SANDIA REPORT

SAND89—0926/1 • UC—~~515~~ 700
Unlimited Release
Printed December 1989

SAVI:
Systematic Analysis of Vulnerability to Intrusion
Volume 1 of 2

Nuclear Security Systems Directorate
and
Science & Engineering Associates, Inc.

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A16
Microfiche copy: A01

SAND89-0926/1
Unlimited Release
Printed December 1989

Distribution
Category UC-515

SAND--89-0926/1

DE90 008574

SAVI: SYSTEMATIC ANALYSIS OF VULNERABILITY TO INTRUSION
VOLUME 1 OF 2

Nuclear Security Systems Directorate
Sandia National Laboratories
Albuquerque, New Mexico 87185

Science & Engineering Associates
Albuquerque, New Mexico 87110

ABSTRACT

SAVI (Systematic Analysis of Vulnerability to Intrusion) is a PC-based software package for modeling and analyzing physical protection systems. This report is the complete documentation of the SAVI project.

CONTENTS

INTRODUCTION

SAVI (Systematic Analysis of Vulnerability to Intrusion) is a PC-based software package for modeling and analyzing physical protection systems. SAVI implements several features that make it a unique product. First, the user interface for site modeling and data entry is simple and flexible. Second, the SAVI model analyzes all adversary paths to the target location and, if selected, all exit paths from the target location. Third, a reference catalog and database are included that define the protection elements and safeguards components, and give detection and delay performance values for the components. Finally, SAVI's results are output in graphic form and include recommendations for upgrade.

This report is the complete documentation of the SAVI software package. Volume 1 of this report consists of Sections A through H, and Volume 2 consists of Section I. A brief description of all sections is provided below.

Section A, *SAVI Vulnerability Assessment Method*, describes the basic features of SAVI, defines its concepts and terminology, and gives an overview of the method used to define a site protection system. This section describes the type of threats that can be specified and presents concepts that the user should consider in selecting a threat. The section also discusses the selection of a Response Force Time and outlines the path algorithm that calculates the Probability of Interruption for each adversary path in the facility.

Section B, *SAVI Software Manual*, is the user's manual for SAVI and explains how to install and operate the SAVI software. The manual also includes a step-by-step tutorial session.

Section C, *SAVI Components Lists*, is a hardcopy of the components lists that are associated with each protection element. These lists appear on the computer screen as the component choice lists for individual protection elements. The hardcopy lists are helpful in gathering and documenting security information at the site for later input to the SAVI program.

Section D, *SAVI Protection Element Diagrams*, provides the graphic layouts for each protection element. The layouts show the locations of the detection and delay components that can be selected for a protection element. The Generic Adversary Sequence Diagram is also provided in this section.

Section E, *SAVI Algorithm*, describes the interaction of the detection, delay, and response parts of the security system involved in calculating the Probability of Interruption for each path. This section details the exhaustive tree traversal algorithm implemented in the Probability of Interruption calculation.

Section F, *SAVI Element Scenario Equations*, identifies the boolean equations that group the detection and delay components associated with each defeat scenario. Each equation describes a force or deceit scenario that the adversary may choose in traversing each element along a path.

Section G, *SAVI Component Assignments and Component Performance Values for Protection Elements*, specifies the detection and delay components that are associated with the protection elements and provides their locations. The performance values associated with each component are listed at the end of this section.

Section H, *SAVI Data File Structure*, specifies the format of the Physical Protection System (PPS) data files, which are used by the SAVI program.

Section I, *SAVI Source Code*, is the documented listing of the source code for the SAVI program.

SECTION A

SAVI Vulnerability Assessment Method

CONTENTS

SAVI VULNERABILITY ASSESSMENT METHOD

INTRODUCTION

Physical protection systems at operating nuclear facilities generally cannot be exhaustively tested. These facilities often contain sensitive material, and combined with the high cost of realistic tests, it is prohibitive to conduct frequent comprehensive on-site field tests of the entire protection system. The testing that is done is realistic, but it usually involves penetration attempts and adversary/response force simulated engagements on only a few intruder paths and targets.

Consequently, there is a need for other techniques that can help to evaluate existing physical protection systems (PPS) and to optimize the design and evaluation of upgraded or new systems. The SAVI (Systematic Analysis of Vulnerability to Intrusion) computer software and methodology presented in this report is one effective technique that can be used in this process. By combining information obtained from on-site field tests and SAVI analyses, plant managers and security analysts can improve the evaluation and upgrading processes.

SAVI Features

SAVI is a PC-based vulnerability assessment model that evaluates the effectiveness of physical protection against a specified threat and a specified target. The model addresses the outsider threat, either acting alone or in collusion with an insider. It can analyze sabotage and theft attacks where adversaries are interrupted at the target as well as theft attacks where adversaries are contained within the site boundary.

SAVI provides a systematic and thorough way of modeling all of the potential paths the adversary might take to reach the target. It integrates the interaction of delay, detection, and response in calculating path vulnerabilities.

The measure of effectiveness is the probability of interruption P(I of the adversary. After specifying target, threat, facility, and protection systems characteristics, SAVI calculates the P(I) for the ten most vulnerable paths. SAVI provides two types of permanent records that are compiled for each analysis of baseline or upgraded protection systems - disks and hard-copy printouts.

Concepts and Terminology

The following are concepts and terms used within the SAVI system:

- Adversary Sequence Diagram (ASD)
  A graphic representation of a physical protection system, comprised of protection elements connecting physical areas

- Component Delay Time
  Following detection, the component and transit delays encountered by an adversary along a specific path

- Component Detection Probability
  The probability of detecting an adversary at a component along a specific path, given that he has not been previously detected

- Critical Detection Point (CDP)
  The last point on a given path at which detection must occur if the response force is to have enough time to interrupt the adversary before he completes his mission

- Cumulative Path Delay
  The total delay from off-site to the mission completion point of the path. This delay is provided by the barrier and delay components encountered by the adversary for a particular scenario

- Cumulative Path Delay Deficiency
  The time that must be added to the cumulative path delay on a deficient path to allow interruption to occur. This time is given by subtracting the RFT from the cumulative path delay and adding one second (to break a tie)

- Path
  A specific route through the facility consisting of an ordered sequence of physical areas and protection elements that an adversary can traverse to accomplish his mission

- Path Scenario
  The specific sequence of force or deceit actions the adversary uses to sequentially defeat each protection element on a path

- Path Segment
  The part of the path leading into or out of a protection element where the adversary delay times and detection probabilities are assigned

- Physical Protection System (PPS)
  The collective interaction of delay and detection components, assessment and communication components, and security and response force personnel that provide protection for facility targets

- Probability of Interruption P(I)
  The probability that the response force will interrupt the adversaries prior to completion of their mission

- Protection Element (PE)
  The basic building block of a physical protection system consisting of components which delay and detect adversary actions

- Protection Layer
  A connected set of protection elements between physical areas of a facility

- Response Force Time (RFT)
  After receiving the first alarm, the assessment, communication, and deployment time expended by the response force to reach a specified interruption point

- Timely Detection
  A security system requirement whereby the adversary must be detected in time for the response force to interrupt him prior to the completion of his mission

- Time Remaining (TR)
  The time remaining from the point the adversary has reached on a path to the point where he completes his mission for a specified path scenario

- TR*
  The point on a specified path scenario where the time remaining is equal to the RFT

- Time Remaining After Interruption (TRI)
  The surplus in the response force time, that is, the amount of time the adversary still needs to complete his mission at the point where interruption must occur on a given path

- Time Remaining After CDP
  The minimum time required for an adversary to complete his mission from the critical detection point on a given path

METHODOLOGY OVERVIEW

Adversaries accomplish their objective by moving along a path through a facility attempting to defeat the protection elements encountered along the path. They must be detected and an alarm must be received by the security forces in time to assess the alarm, initiate a response, and interrupt the adversaries before they complete their mission.

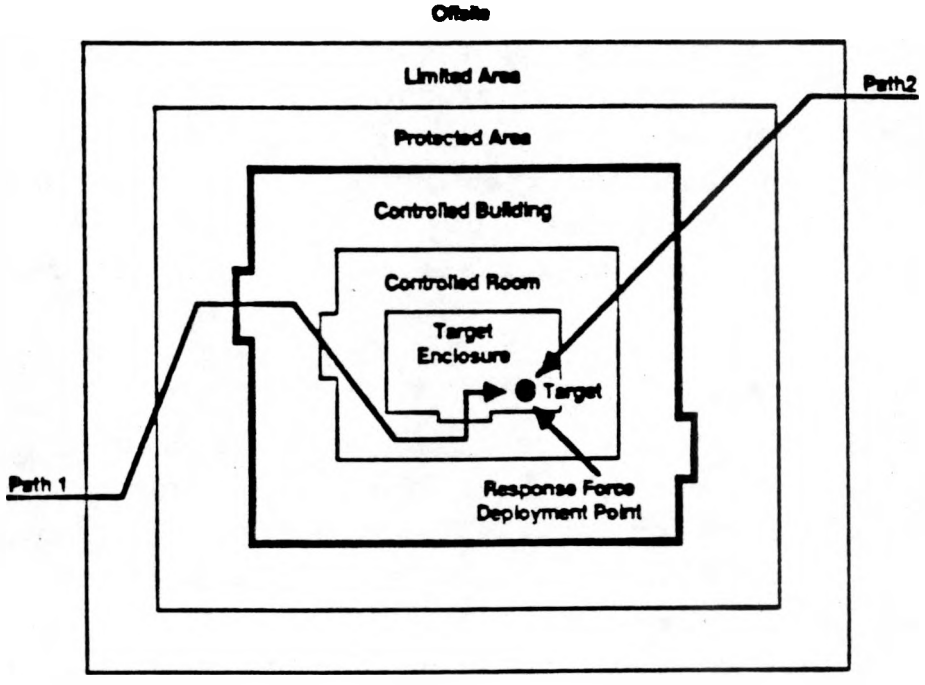


Figure A-1 Adversary and Security Interaction For a Hands-On Theft or Sabotage Threat

Figure A-1 shows two representative paths that adversaries might take to a target. If the security objective for the analysis is to prevent removal of the target from its location (hands-on theft) or to prevent sabotage at the target, then the response force deployment point used by SAVI is the target location as shown. However, if the security objective is to prevent removal of the target from the facility (theft containment), then the deployment point used by SAVI is on the site boundary.

In a typical facility, there are usually hundreds of alternative paths an adversary might take to reach a target that he wants to steal or sabotage and each path can be traversed in a large number of ways called scenarios. Using force or deceit, the adversary can defeat the various detection and delay components and security inspectors located at each element along a path. Thus, each scenario consists of a specific path and a set of adversary actions at each element that can result in the achievement of the adversary's objective.

SAVI models the physical protection system using protection elements (PE). Each PE is comprised of detection and delay components that act together to impede and discover the adversary. SAVI identifies the potential path scenarios that adversaries can use to defeat the PEs, selects the worst-case path scenarios, and calculates the effectiveness of the PPS for all paths in a facility.

Protection System Functions

An effective physical protection system includes both people and hardware and integrates three basic functions: detection, delay, and response. Detection is implemented using components such as: penetration detectors, intrusion sensors, entry monitors, alarm communication and alarm assessment units, and security inspectors. Delay is implemented with components such as: fixed barriers, movable barriers to restrict unauthorized access through normal passageways, activated denial systems, and security inspectors. Response is accomplished by on-site security inspectors, special response teams, and by off-site forces. Alarm assessment, communications, and deployment of security forces must be adequate to interrupt the adversaries. SAVI considers the relationship of these detection, delay, and response functions when it calculates P(I) for each path.

Measures of Effectiveness

As mentioned above, the evaluation measure used by SAVI to assess PPS effectiveness is P(I). P(I) is defined as the probability that the response forces will interrupt the adversaries before they can

complete their mission. SAVI provides only a partial measure of system effectiveness as it does not address the capability of the response force to neutralize the adversaries after they have interrupted. The overall measure is called the probability of effectiveness, P(E). P(E) is calculated by combining the interruption and neutralization measures by the equation:

$$P(E) = P(I) \times P(N).$$

In the methodology presented here, the evaluation of overall effectiveness is accomplished in two stages: 1) SAVI is used to calculate P(I), and 2) P(N) is independently estimated by the analysis team based on adversary and response force capabilities, protection features, and tactics.

Security Framework

Before using SAVI, a security framework must be established. This framework includes 1) threat definition, 2) facility characteristics, and 3) target identification.

Threat Definition

The site-specific threat must be defined in terms of adversary type, objective, and capability. The SAVI model addresses two types of threat: 1) outsider adversaries acting alone, and 2) outsiders in collusion with a single non-violent insider. The adversary objective can be either theft or sabotage, but the training example is based on a theft scenario. It is assumed that the adversaries have equipment and explosives and are knowledgeable, well-trained, and armed. They may have vehicles, including helicopters. The insider is assumed to be knowledgeable and may assist by opening emergency doors, ignoring alarms, or other unauthorized actions. The number of adversaries is not directly used in the calculation of P(I).

SAVI performs both theft and sabotage vulnerability analyses by calculating the value of P(I) for each path and listing the most

vulnerable paths. As noted previously, the analysis for theft can be based on either the assumption that adversaries are interrupted before they can accomplish removal of target material from its normal location or that they are contained (i.e., that interruption occurs at the site perimeter). For sabotage, the analysis is based on the assumption that adversaries are interrupted before completion of their sabotage task at the target location.

SAVI incorporates two conservative assumptions: 1) adversaries have knowledge of the protection system characteristics, and 2) they use an optimal penetration strategy - minimizing detection until the remaining delay time is less than the RFT, then minimizing delay without regard to further detection. As discussed more fully below, the second assumption makes it possible for SAVI to consider delay times independent of detection probabilities, because at each point on the path, the adversary is concerned with either delay or detection, but not with both. These two assumptions ensure that the most vulnerable paths are identified and provide a worst-case bound on system effectiveness.

Facility Characteristics

Site layouts, plan, and elevation drawings of buildings containing potential targets should be compiled. A description of plant processes, systems, and operations should be obtained. Operational and safety procedures and concerns should be reviewed. Also, specifications and operational information on existing protection system components should be available.

Target Identification

The location and description of all of the potential targets in the facility should be compiled. A priority ranking of targets based on consequences should be made.

MODEL DESCRIPTION

After the security framework has been established, SAVI is used to construct a site-specific model of the facility protection system and to analyze its effectiveness. The model has four parts: 1) a graphic representation of the facility, called an adversary sequence diagram, 2) a set of protection element detection and delay values (obtained from component lists), 3) a response force time determination, and 4) an algorithm that calculates P(I) for all of the potential adversary paths to the target, and ranks the ten most vulnerable paths. Each of these parts is described below.

Adversary Sequence Diagram

In order to use a computer model to represent a PPS, it is necessary to transform the salient features of the facility and protection system into a two-dimensional logical structure which accurately represents these features. SAVI accomplishes this by using a graphical representation called an adversary sequence diagram.

Generic Adversary Sequence Diagram

SAVI considers a generic facility, Figure A-2, that is comprised of a sequence of six concentric physical areas: 1) off-site, 2) limited area, 3) protected area, 4) controlled building, 5) controlled room, 6) target enclosure; and a target. It models the protection system for this facility using the concept of a generic adversary sequence diagram (ASD). The generic ASD consists of the six physical areas which are separated from one another by protection layers as shown in Figure A-3. Each protection layer is comprised of a continuous set of protection elements. The adversary attempts to sequentially defeat an element in each layer as he traverses a potential path through the facility.

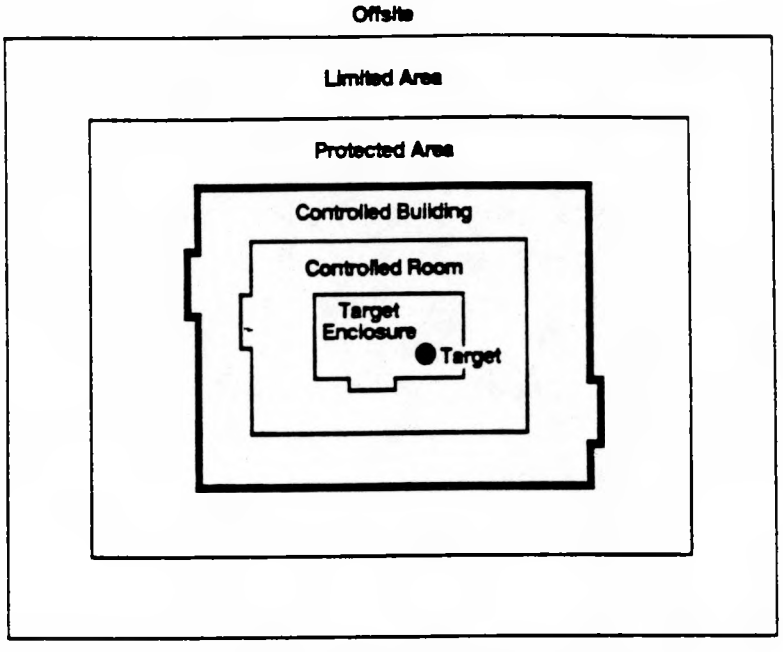


Figure A-2 Basic Areas at a Generic Facility

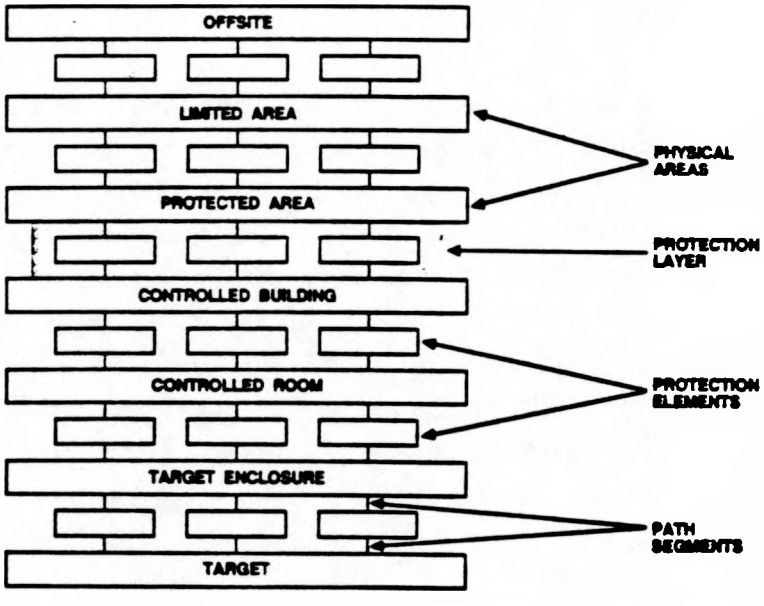


Figure A-3 Adversary Sequence Diagram Conceptualization

The detection and delay functions provided by each PE depend on which components the adversary attempts to defeat using either force or deceit. Figure A-4 shows a PE with its input and output path segments. These segments are where the aggregate delay and detection values are assigned. On each segment, delay is considered before detection because it is usually the penetration of a barrier that sets off the associated detector. However, if this is not the case, detection can be considered before delay by assigning the input delay to the output path segment. This is done by using the write-in setting feature on the component lists.

SAVI can model both entry and exit parts of a path. The entry part is from off-site to the target, and the exit part is from the target back to off-site. A given PE may be traversed once, either on entry or on exit, (i.e., independent traversal); or it may be traversed twice, on entry and in the opposite direction on exit (i.e., dependent traversal). Note that the input and output segments refer to transversal of the PE as the adversary approaches the target during entry. If the element is traversed on exit as he leaves the target location, the output segment is then encountered first.

The SAVI generic ASD utilizes a set of fifteen basic elements, listed in Table A-1, that were compiled from those typically found at DOE facilities.

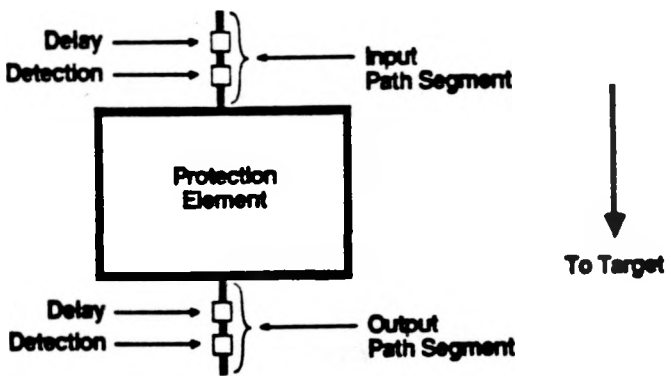


Figure A-4 Delay and Detection Relationship on Path Segments

Figure A-5 shows the complete ASD used in SAVI to model the generic facility using six physical areas and fifteen PEs.

If adversaries are to be interrupted before sabotage or removal tasks are completed at the target location, then the ASD shown in Figure A-5 represents all of the entry paths. In this case, the PEs are traversed in only one direction; only delay and detection values associated with the entry path are used to calculate the P(I). However, if adversaries are to be interrupted before exiting the site boundary (i.e., contained), then the ASD shown is utilized both on entry to the target and on exit from the target.

When the entry-exit case is evaluated, the total number of possible paths represented by the ASD in Figure A-5 is the number of entry paths squared. Additionally, some of the possible exit paths will include PEs that were traversed by the adversary during entry. The exit delay and detection values associated with these PEs depend upon the way the adversary defeated the element at entry. For example, if explosives were used to penetrate a wall during entry, then the delay would be zero at exit. SAVI uses a component data base that includes the appropriate dependent and independent detection and delay values for force and deceit scenarios.

Site-Specific ASD

A site-specific ASD is constructed for each target, or set of targets having a common location, by utilizing the generic ASD together with facility and PPS layout and drawings. The objective is to correctly model the PPS that currently exists at a site or to model an upgrade that is being considered. This site-specific ASD is created by selecting those elements that are present at the facility from the complete set presented in the generic ASD.

Figure A-6 shows a simplified sample facility and PPS layout. Figure A-7 shows the resulting site-specific ASD that is constructed by SAVI when the analyst uses the information given in Figure A-6.

