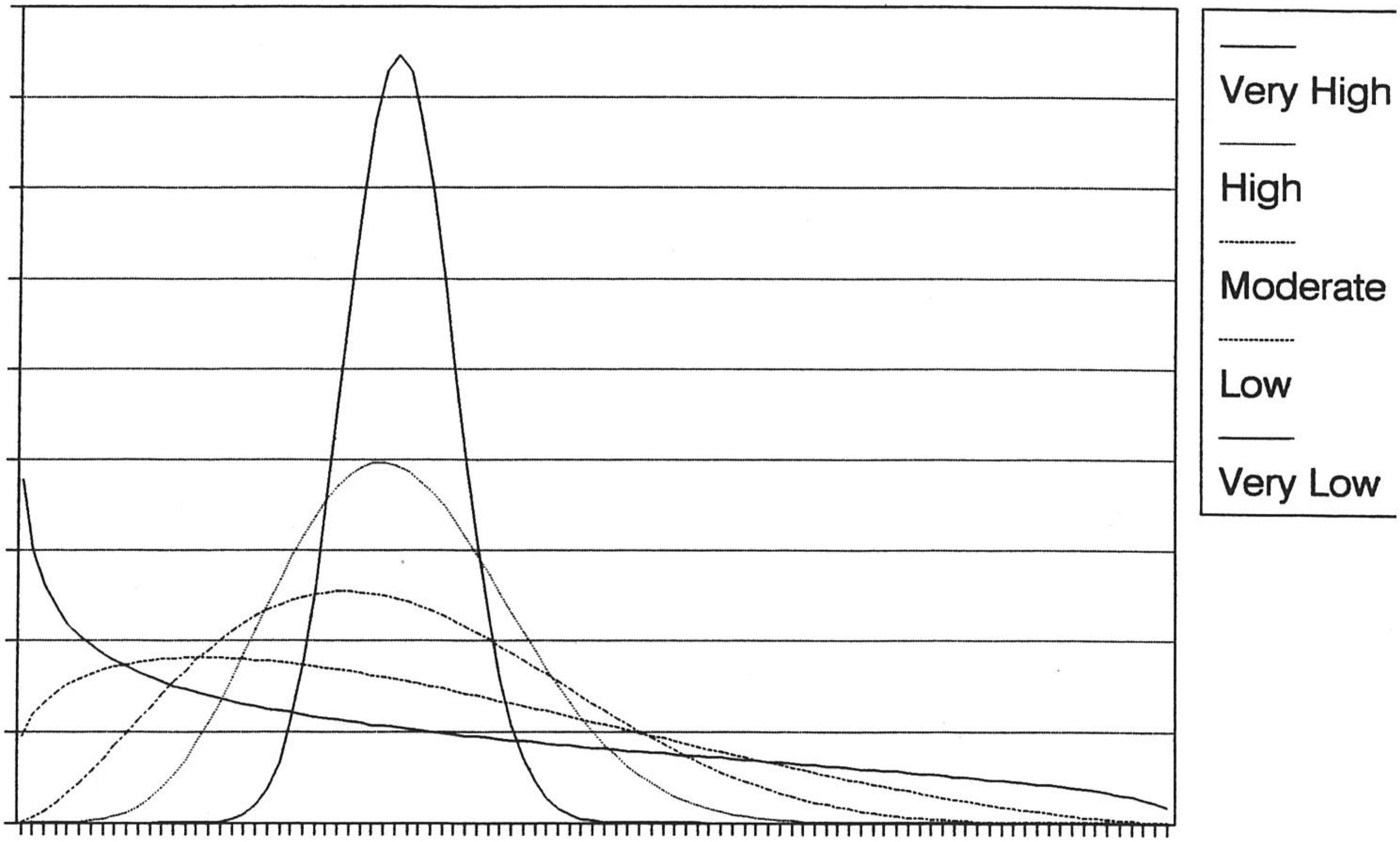
Initial Probability Functions for P = 0.20



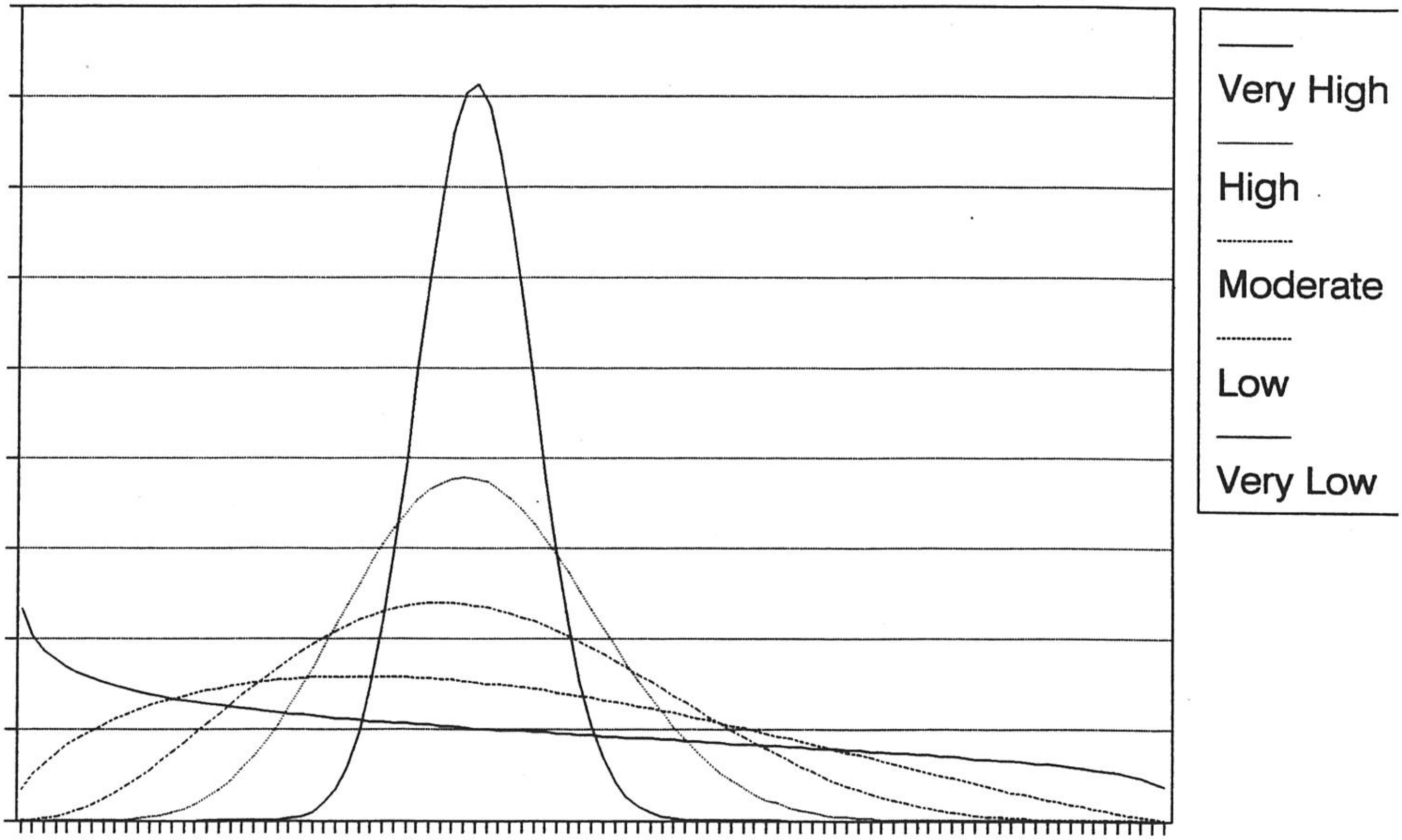
Initial Probability Functions for P = 0.25



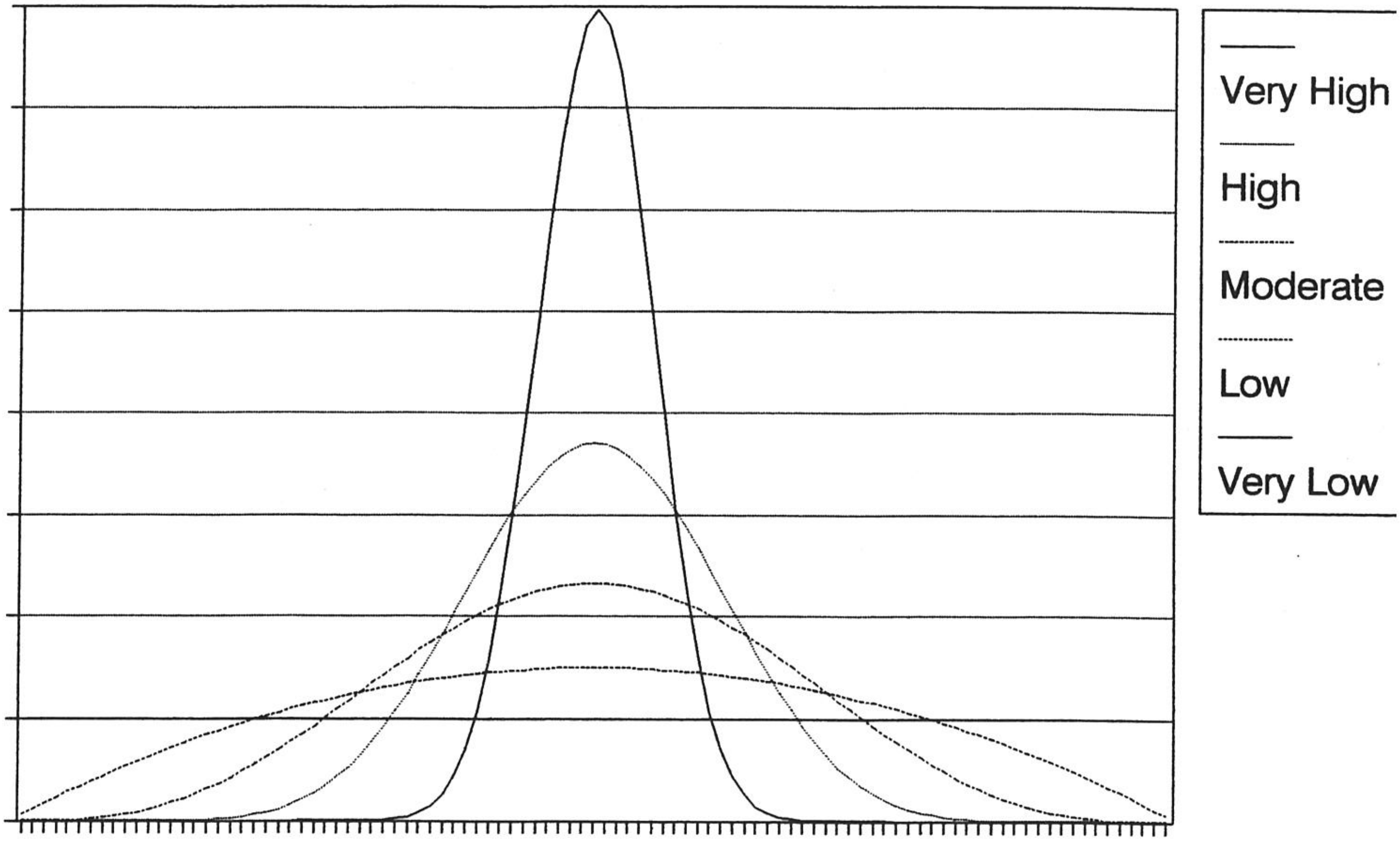
Initial Probability Functions for P = 0.33



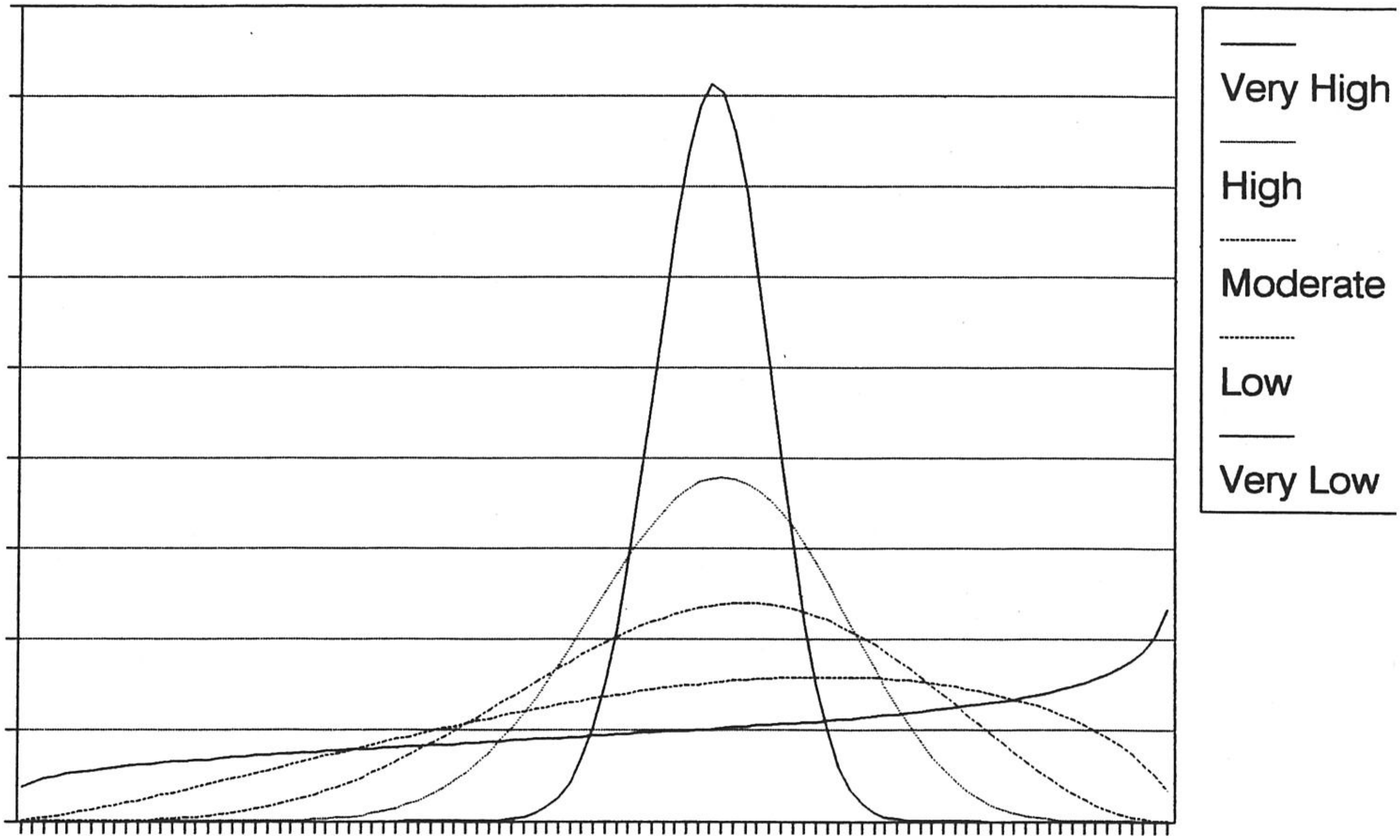
Initial Probability Functions for P = 0.40