DOR	Door	PER	Personnel Portal
EVC	Evacuation Shelter	RAL	Rail Portal
FEN	Fence	SHP	Shipping Area
GEN	Generic Element	SUR	Surface
GAT	Gate	TSK	Task
HEL	Helicopter Flight Path	TUN	Tunnel
ISO	Isolation Zone	VEH	Vehicle Portal
MAT	Material Portal		

Table A-1 Protection Elements

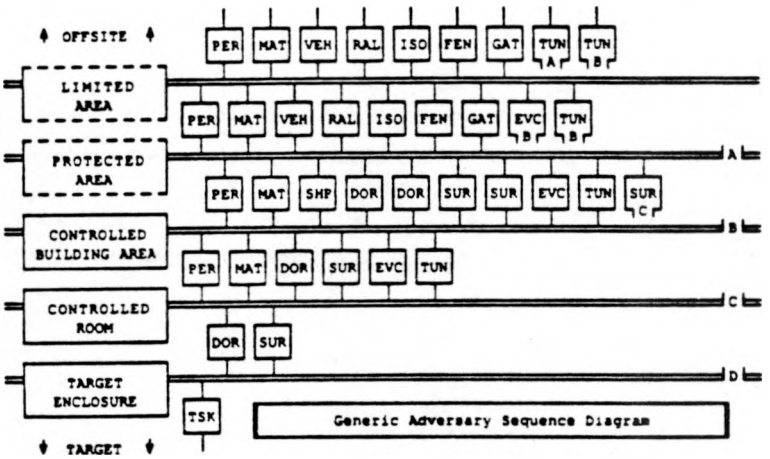


Figure A-5 SAVI Generic Adversary Sequence Diagram

ASD Jump and Bypass Features

Deviations from the orderly sequence of physical areas and protection layers that comprise the generic ASD will often be necessary in order to create an accurate site-specific ASD. Jump and bypass features are

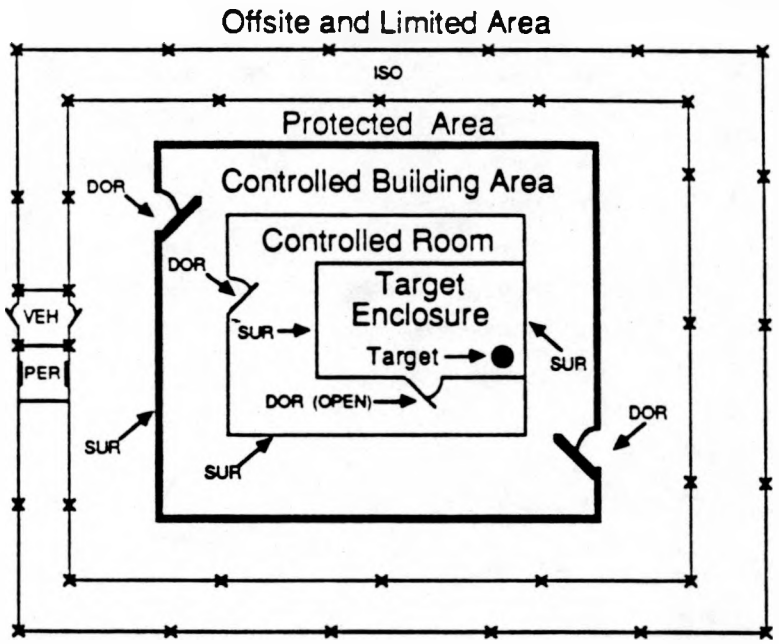


Figure A-6 Sample Facility

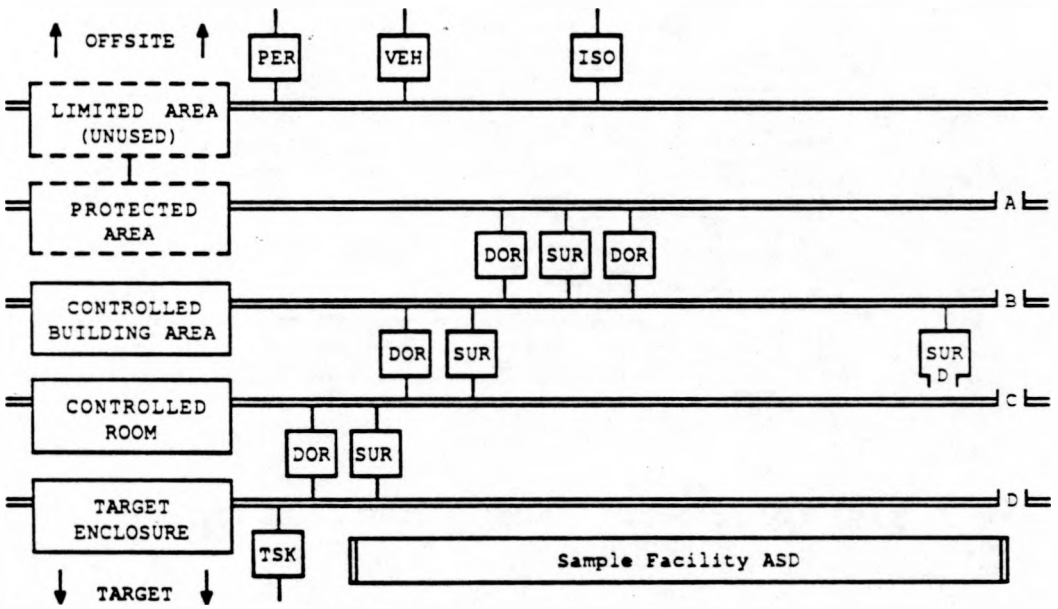


Figure A-7 Sample Facility ASD

included in the SAVI modeling technique. A jump is used to model a site element that does not directly connect to the adjacent area shown on the generic ASD. A bypass is used to model the absence of a protection layer.

ASD Jump - As shown in Figure A-6, there is a wall common to the controlled building area and to the target enclosure making it possible to go directly to the target enclosure without passing through the controlled room. This situation is modeled (in Figure A-7) by using the "SUR" jump element with the letter "D" at the bottom and placing it after the controlled building area. In Figure A-7, the site-specific ASD then shows a direct path from the controlled building area to the target enclosure in addition to all other selected indirect paths.

ASD Bypass - It is possible to bypass features of the generic ASD by eliminating all of the elements in a layer. If, for example, as shown in Figure A-6, a facility does not have a limited area. The resulting site-specific ASD configured by SAVI would have a direct connection between the off-site area and the protected area. The bypass is accomplished by eliminating all of the protection elements in the layer between the limited area and the protected area. Figure A-7 also shows this bypass.

Threat Specification

Attributes

Because of the availability of arms, penetration tools and equipment, and explosives, SAVI assumes all adversaries will carry them. Three modes of transportation are considered - foot, vehicle, and helicopter; and the analyst can select any one of these for analysis.

Other conditions that must be considered are whether the attack occurs during day-shift, off-shift, or emergency plant states. This is done by selecting those components that are operative for the specified state from the component lists provided for each element. The threat where outsiders act in collusion with an insider is also considered by setting zero value to the components that the insider could defeat. SAVI does not directly input the number of adversaries. However, the size of the adversary force must be considered in estimating the response force time.

Objectives

The objective of the adversary may be to sabotage the facility or to steal material. SAVI considers the objective together with the response force strategy of interruption.

In the case of sabotage, interruption must occur prior to or at the hands-on actions necessary for sabotage.

In the case of theft, a conservative strategy of interruption prior to or at the target, before the adversary can effect hands-on removal of material, can be used. Alternatively, a strategy of theft containment can be used whereby the adversary is interrupted prior to or at the site boundary.

SAVI provides the capability of selecting a hands-on theft or sabotage strategy that models a worst-case interruption at the target. It also provides for selection of a theft containment strategy that models a worst-case interruption at the site boundary.

Response Force Time

The response force time (RFT) is the time for arrival of the appropriate number of response personnel at the specified deployment point after receiving the first alarm. The RFT includes assessment, communication, and deployment time. The specified value for RFT can be based on actual field trials or on estimated performance. The analyst must determine the appropriate response force stations and deployment locations so that the interruption objective can be met. After the ten most vulnerable paths are calculated based on an initial estimate of RFT, the analyst may want to change the deployment configuration and RFT based on the vulnerable path exit locations and then rerun the analysis.

The RFT should be based on time to deploy a sufficient number of response persons to stop the forward progress of the adversary long

enough to allow for reinforcements to arrive. This initial number will vary depending upon many factors, such as the number of adversaries and the amount of exposure of the on-site forces.

COMPONENT SELECTION LISTS

The SAVI model uses a systematic procedure for obtaining a complete list of components associated with each PE of the specific ASD. Component selection lists are provided that contain the typical candidate components for a particular element. Also listed are reference detection and delay values for these components that experience has shown to be realistic. Two forms of the same component lists are provided: 1) hard-copy lists for use in the field component identification process and 2) computer display windows that allow transfer of component information from hard-copy to computer and subsequent processing in the path analysis algorithm.

SAVI uses mean or average-value point estimates of performance based on a worst-case adversary attack. It assumes that data links, alarm and assessment units, and security procedures are reliable. The reference values for component performance are generally based on field experiments performed under varying conditions at DOE national laboratories and other facilities. When adequate test data is not available, engineering judgement is used. Actual component performance depends upon many factors such as initial quality, installation and maintenance procedures, security procedures, and adversary capabilities. If any of these factors are substandard or if there are single-point vulnerabilities or other common-mode failures, then the reference or analyst-selected mean values of performance should be degraded to reflect realistic performance. Good data on the standard deviation from the mean value of performance is not generally available. Therefore, if there is concern about the accuracy of the mean value, the analyst should vary it and rerun the analysis to determine the effect on P(I). Whenever possible, component performance values should be obtained by tests conducted at the facility being evaluated.

The analyst takes the component lists for each PE to the field and marks the components on the lists that most closely represent the existing ones. Alternatively, he can write in his own estimated

values if there is no reference component that is sufficiently similar to the one at the site.

Component-Threat Considerations

The hard-copy component lists show values for one threat, namely adversaries on foot with equipment and explosives. However, the component lists in the computer model are configured to allow the SAVI code to show component performance values for three different threat capabilities: 1) on foot with equipment and explosives, 2) in a vehicle with equipment and explosives, and 3) in a helicopter or aircraft with equipment and explosives. For example, if adversaries are on foot, then a zero delay time for vehicle barriers is selected. If adversaries are in a vehicle, then the appropriate vehicle barrier delays are selected. If adversaries use a helicopter, either the limited or protected area (or both) may be jumped by using the helicopter element.

For all paths that include the helicopter element, SAVI considers that the adversary travels over the jumped area by helicopter on both entry and exit. All other elements on that path, and on all other paths that do not include the helicopter element, are considered to be traversed by foot.

For a scenario including collusion with an insider, the appropriate component values are selected by the analyst. For example, for emergency doors with panic bars, a zero time delay is used even though the door is normally locked, because the insider can open it for the outsider adversary.. If a guard badge check is used with the guard postulated to be the insider adversary, a zero detection probability would be selected for the identity check value at that location.

SAVI CALCULATION OF PE AGGREGATE DELAY AND DETECTION VALUES

There are many ways an adversary can attempt to defeat a PE. For example, an adversary can attempt deceitful passage through a portal by counterfeiting a credential and smuggling contraband. Alternatively, he can force open or penetrate the portal doors or penetrate the walls with tools or explosives. The appropriate detection and delay element values for each defeat method are automatically calculated by combining the appropriate component values. The aggregate values for the worst-case method of defeating the element are then used in determining the path vulnerability.

Figure A-8 shows an example of a personnel portal protection element that typically has several components that act together to perform detection and delay functions. The individual values of components that work together are aggregated or combined by the SAVI code, as shown in Figure A-9 . The force or deceit delay times (t) for the individual components are added to obtain the aggregate delay time (T). The non-detection probabilities ($\bar{p}$) for the individual components are multiplied and subtracted from one to obtain the aggregate detection probability (P). It should be noted that the non-detection probability is given by $\bar{p} = 1-p$.

Component Element, and P(I) Value Truncation

The field tests of component delay times give results that are usually valid to a few seconds, so delay values are given to the nearest second. The field tests of component detection probabilities give results that are usually valid to two-figure accuracy, so these detection values are truncated to two-place significance. Because the element aggregate detection probability is usually obtained from two or more detectors, the PE detection values are truncated to three-place significance. Also, because a path generally is comprised of several PEs, the P(I) values are truncated to four-place significance. Truncation of the path P(I)s in this manner allows a practical ranking of paths without presenting more accuracy in the results than is warranted by the input data.

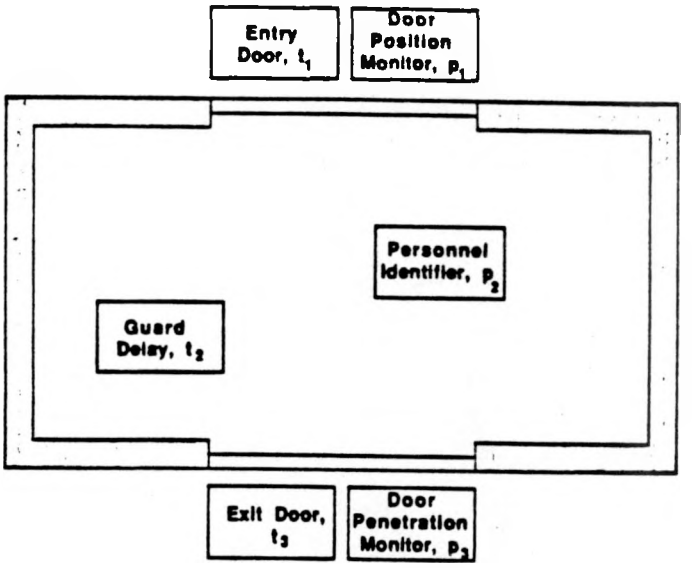


Figure A-8 Personnel Portal Element

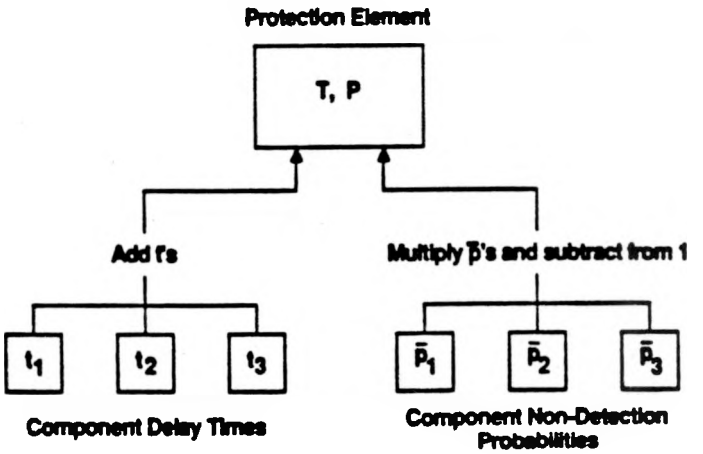


Figure A-9 Element Aggregate Delay and Detection Values

Although conservative estimates of component values are used, some analysts will be concerned that the resulting P(I) values do not accurately reflect actual PPS vulnerabilities. In this case, they can put lower estimates on the component values. It is important to realize that the P(I) measure gives a realistic relative ranking among paths. It should be used as an absolute measure of PPS effectiveness only when validated by component performance tests and by field tests conducted at the facility.

Transit Times

SAVI considers two types of adversary transit times - 1) area transit times, and 2) element transit times. SAVI automatically calculates traversal times for the current threat transportation mode when the analyst has input the site-specific distances. For the physical areas, the analyst initially uses the minimum distance required to traverse the area to reach the next area. For the elements, the distance across the element, such as a tunnel or isolation zone is used.

After SAVI calculates path P(I)s, the analyst may decide to rerun SAVI using actual area transit distances along a path rather than minimum distances. If a path is one of the most vulnerable ones, the analyst determines the actual distance from one physical area to the next physical area when the adversary actually goes through each specific PE on the path being analyzed. He then replaces the minimum area distances with these specific distances and reruns SAVI to see if the path is still one of the ten most vulnerable ones.

THE SAVI P(I) CALCULATION ALGORITHM

For interruption to occur, two conditions must be met: 1) the adversaries must be detected, and 2) they must be detected while there is still time for the response force to arrive. Therefore, the optimal adversary strategy is to avoid detection until a point on the path is reached where the minimum delay time remaining, TR, is less than the response force time, RFT. After this point, detection is ineffective because there is no longer enough delay to allow interruption.

This strategy can be demonstrated by considering the relationship of detection, delay, and response along a path. On the ASD, a path consists of an ordered sequence of protection elements through the facility to the mission completion point. However, a path can also be represented by an event line as seen in Figure A-10a. This line represents the events on the path the adversary takes from off-site to the end location. The dotted part of the line is the distance already traversed by the adversary, and the solid part of the line is the time remaining to mission completion (TR). The events shown on the line are: 1) the location of the detection components p1, p2, etc., 2) the accumulated delay times T1, T2, etc., representing the sequence of delays provided by barrier, delay components, transit and task times, and 3) the point where the TR is equal to the RFT; namely TR*.

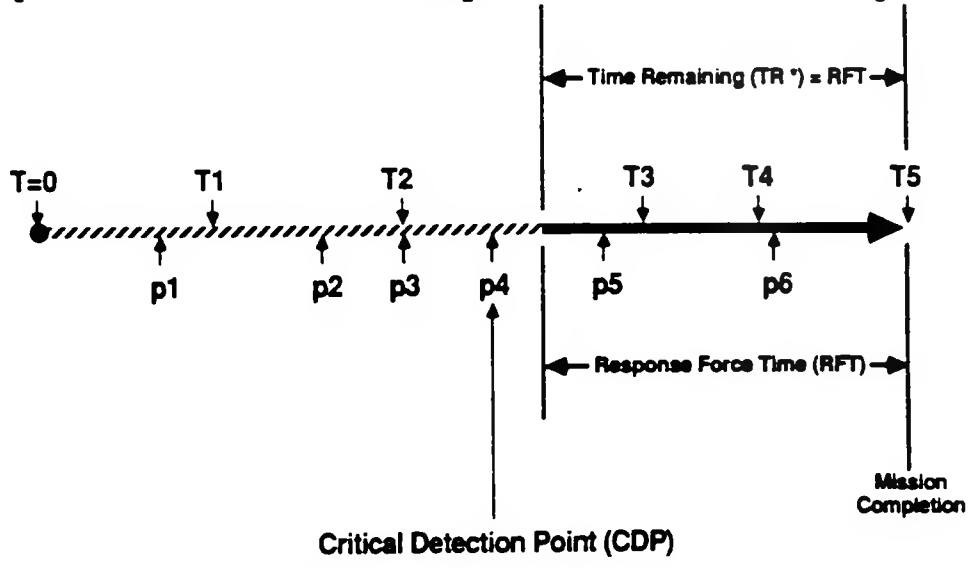


Figure A-10a Adversary Path Event Time Line

The first detection point encountered on the line prior to TR* (in this case p4) is called the critical detection point, CDP, because detection must occur either before or at this point for interruption to occur. It should be noted in Figure A-10b that detectors located beyond the CDP (in this case p1 and p2) are ineffective. Even if the adversary is detected after the CDP, the remaining path delay is insufficient to allow the timely arrival of the response force after they receive the alarm.

A path can have a CDP but still have a P(I) = 0. This occurs if the total path time (in this case t5) is greater than the RFT, but there is no detector on the path prior to the TR* point as shown in Figure A-10b. Furthermore, there must be a CDP on the path for interruption to occur. If the total path time is less than the RFT as shown in Figure A-10c. then there is no CDP and P(I) = 0.

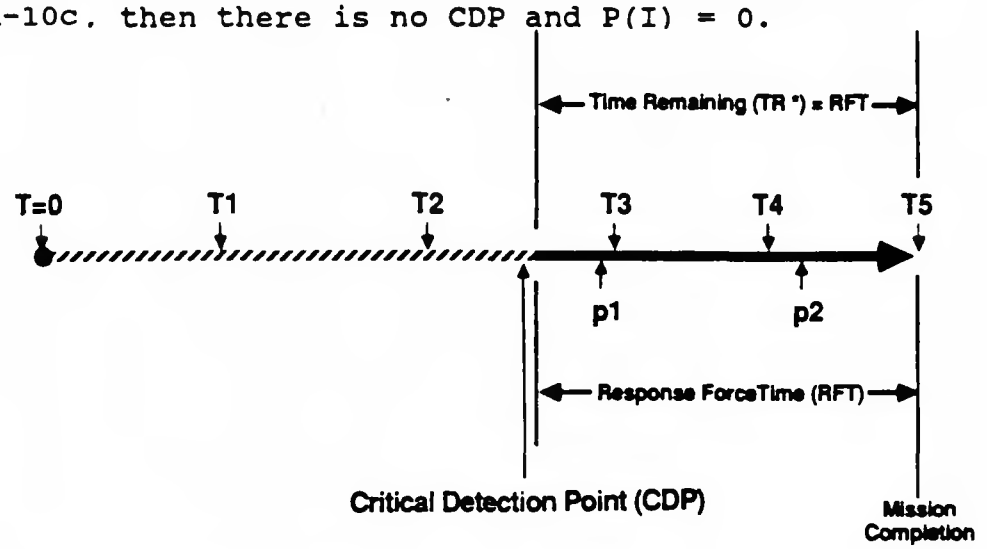
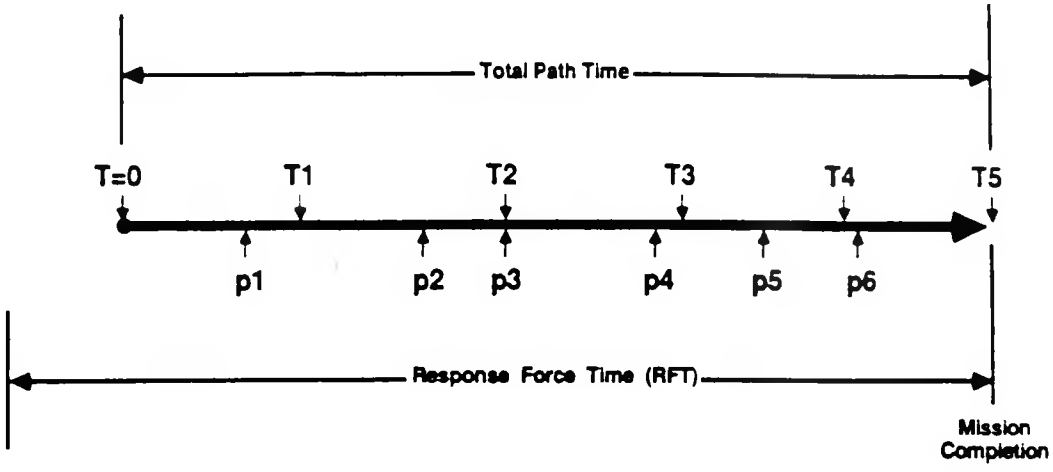


Figure A-10b Adversary Path Event Time Line

Stated more fully then, the optimal strategy is the one that would be used by an adversary who knew all the delay and detection values, the RFT and who could make the same calculations as SAVI does. He would proceed along a path minimizing detection until the remaining time to target is less than the response force time, and then minimize delay without further regard to detection. This strategy decouples the detection and delay functions because the adversary attempts defeat



Total path time is less than RFT, so there is no TR * or CDP on the path.