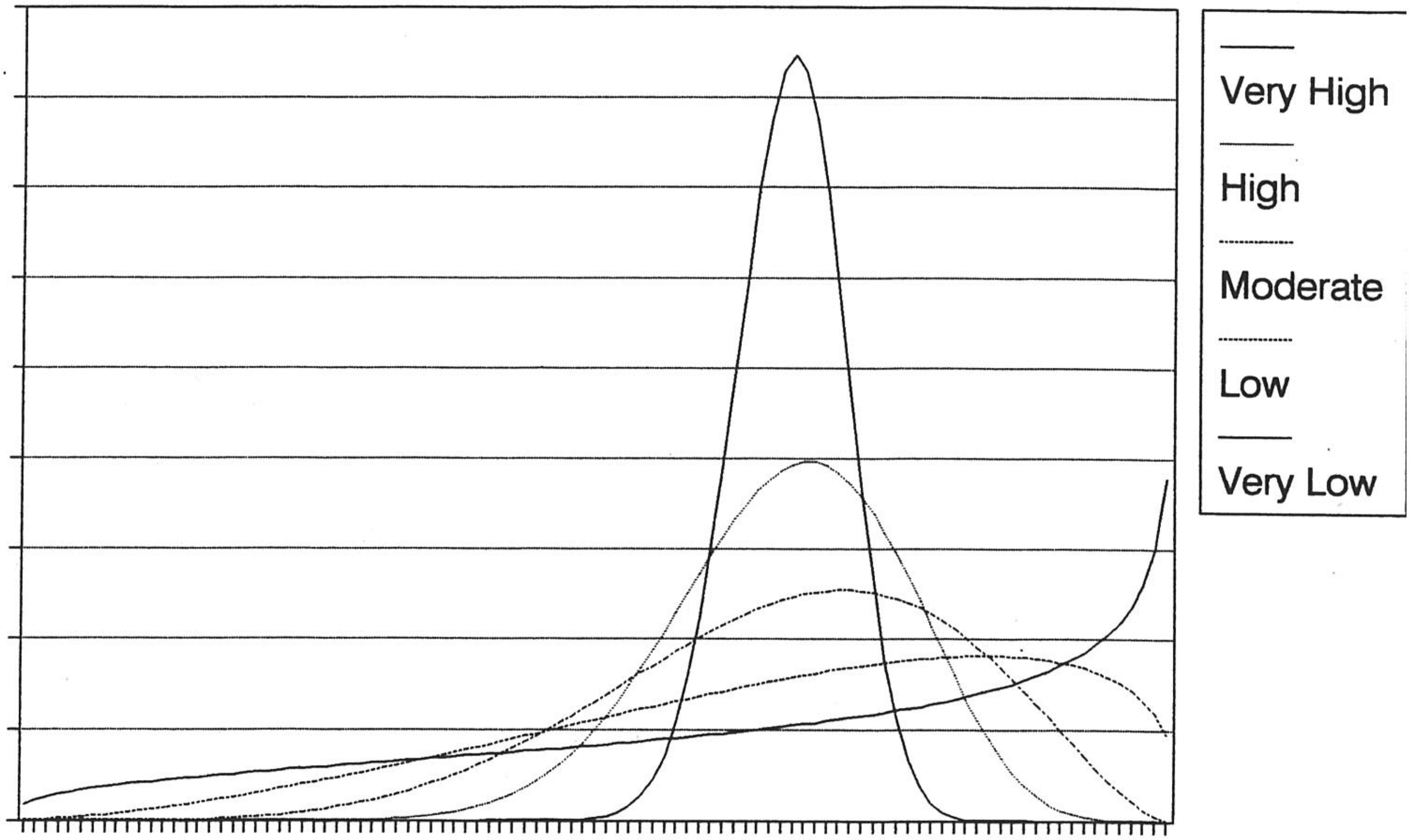
Initial Probability Functions for P = 0.50



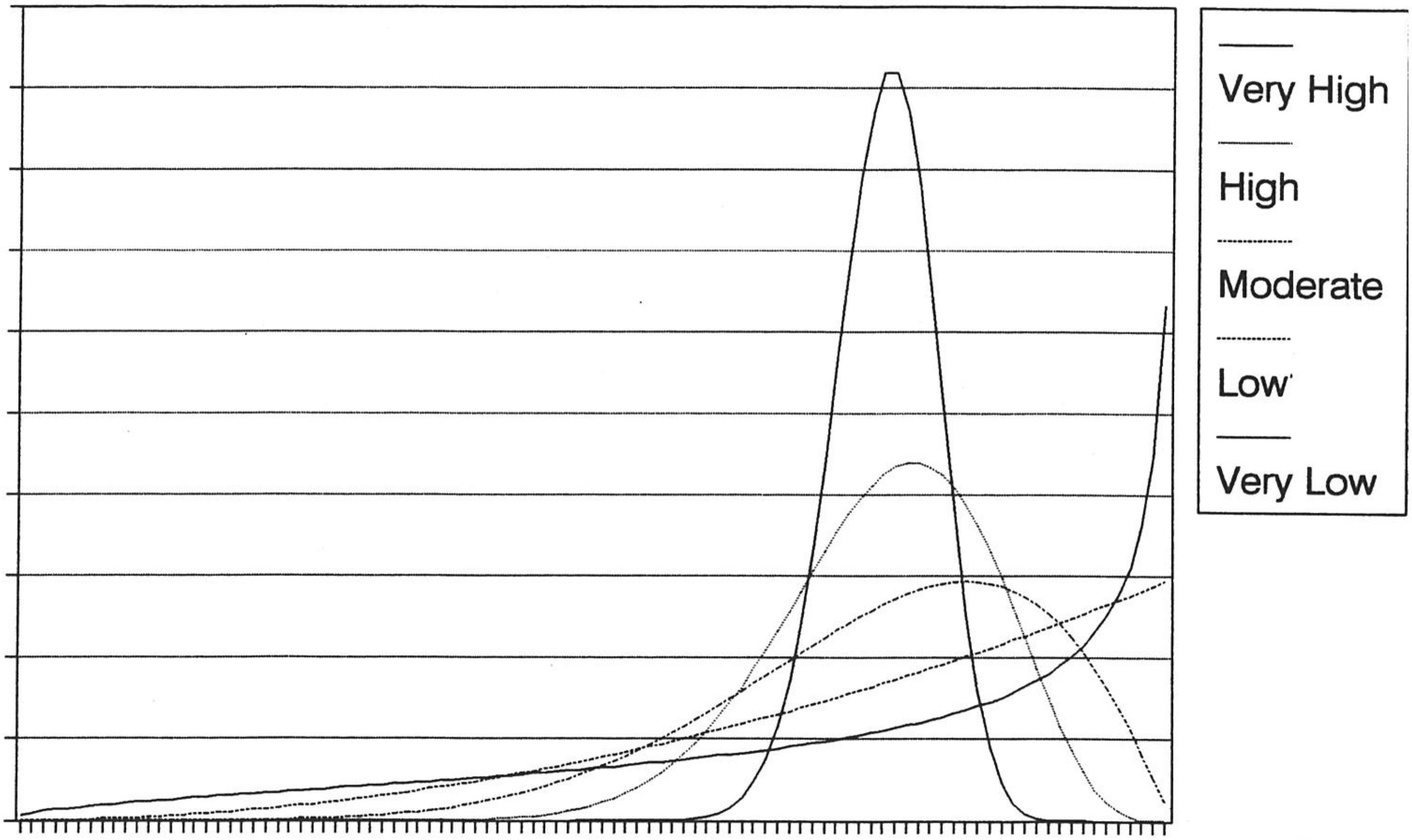
Initial Probability Functions for P = 0.60



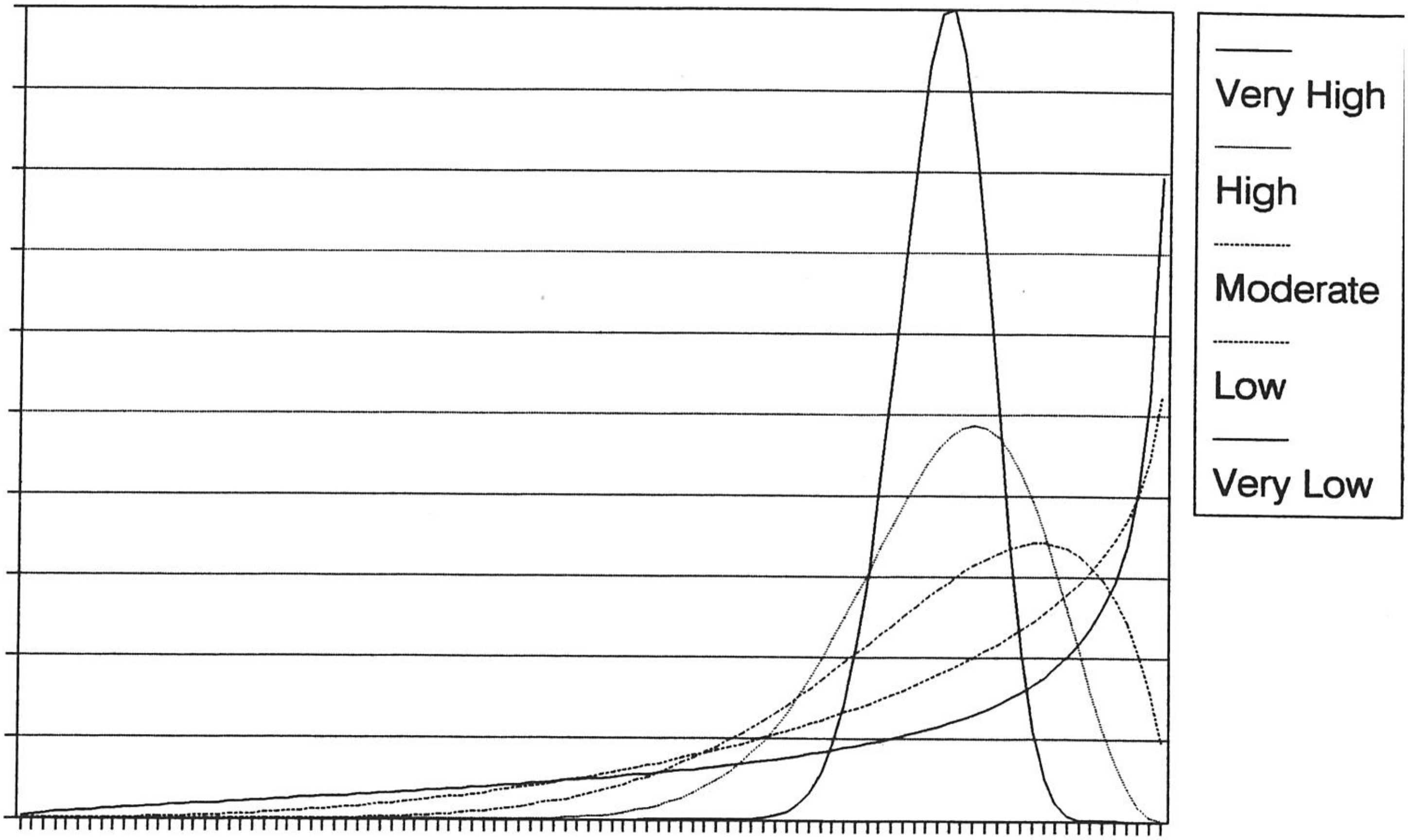
Initial Probability Functions for P = 0.67



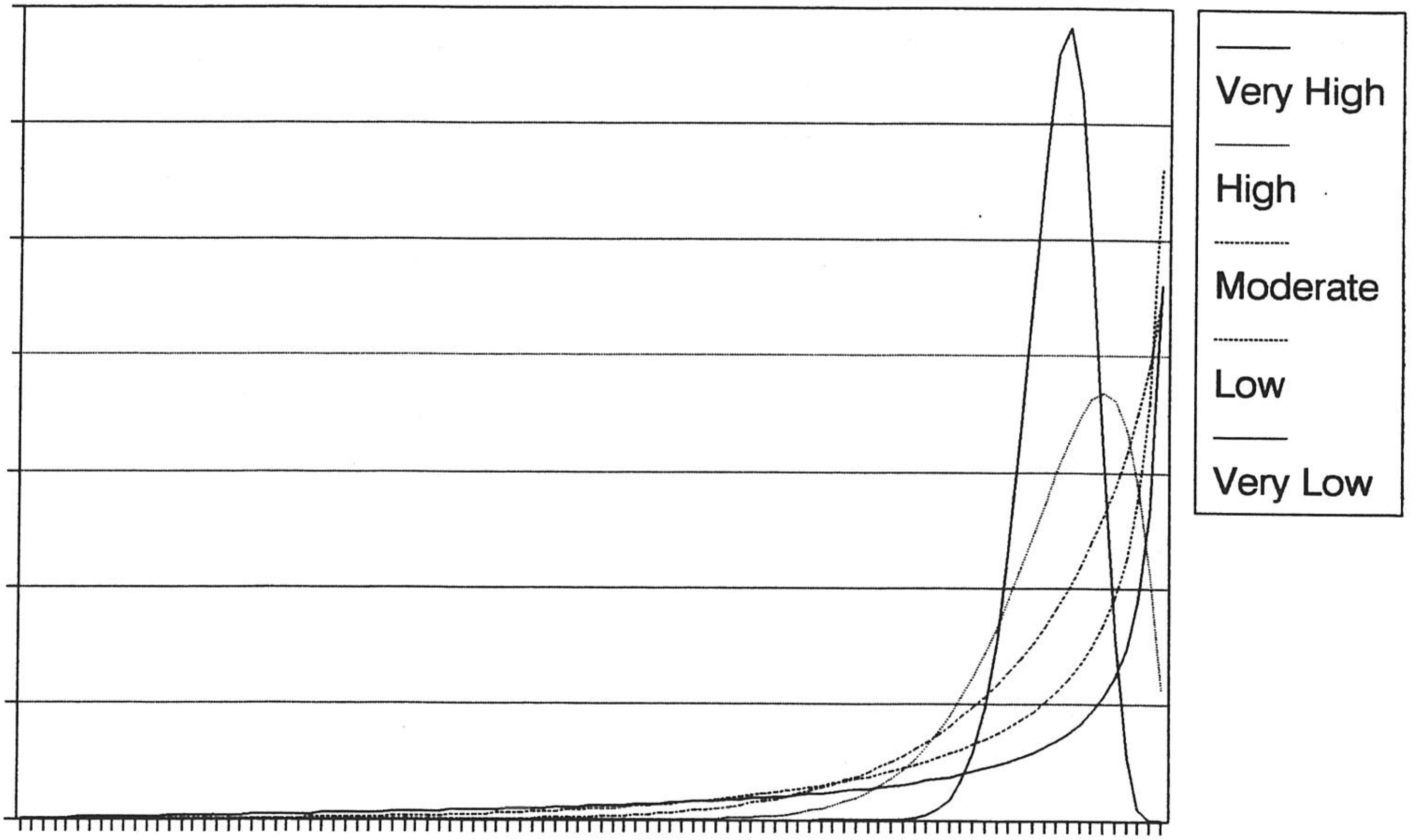
Initial Probability Functions for P = 0.75



Initial Probability Functions for P = 0.80



Initial Probability Functions for P = 0.90



HOW MUCH TESTING IS NECESSARY? HOW CAN WE OBTAIN THE BEST PRACTICAL QUANTIFICATION OF OUR SAFEGUARDS DETECTION ELEMENTS?

Joseph D. Rivers
U.S. Department of Energy
Washington, DC 20545

Presented at
Institute of Nuclear Materials Management
Annual Meeting
July 17, 1990
Los Angeles, California

ABSTRACT

The Department of Energy (DOE) requires its facilities which have custody of special nuclear material (SNM) to demonstrate that their safeguards systems achieve a designated level of performance in detecting the theft or diversion of SNM. A major portion of the effort in conducting these vulnerability assessments is the determination of a quantitative value that describes the facility's capability of detecting and neutralizing the theft or diversion. However, the primary objective of these analyses is to assist DOE in making a qualitative statement regarding the adequacy of the safeguards programs throughout the DOE complex. In order to obtain a technically defendable quantification of the overall performance of the facility's system, facilities will need to obtain valid estimates of the individual elements that contribute to the overall performance of the safeguards and security system. This will require facilities to conduct performance tests on individual detection elements. However, performance testing can be costly and time consuming. It is possible that too much performance testing could result in a degradation of the safeguards system performance if resources are transferred from protection to testing. Therefore, it is necessary to design a performance testing approach that will yield the best quantification of the overall safeguards system performance without adversely impacting the protection of the SNM. This will enable DOE to make more realistic statements regarding the quality of safeguards performance at its facilities.

INTRODUCTION

The most common method that has been used to quantify safeguards elements for the detection of insider adversaries has been the use of expert judgement. The use of expert judgement is commonly used in other industries to quantify difficult to measure values. The Delphi approach, that arrives at a value from expert judgement in an iterative manner is commonly employed. However, expert judgement can be highly dependent upon the experts that are used.

In order to assure that facilities will have technically defendable safeguards system performance levels, DOE has directed its facilities to implement programs of performance testing of detection elements of the safeguards and security systems. Most facilities have been performance testing many of their safeguards detection elements. For these elements, there may be sufficient data for the facilities to accurately estimate the level of performance for those elements. Most of the detection elements that provide detection for the theft or diversion of SNM by insider adversaries have not been incorporated into testing programs, or have only been recently incorporated into these programs. Therefore, there is little or no data available to accurately quantify these elements.

It is impractical to expect facilities to run a large number of performance tests on each of the individual elements in a very brief period of time. It would be too expensive and time consuming, resulting in a potential degradation of protection. The heightened awareness of the performance tests would result in biased estimates for individual elements. Yet, due to the nature of the performance tests resulting in either a success or a failure, a large number of tests are required to yield an accurate estimate of the capability of each element. It is essential to implement an approach that enables facilities to use the data from performance tests to quantify its detection elements.

Bayesian estimators are useful in these situations. These estimators combine the data from performance tests with expert judgement to estimate the detection capability of the individual elements. Bayesian estimators are especially useful when there is a prior understanding of the probabilities of detection as well as a small number of performance tests to adjust the prior probabilities.

Therefore, there are two approaches that can be used to quantify detection capabilities of safeguards elements if performance tests are used: estimates based solely on the performance tests, and Bayesian estimates.

QUANTIFICATION BASED SOLELY ON PERFORMANCE TESTS

Performance tests on safeguards elements are designed to determine whether the individual element will succeed of fail in its attempt to detect anomalous activities. Each test is a Bernoulli trial. The individual tests are aggregated to yield results that follow a binomial distribution. The distribution is defined by the number of trials n, and the probability of success p. The probability of failure is (1 - p) or q. The true value of p is unknown and must be estimated by the results of the performance tests. In order to obtain reasonably accurate estimates for p, a large number of tests is required. If p is between 0.4 and 0.6, 20 to 50 individual tests must be run to obtain accurate estimates for p. For p = 0.3 or 0.7, approximately 80 tests would be required. If p is less than 0.25 or greater than 0.75, more than 100 tests would be required.

As can be seen above, a large number of tests is required to accurately estimate the probability of detection for individual detection elements. Most facilities will have sufficient data for elements such as metal detectors, SNM monitors, motion detectors, etc. Most elements at most facilities have not undergone sufficient testing to yield accurate estimates of their performance. However, over the next several years, sufficient tests may be able to be run to provide accurate estimates solely through the use of performance tests.

BAYESIAN ESTIMATORS

Bayesian estimators can provide a useful solution to the problem of the lack of sufficient tests to provide accurate estimates element performance. They allow the user to take advantage of all available information to generate an estimate. A Bayesian estimator takes prior information regarding detection capability, combines it with the results of performance tests to yield a posterior estimate of detection capability. The estimate can be adjusted after each performance tests or on some periodic basis. If sufficient tests are eventually run, an estimate based slowly on performance tests can replace the Bayesian estimate.

There are several sources for supplying the Bayesian estimator with prior information. The most common approaches would be expert judgement, data bases generated by DOE laboratories, and DOE complex-wide standards. Expert judgements would be developed by each facility for its facility specific conditions. Data bases generated by DOE laboratories would include data bases on sensor detection capabilities. Complex-wide standards are currently under development for elements such as observation by general staff, intra-facility transfers, and emergency evacuation procedures.

The Bayesian estimator requires a prior distribution of probability values, but many of these sources might only provide a single point estimate of detection capability. For example, if expert judgement estimated that the detection capability of a given element was 0.3, we would have to create a prior distribution based on that estimate. One approach would be to say that there were three likely values for the probability of detection. We might assume that there was a 0.6 probability that 0.3 was the correct value. Then, we might add to the distribution, values that are 50% higher and lower than the point estimate. Each of these would have a probability of 0.2 in the prior distribution. This results in the following distribution.

$P(\theta)$	θ
0.2	0.15
0.6	0.30
0.2	0.45

This distribution has an expected value of 0.3 like the point estimate generated by expert judgement. After a number of performance tests are conducted, a posterior distribution can be generated from the prior distribution based on the likelihoods associated with the test results. If three tests are conducted and all are successful, the posterior distribution would be as follows.

$P(\theta)$	θ
0.02	0.15
0.46	0.30
0.52	0.45

This would result in a new estimate of the detection probability of 0.375, an increase of 0.075. If however, the detection element failed all tests, the posterior distribution would be as follows.

$P(\theta)$	θ
0.34	0.15
0.57	0.30
0.09	0.45

This would result in a new estimate of the detection probability of 0.263, a decrease of 0.037. If the testing resulted in one success and two failures, the posterior distribution would be as follows.

$P(\theta)$	θ
0.16	0.15
0.64	0.30
0.20	0.45

This would result in a new estimate of the detection probability of 0.306, an increase of 0.006.

Based on the example provided, the Bayesian estimator would allow the facility to generate a prior estimate of performance, and modify that estimate based on a small number of tests. The newly calculated posterior estimate could be used to form a new prior distribution from the next several tests. This iterative procedure would allow the facility to adjust previous estimates of performance based on a small number of additional tests.

CONCLUSION

The title of this paper asks "How much testing is necessary?" If we rely solely on the execution of performance tests to generate estimates of safeguards element detection probabilities, we find that a large number of tests is required to obtain accurate estimates of the detection probabilities. However, if sufficient tests have not been conducted, it might be more appropriate to use expert judgement or complex-wide standards adjusted based on the conduct of a limited number of performance tests, using Bayesian estimators. This will allow facilities to generate more useful estimates during the early phases of the implementation of testing programs, or when new elements are introduced to the safeguards and security system, prior to extensive performance testing.

Bayes Estimation References

Technical

DeGroot, M.H.; Probability and Statistics; Addison Wesley; 1986; p. 330.

Hartigan, J. A.; Bayes Theory; Springer-Verlag, 1983.

Hogg, R.V., Craig, A.T.; Introduction to Mathematical Statistics; Macmillan; 1978; p.227.

Lee, Peter M.; Bayesian Statistics: An Introduction; Oxford; 1989.

Less Technical

Bowen, W. M., Bennett, C. A.; Statistical Methods for Nuclear Material Management; U.S. Nuclear Regulatory Commission, NUREG/CR-4604; 1988; p. 102.

Hoel, P.G.;Introduction to Mathematical Statistics; John Wiley & Sons; 1971; p. 20, 348.

Mendenhall, W.; Introduction to Probability and Statistics; Wadsworth; 1967.

Wonnacott, T.H., Wonnacott, R.J.; Introductory Statistics; John Wiley & Sons; 1972; p. 363.

10. VA QUALITY

VA QUALITY

- PRIMARY FACTORS
  - "DO IT RIGHT THE FIRST TIME" APPROACH
  - VA TEAM SELECTION AND PREPARATION
  - MANAGEMENT SUPPORT
  - PERFORMANCE TESTING
  - PEER REVIEW
- KEY QUALITY TESTS
  - VA TEAM QUALIFICATIONS AND DIVERSITY
  - KEY THREATS AND TARGETS ADDRESSED
  - "SNAPSHOT IN TIME" CHARACTERIZATION OF FACILITY AND S&S SYSTEM
  - FULL-RANGE VULNERABILITY SEARCH
  - CREDIBILITY OF ADVERSARY SCENARIOS
  - VALIDITY OF EFFECTIVENESS PROBABILITIES
  - SCOPE OF S&S SYSTEM CHANGE EVALUATION

11. SUMMARY

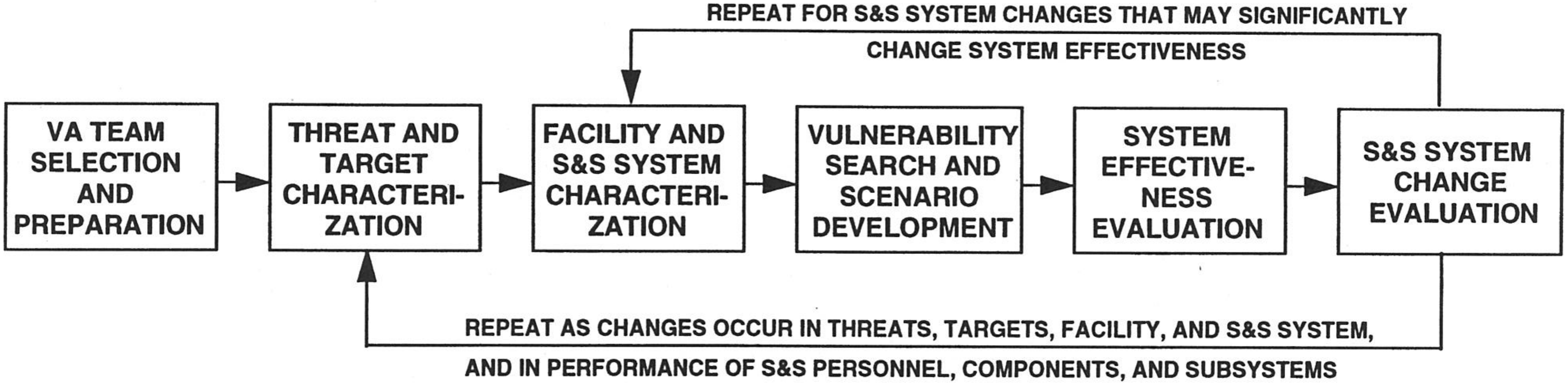
PURPOSE OF
TABLE-TOP VULNERABILITY ANALYSIS WORKSHOP

To provide participants an understanding of the vulnerability analysis (VA) process and to prepare them to participate on VA teams to perform table-top VAs in roles consistent with their security training and experience. Participants should also gain a broad view of how many, diverse safeguards and security measures can work together to protect designated targets against design-basis threats. An understanding of the VA process is an essential prerequisite to effective and efficient use of any computer VA method.