Figure A-10c Adversary Path Event Time Line

of either the element delay or the detection components depending on whether or not he has passed the CDP. Because delay is thus decoupled from detection, the calculation algorithm is simplified.

Based on this optimal strategy, the SAVI path P(I) calculation algorithm: 1) starts backward from the last task at the target (or the path end point), 2) locates the TR* point by summing the minimum delays for each element until they equal or just exceed the RFT, 3) locates the CDP at the first detector encountered prior to the TR* point, 4) if there is a CDP, then it accumulates detection probabilities from the CDP to off-site to obtain P(I), 5) calculates the minimum delays from the CDP to the target (or path end point) and subtracts the RFT to obtain the time remaining after interruption, and 6) if there is no CDP on the path, it sets P(I) equal to zero.

SAVI ANALYSIS

The SAVI analysis procedure consists of three steps: 1) input data and execute SAVI, 2) perform upgrade analyses, and 3) perform sensitivity analyses.

Input Data and Execute

The site-specific ASD is created by selecting the PEs at the facility. The detection and delay data from the component lists for the selected threat, target, plant state, and site-specific PPS is entered into the SAVI program. Area and element transit distances are entered. The value of the RFT is entered and after all inputs are checked for accuracy, the analysis is executed.

The SAVI code determines the value of P(I) for each path scenario on the ASD. It lists the first ten most vulnerable path scenarios and ranks them in order of their vulnerability. If two paths have the same P(I), then they are ranked on the time remaining after interruption (TRI) that the adversary still needs to completes his mission. Before deciding that the P(I) value for a given path is acceptable, the TRI should be reviewed to see if there is a sufficient surplus time to ensure interruption if the response is actually somewhat longer than estimated.

Upgrade Analyses

SAVI does not determine whether the P(I) values are acceptable; the analyst must make that determination. SAVI does provide assistance for the analyst in considering possible upgrades to the most vulnerable path scenarios. A blinking arrow is displayed on the path segment of the element where the CDP is located. The direction of the arrow shows whether it is on the entry or exit part of the path. Also, each path element displays whether it has been defeated by force or deceit. If defeat is by force, the side of the element is broken. Thus, the ten worst-case scenarios and their P(I)s and TRIs are presented.

SAVI displays a "Cumulative Path Delay Deficiency" warning if the cumulative path delay is less than the RFT, which means that there is no CDP on the path and P(I) = 0. When there is a CDP on the path, recommendations are shown stating that a path can be upgraded by adding detectors to path segments prior to the CDP. Adding them at the beginning of the path is generally preferred if costs allow. A path can also be upgraded by adding delay to path segments past the CDP. Adding delays close to the target or at the surfaces and entryways of buildings and rooms is generally preferred.

It is left to the analyst to determine whether the vulnerability is caused by inadequate detection, insufficient delay, or both. Furthermore, even though P(I) is adequate, the analyst may decide that the TRI is marginal and more delay or faster response is needed. SAVI displays the RFT as well as the surplus or deficiency in TRI which assists the user in making this determination.

Alternatively, the analyst may determine that protection is not balanced with some paths having insufficient or excessive delay or detection relative to other paths. Furthermore, some paths may not have protection in depth and instead concentrate protection in a single element. It is good design practice to obtain the required P(I) by using more than one layer of protection.

A number of upgrade alternatives should be considered before a final upgrade design is selected. Both hardware and response force upgrades should be considered and the necessary delay/response trade-off studies made. For example, it may be more cost-effective to reduce the response deployment time by stationing forces at different locations than by adding concrete walls.

In reviewing the vulnerable paths, the presence of an element that is common to many paths should be sought. The addition of an element that is not in the current ASD should be considered especially if it can reduce common path vulnerabilities. Also, there may be "quick fix" upgrades that produce large changes in PPS effectiveness for small costs and these should be looked for. A survey of all of the

most vulnerable paths should be made before any upgrade decisions are made.

If all of the paths have very high P(I)s, then it is likely that unrealistic component detection and delay values were selected. The analyst should reconsider these values to be sure that they are justified.

Three types of graphs, shown in Figures A-11, A-12, and A-13, are produced by SAVI: 1) a graph showing P(I) and TRI for each of the ten most vulnerable paths when an RFT is specified, 2) a graph showing the distribution of P(I)s by giving the percentage of path scenarios that have a given P(I) value, and 3) a graph showing the variation of the worst-case path P(I) with changes in RFT.

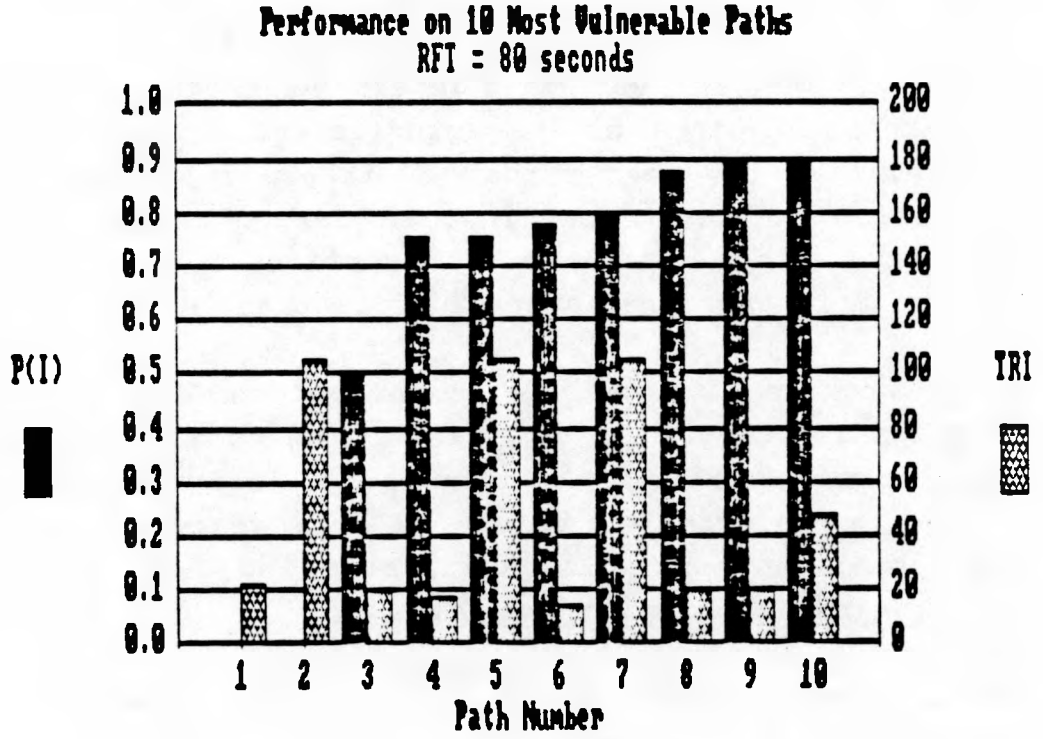


Figure A-11 P(I) and TRI as a Function of Response Time

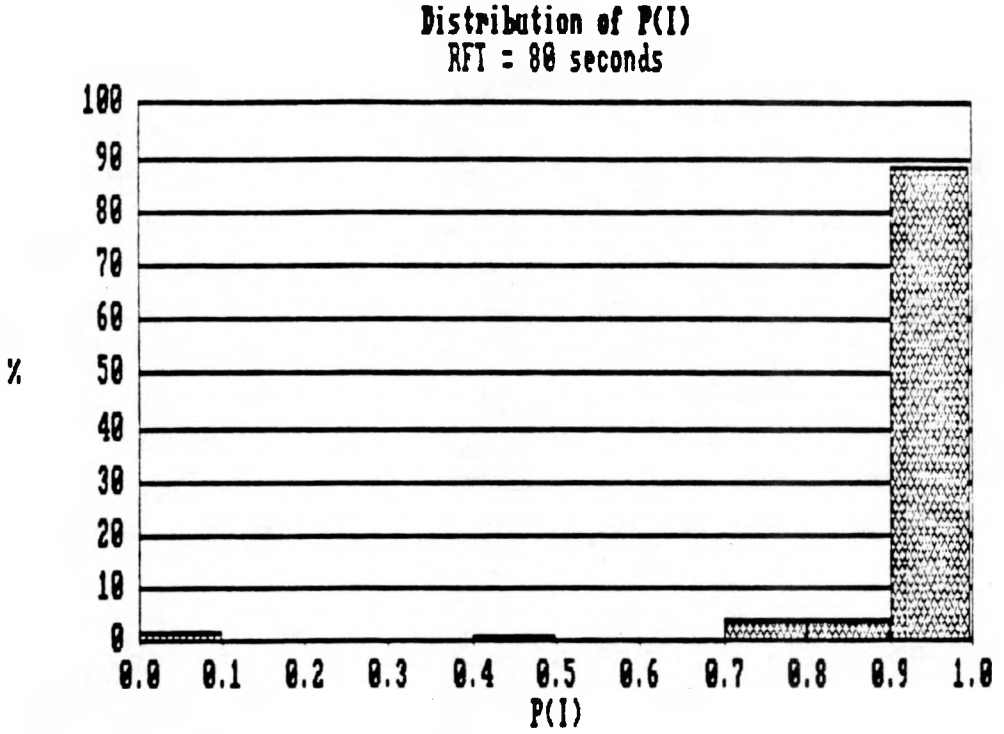


Figure A-12 Distribution of P(I) for All Paths and Specified RFT

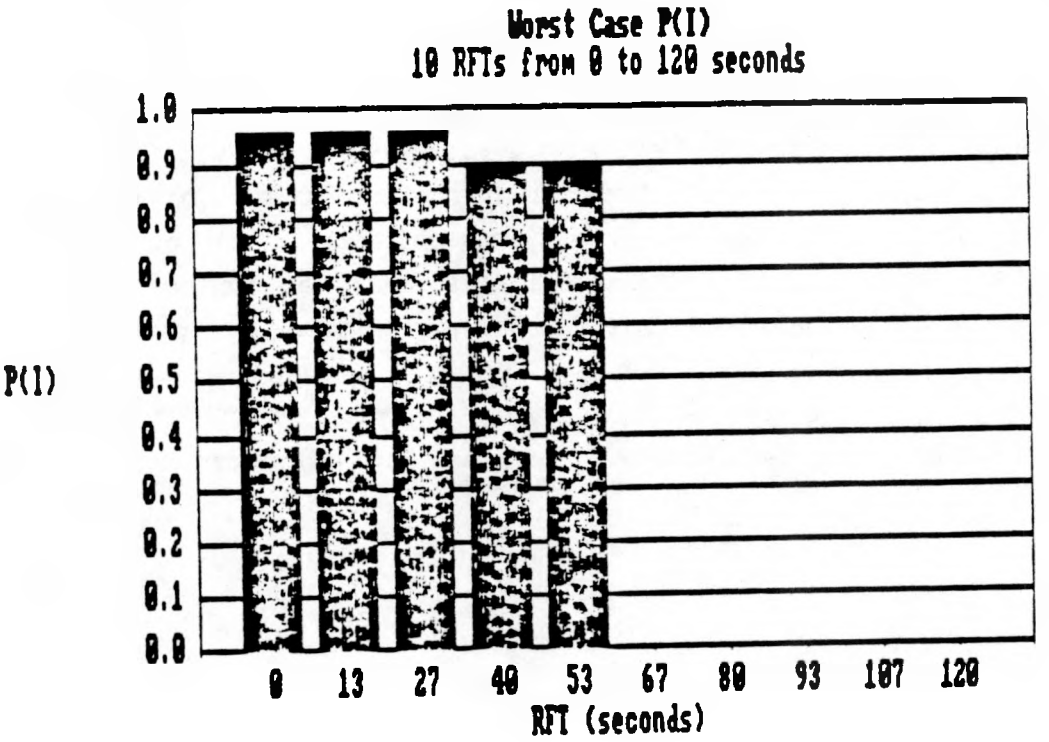


Figure A-13 Worst-Case Path P(I) for Each RFT in Range

Sensitivity Analyses

Sensitivity analyses are performed on a PPS design to determine the effect of incremental changes in the elements and components, and in the response capabilities. An intelligent analysis can uncover places where relatively small changes can produce significant improvements in PPS effectiveness. It can also uncover whether small changes in RFT can result in large changes in P(I). Because the most critical PPS parameter is RFT, SAVI allows the analyst to vary the RFT over a specified range and then calculates the variation in P(I) over this range for worst-case vulnerable path. Figure A-13 shows this graph of the variation in P(I) with RFT.

Detailed analysis of a single path can be done after SAVI has calculated the P(I)s for a specific PPS. By constructing a new ASD consisting of only path, any of the vulnerable paths listed by SAVI can be analyzed to determine the effect of changing elements on that path, components in an element, area or element transit times, and response force time.

Changes can also be made to the specific ASD by adding or deleting elements with postulated aggregate element values. This approach allows a rapid means of determining whether a "quick" fix is useful. If a useful change is uncovered at this level of analysis, then a more detailed look at the proposed element to determine what components are necessary to obtain the specified aggregate performance can be made.

Finally, if all paths have very high (.9999) values for P(I), a sensitivity analyses based on varying component performance values should be made.

SUMMARY

SAVI models a facility protection system and evaluates its effectiveness against a specified threat and specified target. The model results are based on performance at the component level - the level at which the adversary attempts system defeat. Current knowledge and experience on component performance is utilized.

SAVI calculates the value of P(I) for each path scenario on the ASD but does not determine whether the P(I) values are acceptable; the analyst must make that determination. SAVI does provide help for the analyst in considering possible upgrades to the most vulnerable path scenarios. It lists the first ten most vulnerable paths and ranks them in order of their vulnerability. If two paths have the same P(I), then they are ranked on the time remaining to complete the adversary mission after interruption occurs. The location of the critical detection point on each path is displayed and prior to this point, the path can be upgraded by adding detectors. A path can also be upgraded by adding delay past this point.

The site-specific ASD data files and printouts are permanent records of protection system designs and performance. Once the initial configuration of the baseline PPS at a site is modeled, both sensitivity and upgrade analyses can be performed and recorded quickly and easily.

ATTACHMENT A-1

DESCRIPTION OF PROTECTION ELEMENTS

There are 15 different protection elements as shown in Table A-A1. Each element is composed of delay and detection components. These components are the links in the protection chain that the adversary attempts to defeat. The components work together to perform a unique security activity.

DOR	Door	PER	Personnel Portal
EVC	Evacuation Shelter	RAL	Rail Portal
FEN	Fence	SHP	Shipping Area
GEN	Generic Element	SUR	Surface
GAT	Gate	TSK	Task
HEL	Helicopter Flight Path	TUN	Tunnel
ISO	Isolation Zone	VEH	Vehicle Portal
MAT	Material Portal		

Table A-A1 Protection Elements

A brief description of each protection element is given below. A layout of each element is provided that shows the components that comprise the element.

Note that on many elements the terms input and output components are used. Input and output segments (on which the components are located) refer to the traversal of a PE as the adversary approaches the target during entry. When an element is traversed by the adversary as he leaves the target and exits the facility, the output segment components will then be encountered first.

Door

A single controlled door, shown in Figure A-A1, is a protection element that allows unrestricted passage of authorized persons, vehicles, and material and impedes passage of unauthorized persons, vehicles, and material. All doors that are not part of a portal are modeled using this construction. It should be noted that portals have dual-interlocking doors.

If a controlled door is used for normal authorized passage, it will either be remotely operated or a security guard will be present. When remotely operated, identification is usually by CCTV credential or badge verification, although other means may be used. Controlled doors are generally used to allow infrequent authorized passage. They are usually unlocked only when a security inspector is present. However, if they allow emergency exit, they have an interior panic bar. This feature provides no delay if an insider adversary is present to open the door using the panic bar.

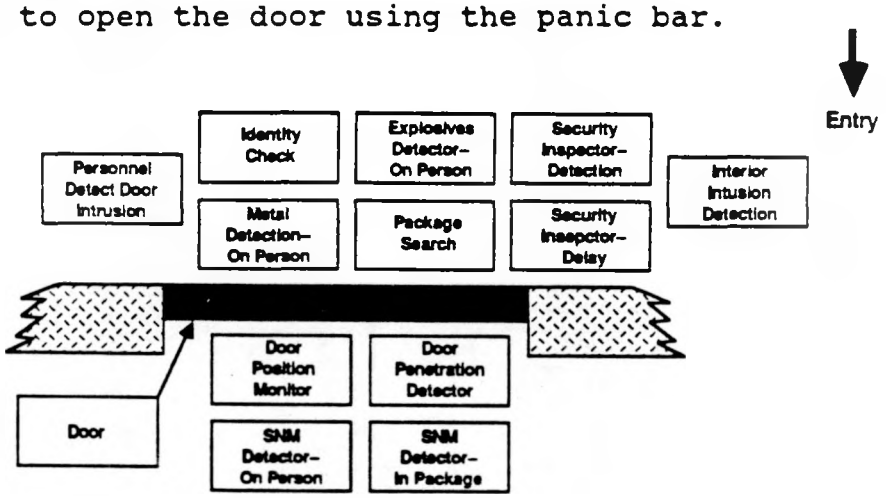


Figure A-A1 Door

Evacuation Shelter

The evacuation shelter PE models a safe haven type of evacuation system. Currently, most facilities do not have safe-haven evacuation shelters and evacuation is via a panic-bar emergency exit door. If

this is the case, the DOR PE, rather than the EVC PE, is used to model evacuation.

The evacuation shelter, PE, shown in Figure A-A2, is configured as a protection element that provides a secure emergency exit to a safe haven and eventual exit to a protected area.

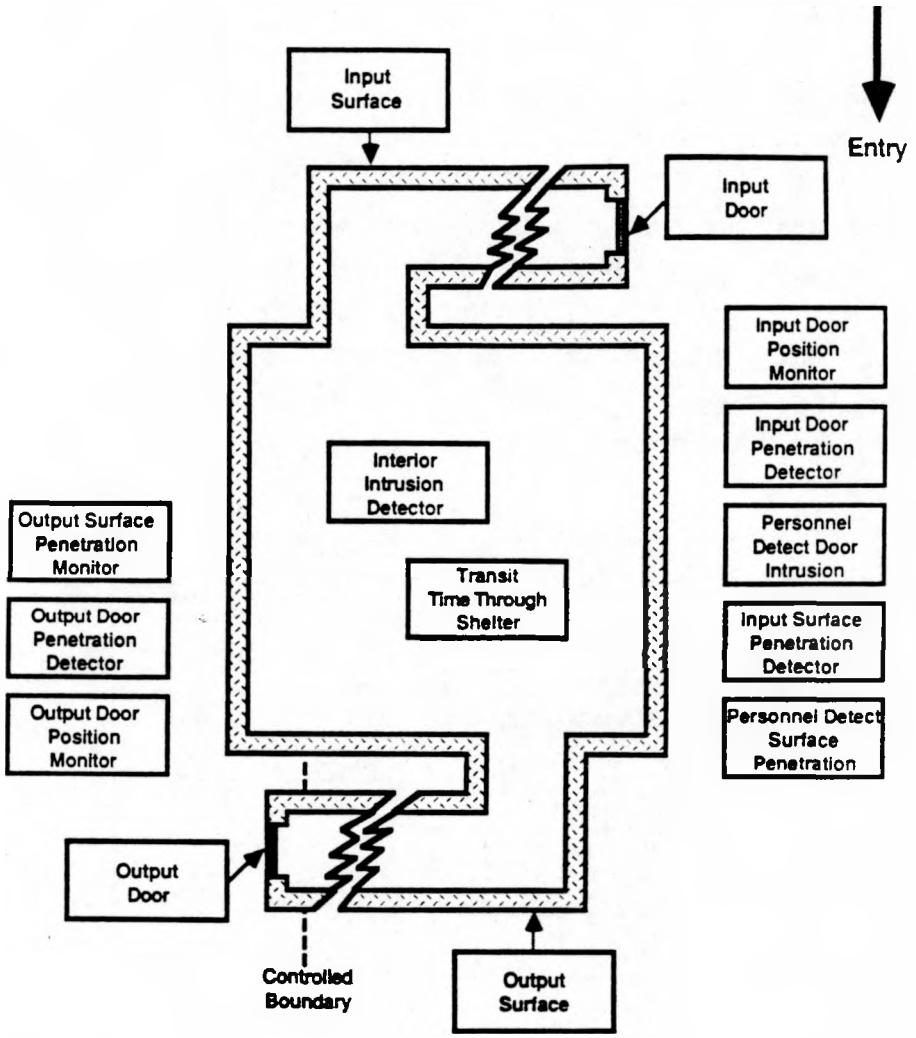


Figure A-A2 Evacuation Shelter

Fence

A single fence, shown in Figure A-A3, is a protection element that impedes passage to a limited area or to a protected area. It is used if the facility does not have the standard dual-fence isolation zone around the protected area.