WHY PERFORM VULNERABILITY ANALYSES?

- VAs PROVIDE A “YARDSTICK” FOR DETERMINING HOW WELL A SYSTEM PERFORMANCE REQUIREMENT IS MET.

FLOWCHART OF VA PROCESS


REPEAT FOR S&S SYSTEM CHANGES THAT MAY SIGNIFICANTLY CHANGE SYSTEM EFFECTIVENESS
VA TEAM SELECTION AND PREPARATION
THREAT AND TARGET CHARACTERIZATION
FACILITY AND S&S SYSTEM CHARACTERIZATION
VULNERABILITY SEARCH AND SCENARIO DEVELOPMENT
SYSTEM EFFECTIVENESS EVALUATION
S&S SYSTEM CHANGE EVALUATION
REPEAT AS CHANGES OCCUR IN THREATS, TARGETS, FACILITY, AND S&S SYSTEM, AND IN PERFORMANCE OF S&S PERSONNEL, COMPONENTS, AND SUBSYSTEMS

GENERAL OBSERVATIONS ON VA PROCESS

- VA Process - Based on first principles
- VA Team - Diversity in S&S training and experience of team members helps improve objectivity of many judgements required by VA team.
- Threats and Targets - Prescribed by DOE guidance on design-basis threats.
- Facility and S&S System Characterization - Snapshot in time.
- Vulnerability Search - All adversary strategies, tactics, and paths and all facility conditions should be considered.
- Scenario Development - Scenarios should be developed so as to ensure every essential adversary action, without security intervention, succeeds.
- System Effectiveness Evaluation - Should be based on practices, not plans, for operational facilities.
- Performance Testing - Should be an integral part of VA process.
- S&S System Change Evaluation - Should address improving security and/or saving money, depending on situation.
- Effort required to perform VAs increases as system effectiveness improves.

TYPES OF THREATS

Type	Description	Use
Historical Threat (Product of Historians)	Record of malevolent acts including targets, adversary tactics and equipment used, and, in some cases, identity of adversaries.	Record of malevolent acts provides insight on adversary motivations, tactics and capabilities.
Threat Estimate (Product of Intelligence Analysts)	Current information collected and analyzed by intelligence specialists about potential adversaries and their plans.	May provide basis for preemptive action against potential adversaries or for security alert at one or more facilities
Design-Basis Threat (Product of Policy Makers)	Description of malevolent acts and adversaries that safeguards and security system is to protect against.	Together with system effectiveness requirement, provides system performance requirement.

LEVEL OF EFFORT FOR VULNERABILITY ANALYSIS

LEVEL OF EFFORT FOR VA	NUMBER OF THREATS	NUMBER OF TARGETS	VA CORE TEAM	VA SUPPORT TEAM	FACILITY INSPECTION	STANDARD PERF. TESTS	STRESS PERF. TESTS	DOCUMENTATION	DURATION
MINIMUM	1	1	2-3 SPECIALISTS	NONE	DOCUMENT REVIEWS	AS AVAILABLE	AS AVAILABLE	SUMMARY REPORT	1-3 DAYS
	2-4	1-3	3-5 SPECIALISTS	1-5 PEOPLE	DOCUMENT REVIEWS AND WALK-THROUGHS	AS AVAILABLE	AS AVAILABLE	10-30 PAGE REPORT	1-3 WEEKS
	≥4	3-4	4-6 SPECIALISTS	5-10 PEOPLE	DOCUMENT REVIEWS AND EXTENSIVE OBSERVATIONS	AS AVAILABLE	DETECTION, ALARM ASSESSMENT, ENGAGEMENT	DETAILED REPORT	1-3 MONTHS
MAXIMUM	≥6	4-6	5-7 SPECIALISTS	5-10 PEOPLE	DOCUMENT REVIEWS & EXTENSIVE OBSERVIATIONS	SUPPLEMENT AS APPROPRIATE	DETECTION, ALARM ASSESSMENT, ENGAGEMENT, NEUTRALIZATION	DETAILED REPORT	3-6 MONTHS

USES FOR VULNERABILITY ANALYSES

	M&O CONTRACTOR	DOE FIELD OFFICE	DOE HEADQUARTERS
SSSP PREPARATION	PERFORM	REVIEW	REVIEW
S&S SYSTEM DESIGN	PERFORM	REVIEW	REVIEW
PROTECTIVE FORCE RESPONSE PLAN DEVELOPMENT	PERFORM	REVIEW	REVIEW
S&S SYSTEM CHANGE EVALUATION	PERFORM	PERFORM	PERFORM
S&S SELF-ASSESSMENTS	PERFORM	REVIEW	REVIEW
S&S SURVEYS/INSPECTIONS		PERFORM	PERFORM
S&S INDEPENDENT ASSESSMENTS	PERFORM	PERFORM	PERFORM
S&S TRAINING	PERFORM	PERFORM	PERFORM

STRENGTHS AND WEAKNESSES OF TABLE-TOP VA METHOD

STRENGTHS

- FLEXIBLE
  - TREATS ALL TYPES OF THREATS AND TARGETS.
  - TREATS ALL TYPES OF FACILITIES AND S&S SYSTEMS.
  - TREATS ALL TYPES OF ADVERSARY STRATEGIES, TACTICS AND PATHS.
  - ADAPTABLE TO MANY USES AND LEVELS OF EFFORT.
  - ANALYSIS CAN BE QUANTITATIVE OR QUALITATIVE.
  - PERFORMANCE DATA CAN BE ESTIMATED OR MEASURED.
- EFFICIENT
  - FOCUSES ON KEY PERFORMANCE DATA.
  - DIRECTLY INTEGRATES RESULTS OF PERFORMANCE TESTS INTO VA PROCESS.
- EASY TO USE
  - COMMON SENSE APPROACH.
  - VA PROCESS AND RESULTS ARE TRANSPARENT

WEAKNESSES

- QUALITY OF RESULTS DEPENDS ON TRAINING, EXPERIENCE, INTEGRITY, AND EFFORT OF THOSE WHO PERFORM AND REVIEW VAs AND PTs

JACKPOT

BIGGEST PAYOFF FOR VAs OCCURS
WHEN THE VA PROCESS BECOMES INSTITUTIONALIZED IN
THE M&O CONTRACTOR, FIELD OFFICE, AND
HEADQUARTERS ORGANIZATIONS
AS THE ROUTINE WAY TO LOOK AT S&S SYSTEMS
THAT MUST PROVIDE PROTECTION
AGAINST DESIGN-BASIS THREATS.

SANDIA TECHNOLOGY TRANSFER MANUAL BIBLIOGRAPHY

1. SAND90-0729·UC-515, Alarm Communication and Display Technology Transfer Manual (UCNI), Printed November 1990.

2. SAND89-1924·UC-515, Video Assessment Technology Transfer Manual (UCNI), Printed October 1989.

3. SAND89-1923·UC-515, Exterior Intrusion Detection Technology Transfer Manual (UCNI), Printed May 1990.

4. SAND90-0937·UC-515, Protecting Security Communications Technology Transfer Manual (UCNI), Printed March 1990.

5. SAND87-1926/1·UC-515, Access Delay Technology Transfer Manual (UCNI), Printed September 1989. A classified version also exists.

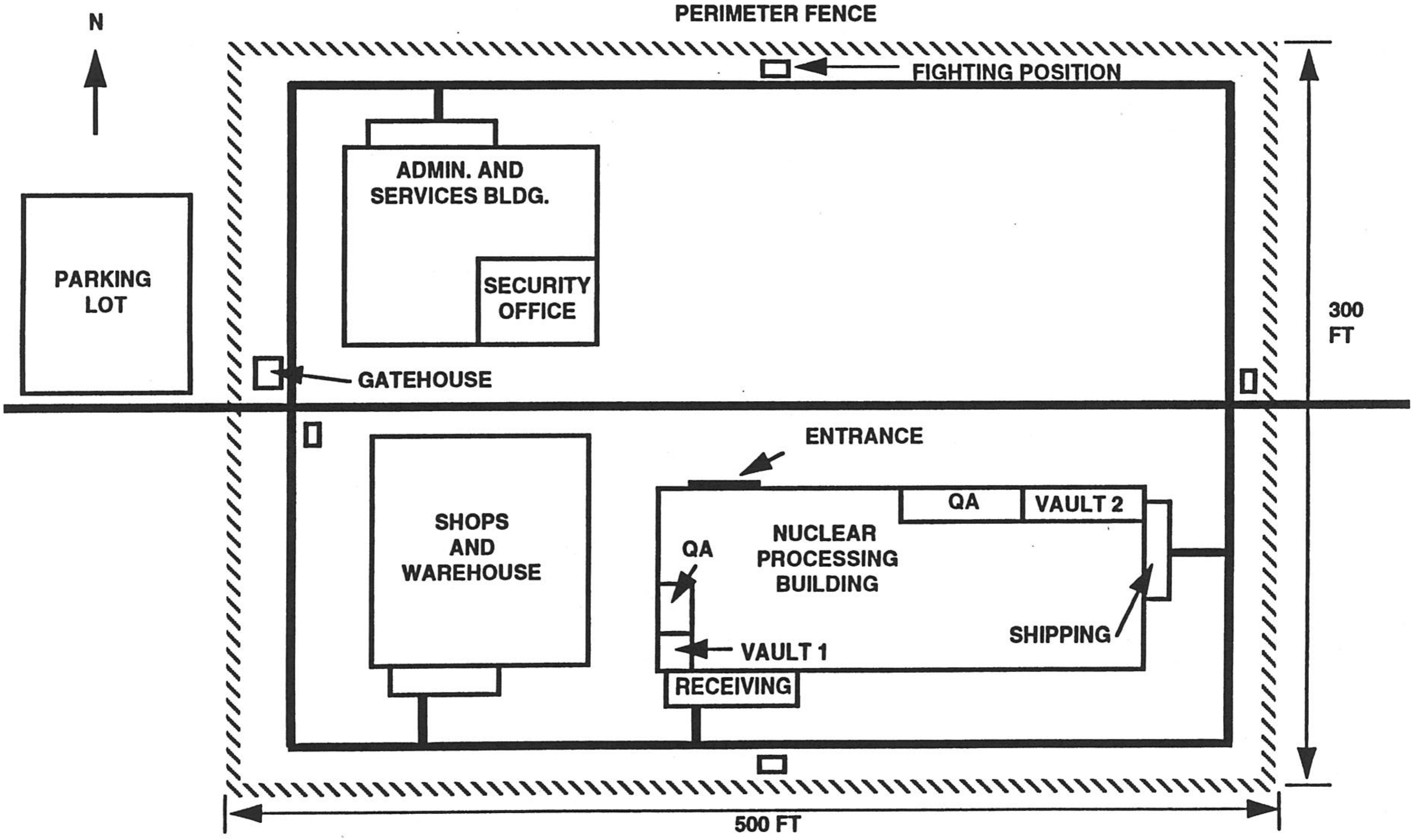
6. SAND87-1927, Entry-Control Technology Transfer Manual (UCNI), Printed May 1989.

Sandia also provides consulting help in these areas. For more information, contact Mary Green at (505) 844-7746 or FTS 844-7746 and she can put you in touch with an expert in that field. (She can also give you more information about how to get these manuals.) Sandia also operates a number of libraries:

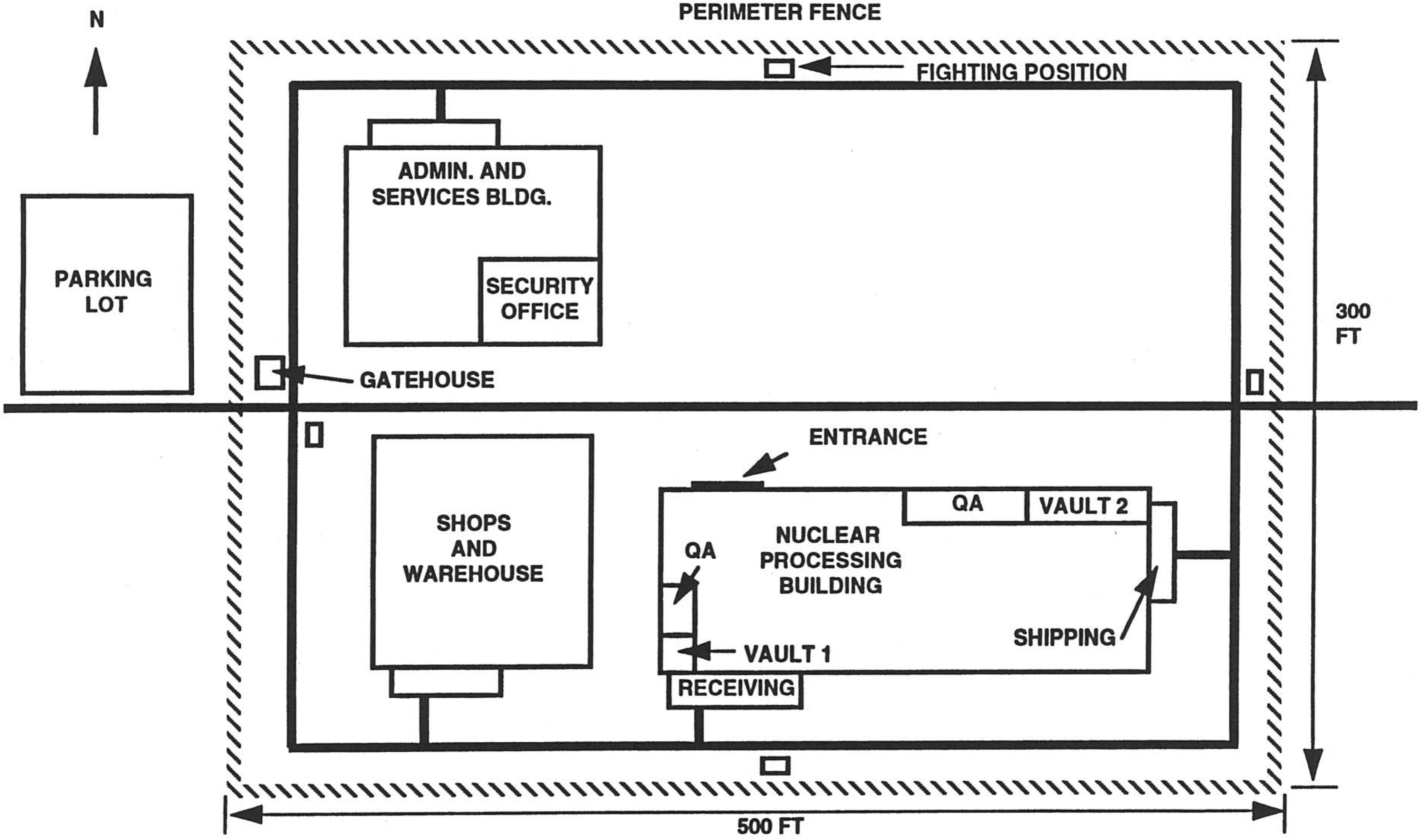
Library	Librarian Phone Number
Access Delay Library	(505) 844-7803 or FTS 844-7803
Sensors Library	(505) 845-3364 or FTS 845-3364
Video Assessment Library	(505) 844-4818 or FTS 844-4818
Entry Control Library	(505) 844-3836 or FTS 844-3836