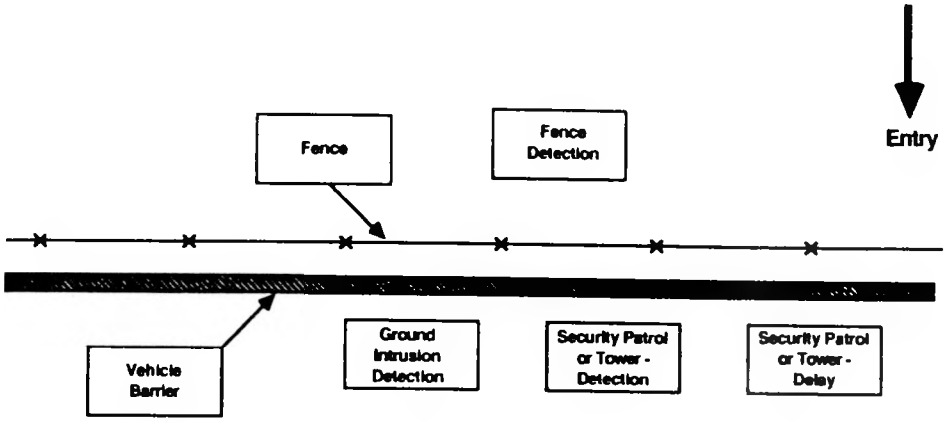


Figure A-A3 Fence

Generic Element

The generic protection element, shown in Figure A-A4, is provided to enable the analyst to model a situation not covered by any of the standard elements. It should be noted that when this element is used, the detection and delay values of the element must be calculated to give the worst-case force or deceit scenario values for each threat. These values are used for the SAVI input when a specific threat is analyzed.

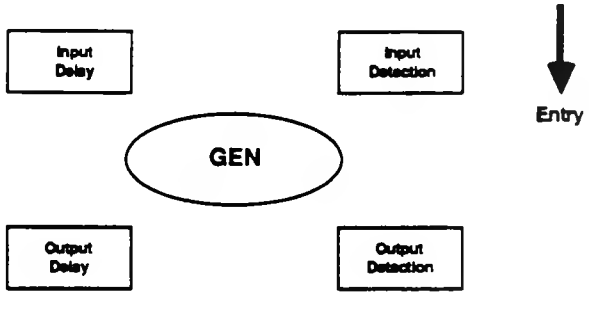


Figure A-A4 Generic Element

Gate

A single gate, shown in Figure A-A5, is a protection element that impedes vehicle or personnel passage. It is generally associated with a single fence barrier system where a standard vehicle portal is not installed.

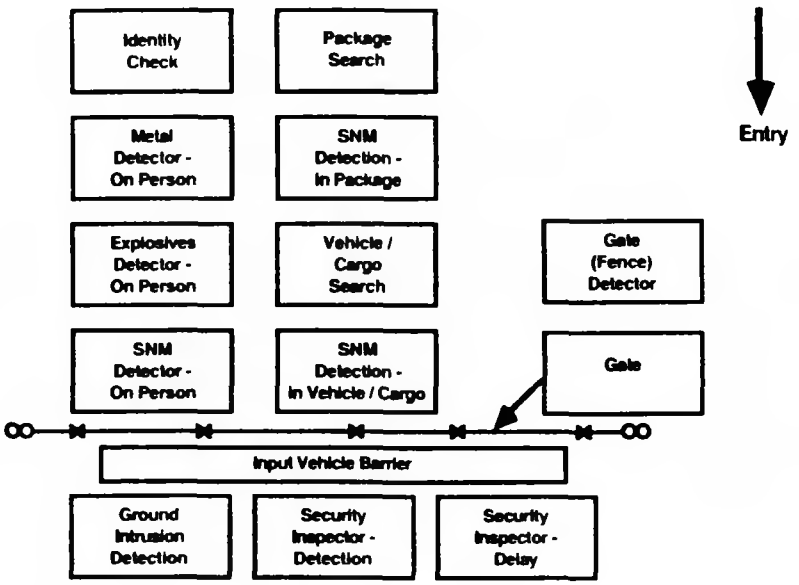


Figure A-A5 Gate

Helicopter Flight Plan

The helicopter flight plan protection element, shown in Figure A-A6, is used to model the traversal of physical areas by an aircraft. It is included as a PE because there is delay and detection associated with the flight path. This element can be inserted in the ASD only when the adversary attributes include a helicopter.

Isolation Zone

An isolation zone, as shown in Figure A-A7, is the protection element surrounding the perimeter of a facility that impedes unauthorized passage to the protected area. It provides the first line of defense against intrusion. It generally is made up of two chain-link fences

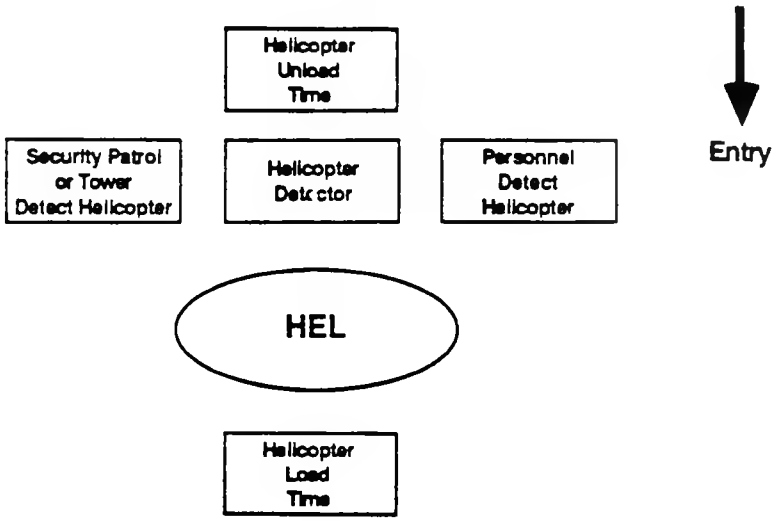


Figure A-A6 Helicopter Flight Plan

with intrusion detectors along the outer fence, between the fences, and on the inner fence. A vehicle barrier typically runs just inside the inner fence to delay motorized attack. The roofs of buildings that span the isolation zone should have detection and delay equivalent to that of the ground system. Care must be taken in the installation of the detection system to ensure that no detection gaps occur at zone transition points such as vehicle portals and building walls.

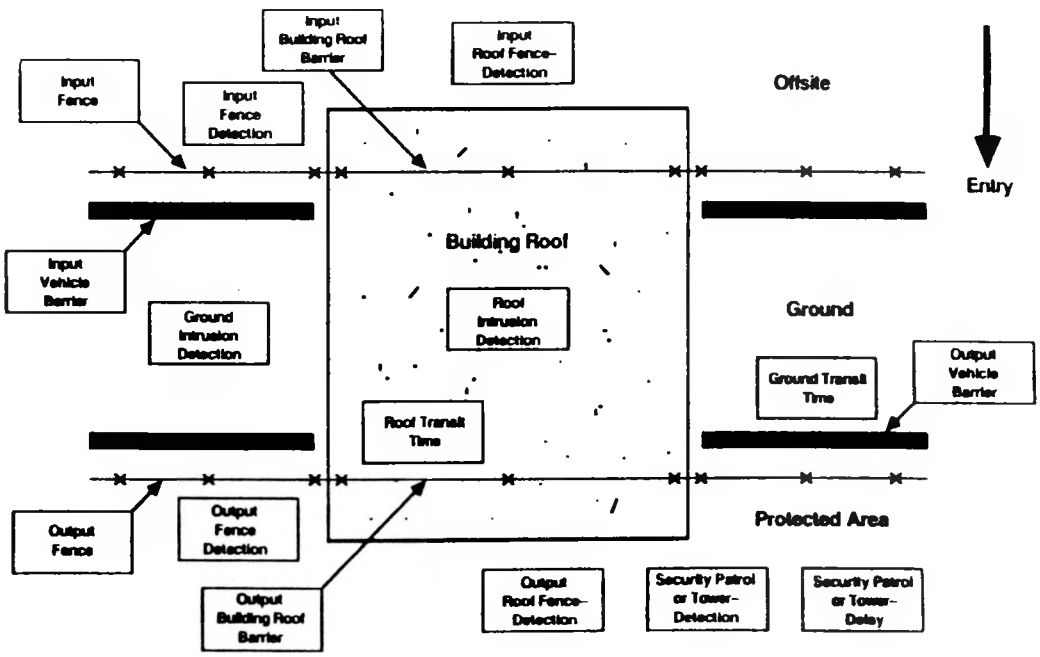


Figure A-A7 Isolation Zone

Material and Personnel Portals

The material and personnel portals shown in Figures A-A8 and A-A9 are protection elements that allow unrestricted passage of authorized persons and material, and impede passage of unauthorized persons and material. In a security context, portals are secure passageways that can be booths, rooms, or controlled areas. They are surrounded by fixed barriers such as walls or wire mesh. They have controlled, movable barriers such as doors, gates, or turnstiles at both entry and exit which normally operate in an airlock mode to allow authorized passage.

Portal entry doors are frequently left unlocked and alarms are suppressed during daytime operations or heavy traffic periods to facilitate passage. In this case, a security guard is usually present to prevent unauthorized passage. The guard can serve in both detection and delay roles.

Portal Operations - Within the personnel portal an entrant is generally subjected to identity verification and is checked to see if he is carrying contraband. If packages or other material are allowed through a personnel portal, they are usually checked independently for contraband. Similarly, if personnel are allowed through a material (or vehicle portal), they are subjected to independent verification and contraband checks in addition to inspection and searches of packages, material, or cargo.

When traffic is infrequent, a portal can be remotely operated. In this case, both doors are locked and alarmed. An entry request unit, such as a buzzer, is provided and entry into the portal is automatically allowed upon normal request. The entrant's identity is then remotely verified. There may not be a contraband check for remote operation.

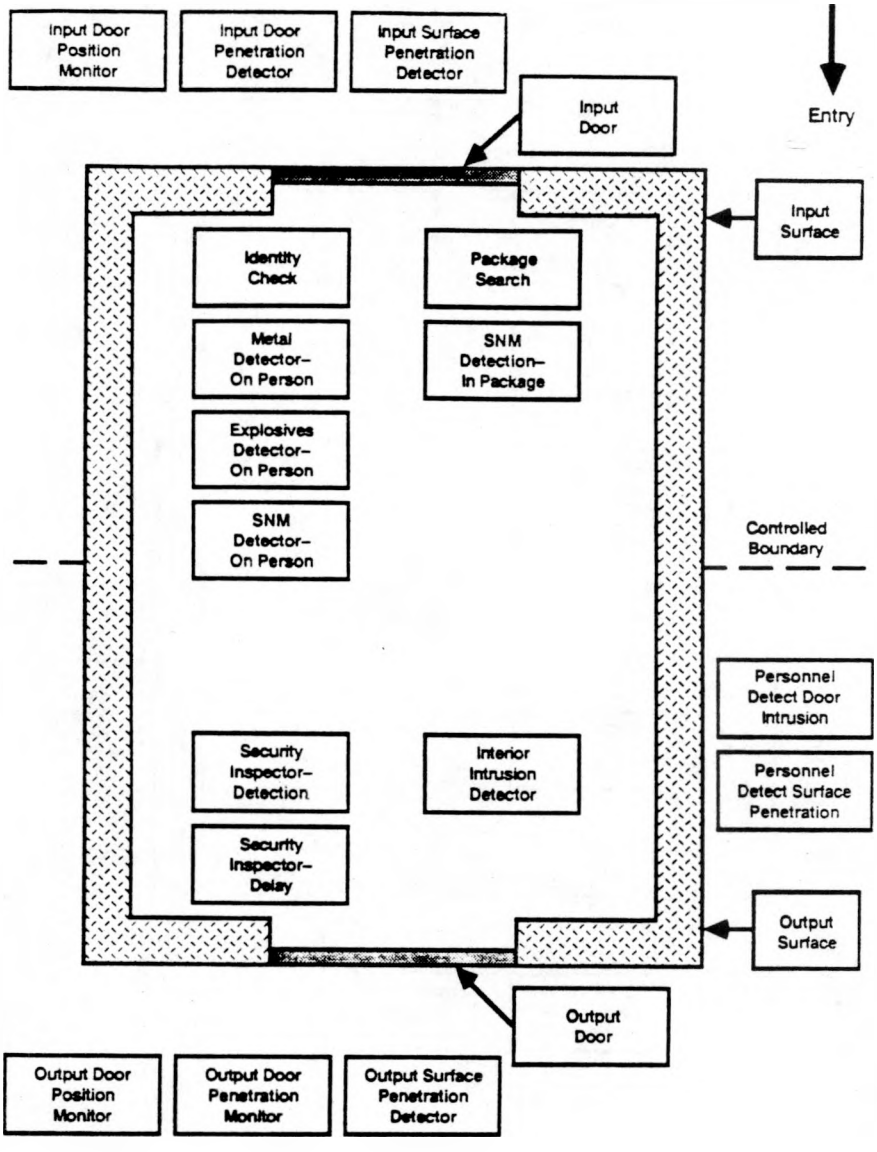


Figure A-A8 Material Portal

Different detection and delay components may be in use depending upon the state of the plant. During off-shift or shutdown states, both portal doors are locked and alarmed. If there is an interior intrusion monitor, it is turned on and other portal monitors are off. During an emergency state, material portals would be locked, personnel portals evacuated and then locked, but some vehicle portals would be opened and reinforced by guards to allow passage by emergency vehicles.

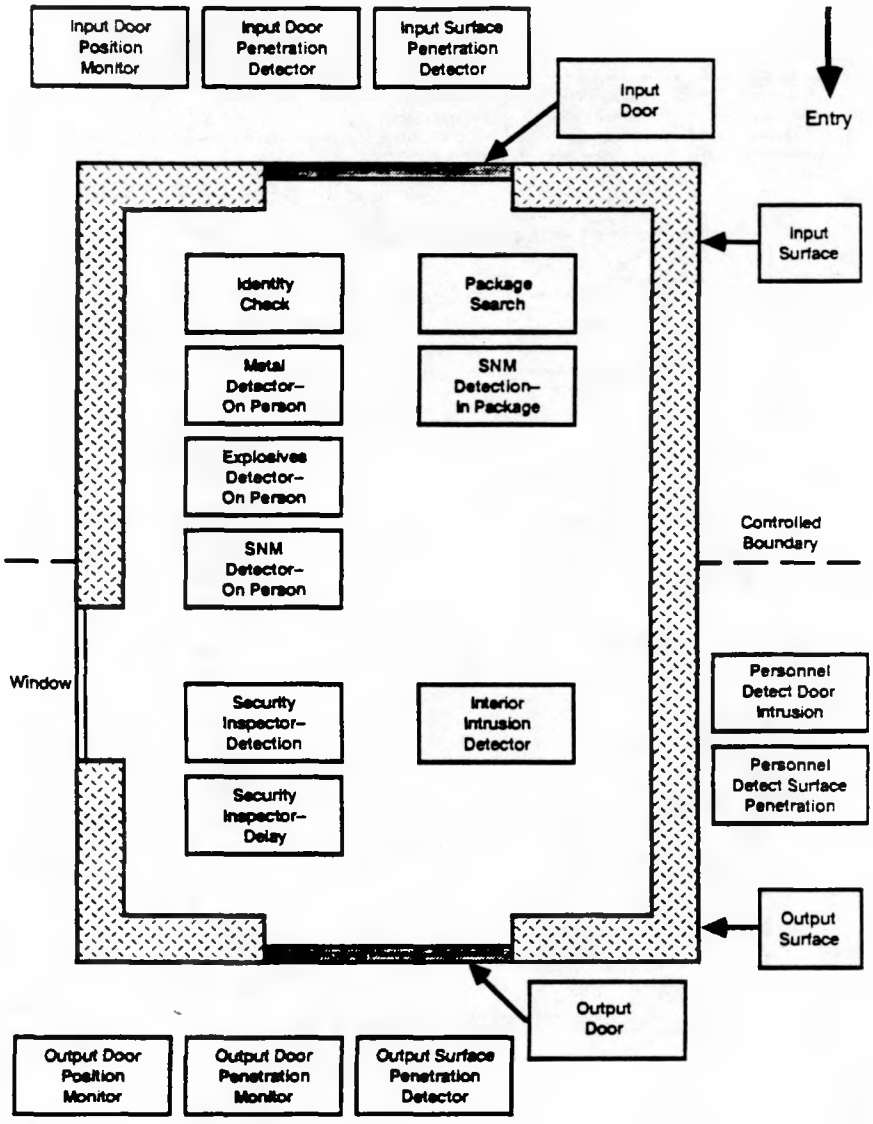


Figure A-A9 Personnel Portal

Rail Portal

A rail portal, as shown in Figure A-A10, is a protection element generally located at the protected area perimeter and spans the isolation zone. Chain-link vehicle gates are used that are controlled by a security inspector when the portal is in operation. A movable rail barrier is generally used to impede forcible train passage. Train and cargo searches are generally done at this portal. Drivers and other passengers are required to dismount and enter the protected

area via a personnel portal for identity and contraband checks. If they are allowed passage via the rail portal, they are required to pass the identity and contraband checks at this point.

Shipping Area Portal

A shipping area is a vehicle and cargo portal that is part of a building, as shown in Figure A-A11. This portal is similar to the vehicle portal except it usually has a roll-up door instead of a gate and concrete walls instead of fencing.

Surface

A surface that envelopes an area includes walls and berms, roofs, ceilings, floors, and surface openings is shown in Figure A-A12. It is a fixed barrier protection element consisting of detection and delay components. The entire surface enclosing an area or room is considered, and the weakest part is selected for the barrier delay time. A room may have an unbarred window or a tin roof as the weak part even though the walls may be reinforced concrete. Because the optimal adversary strategy is to either minimize detection or minimize delay at each element, the detection value associated with this element is selected independently of the weakest delay. That is, an alarmed window may be the weakest delay route, but an unalarmed wall may be the weakest detection route.

A surface is modeled in two stages: 1) barriers that can be penetrated in a single action - both detection and delay occur during the first stage, 2) thick, hardened walls or heavy earthen covers - two penetration actions are required, and detection is assumed to occur during the first stage (e.g., when explosives are detonated) prior to the second stage delay (e.g., rubble clearing and cutting of rebar).

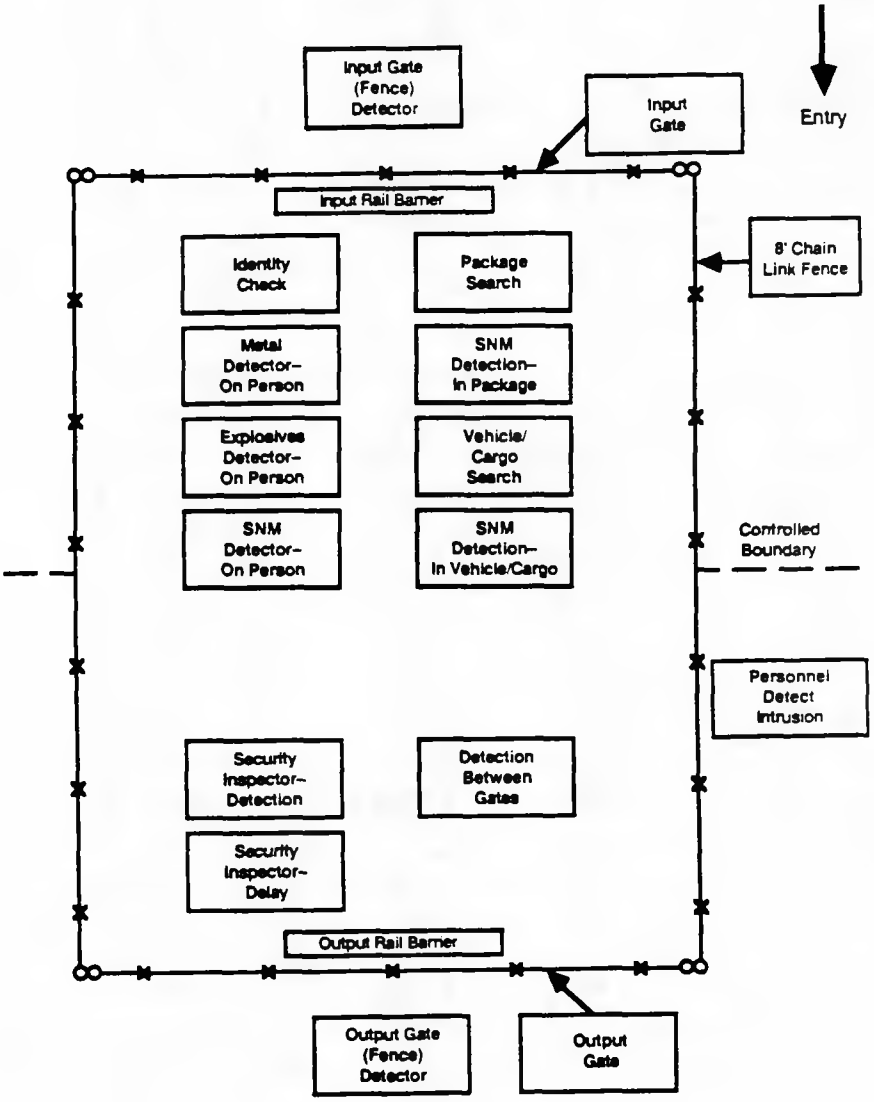


Figure A-A10 Rail Portal

Theft or Sabotage Task

The theft or sabotage task protection element, shown in Figure A-A13, provides protection at the target location. Interior intrusion detectors in the target enclosure are associated with the task element. Detection and delay components can be installed at the target to impede and monitor unauthorized activity. Co-workers for ad-hoc monitoring of operations can be effective. However, unless they are dedicated to surveillance or monitoring of specific tasks for

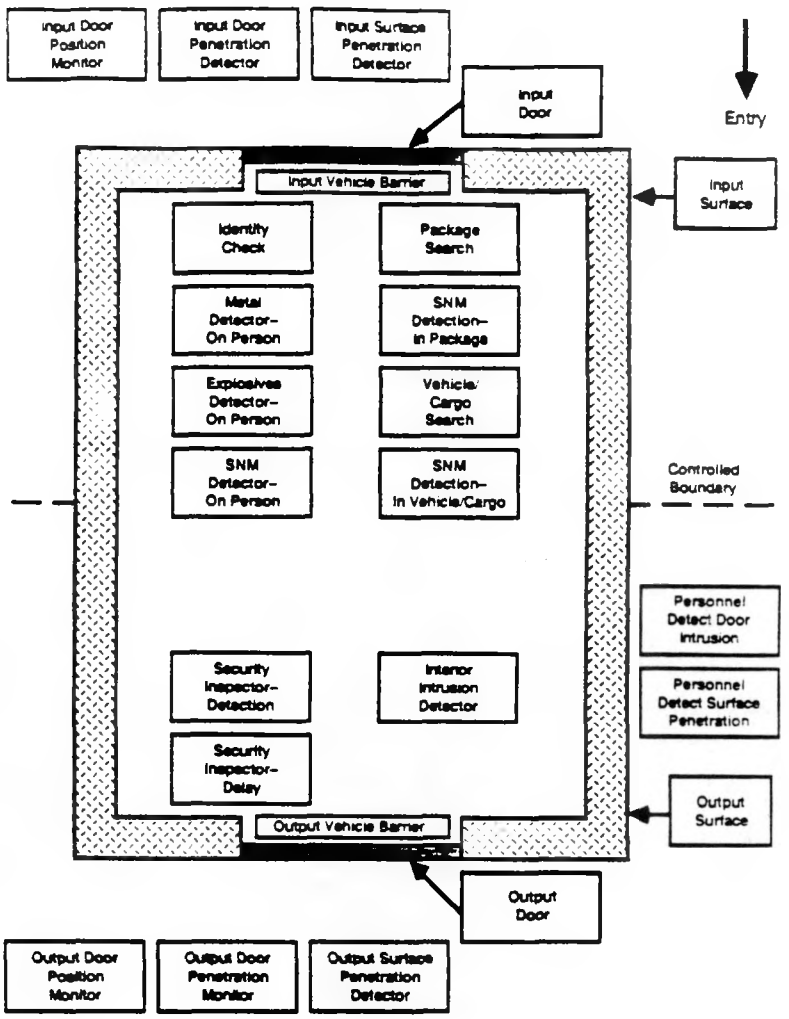


Figure A-A11 Shipping Area

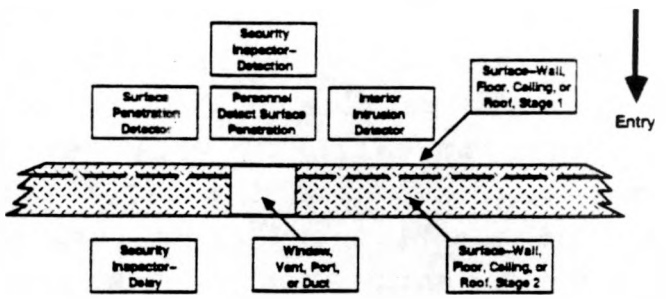


Figure A-A12 Surface

only short periods of time, they are not likely to observe improper actions by an insider employee. Furthermore, they should have duress alarms or protected positions to ensure that they can reliably transmit an alarm to security.

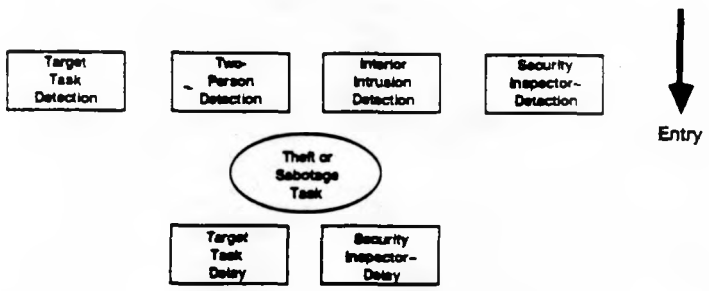


Figure A-A13 Theft or Sabotage Task

Tunnel, Pipe, or Drain

The tunnel, pipe, or drain, shown in Figure A-A14, is not a protection element in the strictest sense, but components should be present to provide protection against entry through this element. Detection and delay components can be installed at both ends of the element. In addition, an interior intrusion detection system can be added within the element. Transit time through the element is usually significant.

Vehicle Portal

Vehicle portal, as shown in Figure A-A15, is a protection element generally located at the protected area perimeter and spans theisolation zone. Chain-link vehicle gates are used that are controlled by a security inspector when the portal is in operation. Additionally, a movable vehicle or rail barrier is generally used to impede forcible vehicle passage. Vehicle and cargo searches are usually done at this portal. Drivers and other passengers are generally required to dismount and enter the protected area via a personnel portal for identity and contraband checks. If they are allowed passage via the vehicle portal, they are required to pass the identity and contraband checks at this point.

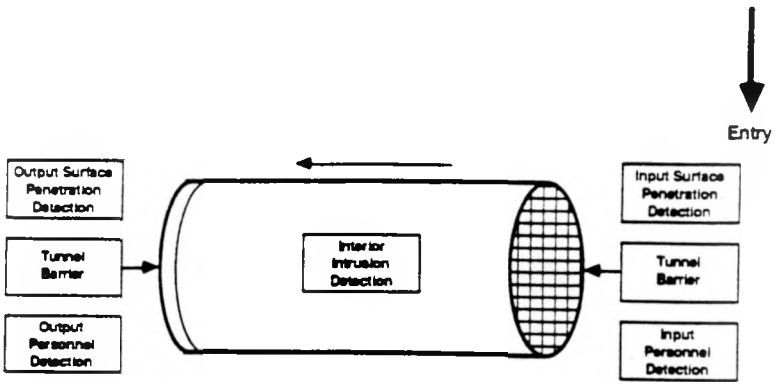


Figure A-A14 Tunnel, Pipe, or Drain

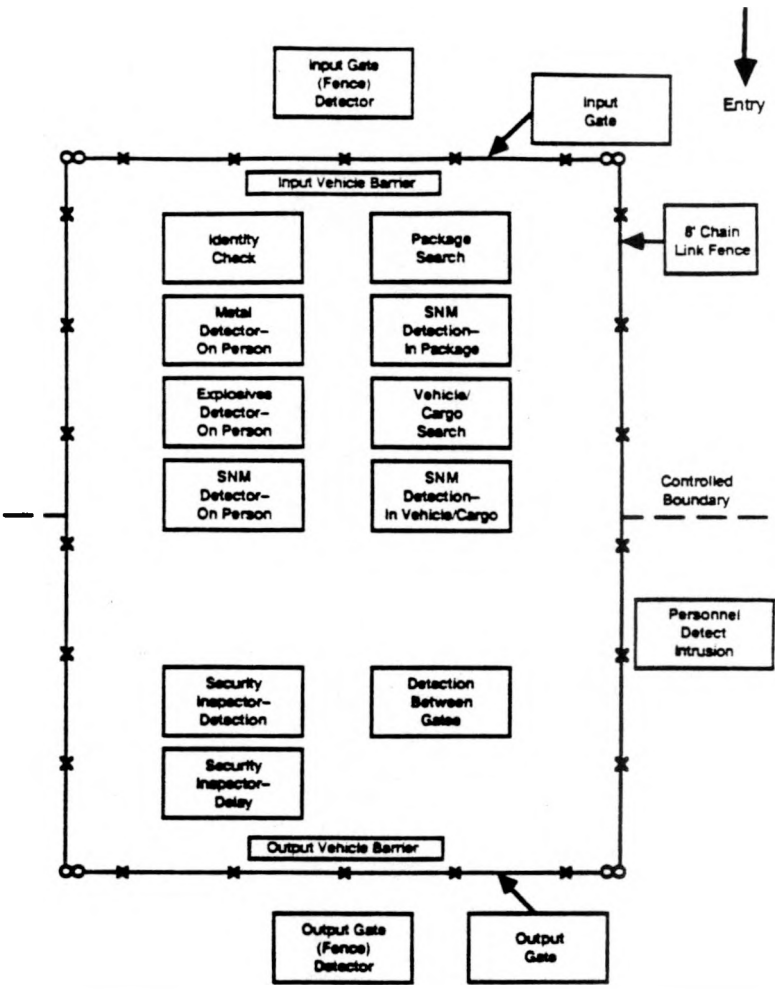


Figure A-A15 Vehicle Portal

SECTION B

SAVI Software Manual

SAVI

Systematic Analysis of Vulnerability to Intrusion

Physical Protection System Analysis Software

Version 2.2

If you have comments about or problems with the SAVI software or this manual, please complete the SAVI Report Form provided at the back of this manual and mail it to the address listed.

About SAVI

SAVI (Systematic Analysis of Vulnerability to Intrusion) is a powerful, easy-to-use software package for evaluating the effectiveness of physical security systems against outsider threats. The package incorporates several innovative concepts including the adversary sequence diagram methodology which was developed by Sandia National Laboratories and an advanced path vulnerability analysis algorithm developed by Science and Engineering Associates, Inc. A highly interactive interface allows the user to accurately model complex facilities, calculate the most vulnerable paths through a facility and maintain a library of these models and analyses results on disk. Recommendations are given as to modifications which might reduce the vulnerability to intrusion for the most vulnerable paths. Results can be displayed and printed in a variety of forms to aid in developing security system upgrade plans and performing sensitivity analyses.

SAVI Features

The SAVI software package includes the following features:

- Runs on IBM PC compatibles
- Provides a highly interactive user interface
- Constructs and archives physical protection system models
- Allows threat to be specified including attributes, objective, and intrusion tactics
- Includes a database of delay and detection components for modeling a wide range of security systems
- Models time necessary for intruders to traverse distances through the facility

- Evaluates adversary paths through a modeled facility and determines the most vulnerable paths
- Displays path vulnerability diagnostics and recommendations for decreasing path vulnerabilities
- Provides graphs of vulnerability analyses including sensitivity to variations in response force times.

Overview of SAVI

SAVI makes use of a highly interactive user interface where information is presented in graphic form. Pop-up windows are used throughout for entry and display of information. A single line menu at the top of the screen presents all options to the user. These options are further explained on a message line directly below the menu. The remainder of the screen is dedicated to a diagram which represents the current protection system model. All input is checked for accuracy, and data is presented in a logical and clear manner.

SAVI utilizes a security system analysis technique based on the Adversary Sequence Diagram (ASD). These diagrams provide a method of graphically representing Physical Protection Systems (PPS) composed of physical areas and Protection Elements (PE). As an adversary attempts to move from area to area through the system, he must defeat these elements. Elements are composed of associated delay and detection components and are the basic building blocks of ASDs. The user is given the ability to specify the PEs which exist within the facility including the associated delay and detection components.

The characteristics of the threat can be specified including intruder attributes, objectives and tactics. SAVI then calculates the system vulnerabilities, ranks the most vulnerable paths for a range of security force response times and provides recommendations for improving the PPS.

Data file functions support the archiving of ASDs and analysis results to disk, while print utilities provide hard copies of all results. Extensive graphic and tabular output is available to document the modeling process.

About This Manual

This software manual is divided into two parts: a User's Guide and a Reference Manual. The User's Guide supplies the information necessary to operate the SAVI system including directions for getting started and using the software. A step-by-step tutorial covers all aspects of using SAVI to analyze a sample security system. The Reference Manual provides the user with an alphabetized reference to all menus and functions, providing a precise explanation of all features.

Acknowledgements

SAVI was developed jointly by Sandia National Laboratories (SNL) and Science & Engineering Associates, Inc. (SEA). Richard McAniff of Sandia was the senior project leader with Brad Key of SEA leading the software development. Al Winblad (SNL) provided the physical protection system modeling expertise and Bill Paulus (SNL) led the software testing and verification effort, ensuring the accuracy of SAVI analyses.

Scott Walker and Malcolm Moore (SEA) completed the software design team, implementing the vulnerability analysis algorithm and the Graphs functions. Bret Simpkins (SEA) supported the design of the user interface, and produced the Reference Manual.

This software manual was created with input from all individuals previously mentioned along with Betty Biringer (SEA). Janis Burdick and Jeri Goff (SEA) provided technical editing and typesetting support.

The original adversary sequence diagram concept was developed by the team of Miller Cravens, Carl Clark and Al Winblad (SNL). They also produced Path Analysis (PANL), a mainframe computer code for analyzing ASDs. John Darby (SEA) was a foundational contributor to the SAVI modeling effort.

The combined work of all of these individuals produced SAVI Version 2.2.

User's Guide

USER'S GUIDE

The SAVI User's Guide contains installation procedures, directions for software use, and includes background information and terminology necessary for effective system operation. A tutorial chapter guides the user step-by-step through a sample problem which includes modeling a facility, analyzing the vulnerabilities, and investigating security system improvements.

CONTENTS

CONTENTS (continued)

FIGURES

TABLES

Getting Started

1.0 Getting Started

Before using SAVI for the first time, you should back up your original software and create a data disk. This section covers these topics and includes a section for first time users of IBM PC compatible personal computers.

1.1 Hardware Requirements

SAVI is written for the IBM PC and true compatibles running MS-DOS Version 2.0 or later.

The hardware required to run SAVI is:

- An IBM PC or compatible with 640 KB of memory
- Two Double Sided/Double Density (DS/DD) 360 KB floppy disk drives or a hard disk and one floppy drive
- A standard IBM Color Graphics Adapter (CGA) or functional equivalent with an appropriate graphics monitor (monochrome or color)
- A parallel printer port with an Epson FX series or compatible printer (the printer must recognize the IBM graphic character set to produce correct diagrams and support the IBM graphic command language for graph printouts)
- An 8087 math co-processor is suggested to reduce analysis times but is not required

1.2 Package Contents

The SAVI software package contains the following programs and files distributed on the original SAVI system and catalog disks.

SAVI System Disk Contents:

SAVI.EXE	The SAVI program
RUNSAVI.BAT	A batch file to allow SAVI to be run easily on a two floppy disk system
README.DOC	Contains latest documentation on SAVI

SAVI Catalog Disk Contents:

PE.CAT	Protection element definitions catalog
DEL.CAT	Delay component catalog
DET.CAT	Detection component catalog
THREAT.CAT	Threat definitions catalog
STARTUP.ASD	The ASD file that SAVI loads at startup
SAMPLE.ASD	The ASD file that is used in the tutorial
SAVIFONT.FNT	Graphic font file

1.3 Backing Up Your SAVI Disks

For your own protection, it is recommended that you make a backup copy of the original SAVI system and catalog disks. To accomplish this you will need:

- The original SAVI system and catalog disks
- Two (2) blank DS/DD 5.25" disks
- A copy of DOS (Version 2.0 or later)

Place the DOS disk into Drive A, and at the "A>" prompt, type:

```
DISKCOPY A: B:
```

The following message should appear:

```
Place the source disk in Drive A
and the destination disk in Drive B
Press RETURN when ready
```

Remove the DOS disk from Drive A, and replace it with the original SAVI system disk. Place the blank disk in Drive B, and press [↵] to start the copy operation.

When the copy is complete, type [Y] when prompted to make another copy.

Remove the original SAVI system disk from Drive A, and store it in a safe place. Remove the disk from Drive B, and label it:

SAVI System Disk Backup

Now place the original SAVI catalog disk in Drive A. Place the second blank disk in Drive B, and press [↵] to start the catalog disk copy operation. When copying is complete, remove the original catalog disk from Drive A and label the disk from Drive B:

SAVI Catalog Disk Backup

1.4 Making a Data Disk

When running SAVI, a blank formatted data disk is required to store facility models. To create one you will need:

- A blank DS/DD 5.25" disk
- A copy of DOS (Version 2.0 or later)

Place the DOS disk in Drive A.

At the "A>" prompt, type: `FORMAT B:`

The following message should appear:

```
Insert new disk in Drive B
Press RETURN when ready
```

Place the blank disk in Drive B, and press [↵] to begin the format operation.

When formatting is complete you will be prompted to enter a label for the new disk.

Type an appropriate label such as:

```
SAVI DATA
```

or simply press [↵] for no label.

Type [N] when prompted to format another disk.

Remove the disk from Drive B and label it:

SAVI Data Disk

1.5 Running SAVI

SAVI can be run from either a floppy disk or a hard disk. Follow the instructions for your system.

Note - The DOS graphics driver (GRAPHICS.COM or GRAPHICS.EXE) must be loaded prior to running SAVI so that graphic printouts can be made. You may want to ensure that this is automatically loaded each time your system is booted by including the line "GRAPHICS" in your autoexec batch file. See your DOS manual for more on this topic. You must also ensure that no other memory resident software is loaded since SAVI requires nearly 640KB of memory to execute.

Two Floppy Disk System

To run SAVI from a floppy disk you will need to boot the computer system from DOS. Simply place a bootable DOS disk (Version 2.0 or later) in Drive A and boot the system either by pressing the [Ctrl][Alt] and [Del] keys simultaneously or by turning the system power off and back on. Now place a copy of the SAVI system disk in Drive A and a copy of the SAVI catalog disk in Drive B. Run SAVI by typing "RUNSAVI" at the "A>" prompt. Once SAVI is running you can replace the catalog disk in Drive B with a blank formatted data disk to store and retrieve SAVI data files.

Hard Disk System (Install on drive C)

Place a copy of the SAVI system disk in Drive A and a copy of the SAVI catalog disk in Drive B.

Create a sub-directory on the hard disk by typing:

```
MKDIR C:\SAVI
```

To copy all SAVI files to the hard disk type:

```
COPY A:*.* C:\SAVI
COPY B:*.* C:\SAVI
```

Although data can be stored on the hard disk, you may wish to place your SAVI data disk in Drive B to save and retrieve data files.

To run SAVI from the hard disk, set the current working directory by typing:

```
CHDIR C:\SAVI
```

and then type:

```
SAVI
```

1.6 Personal Computer Basics

This section provides basic information relating to the use of IBM PC compatible personal computers. To use SAVI you should be familiar with the general operation of your computer. You need to be able to run programs, manipulate files, make copies, and format disks. If you need further help in this area, consult the user's manual and documentation provided with the computer that you will be using. Some basic terms that you should know are presented here for your convenience.

Boot To load the operating system from a disk containing DOS. Simultaneously pressing the [Ctrl][Alt] and [Del] keys resets the system and boots the disk in Drive A.

Dir A DOS command to display a listing of disk files.

Directory A grouping of files on disk. The main directory is called the root directory and is indicated by a single backslash (\). Directories within directories are called sub-directories.

DOS Disk Operating System. Allows the user to create and handle data files, run programs, and access peripheral devices such as printers and disk drives.

Drive The device which reads and writes information to a disk. Each drive is assigned a unique letter by DOS. Usually the floppy disk drives are assigned A and B and the hard disk, if one exists, is C.

Format The process of preparing a disk to accept information.

Load To copy a program from disk to the computer memory so that it can be run.

Path A unique sequence of directory names separated by backslashes (\). The path indicates the location of a file on disk.

Prompt The request from DOS for a command. Usually indicated by the current disk drive letter followed by a prompt character (Example: "A>").

Using SAVI

2.0 Using SAVI

This chapter covers the basic information needed to use SAVI, including the screen display, menu usage, entering data, and special keys. The best way to learn this material is to begin running SAVI as outlined in Section 1.5. Before continuing, ensure that the instructions in Sections 1.3 through 1.5 have been completed, including backing up your disks and loading the DOS graphics driver.

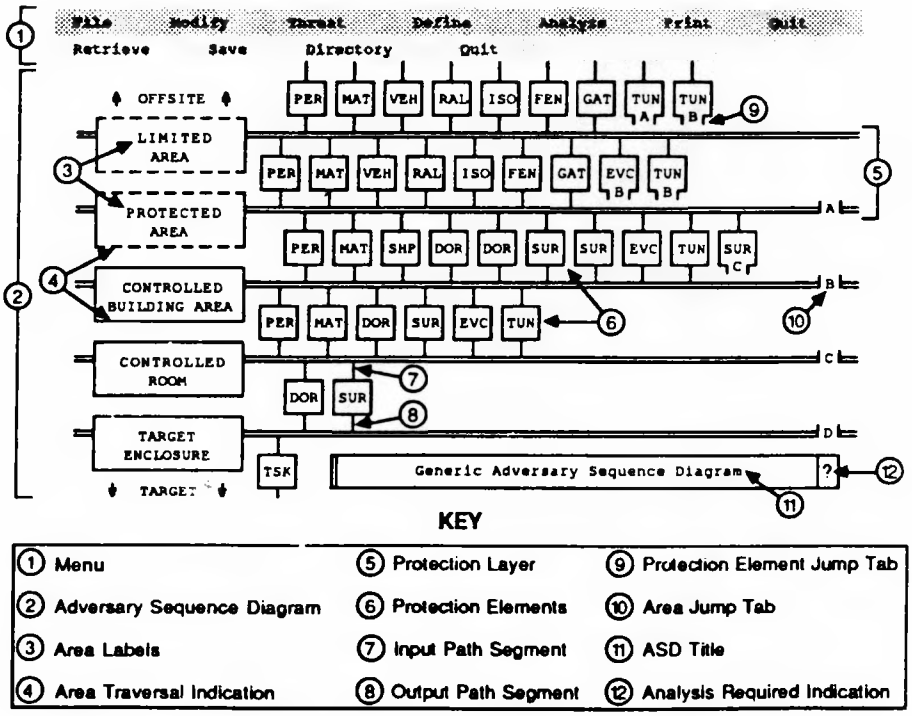
2.1 The SAVI Screen

The SAVI screen is divided into two sections: 1) the menu which appears at the top of the screen, providing access to all SAVI functions, and 2) the current Adversary Sequence Diagram (ASD) which represents a Physical Protection System (PPS). These are shown in Figure 2.1. The key at the bottom of the figure describes various features of the SAVI screen which are discussed in detail in the following sections.

2.2 The Current ASD Display

SAVI represents physical protection systems with a graphic known as an adversary sequence diagram. The ASD represents a physical facility and its security system as layers of protection separating an offsite intruder from a target inside the facility. The offsite and target points are indicated toward the top and bottom of the screen, respectively (see Figure 2.1).

When the SAVI program is first started, the ASD that appears is a generic version of a PPS. Any number of ASDs can be created, saved to disk, and retrieved later. The version that appears on the screen at any given time is called the "current" ASD, and changes to it do not affect other ASD versions on the disk.



KEY

① Menu	⑤ Protection Layer	⑨ Protection Element Jump Tab
② Adversary Sequence Diagram	⑥ Protection Elements	⑩ Area Jump Tab
③ Area Labels	⑦ Input Path Segment	⑪ ASD Title
④ Area Traversal Indication	⑧ Output Path Segment	⑫ Analysis Required Indication

Figure 2.1
SAVI Screen

The ASD shows areas of the facility, such as buildings and yards, as double horizontal bars labeled on the left side of the screen with large rectangular boxes. The boxes which contain these labels also indicate how the area can be traversed. Those areas which can only be crossed on foot (interior areas) are labeled with a solid outlined box. Areas which can also be traversed by a vehicle (exterior areas) are indicated by a dashed box. The areas are separated by layers of small boxes which represent doors, fences, and other protection elements (PEs). Protection element types are designated by a three letter abbreviation; for example, a door is labeled as "DOR." A list of the PEs available in SAVI and their acronyms are presented in Table 2.1.