WORKSHEETS

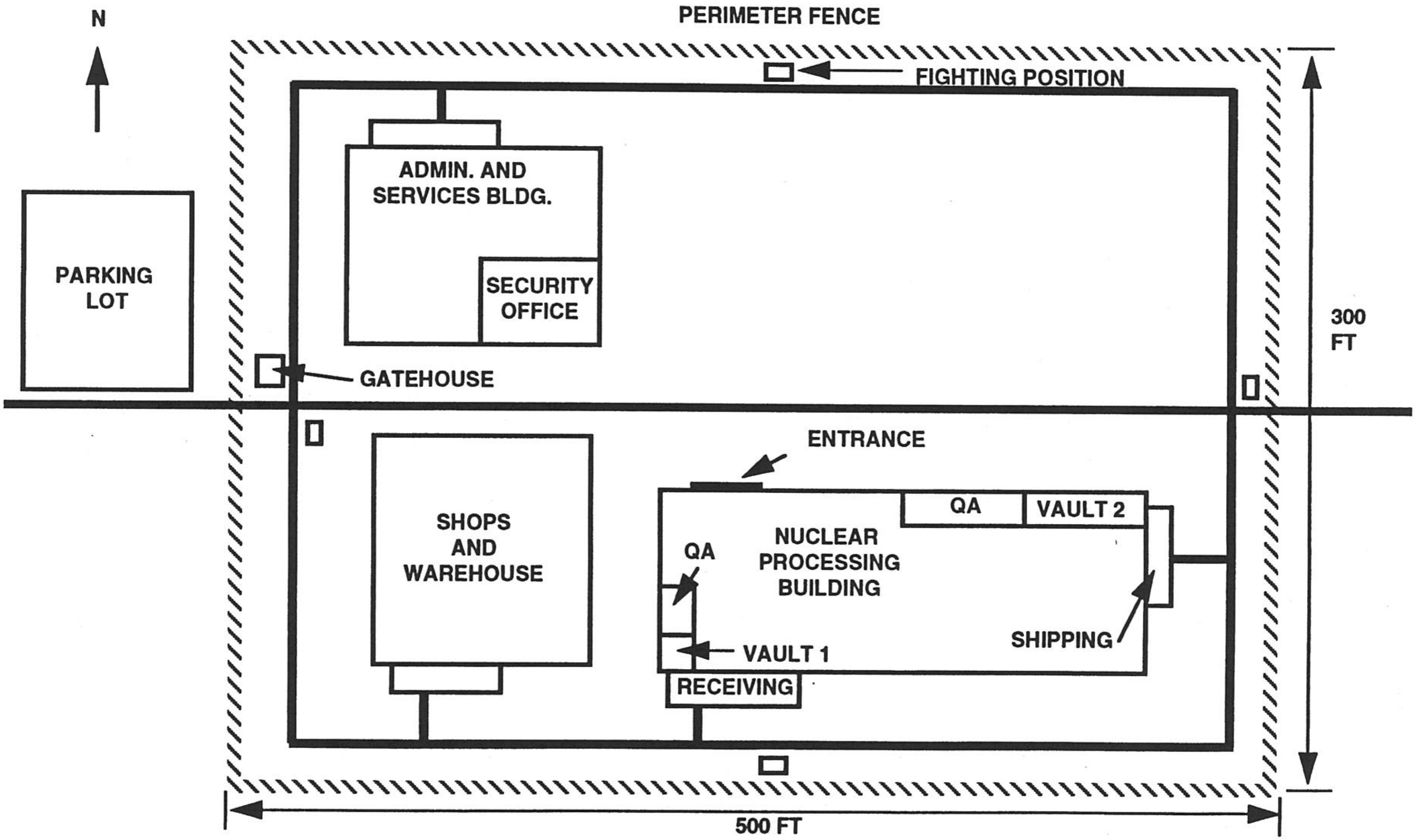
EXAMPLE NUCLEAR PROCESSING PLANT (SNM)



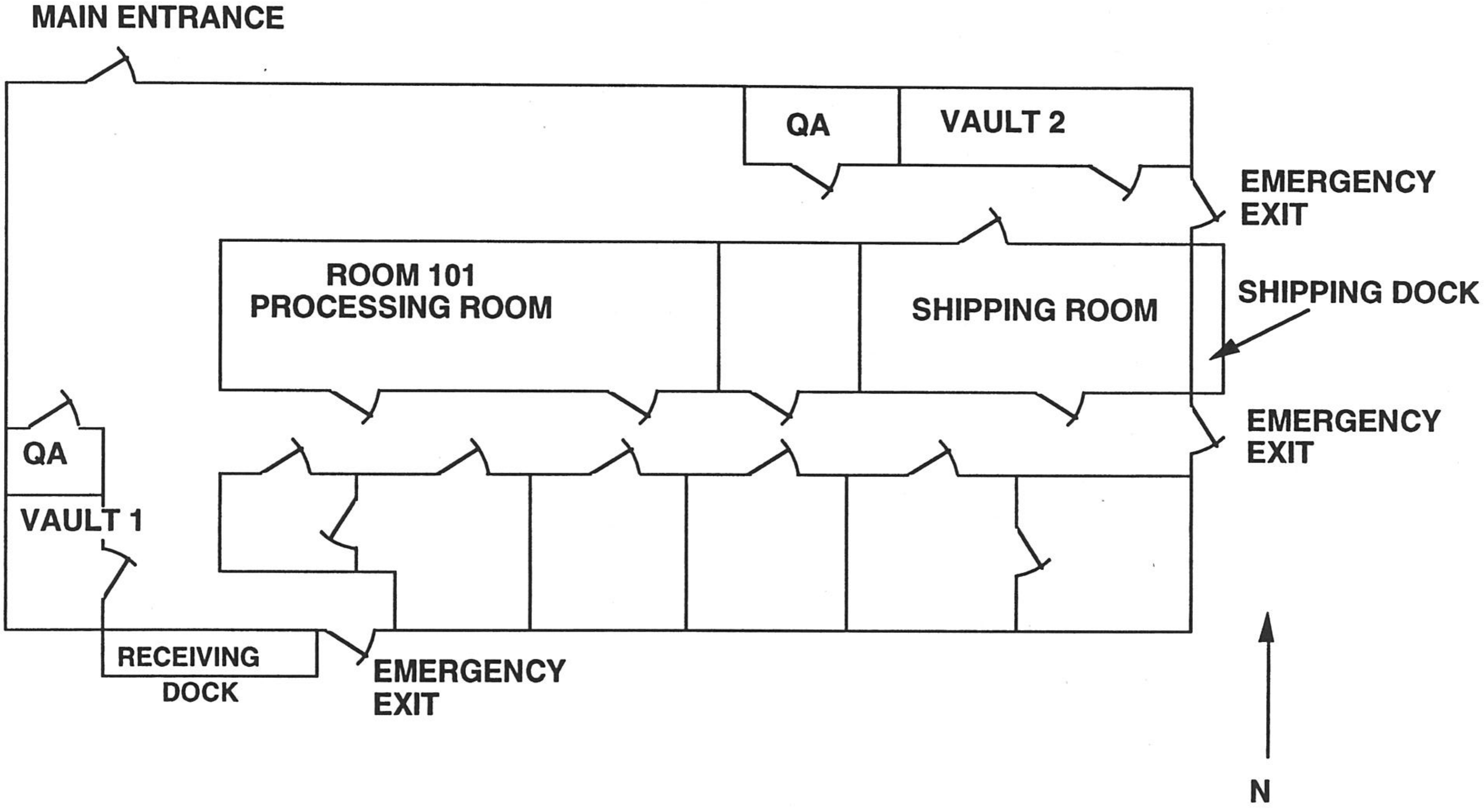
EXAMPLE NUCLEAR PROCESSING PLANT (SNM)



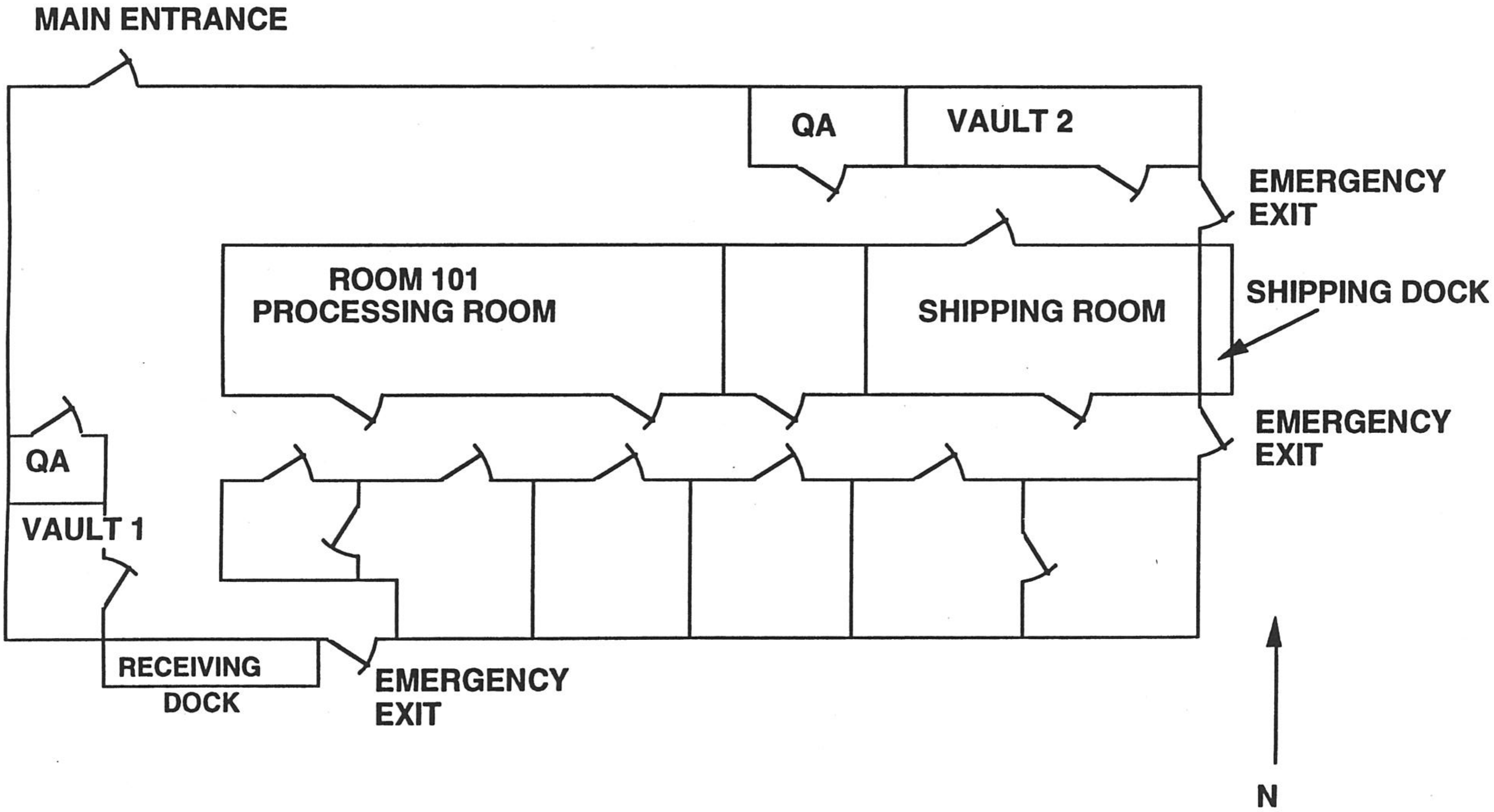
EXAMPLE NUCLEAR PROCESSING PLANT (SNM)