DOR	Single Door	**PER**	Personnel Portal
EVC	Evacuation Shelter	**RAL**	Rail Portal
FEN	Fence	**SHP**	Shipping Area
GAT	Gate	**SUR**	Surface
GEN	Generic PE	**TSK**	Target Task
HEL	Helicopter Flight Path	**TUN**	Tunnel
ISO	Isolation Zone	**VEH**	Vehicle Portal
MAT	Material Portal		

Table 2.1
SAVI Protection Element Type Acronyms

As an adversary moves through a facility, he must pass through the PEs along his path. Each PE has an associated input path segment and output path segment. The input path segment is a single line on the upper, or offsite, side of the PE box; and the output path segment is a line on the lower, or target, side. These vertical lines connect to the facility areas (horizontal bars) on either side. In Figure 2.1, note that some output path segments do not directly connect to the area below, but are marked by tabs with a single letter. These represent "jumps" where an adversary can bypass facility areas and lead directly to another area closer to the target. Corresponding jump tabs are

marked with letters (A – D) on the double area lines as well, indicating jump destinations.

The current ASD title is displayed at the bottom of the screen. If analysis has not been completed on the current ASD, then a "?" appears at the right end of the title box. This indicator disappears when vulnerability analysis is completed. Once analysis results are calculated, they are associated with the ASD and are saved and retrieved along with the ASD itself.

2.3 Using the Menu

When the SAVI program is started, the top line of the menu displays categories of SAVI functions. Use the cursor keys to highlight any choice and press [↵] to select it. Any category can also be selected by pressing its first letter, such as [M] for Modify.

Since the SAVI menu is a tree structure, many selections, called sub-menus, lead to branches of associated functions. When a sub-menu item is highlighted, its associated choices appear on the second line of the menu. When a sub-menu selection is made, these choices then move up to the top line. The new items may then be selected, with some leading to further branches, and so on.

If a menu choice offers no further branches, it is a SAVI function, and a brief explanation of its capabilities appears on the second line. This function will be invoked if selected. For example, to invoke the Modify-Title function, first select Modify from the main menu. Several associated functions move up to the top line, and Title can then be selected. Rather than choosing and selecting with the cursor keys, it may be simpler to press [M] and then [T].

Throughout SAVI the [Esc] key will back you up one level from the current state. The Quit function also appears on all levels of

the menu and will back you up one menu level at a time when selected. The main menu choices are displayed when SAVI is first started, and can always be reached by pressing [Esc] or selecting Quit repeatedly until the top menu level is reached.

2.4 Entering Data

Throughout SAVI you will be required to input both text and numeric data, or to select data settings from a list or range. SAVI accepts input in different ways depending upon the type of data and range of acceptable values. When data are to be entered, the current settings are highlighted within a pop-up window. On color screens, this highlighting is seen as a solid blue area surrounding the data, while single color monitors show a grey area. This state is known as the "edit mode".

Some SAVI functions, such as Modify-Title and Modify-Area-Labels, are designed to accept text from the keyboard. To enter text in edit mode, SAVI operates like a simple word processor. The cursor keys move a cursor (blinking underline) to indicate your position in the text. New words can be typed in, with the old text replaced character by character. If errors are made, the cursor can be moved back and the entry retyped. The backspace key deletes text while backing over it. The [Del] key can be pressed at any time to delete the character which appears above the cursor. [Ins] is a toggle key which allows you to insert new words into existing text (insert mode) or to replace the existing text by writing over it (replace mode). The replace mode is indicated by the normal blinking cursor, while the insert mode is indicated by an increase in the height of the cursor. At any time, you can undo all changes made while in edit mode by pressing the [Esc] key. When the new text is satisfactory, pressing the [↵] key enters it into SAVI and exits the edit mode.

Other functions in SAVI, such as Define-Distance-Areas allow you to enter numeric data. When entering numbers, simply type

in the new values over the old. Again, the [Esc] key will leave the edit mode without changing the values, and [↵] will save the new data. Sometimes the numbers must be within a certain range, and SAVI will indicate immediately if an attempt is made to save invalid values. In some cases, SAVI will simply not allow values outside of the required range to be typed. For example, when entering time in seconds, numbers greater than 59 cannot be entered.

With some SAVI functions, including Modify-Element-Jumps and Types, changes are made by highlighting the current setting and scrolling through the alternate choices using the cursor keys. You may stop on the desired entry and set the data by pressing [↵], or reset to the original choice by pressing [Esc].

Still other functions are designed to allow you to select from a list of choices, including Define-Component-Settings and the Threat functions. Here SAVI uses a pointer to indicate the current setting within a list of choices. The list is displayed in a pop-up window; however, in some cases only a few of the entries will fit the window. This is indicated with arrows and the word "MORE" above and/or below the list. Use the cursor keys to scroll up or down to view all choices and highlight the desired one. Pressing the [↵] key will select the highlighted choice, and the [Esc] key will exit the window, leaving the current setting where the pointer indicates.

SAVI makes extensive use of pop-up windows to display information and to accept input. These windows appear automatically within SAVI functions. If you would like to remove a window from the screen to see the current ASD more clearly, press the [space] bar. Press the bar again to bring the window back. Throughout SAVI, windows can be toggled on and off the screen using the [space] bar. However, if you are editing the data within a window, you must first save your changes by pressing [↵] before removing the window from the screen.

2.5 Sub-Menus and Functions

The SAVI menu system is structured to encourage systematic modeling and analysis of physical protection systems. The main menu is made up of several sub-menus which contain all SAVI functions. The functions contained within the Modify, Threat, Define, and Analyze sub-menus provide the protection system modeling capabilities, allowing the user to:

Modify Model a specific facility by modifying the current ASD.

Threat Specify a particular threat to the facility.

Define Define the security components which delay an intruder and increase the probability of his detection, the range of response force times, and the facility distances.

Analyze Analyze the vulnerability to intrusion of all paths, and display the sensitivity to variations in the response time of security forces.

See Figure 2.2 for a diagram of the SAVI menu structure.

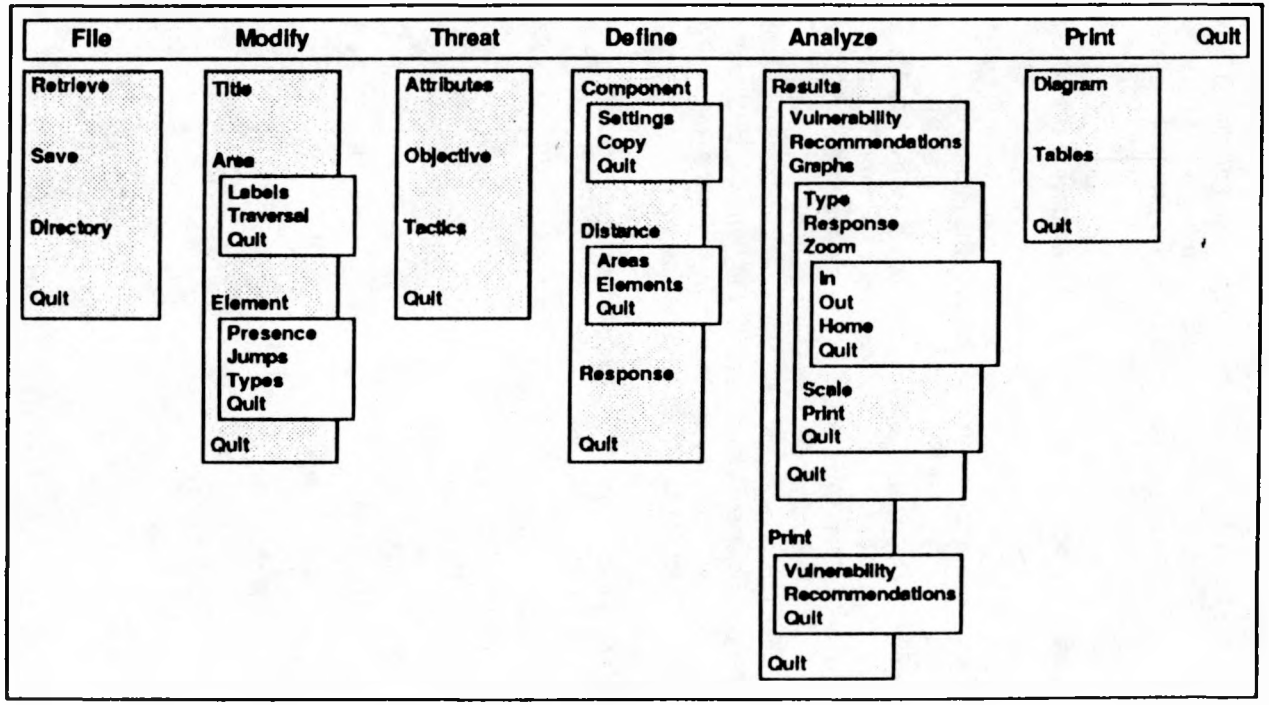


Figure 2.2
SAVI Menu Structure

The SAVI menu is designed to encourage a logical selection sequence when progressing left to right. In other words, the Modify functions should be selected before the Threat functions, and so on. While these can be selected in any order, a logical sequence follows, with a brief explanation of each function.

File Functions

The File sub-menu is the first entry in the main menu and contains functions which are used to retrieve and save ASDs to disk.

File - Retrieve:
Retrieve the ASD file from disk which most closely resembles the facility to be modeled. If desired, you can simply modify the generic ASD which appears at the start of SAVI (STARTUP.ASD).

File - Save:
Save the current ASD to disk periodically to ensure that no data is inadvertently lost.

File - Directory:
Set the disk directory for the Retrieve and Save functions.

Modify Functions

These functions allow the current ASD to be modified to represent a site-specific facility.

Modify - Title:
Input the new ASD title.

Modify - Area - Label:
Modify area labels to site-specific names.

Modify - Area - Traversal:
Specify the traversal limitations for each area.

Modify - Element - Presence:
Select PEs which exist in the new ASD.

Modify - Element - Jumps:
Modify the output areas of the PEs within the current ASD to indicate indirect connections between areas.

Modify - Element - Types:
Modify the PE types within the current ASD.

Threat Functions

The Threat functions specify characteristics of the threat.

Threat - Attributes:
Specify the properties of the threat.

Threat - Objectives:
Identify the adversary's goal.

Threat - Tactics:
Indicate whether the intruder will attempt to intrude into the facility using both force and deceit tactics or will simply force each PE.

Define Functions

These functions allow detection and delay components to be selected, and response force times and traversal distances to be set.

Define - Component - Settings:
Define delay and detection component settings for each PE.

Define - Component - Copy:
Copy PE component settings from one element to another.

Define - Distance - Areas:
Define the distance across each area.

Define - Distance - Elements:
Define the distance across each protection element.

Define - Response:
Define the range of response force times.

Analyze Functions

Path vulnerabilities are calculated and results displayed inside the Analyze sub-menu. If analysis results are not current (indicated by a "?" at the right side of the ASD title box), they are automatically calculated upon entering the Analyze sub-menu. See these functions in the Reference Manual for a complete explanation of the display of analysis results.

Analyze - Results - Vulnerability:
Provides functions to display the most vulnerable paths and vulnerability diagnostics for each path.
Analyze - Results - Recommendations:
Suggests changes to detection or delay values on the most vulnerable paths in order to improve effectiveness of the PPS.
Analyze - Results - Graphs:
Provides functions to display and print the analysis results graphically.
Analyze - Print:
Provides the ability to print out analysis results.

Print Functions

The Print sub-menu provides hardcopy records of all input data.

Print - Diagram:
Prints the current ASD in graphic form.
Print - Tables:
Prints the current ASD protection system settings in tabular form.

From this point you can reselect any function and modify the ASD as necessary to reduce the system vulnerabilities. Each function is explained further in the Reference Manual. See the

Tutorial in Chapter 4 for a more detailed example. Be sure to save your ASD periodically. You can Quit SAVI at any time, and continue analysis later by retrieving your ASD file from disk.

2.6 Special Keys

The following keys provide special functions within the SAVI system.

- **Cursor Control**
  [↑] [↓] [←] [→]

  Use these keys to highlight menu selections, move between protection elements within the current ASD, or to scroll between paths and RFT values within the Analyze functions.

  Note - The cursor keys are disabled by the [NumLock] key above the numeric keypad. If your cursor keys do not seem to work, you may have inadvertently pressed this key. Simply press the [NumLock] key again to regain cursor control.

- **Select**
  [↵] or [Return]

  Use this key to select functions from the menu and protection elements within functions, and to set data when in edit mode.

- **Escape**
  [Esc]

  Use this key to back up to the preceding level within the menu, or to undo changes made while editing within a window.

- **Window Toggle**
  [Space] bar

  Use this key to remove any pop-up window which is currently on the screen or to replace it if it has been removed.

- **Maximum Vertical Movement**
  [PgUp] [PgDn]

  Use these keys to move quickly to the top or bottom of the current ASD display while in an ASD function, or to the top or bottom of a list when appropriate.

- **Maximum Horizontal Movement**
  [Home] [End]

  Use these keys to move quickly to the far left or far right of the current ASD display while in an ASD function, or to the beginning or end of a list when appropriate.

- **Insert/Delete**
  [Ins] [Del]

  Use these keys to insert or delete the highlighted PE within the current ASD while in the Modify-Element-Presence function, or to enter data when in edit mode.

- **Insert/Delete Protection Layer**
  [*] followed by [Ins] or [Del]

  Press the [*] key prior to pressing insert or delete, in order to insert or delete all PEs on the current protection layer while in the Modify-Element-Presence function.

- **Clear Component Settings in a Single Protection Element**
  [?]

  Press this key to clear component settings while in the Define-Component-Settings function.

- **Clear All Component Settings in Current ASD**
  [*] followed by [?]

  Press the [*] key prior to pressing [?] to clear all component settings after just entering the Define-Component-Settings function.

- **Direct Setting**
  [#]

  Press the [#] key while in a component settings window in the Define-Component-Settings function to quickly enter a direct setting.

Terms and Concepts

3.0 Terms and Concepts

This chapter defines the terms and concepts which underlie the SAVI technique of vulnerability analysis.

3.1 Terminology

The following are important terms used within the SAVI system:

- **Adversary Sequence Diagram – ASD**
  A graphic representation of a physical protection system comprised of protection elements connecting physical areas.

- **Critical Detection Point – CDP**
  The last point on a given path where detection must occur if the response force is to have enough time to interrupt the adversary before he completes his mission.

- **Cumulative Path Delay**
  The total delay from offsite to the end of the path. This delay is provided by the delay components encountered by the adversary along a given path.

- **Cumulative Path Delay Deficiency**
  The time that must be added to the cumulative path delay on a deficient path if interruption is to occur. This time is the difference in the response force time and the cumulative path delay plus one second to break a tie.

- **Path**
  A specific route through the facility consisting of a sequence of physical areas and protection elements that an adversary can traverse to accomplish his mission.

- **Path Scenario**
  The specific sequence of force or deceit actions that an adversary may use to sequentially defeat each protection element on a path.

- **Path Segment**
  The point leading into or out of a protection element where the adversary delay times and detection probabilities are assigned based on the component settings.

- **Physical Protection System – PPS**
  The collective interaction of delay, detection, assessment and communication components, and security and response force personnel that provide protection for facility targets.

- **Probability of Interruption – P(I)**
  The probability that the response force will interrupt the adversaries prior to completion of their mission.

- **Protection Element – PE**
  The basic building block of a physical protection system consisting of components which delay the adversary and provide associated detection probability.

- **Protection Layer**
  A set of protection elements which separate two physical areas within a physical protection system.

- **Response Force Time – RFT**
  The assessment, communication, and deployment time expended by the response force in order to reach a specified interruption point, after receiving the first alarm.

- **Timely Detection**
  A security system requirement whereby the adversary must be detected in time for the response force to interrupt him before he completes his mission.

- **Time Remaining after CDP**
  The minimum time required for an adversary to complete his mission from the critical detection point on a given path.

- **Time Remaining after Interruption – TRI**
  The time remaining on a path after interruption occurs. This is the difference in the time remaining after CDP and the response force time.

3.2 The ASD and Timely Detection

The adversary sequence diagram is a tool designed to model physical protection systems. When combined with the concept of timely detection, the ASD provides a means of evaluating vulnerability to intrusion of all paths through a facility. This capability provides the basis for designing, evaluating, and improving physical protection systems in a thorough and systematic way.

The concept of timely detection integrates detection, delay, and response force time. This is accomplished by calculating the minimum probability of detecting the adversary while there is still time for the response force to interrupt. That is, it measures the probability of interruption P(I).

The P(I) along any path is determined by calculating the critical detection point (CDP). This is defined as the point where the adversary delay time along the remaining path just exceeds the response force time. The probability of interruption is then the likelihood of detecting the intruder at or before the CDP.

SAVI uses the concept of timely detection to compute the probability of interruption along every path within an ASD. Paths are ranked according to the P(I), with the most vulnerable path having the lowest probability of interruption. Paths with equivalent P(I)s are sub-ranked according to the time remaining after interruption (TRI).

3.3 SAVI Modeling Concepts

SAVI is designed to be used to construct a site-specific model of the facility protection system and to analyze its effectiveness. This process requires several pieces of information:

- Construction of a site specific ASD
- Specification of the threat characteristics including the intruder attributes, objective (entry or entry/exit) and tactics (force-only or mixed force/deceit)
- A set of protection system detection and delay components assigned to the protection elements in the ASD
- Distances across facility areas and protection elements
- A range of response force times.

The SAVI analysis utilizes all of these settings to calculate the vulnerability to intrusion for each of the possible adversary paths through the defined facility and ranks the ten most vulnerable ones. Each piece of information necessary to determine these vulnerabilities is discussed further in the following sections.

3.3.1 Adversary Sequence Diagram

An ASD is a graphic representation of a facility and its PPS comprised of protection layers which separate physical areas. A protection layer includes everything between two physical areas that would impede or expose an adversary. In SAVI, these are called PEs and must be identified and defined in order to model a specific facility. Doors, surfaces (walls, floors, ceilings), portals, and isolation zones are examples of protection elements. These elements can be thought of as the basic building blocks of the physical protection system. A list of the protection elements which are used in SAVI can be found in Table 2.1.

As an adversary attempts to accomplish his goal, he must pass through a single PE within each layer of protection. Each PE has an input path segment which leads into the element itself and an output path segment which leads into the next physical area.

Protection elements are composed of delay and detection components which must be assigned specifically for each facility. A path through the system is then a unique, ordered sequence of these path segments. Figure 3.1 provides a conceptual view of the interrelationships between physical areas, protection layers, PEs, and path segments.

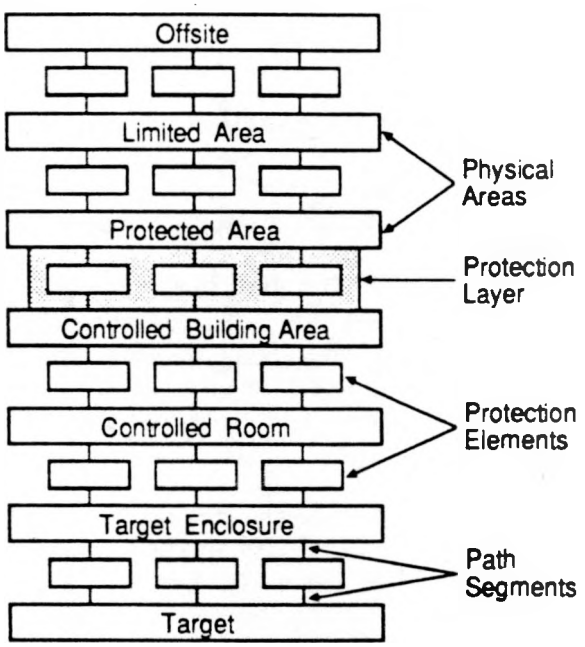


Figure 3.1
ASD Concept

Within SAVI a site-specific ASD is constructed for the target, or set of targets having a common location, by utilizing the generic ASD together with specific facility and PPS layouts and drawings. This site-specific ASD is created by selecting those elements that are present at the facility from the general set presented in the generic ASD.

Deviations from the orderly sequence of physical areas and protection layers that comprise the generic ASD will often be necessary in order to create an accurate site-specific ASD. Both jump and bypass features are supported in the SAVI modeling technique. A jump is used to model a site element that does not connect to the adjacent area shown on the generic ASD. A bypass is used to model the absence of a protection layer.

- **ASD Jump** – As shown in Figure 3.2, there is a wall which is common to both the controlled building area and the target enclosure making it possible to go directly to the target enclosure without passing through the controlled room. This situation is correctly modeled in Figure 3.3 using a surface PE which jumps from the controlled building area to the target enclosure (area "D"). Note the "SUR" protection element with the letter "D" on the jump tab. This indicates that a direct path exists from the controlled building area to the target enclosure through the shared surface.

- **ASD Bypass** – It is possible to bypass entire protection layers by eliminating all of the elements on a layer. Notice that the facility shown in Figure 3.2 has only a protected area between offsite and the controlled building area. Therefore, any PEs leading between the limited area and the protected area do not exist since there is no limited area in this example. A bypass line indicates when all of the PEs on this layer are deleted. Again Figure 3.3 shows the resulting site-specific ASD with this bypass.

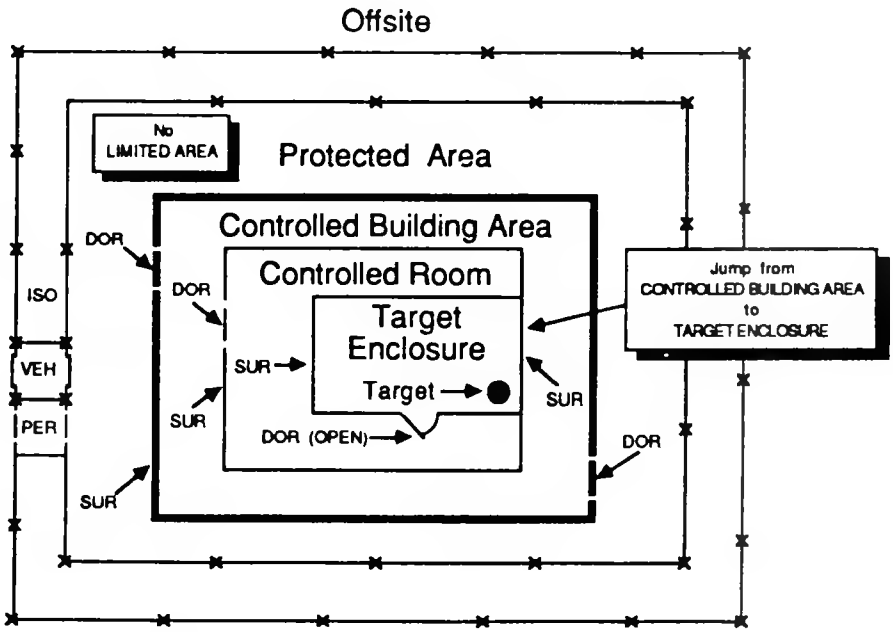


Figure 3.2
Sample Facility with Jump and Bypass

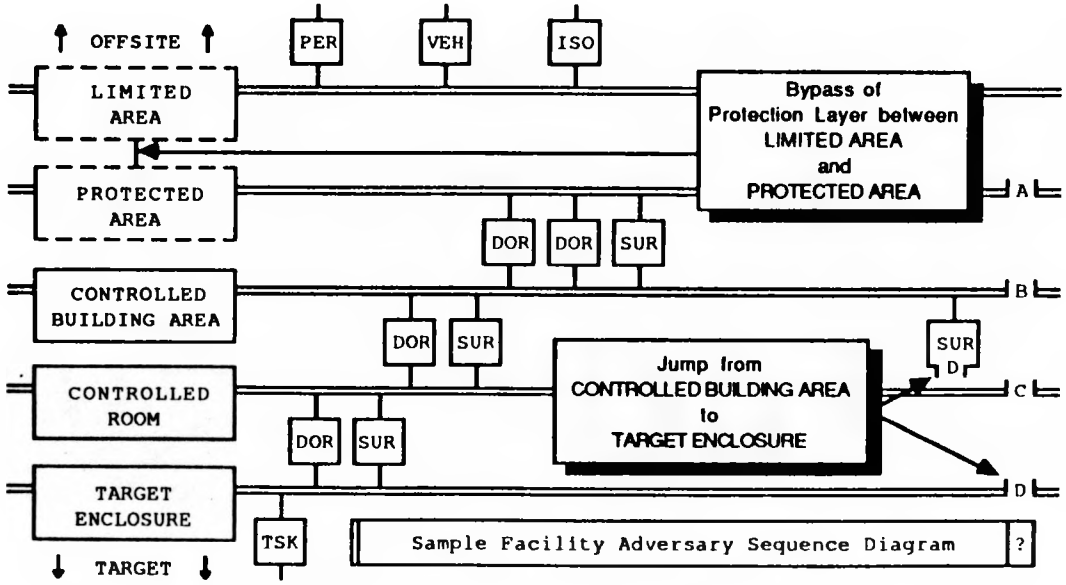


Figure 3.3
Sample Facility ASD with Jump and Bypass

3.3.2 Threat Characteristics

The characteristics of the threat must be specified for any vulnerability analysis. These characteristics include setting the adversary attributes, objective and intrusion tactics. Analysis for normal day shift, off-shift hours, or during an emergency state may affect the choices made for the threat characteristics.

SAVI supports analysis for three different sets of threat attributes:

1) Outsiders with metal and explosives traveling on foot
2) Outsiders with metal and explosives traveling by truck
3) Outsiders with metal and explosives traveling by helicopter

The inclusion of "metal" indicates that equipment, tools and/or weapons are carried and will be subject to metal detectors if the intruders submit to these tests. The "explosives" are also carried by the intruders and will be subject to explosives detectors if present. SAVI calculates the time to travel across discrete distances within a facility, and the mode of transport (example: "on foot") will affect the time required to traverse the facility. SAVI also takes into consideration those areas and elements which cannot be traversed by a vehicle (example: building interiors) and restricts travel to foot when appropriate.

Finally, the threat tactics can be specified. SAVI will model intruders that forcibly penetrate all PEs or intruders that mix force and deceit tactics along a path.

3.3.3 Detection and Delay Components

As noted in Section 3.2, SAVI utilizes the concept of timely detection in analyzing PPS vulnerabilities. This requires specifying delay times and detection probabilities for each PE. The delay time is defined as the delay presented to an adversary along a specific path segment given that the intruder has already

been detected. Detection probability is the likelihood of detecting an adversary along a specific path segment given that he has not yet been detected. The element delay and detection probabilities are calculated by SAVI from choices made from component lists.

To help the user obtain detection and delay values for the security system, the SAVI model provides a database of possible security components associated with each element of the specific ASD. The associated detection and delay values for these components are shown. These values are based on laboratory and field experiments, and engineering judgements. Since some components vary in effectiveness depending on the threat, SAVI allows the user to specify which components exist in the PPS, and the delay and detection performance is automatically adjusted for each component based on the specified threat characteristics discussed above. If desired, the user may directly input threat specific component values.

SAVI also considers the delays along each path associated with traversing areas and PEs. Element transit times are normally used only for elements that have considerable length such as tunnels or wide isolation zones. The area and element traversal times are calculated automatically by SAVI based on the minimum distances across each physical area and PE in combination with the threat mode of transportation.

3.3.4 Response Force Time Range

The response force time (RFT) is the time it takes to interrupt the intruders after receiving the first alarm. This time should include assessment, communication, and deployment time. The specified values for RFTs can be based on actual field trials or on estimated performance. The analyst must determine the appropriate response force station and deployment location for each target so that the interruption objective can be met. It is recommended that the analyst use an RFT value that reflects the

time associated with the arrival of a sufficient number of response persons to successfully stop the forward progress of the specified intruders. Therefore, the size of the adversary force should be considered in estimating the number of response personnel that must be deployed to achieve the specified RFT.

SAVI allows the user to input a range of up to ten values for RFT. The probability of interruption, P(I), for each path is calculated for the range of RFT values. A graph can be displayed which depicts the sensitivity of the most vulnerable path to variations in the RFT.

3.4 SAVI Vulnerability Analysis

Once the required data is entered into SAVI, vulnerability analysis can be done. SAVI calculates P(I) and TRI for each path through the specified ASD. It will display the ten most vulnerable paths ranked in order of their vulnerability. If two paths have the same P(I), then they are sub-ranked by the time remaining after interruption.

SAVI provides several features which help the user in considering possible upgrades to the most vulnerable paths. The critical detection point (CDP) is displayed graphically for the top ten most vulnerable paths for any RFT in the given range. A path can be upgraded by improving the detection components in the PEs prior to the CDP. These upgrades will directly improve P(I) for the most vulnerable path. A path can also be upgraded by improving the delay components in PEs past the CDP. This action may move the CDP closer to the end of the path, thus gaining the effect of additional detectors and possibly improving P(I).

In addition to display of the most vulnerable paths and the associated diagnostics for each, three types of graphs are available. These graphs are: 1) Vulnerability - a graph of P(I) and

TRI for each of the ten most vulnerable paths for any RFT in a given range, 2) Sensitivity - a graph showing the variation of the most vulnerable path's P(I) with changes in RFT, and 3) Distribution - a histogram plot of the percentage distribution of P(I)s for all paths for any RFT in a given range.

Sensitivity analyses can be performed on a PPS design to determine the effect of incremental changes in the elements and components. Because the most critical PPS parameter is RFT, SAVI allows the analyst to vary the RFT over a specified range and then calculates the variations in P(I)s over this range for the most vulnerable paths. This information is displayed in the Sensitivity plot (see Figure 3.4) and clearly indicates the time in which the response force must respond to maintain a desired P(I) for the most vulnerable paths.

3.4.1 The Analysis Technique

Although the SAVI software package is very complex and powerful, the underlying concept for determining path vulnerabilities can be stated simply.

The SAVI vulnerability analysis technique makes two assumptions: 1) adversaries have knowledge of the protection system characteristics, and 2) they use an optimal penetration strategy – minimizing detection until the remaining delay time is less than the RFT, then minimizing delay without regard to further detection. The second assumption makes it possible for SAVI to consider delay times independent of detection probabilities, because at each point on the path, the adversary is concerned with either delay or detection, but not with both.

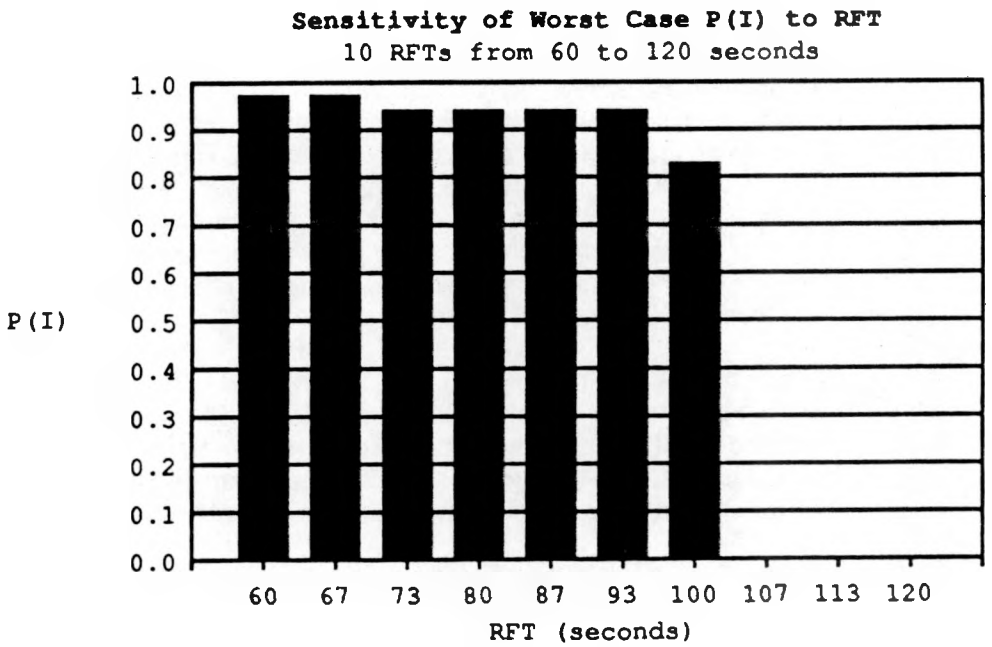


Figure 3.4
Sensitivity Plot

In other words, the optimal penetration strategy is to avoid detection until a point is reached on the path where the minimum delay time remaining is less than the response force time (RFT). After this point, detection is ineffective because there is no longer enough delay to allow interruption. This strategy can be demonstrated by considering the relationship of detection, delay, and response along a path.

A path can be represented by an event line as seen in Figure 3.5. This line represents the delay, detection and response events on a given path. The dotted part of the line represents the portion of the path which has already been traversed by the intruder; the solid part of the line represents the delay time remaining on the path. The events shown on the line are: 1) the location of the detection components p1, p2, etc., 2) the accumulated delay times T1, T2, etc., representing the sequence of delays provided by delay components, and task times, and 3) the point where the time remaining on the path is equal to the RFT; namely TR *.

The first detection point encountered on the line prior to TR * (in this case p4) is called the critical detection point (CDP) because detection must occur either at this point or before it for interruption to occur. If the total path delay is less than the RFT, then a CDP cannot be specified and interruption is not possible.

If there is a CDP on the path, then detection probabilities are accumulated from off-site up to and including the CDP, and this gives P(I) for the path. If there is no CDP on the path, then P(I) is defined as zero.

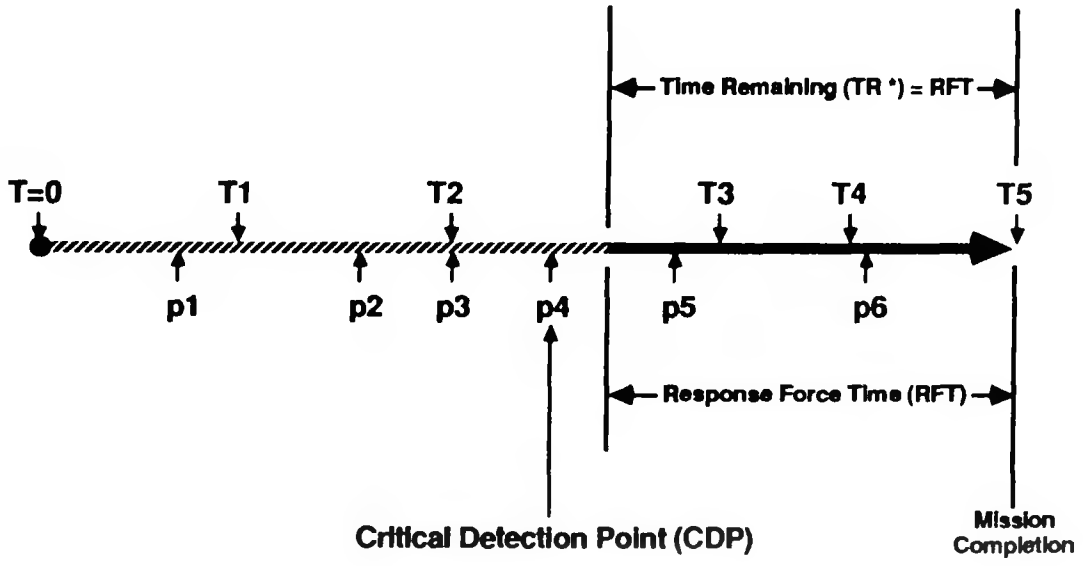


Figure 3.5
Adversary Path Event Line

Tutorial

4.0 Tutorial

This section provides a step-by step tutorial session designed to introduce you to the process of analyzing a physical protection system. All of the necessary steps are covered including: 1) modeling a sample facility, 2) specifying the threat characteristics, 3) defining the protection system values, 4) analyzing the relative path vulnerabilities, and 5) interpreting the displayed results to improve the protection system. To use the tutorial most effectively, you should be at your computer running SAVI before proceeding. You should also be familiar with the SAVI system as explained in Chapter 2, Using SAVI. See Chapter 1 if you need help getting the software started. Allow approximately one hour to work through this tutorial completely.

4.1 Sample Problem

In modeling a PPS, we begin by gathering all relevant data about the facility to be analyzed. This data may come from several sources including, but not limited to, expert judgement, plant layouts, and published information. Once this initial information is obtained, you are ready to begin using SAVI.

A sample facility is shown in Figure 4.1. In examining this figure, note that the facility can be broken down into several distinct physical areas. The area outside of the facility is always referred to as offsite and the point or item to be protected is always referred to as the target. In this case, a protected area, a controlled building area, a controlled room, and a target enclosure make up the facility areas. Notice that this facility has no limited area.

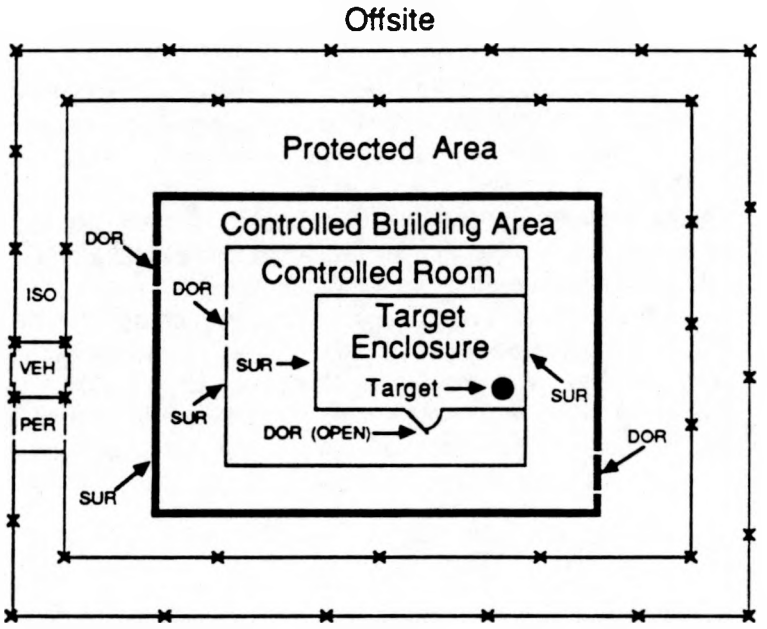


Figure 4.1
Sample Facility

A personnel portal (PER), vehicle portal (VEH), and isolation zone (ISO) separate offsite from the protected area. In addition, two doors (DOR), and a surface (SUR), are between the protected area and the controlled building area. The controlled building area is separated from the controlled room by a single door and a surface. Notice that the controlled building area is also adjacent to the target enclosure separated by a single surface. This arrangement is referred to as a jump.

Finally, a single door and a surface lead from the controlled room to the target enclosure. The target itself is always associated with a target task which the adversary must perform to accomplish his mission.

Although this sample facility represents a simple protection system, analyzing it will demonstrate all of the steps necessary to model much more complex systems within SAVI.

4.2 Modifying the ASD

The sample facility must be modeled correctly within the SAVI system before a vulnerability analysis can be obtained. Upon entering SAVI, a generic ASD is displayed. Your job is to modify this ASD so that it correctly models the sample facility shown in Figure 4.1. If you are not familiar with finding and selecting functions within the SAVI menu system, refer to Chapter 2 before continuing.

4.2.1 Modify - Title

All SAVI functions for modifying the current ASD are found within the Modify sub-menu. The first step in modifying the ASD is to change the ASD title. Select the Modify-Title function and you will be immediately placed in edit mode within a window which contains the current ASD title. Delete the word "`Generic`" by pressing the [Del] key repeatedly. Press the [Ins] key to allow insertion of characters without overwriting. Notice that the blinking cursor increases in height to indicate that you are in insert mode. Type in "`Sample Facility`". The label should now read "`Sample Facility Adversary Sequence Diagram`". Press [↵] to set the new title, and you will return back to the Modify sub-menu.

4.2.2 Modify - Area - Labels

The next step in creating the sample facility model is to specify information regarding the ASD areas. Specifically, we may want to change area label names, or more importantly, specify the traversal limitations for the areas.

You should still be in the Modify sub-menu, so select the Area-Labels function. The first area label is now highlighted. Let's change this title to "LIMITED AREA (UNUSED)" to indicate that there is no limited area in the sample facility model. Press [↵] to enter edit mode for this label. Now use the cursor keys to position the blinking cursor to the right of the word "LIMITED" and type "AREA". Now move the cursor to the second line of the label and type " (UNUSED) " over the original word "AREA". Press [↵] and the area label now reflects your change. SAVI has been designed to allow you to change area label names to reflect the semantics of your particular facility. You could now modify the other area labels, however, this is not necessary for the sample facility that we are modeling. Press the [Esc] key to exit this function and return to the Modify-Area sub-menu.

4.2.3 Modify - Area - Traversal

The Modify-Area sub-menu also provides a function to set the traversal limitations of the facility areas. Select Traversal to see how this function operates. Note that the area labels which are displayed in a dashed-line box (Limited Area, Protected Area) indicate exterior areas which can be traversed by a vehicle. Areas which are labeled with a solid box are restricted to foot traversal only. A pop-up window displays the current traversal setting for the highlighted area. You can press [↵] to modify the setting for the selected area and choose either "INTERIOR" or "EXTERIOR" as appropriate. The settings for the generic ASD are correct for the sample facility that we are modeling, so press [Esc] once to exit this function and again to return to the Modify sub-menu.

4.2.4 Modify - Element - Presence

We now want to specify the protection element layout for the sample facility by modifying the current ASD which appears on

the SAVI screen. The functions which provide this capability are found in the Modify-Element sub-menu. If you are still in the Modify sub-menu, press [E] to enter this sub-menu. The general idea behind these functions is to provide you with a palette of protection elements which you can use to model your specific facility.

Select the Presence function to add or delete PEs for the sample facility. Notice that the first PE within the current ASD is now highlighted, and a window has popped up which displays specific information concerning this PE. You can remove this window if you like by pressing the [space] bar. Pressing the [space] bar again will bring the window back. In this case, you need to delete several PEs to create the sample facility ASD.

Delete all PEs which are not present in our model. Refer again to Figure 4.1. Use the cursor keys to highlight the PEs which need to be removed and press [Del]. Notice that protection elements which are deleted are displayed with dashed lines to indicate that they are no longer present within the model. Continue deleting PEs until you have created the sample ASD. If you delete a PE accidentally, you can re-insert it by pressing [Ins]. Notice that in the sample facility there is no limited area. Therefore, you must delete all PEs which connect the Limited Area to the Protected Area. When you do, a small vertical bar appears between the two area labels to indicate that there is no layer of protection between these areas. This is referred to as a protection layer bypass.

Whenever you want to delete several PEs on a single layer, it may be more efficient to take advantage of a special key sequence provided by SAVI. To delete all PEs on the layer which the highlighted PE is on, simply press [*] followed by [Del]. The [*] key also works with the [Ins] key to insert all PEs on a given layer. Once you have created the desired layout of PEs, exit the function as usual by pressing [Esc].

Note - Helicopter Flight Paths

The Helicopter Flight Path PE cannot be traversed by intruders without a helicopter. For this reason this type of PE cannot be made present in an ASD unless the threat attributes include a helicopter. If the threat does include a helicopter, these intruders are modeled as traveling on foot through the facility after leaving the helicopter at the end of the flight path.

4.2.5 Modify - Element - Jumps

Notice that we also need to specify a jump between the controlled building area and the target enclosure. Select the Modify-Element-Jumps function. Position your cursor on one of the surface PEs between the controlled building area and the controlled room and press [↵]. Notice that the label of the output area within the pop-up window is now highlighted. Use your cursor keys to scroll through the choices for output areas until "TARGET ENCLOSURE" appears. Press [↵] to select this choice. The surface PE which you selected should now indicate a jump directly to the Target Enclosure (area "D"). Press [Esc] three times to exit this function and return to the main menu. You should now have an ASD that looks like Figure 4.2. If you don't, then reselect the appropriate functions to modify the ASD as specified.