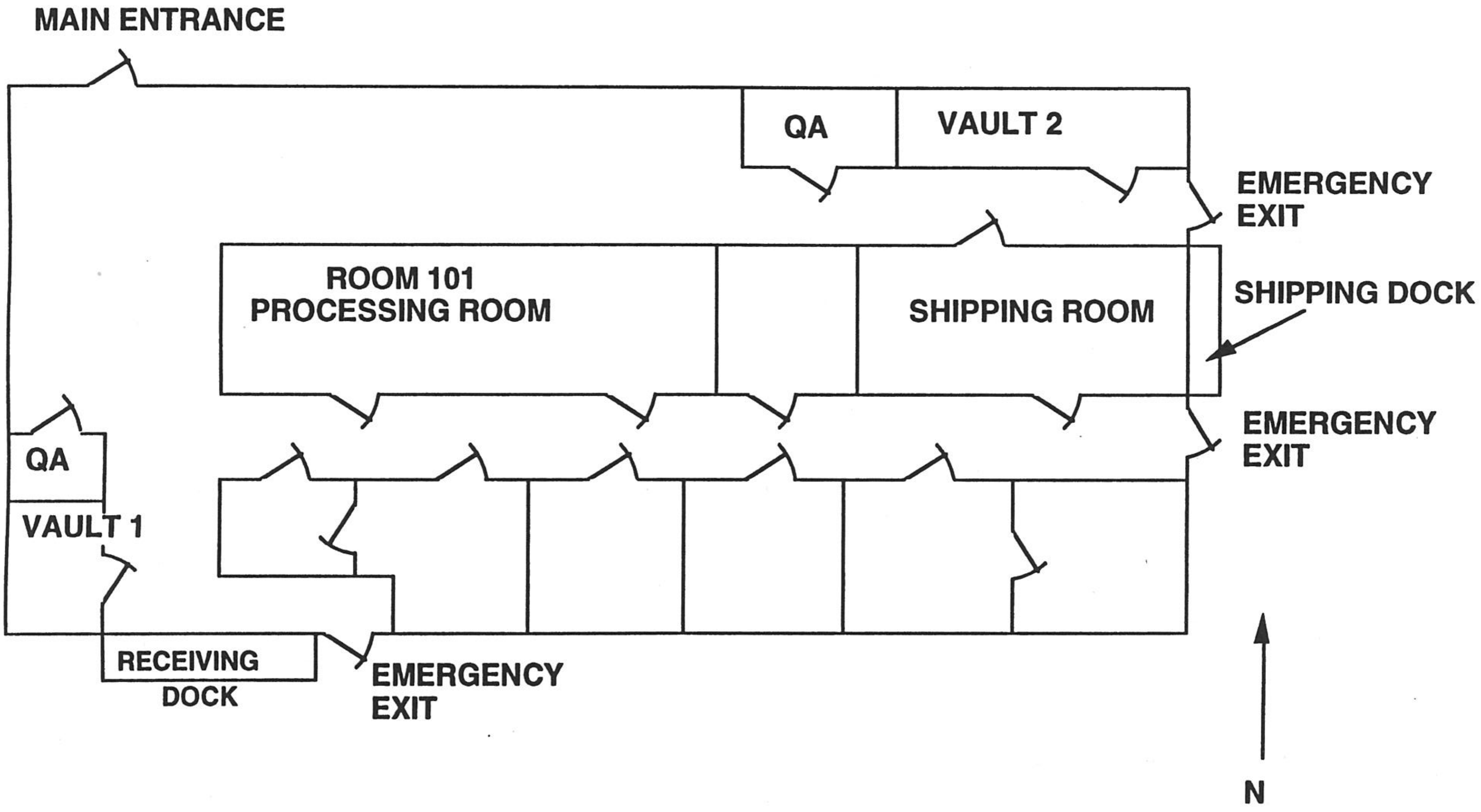
NUCLEAR PROCESSING BUILDING



NUCLEAR PROCESSING BUILDING



NUCLEAR PROCESSING BUILDING



SYSTEM EFFECTIVENESS EVALUATION
-- PROBABILITY WORKSHEET --

ADVERSARY ____________ ACT ____________ TARGET ____________

SCENARIO NO. ____________ CASE ____________

ADVERSARY EVENT LINE	SITE	ENTRY PA	MAA	ACQUISITION	MAA	REMOVAL PA	SITE

ADVERSARY TIME LINE ______ □ ______ ______ ______ ______ □ ______ MINUTES

PD	______	______	______	______	______	______	______
PA	______	______	______	______	______	______	______
PE	______	______	______	______	______	______	______
PN	______	______	______	______	______	______	______
PMIN	______	______	______	______	______	______	______

SE ____

$$SE = PD1 \cdot PA1 \cdot PE1 \cdot PN1 + (1 - PD1 \cdot PA1)\, PD2 \cdot PA2 \cdot PE2 \cdot PN2$$

SYSTEM EFFECTIVENESS EVALUATION
-- PROBABILITY WORKSHEET --

ADVERSARY ______________ ACT ______________ TARGET ______________

SCENARIO NO. ______________ CASE ______________

ADVERSARY EVENT LINE	SITE	ENTRY PA	MAA	ACQUISITION	MAA	REMOVAL PA	SITE
PD	______	______	______	______	______	______	______
PA	______	______	______	______	______	______	______
PE	______	______	______	______	______	______	______
PN	______	______	______	______	______	______	______
PMIN	______	______	______	______	______	______	______

ADVERSARY TIME LINE ______ □ ______ ______ ______ ______ □ ______ MINUTES

SE ____

$$SE = PD1 \cdot PA1 \cdot PE1 \cdot PN1 + (1 - PD1 \cdot PA1)\, PD2 \cdot PA2 \cdot PE2 \cdot PN2$$

SYSTEM EFFECTIVENESS EVALUATION
-- PROBABILITY WORKSHEET --

ADVERSARY ____________________ ACT ________________ TARGET ____________________

SCENARIO NO. ________________ CASE ____

ADVERSARY EVENT LINE | SITE | ENTRY PA | MAA | ACQUISITION | MAA | REMOVAL PA | SITE |

ADVERSARY TIME LINE ________ □ ________ ________ ________ ________ □ ________ MINUTES

PD ________ ________ ________ ________ ________ ________ ________

PA ________ ________ ________ ________ ________ ________ ________

PE ________ ________ ________ ________ ________ ________ ________

PN ________ ________ ________ ________ ________ ________ ________

PMIN ________ ________ ________ ________ ________ ________ ________

SE ____

$$SE = PD1 \bullet PA1 \bullet PE1 \bullet PN1 + (1 - PD1 \bullet PA1)\, PD2 \bullet PA2 \bullet PE2 \bullet PN2$$

SYSTEM EFFECTIVENESS EVALUATION
-- TIME LINE WORKSHEET --

SCENARIO NO. ____________________ DETECTION EVENT ____________________________

ADVERSARY
TIME LINES

W/O INTERVENTION

WITH INVERVENTION

SECURITY
TIME LINES

DETECTION

ASSESSMENT

COMMUNICATION

DEPLOYMENT

____

____

____

____

____

____

SYSTEM EFFECTIVENESS EVALUATION
-- TIME LINE WORKSHEET --

SCENARIO NO. ____________________ DETECTION EVENT ____________________________

ADVERSARY TIME LINES

W/O INTERVENTION

WITH INVERVENTION

SECURITY TIME LINES

DETECTION

ASSESSMENT

COMMUNICATION

DEPLOYMENT

____

____

____

____

____

____

SYSTEM EFFECTIVENESS EVALUATION
-- TIME LINE WORKSHEET --

SCENARIO NO. ____________________ DETECTION EVENT ____________________________

ADVERSARY TIME LINES

W/O INTERVENTION

WITH INVERVENTION

SECURITY TIME LINES

DETECTION

ASSESSMENT

COMMUNICATION

DEPLOYMENT

____

____

____

____

____

____

SYSTEM EFFECTIVENESS EVALUATION
-- TIME LINE WORKSHEET --

SCENARIO NO. ____________________ DETECTION EVENT ____________________

ADVERSARY TIME LINES

W/O INTERVENTION

WITH INVERVENTION

SECURITY TIME LINES

DETECTION

ASSESSMENT

COMMUNICATION

DEPLOYMENT

____

____

____

____

____

____

SYSTEM EFFECTIVENESS EVALUATION
-- TIME LINE WORKSHEET --

SCENARIO NO. ____________________ **DETECTION EVENT** ____________________________

ADVERSARY TIME LINES

W/O INTERVENTION

WITH INVERVENTION

SECURITY TIME LINES

DETECTION

ASSESSMENT

COMMUNICATION

DEPLOYMENT

____

____

____

____

____

____

SYSTEM EFFECTIVENESS EVALUATION
-- TIME LINE WORKSHEET --

SCENARIO NO. ____________________ DETECTION EVENT ____________________________

ADVERSARY TIME LINES

W/O INTERVENTION

WITH INVERVENTION

SECURITY TIME LINES

DETECTION

ASSESSMENT

COMMUNICATION

DEPLOYMENT

____

____

____

____

____

____

SYSTEM EFFECTIVENESS EVALUATION
-- TIME LINE WORKSHEET --

SCENARIO NO. ____________________ DETECTION EVENT ____________________________

ADVERSARY TIME LINES

W/O INTERVENTION

WITH INVERVENTION

SECURITY TIME LINES

DETECTION

ASSESSMENT

COMMUNICATION

DEPLOYMENT

____

____

____

____

____

____

SYSTEM EFFECTIVENESS EVALUATION
-- TIME LINE WORKSHEET --

SCENARIO NO. ____________________ DETECTION EVENT ____________________

ADVERSARY TIME LINES

W/O INTERVENTION

WITH INVERVENTION

SECURITY TIME LINES

DETECTION

ASSESSMENT

COMMUNICATION

DEPLOYMENT

____

____

____

____

____

____

SYSTEM EFFECTIVENESS EVALUATION
-- TIME LINE WORKSHEET --

SCENARIO NO. ____________________ DETECTION EVENT ____________________________

ADVERSARY TIME LINES

W/O INTERVENTION

WITH INVERVENTION

SECURITY TIME LINES

DETECTION

ASSESSMENT

COMMUNICATION

DEPLOYMENT

____

____

____

____

____

____

DYNAMIC ANALYSIS WORKSHEET

Element Name: ____________________ Date: ____________________

Initial P: ______ Initial A: ______ Initial B: ______

Date: ____________________

N (# of Tests): ______ X (# of Successes): _______

Adjust A to A' = (A + X): ______________
Adjust B to B'= (B + N - X): _________________
Adjust P to P'= [A'/(A' + B')]: _________________

Date: ____________________

Replace A with A' -- A: _________
Replace B with B' -- B: _________
Replace P with P' -- P: _________
N (# of Tests): ______ X (# of Successes): _______

Adjust A to A' = (A + X): ______________
Adjust B to B'= (B + N - X): _________________
Adjust P to P'= [A'/(A' + B')]: _________________

Date: ____________________

Replace A with A' -- A: _________
Replace B with B' -- B: _________
Replace P with P' -- P: _________
N (# of Tests): ______ X (# of Successes): _______

Adjust A to A' = (A + X): ______________
Adjust B to B'= (B + N - X): _________________
Adjust P to P'= [A'/(A' + B')]: _________________

DYNAMIC ANALYSIS WORKSHEET

Element Name: ____________________ Date: ____________________

Initial P: _____ Initial A: _____ Initial B: _____

Date: ____________________

N (# of Tests): _____ X (# of Successes): _____

Adjust A to A' = (A + X): ______________
Adjust B to B'= (B + N - X): ________________
Adjust P to P'= [A'/(A' + B')]: ________________

Date: ____________________

Replace A with A' -- A: _________
Replace B with B' -- B: _________
Replace P with P' -- P: _________

N (# of Tests): _____ X (# of Successes): _____

Adjust A to A' = (A + X): ______________
Adjust B to B'= (B + N - X): ________________
Adjust P to P'= [A'/(A' + B')]: ________________

Date: ____________________

Replace A with A' -- A: _________
Replace B with B' -- B: _________
Replace P with P' -- P: _________

N (# of Tests): _____ X (# of Successes): _____

Adjust A to A' = (A + X): ______________
Adjust B to B'= (B + N - X): ________________
Adjust P to P'= [A'/(A' + B')]: ________________

DYNAMIC ANALYSIS WORKSHEET

Element Name: ____________________ Date: ____________________

Initial P: ______ Initial A: ______ Initial B: ______

Date: ____________________

N (# of Tests): ______ X (# of Successes): ______

Adjust A to $A' = (A + X)$: ______________
Adjust B to $B' = (B + N - X)$: ________________
Adjust P to $P' = [A'/(A' + B')]$: ________________

Date: ____________________

Replace A with A' -- A: _________
Replace B with B' -- B: _________
Replace P with P' -- P: _________
N (# of Tests): ______ X (# of Successes): ______

Adjust A to $A' = (A + X)$: ______________
Adjust B to $B' = (B + N - X)$: ________________
Adjust P to $P' = [A'/(A' + B')]$: ________________

Date: ____________________

Replace A with A' -- A: _________
Replace B with B' -- B: _________
Replace P with P' -- P: _________
N (# of Tests): ______ X (# of Successes): ______

Adjust A to $A' = (A + X)$: ______________
Adjust B to $B' = (B + N - X)$: ________________
Adjust P to $P' = [A'/(A' + B')]$: ________________

DELAY VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary ______________ Act ______________ Target ______________ Date ______________ Worksheet No. ______________

	Adversary Event Line												
ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7	2.8	2.9			
ACQUISITION	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10	3.11	3.12
	Target*	4.1 Normal Access	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9	4.10		
	MAA	5.1 Thru Personnel Portal	5.2 Thru S/R** Portal	5.3 Thru Emergency Exit	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10	5.11	5.12
REMOVAL	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7	6.8	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.

** S/R = Shipper/Receiver

ALARM ASSESSMENT VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER ADVERSARIES

Adversary ____________ Act ____________ Target ____________ Date ____________ Worksheet No. ______

Type of Alarm Assessment							
CCTV Response To Alarm	1.1 Defeat Camera	1.2 Defeat Com. to CAS/SAS	1.3 Use Deceit	1.4 Use Stealth	1.5 Report False Alarm	1.6	1.7
SPO Response To Alarm	2.1 Neutralize SPO	2.2 Defeat Com. to CAS/SAS	2.3 Use Deceit	2.4 Use Stealth	2.5 Report False Alarm	2.6	2.7
Routine SPO Patrol	3.1 Neutralize SPO	3.2 Defeat Com. to CAS/SAS	3.3 Use Deceit	3.4 Use Stealth	3.5 Report False Alarm	3.6	3.7
Multiple Alarms	4.1 Report False Alarm	4.2	4.3				
Duress Alarm	5.1Report False Alarm	5.2	5.3				

Abbreviations

Com. = Communication
SPO = Special Police Officer
CAS = Central Alarm Station
SAS = Secondary Alarm Station

DETECTION VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary ____________ Act ____________________ Target ____________________ Date ____________ Worksheet No. ____________

	Adversary Event Line												
ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6 Movement in Area	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7 Movement in Area	2.8	2.9			
ACQUISITION	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10 Movement in Area	3.11	3.12
	Target*	4.1 Normal Access	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9			
	MAA	5.1 Thru Personnel Portal	5.2 Thru S/R** Portal	5.3 Thru Emergency Exit	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10 Movement in Area	5.11	5.12
REMOVAL	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7 Movement in Area	6.8	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6 Movement in Area	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.

** S/R = Shipper/Receiver

VULNERABILITY DESCRIPTIONS FOR WORKSHEET NO. ____________

Vulnerability Number	Vulnerability Description

Provide descriptions for vulnerability levels VH, H, M and others where appropriate.

DELAY VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER AND INSIDER ADVERSARIES
(Mark expected vulnerability level in each box: VL, L, M, H, VH)

Adversary ______________ Act ________________________ Target ________________________ Date ______________ Worksheet No. ______________

	Adversary Event Line												
ENTRY	Site	1.1 Thru Vehicle Portal	1.2 Thru Personnel Portal	1.3 Thru Fence	1.4 Over Fence	1.5 Under Fence	1.6	1.7	1.8				
	PA	2.1 Thru Fence	2.2 Over Fence	2.3 Under Fence	2.4 Thru Personnel Portal	2.5 Over Personnel Portal	2.6 Thru Vehicle Portal	2.7	2.8	2.9			
ACQUISITION	MAA	3.1 Thru Personnel Portal	3.2 Thru S/R** Portal	3.3 Thru Emergency Exit	3.4 Thru Waste Path	3.5 Thru Window	3.6 Thru Vent	3.7 Thru Wall	3.8 Thru Ceiling	3.9 Thru Floor	3.10	3.11	3.12
	Target*	4.1 Normal Access	4.2 Maintenance Access	4.3 Thru Window	4.4 Thru Vent	4.5 Thru Side	4.6 Thru Top	4.7 Thru Bottom	4.8	4.9	4.10		
	MAA	5.1 Thru Personnel Portal	5.2 Thru S/R** Portal	5.3 Thru Emergency Exit	5.4 Thru Waste Path	5.5 Thru Window	5.6 Thru Vent	5.7 Thru Wall	5.8 Thru Ceiling	5.9 Thru Floor	5.10	5.11	5.12
REMOVAL	PA	6.1 Thru Fence	6.2 Over Fence	6.3 Under Fence	6.4 Thru Personnel Portal	6.5 Over Personnel Portal	6.6 Thru Vehicle Portal	6.7	6.8	6.9			
	Site	7.1 Thru Vehicle Portal	7.2 Thru Personnel Portal	7.3 Thru Fence	7.4 Over Fence	7.5 Under Fence	7.6	7.7	7.8				

* Target is in vault, vault-type room, glove box, storage container, or similar location.

** S/R = Shipper/Receiver

ALARM ASSESSMENT VULNERABILITY SEARCH WORKSHEET FOR OUTSIDER ADVERSARIES

Adversary ________________ Act ________________ Target ________________ Date ______________ Worksheet No. ________

Type of Alarm Assessment							
CCTV Response To Alarm	1.1 Defeat Camera	1.2 Defeat Com. to CAS/SAS	1.3 Use Deceit	1.4 Use Stealth	1.5 Report False Alarm	1.6	1.7
SPO Response To Alarm	2.1 Neutralize SPO	2.2 Defeat Com. to CAS/SAS	2.3 Use Deceit	2.4 Use Stealth	2.5 Report False Alarm	2.6	2.7
Routine SPO Patrol	3.1 Neutralize SPO	3.2 Defeat Com. to CAS/SAS	3.3 Use Deceit	3.4 Use Stealth	3.5 Report False Alarm	3.6	3.7
Multiple Alarms	4.1 Report False Alarm	4.2	4.3				
Duress Alarm	5.1Report False Alarm	5.2	5.3				

Abbreviations

Com. = Communication
SPO = Special Police Officer
CAS = Central Alarm Station
SAS = Secondary Alarm Station

VULNERABILITY ANALYSIS PROCESS FOR EVALUATING PROTECTION AGAINST DESIGN-BASIS THREATS

Lawrence Harris, Jr. and Lewis A. Goldman
Science Applications International Corporation
San Diego, California, USA

ABSTRACT

The Department of Energy (DOE) requires vulnerability analyses (VAs) to be performed in support of three Safeguards and Security programs: Computer Security Program, Operations Security (OPSEC) Program and Special Nuclear Material (SNM) Protection Program. The three types of VAs used to support these requirements will be described briefly and compared. The type of VA used to evaluate SNM protection will be described in more detail as a general six-step process. This general VA process has wide applicability; it has been used to evaluate the protection of nuclear and non-nuclear assets, civilian and military assets when design-basis threats are specified. The applicability of the VA process to evaluation of SNM protection and information protection against design-basis threats will be described.

VULNERABILITY ANALYSES FOR DOE SAFEGUARDS AND SECURITY

Three DOE Safeguards and Security programs require VAs to be performed as part of broader assessments. For computer security, a VA is part of the "Risk Assessment" described in DOE's Risk Assessment Instructions[1]. This VA is performed after an evaluation is made of compliance with applicable DOE orders, identified deficiencies are corrected, and further assessment is merited. When a VA is performed, the vulnerability of the facility, personnel, information, communications, computer hardware and software, system management and fire protection is evaluated for four types of acts: (a) malevolent acts (e.g., sabotage), (b) acts of nature (e.g., storms), (c) accidents (e.g., operator error), and (d) utility failures (HVAC failure). The potential impacts associated with the vulnerabilities for each act of concern are categorized as one or more of the following: (a) damage, (b) destruction, (c) disclosure, and (d) denial. The results of this VA are used as a basis for selecting any necessary countermeasures and preparing actions plans for implementing such countermeasures.

For operations security, a VA is part of the "OPSEC Assessment" described in DOE's Operations Security Procedural Guide[2]. The information targets normally addressed are those on the Critical and Sensitive Information List (CSIL). This list is the facility's prioritized list of information, both classified and unclassified, that is deemed most important to deny an adversary. The CSIL is supplemented by an Essential Elements of Friendly Information (EEFI) that identifies indicators or pathways to information on the list. The VA consists of an analysis of an organization or activity to identify information sources that can be exploited by intelligence threats. Such threats collect information by humans, by signal interception and by imagery. The analysis addresses information available from open sources, communications, and computer operations as well as facility services such as trash collection, construction, and procurement. The results of the VA are used to recommend countermeasures where needed to reduce identified vulnerabilities.

For SNM protection, a VA is part of the "Risk Evaluation" described in DOE's Site Safeguards and Security Plan Preparation Guide[3]. DOE has specified design-basis threats for protection of SNM against theft and sabotage by five types of adversaries: terrorists, criminals, psychotics, disgruntled employees and antinuclear extremists. The VAs are performed to identify vulnerabilities and to determine the effectiveness of protection for applicable SNM targets against the design-basis threats. The ASSESS program[4] is widely used in the DOE community to perform this type of VA. The VA process described can also be performed manually using table-top exercises and field exercises. The results of the VAs are used to identify and prioritize protection upgrades that reduce vulnerabilities sufficiently to achieve desired levels of protection.

Comparison of the three VA types shows several common elements. Each type requires characterization of threats, targets, facility and protection system. Also each type involves a search for vulnerabilities or weaknesses. Perhaps the greatest differences for the three types are the ways threats are represented. For computer security VAs, "threats" consist of four types of acts: malevolent acts, acts of nature, accidents and utility failures. No adversaries are defined. For OPSEC VAs, "threats" are the intelligence threats associated with the various forms of information collection. For VAs to evaluate SNM protection, "threats" are the design-basis threats for SNM theft and sabotage by five types of adversaries. Adversary attributes are well defined in DOE guidance. In contrast to VAs for computer security and OPSEC, VAs for SNM protection determine the effectiveness of protection against design-basis threats. These VAs, when performed using the ASSESS program, usually require much greater levels of effort than those performed for computer security and OPSEC.

The computer security and OPSEC VAs are both focused on the protection of information. The VA process used to evaluate SNM protection has been used to evaluate protection for many other kinds of assets: nuclear and non-nuclear, civilian and military. If design-basis threats are defined for information targets, the same VA process can be used. The dual application of this general VA process to SNM and information protection will be described next.

VULNERABILITY ANALYSIS PROCESS

The general VA process that will be described has been used for some years to evaluate the effectiveness of protection systems against design-basis threats. Key aspects of this VA process have been described in previous INMM papers[5,6,7]. A flow diagram of the process is shown in Figure 1. The six VA steps can be organized several ways; however, this way has been found most straightforward to use and to explain to others. The lower feedback loop points out the need to repeat the process when significant changes occur. The upper feedback loop is part of the last VA step involving protection upgrades and will be discussed when that step is described. Each of the six VA steps will be described in order as applied to both SNM and information protection. For application to information protection, it is assumed that design-basis threats are available to define (a) criteria for identifying the applicable information targets and (b) the adversaries, their objectives and attributes.

VA Step 1. VA Team Selection and Preparation

There are different views on the number of people required to perform a quality VA. Our view is that a wide range of expertise is required to adequately understand the operation of both the facility and the protection system. Furthermore, diversity of education and experience among the team members is important to support the many sound judgements required throughout the VA process. Core teams of four to six qualified persons is recommended. The core team should be augmented as needed with special expertise. Use of permanent onsite personnel has the advantages of having people who know the site and who can help institutionalize the VA process at the site.

All VA teams require team members with expertise in vulnerability analysis, performance testing, physical security systems, protective force and facility operations. In addition, VAs for SNM protection require expertise in material control and accountability (MC&A), and VAs for information security require expertise in computer security, operations security, document control, technical surveillance countermeasures (TSCM), emission security, emanations security, and communications security.

VA Step 2. Threat and Target Characterization

Threats and targets are grouped together in this VA step because specification of a design-basis threat includes criteria that identify the applicable targets. For example, design-basis threats for SNM theft have been applied to Category I quantities of SNM and may be applied to lesser quantities. Details of DOE design-basis threats are described in threat guidance documents.

The types of targets applicable to VAs for SNM and information protection are very different as shown in Table 1. The SNM targets are most likely to be located in an industrial-type facility or laboratory having radiation monitors and controls throughout the area and protected as a vault or material access area. While some information targets will be in the same areas, most will be located in offices, conference rooms, record vaults, computer centers, and communication centers.

To make the analysis more efficient, it is a good practice to group similar targets having the same protection together and to analyze only one target in the group. This is only valid when both protection plans and protection practices are the same for a group of targets.

VA Step 3. Facility and Protection System Characterization

Before the search for vulnerabilities can begin, it is necessary to understand how each target is protected. Detailed information on the site, facility, targets and protection system, together with any information on the performance of protection personnel and equipment, need to be collected, organized and documented. Sources for such information include the following:

- Layout drawings and descriptions of site, facility, SNM and information targets, and protection system.
- Protection plans:
  - security plans, procedures, and records
  - security staffing plans
  - emergency response plans.
- Training plans and records.
- Equipment maintenance plans and records.
- Performance testing plans, procedures, and records.
- Survey and inspection reports.
- Team member tours, inspections, and interviews.

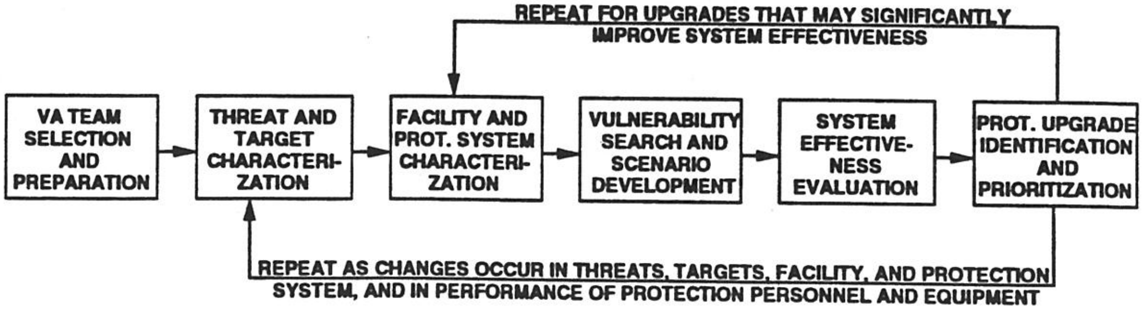

REPEAT FOR UPGRADES THAT MAY SIGNIFICANTLY IMPROVE SYSTEM EFFECTIVENESS
VA TEAM SELECTION AND PREPARATION
THREAT AND TARGET CHARACTERIZATION
FACILITY AND PROT. SYSTEM CHARACTERIZATION
VULNERABILITY SEARCH AND SCENARIO DEVELOPMENT
SYSTEM EFFECTIVENESS EVALUATION
PROT. UPGRADE IDENTIFICATION AND PRIORITIZATION
REPEAT AS CHANGES OCCUR IN THREATS, TARGETS, FACILITY, AND PROTECTION SYSTEM, AND IN PERFORMANCE OF PROTECTION PERSONNEL AND EQUIPMENT

Figure 1. VA Process for Evaluating Protection Against Design-Basis Threats

Table 1. Comparison of Target Types

SNM TARGETS	INFORMATION TARGETS
• ASSEMBLED WEAPON AND PARTS	• PRINTED SHEETS OR DOCUMENTS
- ASSEMBLY/DISASSEMBLY LINE	- STORAGE
- STORAGE	- IN PRINTER, COPIER, OR FAX
- TEST EQUIPMENT	- IN USE
- IN TRANSIT	• COMPUTER INFORMATION
• WEAPON PARTS AND METAL	- REMOVABLE DISK
- PRODUCTION LINE	- FIXED DISK
- STORAGE	- RAM
- TEST EQUIPMENT	- DATA LINES
- ASSAY EQUIPMENT	- DISPLAY
- IN TRANSIT	• COMMUNICATIONS
• METAL, POWDER AND LIQUIDS	- FACE-TO-FACE CONVERSATIONS
- PROCESS LINE	- PHONE CONVERSATIONS
- STORAGE	- FAX TRANSMISSIONS
- ASSAY EQUIPMENT	- DATA NETWORK TRANSMISSIONS
- IN TRANSIT	• ELECTRONIC EMISSIONS

Collecting, organizing and documenting this information begin with this VA step and continue throughout a vulnerability analysis.

VA Step 4. Vulnerability Search and Scenario Development

This VA step is where the analysis begins for each combination of threat and target. For example, one VA might be performed to evaluate the protection of SNM in vault storage against theft by terrorists. Another VA might be performed to evaluate the protection of SNM in transit between two facilities at a site against theft by criminals. The purpose of this VA step is to produce for each threat-target combination a list of vulnerabilities and the adversary's plans of attack for the most credible scenarios. The list of vulnerabilities may be the same or similar for some threat-target combinations. The most differences in vulnerability lists are likely to occur for outsider and insider threats and for SNM targets and information targets.

The search for vulnerabilities that can be exploited by an adversary can be accomplished using a variety of approaches:

- Observation and inspection of facility operations and security practices.
- Performance testing of security capabilities (under routine conditions and under stress conditions of an adversary attack).
- Computer modeling and simulation.
- Blackhatting, gaming and scenario development.

The first two approaches also contribute information like that collected in the preceding VA step as well as to help identify vulnerabilities. The key points to searching for vulnerabilities are to consider all reasonable adversary strategies (covert or covert-overt actions, abrupt or protracted events, diversions, coverup), tactics (stealth, deceit, force), and paths (ground, air, underground), and to consider all facility or system conditions (routine operation, shutdown, maintenance, emergency).

Once vulnerabilities are identified for a given threat-target combination, it is necessary to develop scenarios that represent the adversary's most credible ways to attack the target. The resulting scenarios are used in the next VA step to determine system effectiveness. Scenarios are generally most credible when developed by assuming the adversary seeks the best chance for success and, when feasible, prefers a simple strategy, simple tactics and easy paths.

VA Step 5. System Effectiveness Evaluation

The preceding VA step provides scenarios that include descriptions of the adversary's plans of attack. For attacks that are intended to be entirely covert and the adversary can be assumed to abort if detected, evaluation of system effectiveness only involves determining the probability of getting an alarm and assessing it correctly. For example, if there are two independent detection opportunities associated with an adversary's plan of attack, the system effectiveness (SE) is given by the following equation:

$$SE = \underbrace{PD1 \bullet PA1}_{\text{First Term}} + \underbrace{(1-PD1 \bullet PA1)PD2 \bullet PA2}_{\text{Second Term}}$$

where: PD = conditional probability, given an adversary attempt, an alarm is produced;

PA = conditional probability, given an alarm, it is assessed correctly;

and the numbers 1 and 2 refer to the first and second detection opportunities, respectively.

The first term in the equation represents the probability of getting an alarm at the first detection opportunity and assessing it correctly. The second term represents the probability of not getting a correctly-assessed alarm at the first detection opportunity and getting a correctly-assessed alarm at the second detection opportunity. Determination of values for PD and PA, under the conditions associated with the scenario being analyzed, is usually the most challenging part of a VA. It is important to determine them based on security practices, not security plans. Performance testing under the conditions of the scenario being analyzed should be used as much as possible to determine values for PD and PA.

For adversary plans of attack that begin covertly and then proceed overtly after detection occurs, it is necessary to evaluate the performance of the protection system response after an alarm is received at a security alarm station. For this discussion, the protection system response is assumed to be a protective force that responds to locations from which adversaries can be engaged and neutralized. Neutralized means stopped from achieving their objective, such as escaping from the site with SNM or information, not killed. Adding protective force response to the evaluation results in the following equation for system effectiveness (SE):

$$SE = \underbrace{\underline{PD1 \cdot PA1 \cdot PE1 \cdot PN1}}_{\text{First Term}} + \underbrace{\underline{(1-PD1 \cdot PA1)PD2 \cdot PA2 \cdot PE2 \cdot PN2}}_{\text{Second Term}}$$

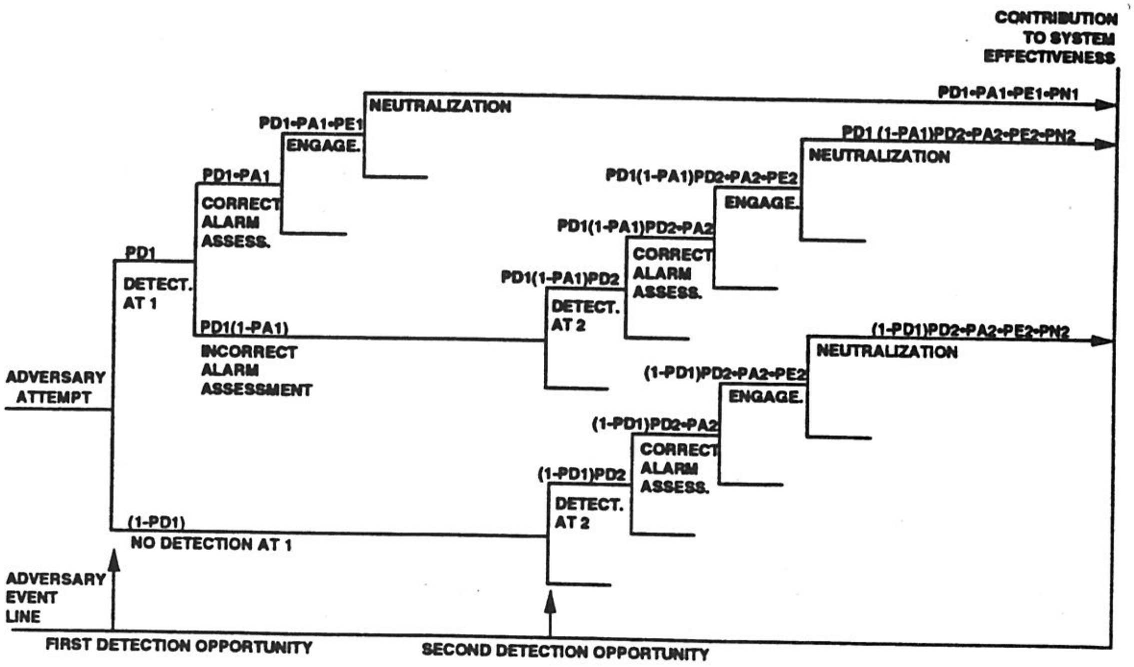
where: PE = conditional probability, given a true alarm, the protective force responds to positions from which the adversary force can be engaged;

PN = conditional probability, given the adversary force can be engaged, the adversary force is neutralized or stopped from achieving its objective;

and the numbers 1 and 2 refer to the first and second detection opportunities, respectively.

The first term represents the probability of getting an alarm at the first detection opportunity, assessing it correctly, and then engaging and neutralizing the adversary. The second term represents the probability of not getting a correctly-assessed alarm at the first detection opportunity and getting a correctly-assessed alarm at the second detection opportunity and then engaging and neutralizing the adversary. Evaluation of the protective force response requires that timelines be determined for both the adversary actions and the protection system response (alarm assessment time, communication time and protective force deployment time). Determination of values for PD, PA, PE and PN is challenging and should be based on security practices, not security plans. Performance testing under the conditions of the scenario being analyzed should be used as much as practical to determine these values.

The equations presented above for system effectiveness are applicable to the evaluation of system performance for most scenarios. However, no single equation is applicable to every possible scenario. The basis for the second equation presented above is shown in the logic diagram of Figure 2. The first equation presented above is a special case of the second equation in which PE1 = PN1 = PE2 = PN2 = 1 or equivalently, the adversary aborts if detected. If the logic diagram in Figure 2 accurately represents the scenario being



$$\begin{aligned} SE &= PD1 \cdot PA1 \cdot PE1 \cdot PN1 + PD1\ (1-PA1)\ PD2 \cdot PA2 \cdot PE2 \cdot PN2 + (1-PD1)\ PD2 \cdot PA2 \cdot PE2 \cdot PN2 \\ &= PD1 \cdot PA1 \cdot PE1 \cdot PN1 + (1-PD1 \cdot PA1)\ PD2 \cdot PA2 \cdot PE2 \cdot PN2 \end{aligned}$$

Figure 2. Logic Diagram to Determine Equation for Protection System Effectiveness (SE) (Example is for two independent detection opportunities)

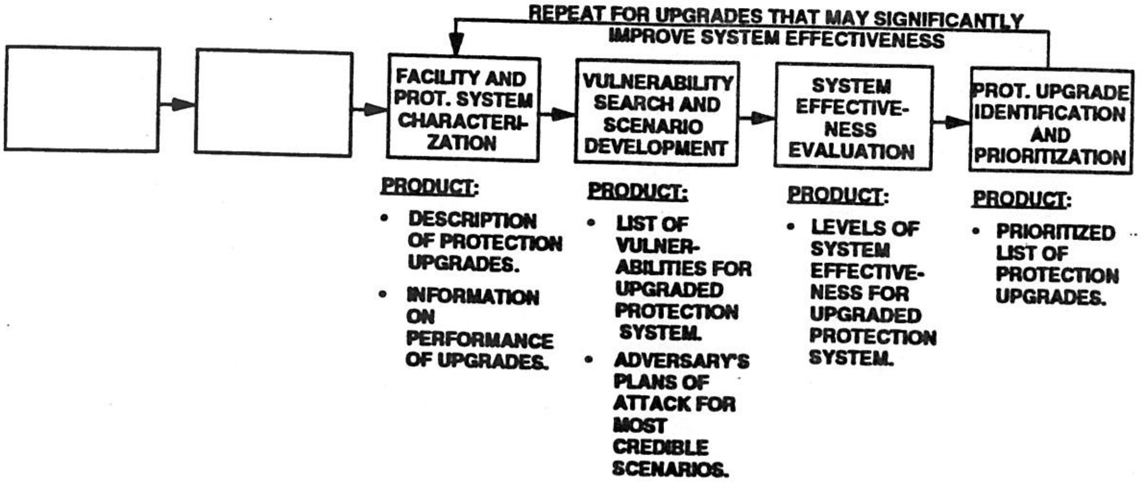

REPEAT FOR UPGRADES THAT MAY SIGNIFICANTLY IMPROVE SYSTEM EFFECTIVENESS
FACILITY AND PROT. SYSTEM CHARACTERI-ZATION
VULNERABILITY SEARCH AND SCENARIO DEVELOPMENT
SYSTEM EFFECTIVE-NESS EVALUATION
PROT. UPGRADE IDENTIFICATION AND PRIORITIZATION
PRODUCT:
• DESCRIPTION OF PROTECTION UPGRADES.
• INFORMATION ON PERFORMANCE OF UPGRADES.
PRODUCT:
• LIST OF VULNER-ABILITIES FOR UPGRADED PROTECTION SYSTEM.
• ADVERSARY'S PLANS OF ATTACK FOR MOST CREDIBLE SCENARIOS.
PRODUCT:
• LEVELS OF SYSTEM EFFECTIVE-NESS FOR UPGRADED PROTECTION SYSTEM.
PRODUCT:
• PRIORITIZED LIST OF PROTECTION UPGRADES.

Figure 3. Extra Analysis Required for Evaluating Major Protection Upgrades

analyzed, the equations given above are valid. If the logic diagram needs to be modified to include more detection opportunities or reflect other changes, the equation should be modified accordingly.

VA Step 6. Protection Upgrade Identification and Prioritization

This VA step can involve considerable effort if significant protection upgrades are required and thus part of the VA needs to be repeated to determine the system effectiveness of the upgraded protection system. This situation is illustrated in Figure 3 where the feedback loop from VA Step 6 to Step 3 is used and the resulting products of VA Steps 3 through 6 are listed.

All types of protection upgrades (facility, equipment, personnel and procedures) should be considered when identifying upgrades. It is useful to select complementary sets of upgrades that have the potential for improving system effectiveness to the desired level. Prioritization of each upgrade set can be based on (a) the improved system effectiveness indicated by the VA for the upgraded system, (b) the additional cost for implementing and maintaining the upgraded system, and (c) other relevant factors such as safety and compatibility with facility operations.

SUMMARY

A general six-step VA process for determining the effectiveness of protection provided any specified targets against design-basis threats has been described. The process has been used successfully for some years to evaluate the protection provided a wide range of assets: nuclear and non-nuclear, civilian and military. It is applicable to the evaluation of protection provided all types of DOE targets, such as SNM and information, for which design-basis threats are specified.

ACKNOWLEGEMENTS

Many co-workers, past and present, have shared their ideas and lessons learned on the vulnerability analysis process and its application during the past 15 years. John D. Veatch and William Knox regularly offer special insights. Noteworthy contributions have also been made by Joseph D. Rivers, Joseph W. James, Kenneth J. Anderson, William R. Owel, Walter A. Vaughan, Jr., Stephen C. Schlegel, and G. Dan Smith.

REFERENCES

1. "DOE Risk Assessment Instructions, Resource Tables, and Completed Sample -- A Structured Approach, Volume I," U.S. Department of Energy, DOE/MA-365, September 1989.

2. "Operations Security Procedural Guide, Volume I, Program and Procedures," U.S. Department of Energy, August 1988.

3. "Site Safeguards and Security Plan Preparation Guide," U.S. Department of Energy, February 1989.

4. "Analytic System and Software for Evaluating Safeguards and Security, ASSESS User's Manual," U.S. Department of Energy, September 1990.

5. L. Harris and W. R. Owel, "VISA-2: A General, Vulnerability-Oriented Method for Evaluating the Performance of Integrated Safeguards/Security Systems at Nuclear Facilities," Nuclear Materials Management, Vol. X, Proceedings Issue, pp. 260-265, July 1981.

6. L. Harris, Jr., et al., "Outsider Threat Vulnerability Analysis," Nuclear Materials Management, Vol. XIV, Proceedings Issue, pp. 330-335, July 1985.

7. L. Harris, Jr., et al., "Neutralization for SAVI Evaluation of Security System Effectiveness," Nuclear Materials Management, Vol. XVIII, Proceedings Issue, pp. 704-707, July 1989.