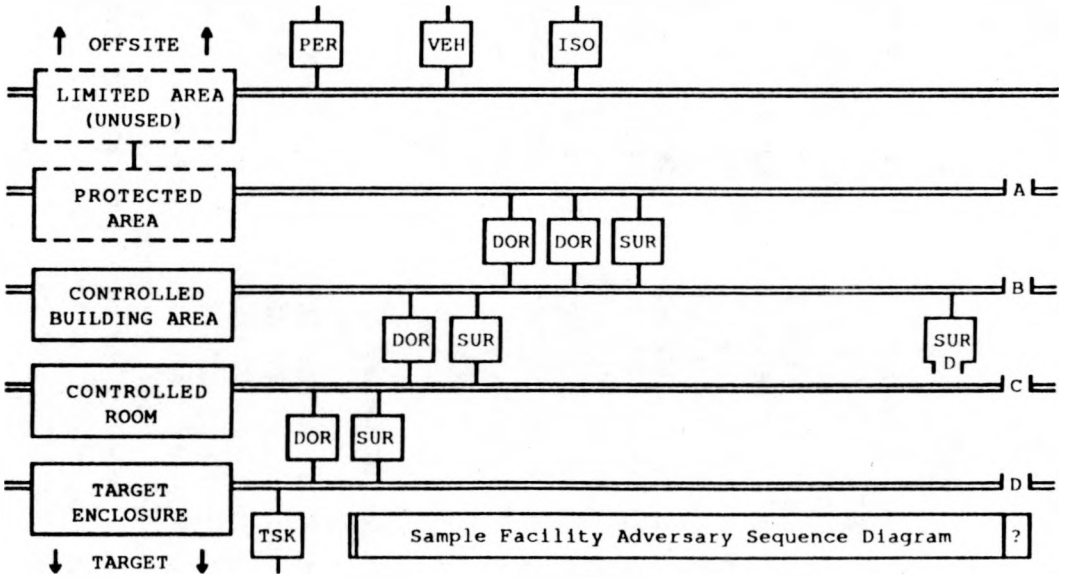


Figure 4.2
Sample Facility ASD

4.3 Specifying The Threat

Now that the current ASD has been correctly modeled to represent a site-specific facility, we need to specify the threat characteristics. The Threat sub-menu provides functions to specify the threat attributes, objectives, and intrusion tactics.

4.3.1 Threat - Attributes

Select the Threat-Attributes function and notice that a window appears displaying three sets of threat attributes. A pointer indicates the current choice, as it does in all SAVI windows which display a list of possible settings in this form. Notice that each set indicates that the intruders are outsiders carrying contraband which will be subject to metal and explosives detectors. The "metal" indicates that the intruders have both weapons and equipment to penetrate structures. The sets differ only in the primary mode of transport (foot, truck, or helicopter). Select the set of threat attributes "`Outsiders With Metal/ Explosives on Foot`" from the list by using the cursor keys to highlight it and pressing [↵] to select it. Once the attribute is selected you will be returned to the Threat sub-menu.

Note - Threat Transport Modes

SAVI models the time for an intruder to traverse distances in the facility based on the best mode of transport available. Therefore, if an intruder has a truck, SAVI will model traversal across an exterior area using the truck for maximum speed. However, each threat can also travel on foot if necessary. SAVI will model traversal by the fastest mode possible, but will switch to foot traversal when required, such as in building interiors. In other words, if an intruder has a vehicle, it will be used when possible, otherwise traversal will be on foot.

4.3.2 Threat - Objective

The next step is to specify the threat objective. Select the Threat-Objective function and another window appears displaying the two types of threat objectives which are supported by SAVI. The threat objective specifies whether you would like SAVI to-determine the vulnerability to intrusion along all paths from Offsite to the Target (Entry Only Analysis) or all paths from Offsite to the Target and back Offsite again (Entry/Exit Analysis). For the tutorial exercise, we will analyze the facility vulnerabilities for an Entry threat. Select this objective in the same way that you selected the threat attributes, and you will be returned again to the Threat sub-menu when complete.

Note - Analysis Complexity

SAVI utilizes an exhaustive search of the entire path space to find the most vulnerable paths through a specific ASD. If N discrete paths exist on entry, then there are N^2 discrete paths for entry/exit analysis. This increase in the number of paths which SAVI must examine for entry/exit may make this analysis impractical for complex systems due to the time required to analyze. It should be noted that if a system is capable of interrupting an intruder before reaching the Target, then it is certainly secure against theft. This is the reason that entry analysis is also referred to as Hands-On theft. If the intruders can't remove the target from its location, they certainly can't steal it. On the other hand, if a security system cannot be designed or upgraded to protect adequately against entry, then entry/exit analysis must be done. It should also be noted that analysis times will be unnecessarily lengthened if multiple PEs with identical settings are ever modeled on the same protection layer. This should always be avoided.

4.3.3 Threat - Tactics

The last threat characteristic that must be set is the intrusion tactics. Select the Tactics function to see another pop-up window with the possible tactics settings. This function allows you to specify the tactics which the intruders will use to penetrate the security system. If the intruders are restricted to forcibly defeating all security components, for example penetrating surfaces and destroying detection systems, then Force Only tactics should be set. However, if the intruders are also able to minimize detection by deception, for example by falsifying ID badges, then Mixed tactics should be selected. Select Mixed tactics for now and you will again be returned to the Threat sub-menu. You have now specified all threat characteristics in preparation for vulnerability analysis. Press [Esc] to return to the main menu.

Note - Force vs Mixed Tactics

Normally a PPS is more secure against intruders who use force tactics only than it is against intruders who both deceive and force protection elements by mixing tactics to minimize detection and delay along a path. Therefore, analysis should be done once for each tactic setting to ensure complete vulnerability analysis.

4.4 Defining System Values

In order to facilitate learning the Define sub-menu, a special tutorial ASD file (SAMPLE.ASD) has been provided with much of the work done for you. This file can be found on your SAVI catalog disk. Make sure that the file directory is set for the disk and sub-directory where the sample ASD can be found. Go to the File sub-menu and retrieve this ASD file. SAVI will ask if you would like to save the changes made so far in this tutorial

session. You may save your work, but it is not necessary since the tutorial ASD which you will retrieve has all the same information with most of the component settings already defined. Once you have retrieved the tutorial ASD, your screen should again look like Figure 4.2.

4.4.1 Define - Component - Settings

The Define sub-menu provides a complete set of functions which allow you to quantify specific information about your facility PPS. The most powerful of these functions, Define-Component-Settings, provides access to the SAVI database of protection element security components.

Choose the Component-Settings function to select the delay and detection components for all PEs in the sample facility ASD. Once this function is entered, notice that the personnel portal within the sample ASD becomes highlighted. Press [↵] to select this PE and a window appears allowing you to choose either delay component or detection component settings. Select delay components, and another window will pop-up with a list of all delay components which might be found in a personnel portal. Select the "INPUT DOOR" component and still another window will pop-up to offer you a list of doors from SAVI's delay component database. Once again a pointer indicates the current choice.

Notice that arrows appear along with the word "MORE" at the top and bottom of the choice list. This indicates that more choices exist both above and below those shown. You can use the cursor keys to view all choices in this list. The [Home] and [End] keys will take you to the beginning and end of the list, respectively and the [PgUp] and [PgDn] keys allow you to move through the list a page at a time.

For the sample facility, the input door into the personnel portal is not locked. Escape from this window and select the delay

component type, "D) OUTPUT DOOR". The output door has been set to, "c) Hollow Core Metal" which offers 12 seconds of delay to the sample threat. When a specific door is selected, yet another window will appear asking you if the door has a panic bar or allows free passage on exit. Select choice "c)" either by highlighting the selection with the cursor keys and pressing [↵] or by simply typing the letter "C". Upon making a choice, the panic bar setting window will pop-up. Notice that a panic bar has <u>not</u> been set for this door. SAVI needs this information to correctly model a door which can be freely opened from the inside. This question will automatically be asked for all delay components which might have this characteristic. Press [Esc] to leave the panic bar setting unchanged or reselect "NO" and the window will disappear, storing your selection.

At the bottom of the choice list you will find the special option, "DIRECT SETTING". This choice gives you the ability to directly input a time delay to be associated with this door. If you choose this option, the value which you enter will be used instead of the value from the delay component database. This capability is available for all delay and detection component settings. When a component value is directly set, this is indicated throughout the component settings windows and on the associated PE itself by a "#". This mark indicates that a component value has been directly set. Notice that the target task PE (TSK) indicates that a direct setting has been made.

Note - Direct Component Settings and the Threat

The SAVI delay and detection databases contain values which are dependent upon the selected threat characteristics. This allows SAVI to re-analyze a PPS for different threats without requiring the user to change any component selections. You can see this by looking at the delay value for a vehicle barrier within an isolation zone. If the current threat attributes include a truck, the vehicle barrier choice window indicates that a concrete

median will delay the intruders by 125 seconds. However, if threat attributes are set so that the intruders are on foot, the time to step over the median becomes negligible and SAVI sets the delay for this component to zero. This automatic modeling based on threat characteristics is only possible when component selections are made from the SAVI database. If component values are directly set, they will be constant for all threats. Therefore, you should reconsider all direct settings whenever the threat characteristics are changed. For this reason, SAVI marks all PEs which have at least one direct setting with a "#" as an aid in finding all such settings.

At the top of each component choice list you will find a choice which is not really a choice at all. The "CLEAR SETTING" allows you to not make a specific choice at this time. If you clear a component, this will be indicated throughout the component settings windows and on the PE itself by a "?". The "?" is SAVI's way of telling you that some component choice has yet to be made.

SAVI cannot analyze an ASD until ALL component choices are made; therefore, if any question marks appear within this function, vulnerability analysis will not be possible until the marks are removed. You can use these indicators to find PEs which you have not finished working on, since there will always be at least one "?" until every PE is completely defined. Make sure that the personnel portal output door component setting is still set to choice "c)", and press the [Esc] key three times to remove all component settings windows.

Notice that the surface between the controlled building area and the target enclosure has a question mark on it indicating that the delay and detection components within this surface have not been set. Refer to Figure 4.3 for the information needed to make these selections.

TITLE: Vault Wall

SURFACE

SUR

INPUT PATH SEGMENT FROM: Controlled Building Area

OUTPUT PATH SEGMENT TO: Target Enclosure

Select the applicable item in each set, or write in component data.

☒ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. SURFACE DELAY STAGE 1 (Note: Choices in Stages 1 and 2 Must Be Identical)	t in seconds
a) Open Port	0
b) Unbarred Window	5
c) Vent, Port, Duct: Standard Louvers	30
d) Vent, Port, Duct: Heavy Grid	60
e) Vent, Port, Duct: Diffusers	120
f) 4" Framed w/ Sheetrock	10
g) 4" Concrete	30
h) 16 Gauge Metal	48
i) 4" Concrete w/ Rebar	84
j) 8" Concrete w/ Rebar	120
k) 12" Concrete w/ Rebar	120
l) 18" Concrete w/ Rebar	120 ●
m) 24" Concrete w/ Rebar	120
n) 36" Concrete w/ Rebar	156
o) 2' Earth	120
p) 3' Earth	120
q) 4' Earth	120
r) 6' Earth	120
s) 10' Earth	156
SET	

B. SECURITY INSPECTOR DELAY	
a) No Inspector	0 ●
b) Unprotected Inspector	5
c) Protected Inspector	30
d) Inspector in Hardened Position	120
SET	

C. SURFACE DELAY STAGE 2 (Note: Choices in Stages 1 and 2 Must Be Identical)	t in seconds
a) Open Port	0
b) Unbarred Window	0
c) Vent, Port, Duct: Standard Louvers	0
d) Vent, Port, Duct: Heavy Grid	0
e) Vent, Port, Duct: Diffusers	0
f) 4" Framed w/ Sheetrock	0
g) 4" Concrete	0
h) 16 Gauge Metal	0
i) 4" Concrete w/ Rebar	0
j) 8" Concrete w/ Rebar	0
k) 12" Concrete w/ Rebar	54
l) 18" Concrete w/ Rebar	180 ●
m) 24" Concrete w/ Rebar	384
n) 36" Concrete w/ Rebar	756
o) 2' Earth	0
p) 3' Earth	54
q) 4' Earth	180
r) 6' Earth	384
s) 10' Earth	756
SET	

DETECTION COMPONENTS

A. SURFACE PENETRATION DETECTION (Select the lowest value surface detection component regardless of the surface delay component selected.)	P
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99 ●
e) Grid Mesh	.99
SET	

B. PERSONNEL DETECT SURFACE INTRUSION	
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99 ●
SET	

C. INTERIOR INTRUSION DETECTION	P
a) No Sensors	0.0 ●
b) Sensors Turned Off	0.0
c) Single Motion Sensor	.5
d) Complementary Motion Sensors	.9
SET	

D. SECURITY INSPECTOR DETECTION	
a) No Inspector	0.0 ●
b) Inspector w/o Duress Alarm	0.0
c) Inspector w/ Duress Alarm	.5
d) Protected Inspector w/ Alarm	.99
SET	

Page 1 of 1

Figure 4.3
Sample Surface Delay/Detection Component Settings

Use your cursor keys to highlight this surface and press [↵] to begin setting the components. Select the delay components and the first delay component type, "SURFACE DELAY STAGE 1". Notice in Figure 4.3 that the correct choice for this component is, "1)- 18" Concrete w/ Rebar". Select this choice either by highlighting it with the cursor keys and pressing [↵] or by simply typing the letter "L". Note that the same choice which you make for the stage 1 delay should be made for the stage 2 delay as well. Continue to refer to Figure 4.3 to make all delay and detection component settings for this PE.

When you complete the settings for this PE, and escape from the component settings windows, notice that the question mark has been removed, indicating that you have made all choices for this PE. Once you have finished, escape from the Component-Settings function. All component settings are now defined in preparation for vulnerability analysis.

4.4.2 Define - Component - Copy

A Copy function is also offered within the Component sub-menu. This function can be very valuable when you have more than one PE in an ASD with exactly the same component settings. In these cases, you can make the component selections once and then copy the entire contents of the PE over to another PE using this function. We do not need this function now, but you may want to experiment with it to see how it operates.

When you select this function, the first PE in the ASD becomes highlighted. Notice also that every PE in the system, even those that are not present in the current ASD are available to copy from or to. This allows you to store PE settings in unused PEs for use later. These settings are all stored when you save your ASD. Use the cursor keys to highlight the PE that you wish to copy, and select it by pressing [↵].

In the sample facility, the surface between the Controlled Building Area and the Target Enclosure has the same characteristics as the surface between the Controlled Room and the Target Enclosure. Knowing this, we could have saved some time by copying the settings from one to the other. You can try it now if you like. Select the surface between the Controlled Room and the Target Enclosure and notice that this PE begins blinking, indicating that it is ready to be copied. Now you may highlight any other PE to copy to, even one of a different type. In this case you want to highlight the surface between the Controlled Building Area and the Target Enclosure. Press [↵] and all settings from the blinking PE are copied over. This function is a real time saver for more complex ASDs. When you finish using this function, press [Esc] twice to return to the Define sub-menu.

4.4.3 Define - Distance - Areas

Next we want to define the traversal distances associated with each area and relevant PE in the sample facility. The Define-Distance sub-menu provides the functions to set these distances.

Select the Define-Distance-Areas function to set the distance across each area. Notice that the top area label becomes highlighted and a window appears displaying the current distance setting for this area. The time associated with traversing this area for the current threat is also displayed. Press [↵] while highlighting any area to enter edit mode. The new distance can now be entered.

Refer to Table 4.1 for the distance across each area. Enter the distance from the table for each area by typing over the old distance settings and pressing [↵] to set the values. When all distances have been entered, press [Esc] to exit this function and return to the Define-Distance sub-menu.

4.4.4 Define - Distance - Elements

Now select the Elements function to enter the distances across the PEs mentioned in Table 4.1. This function operates the same as the Distance-Areas function. Any PEs which do not have a distance specified in Table 4.1 are already set to zero. When you have entered all distances, press [Esc] twice to return to the Define sub-menu.

Areas	Distance (m)
Limited Area (Unused)	0
Protected Area	31
Controlled Building Area	31
Controlled Room	15
Target Enclosure	6
Protection Elements	
Personnel Portal	15
Vehicle Portal	15
Isolation Zone	15

Table 4.1
Sample Facility Traversal Distances

4.4.5 Define - Response

Finally, you must set the response force time range. These values represent the range of times required for the security response force to interrupt the intruders following detection.

Select the Define-Response function and two windows appear, displaying the number of times in the current range, and the range of response force times. These windows are shown in Figure 4.4.

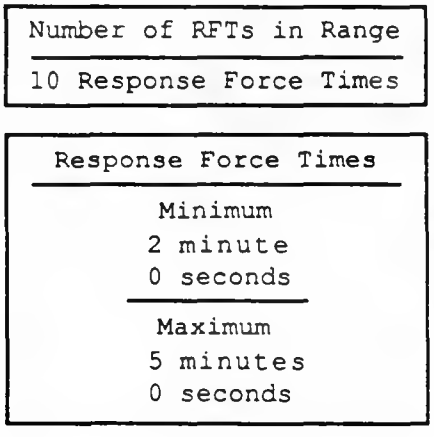


Figure 4.4
Response Force Time Range Input Windows

Notice that the number of RFTs is highlighted allowing you to specify the number of times you would like in the range. Up to 10 RFTs can be set. Set the number of RFTs in the range to 10 and press [↵]. Now you are able to edit the minimum and maximum time values in the range window. These values represent the shortest and longest times that the response force might require to interrupt the intruders following detection. Note that these times must include response force alarm assessment, communication, and deployment. Enter the minimum and maximum times found in Figure 4.4 and press [↵] to set the values. Once this is accomplished, escape from this function all the way back to the main menu.

The sample facility is now completely modeled and site specific protection values are defined. SAVI is ready to calculate path vulnerabilities.

It is a good idea to save your ASD periodically during a SAVI session, especially after all data are entered prior to analysis. Simply select the File-Save function and you will be prompted from there. After the file has been saved, you may also want to print out documentation of the ASD settings. This is done by selecting the functions found in the Print sub-menu, allowing you to print both your facility diagram (ASD) and tables of all current settings.

4.5 Analyzing Path Vulnerabilities

The Analyze sub-menu provides the functions that display the calculated system vulnerabilities, offer improvement recommendations, and produce graphic results. Analysis occurs automatically when Analyze is selected if results have not been previously calculated. Note that a "?" is displayed at the right side of the ASD title box as long as analysis results are not calculated for the current ASD.

Select Analyze now and vulnerability calculations will be done for the current ASD. When analysis begins, an estimate is made of the time that will be required, and this estimate is updated throughout the analysis. If for any reason you do not want to wait for analysis to be completed, you can escape by pressing the [Esc] key.

Once the analysis is finished, notice that the analysis required indicator on the right side of the ASD title has disappeared. You may want to save your ASD again now that analysis is complete since these results are automatically saved along with the ASD if they are available.

When the vulnerability calculations are completed, you are placed in the Analyze sub-menu. The functions within this menu provide the ability to display the most vulnerable paths through the ASD for any response force time in the previously specified range, and produce various graphs of the system

vulnerabilities. The Vulnerability function displays vulnerability diagnostics for each path, the Recommendations function gives simple improvement suggestions for upgrading the system, and the Graphs sub-menu provides access to all graphing capabilities.

4.5.1 Analyze - Results - Vulnerability

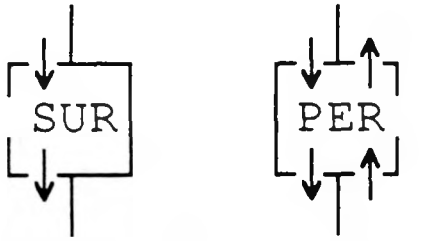
Select the Results-Vulnerability function to view the most vulnerable paths for the current threat. A large window appears on the right of the screen to display the vulnerability diagnostics for each path. The first path displayed is the most vulnerable path (path number 1) for the maximum response force time (RFT # 10). Notice that the paths are ranked by vulnerability (Most Vulnerable Path, Second Most Vulnerable Path, etc.).

The probability of interruption (P(I)) along this path and the time remaining after interruption (TRI) are also displayed. Even though P(I) is generally considered the most important measure of vulnerability, it is also necessary to consider the location of the critical detection point as well as TRI, which represents the time remaining on a path after interruption occurs. These measures are fully discussed in the Reference Manual under Analyze-Results-Vulnerability. Simply press the [space] bar to remove this window to see the corresponding path through the ASD.

The most vulnerable path scenario is displayed as a highlighted chain of all PEs along the path. Notice that arrows along the path indicate the intruders direction. The critical detection point (CDP) is indicated by the arrow which is blinking red. This indicates that the intruders must be detected by the time they reach this point if the response force is to have enough time to interrupt them before the system is defeated.

SAVI also determines and displays the penetration tactics which the intruders would use for each PE along this path. Notice that

the left side is missing from the isolation zone PE. This indicates that the system is most vulnerable if the intruders force this element on entry into the facility. You should think of the hole in the side of the PE as an indication of forced intrusion. Elements which are forced on entry toward the target are then less secure on exit. This dependency is accurately modeled within SAVI. In contrast, notice that the first door into the controlled building area is still intact indicating that the intruders would pass this element by deceit. In this example, the most vulnerable deceit path through this door involves falsifying ID badges. Figure 4.5 shows how to interpret these tactic markings for PEs on a path.



Force Entry

Deceit Entry
Force Exit

Figure 4.5
PE Tactic Markings

Within this function you can use the cursor keys to scroll through the most vulnerable paths and through the range of RFTs. The left and right arrow keys step through the ranked paths, and the up and down arrow keys scroll through the RFT range. Press [Home] to display the most vulnerable path and [End] to display the least vulnerable of the ranked paths. [PgUp] and [PgDn] move directly to the minimum and maximum RFT.

Another pop-up window is displayed to help you move through the most vulnerable paths for the entire range of response force times without getting lost. This small window on the left of the screen indicates at all times the vulnerability rank and RFT for the highlighted path. ~Using this window, you should be able to easily find any combination. For example, the most vulnerable path for the first RFT, or the sixth most vulnerable path for the tenth RFT. This little window can also be removed from the screen at any time by pressing the [space] bar. Press the [space] bar again to return both the diagnostics window and this window.

Now let's look more closely at the vulnerabilities of this system. If the diagnostics window is not on the screen, press the [space] bar again until it reappears. The window indicates that the probability of interrupting the specified threat along this path is only 0.1 (10% chance). The blinking red arrow which marks the CDP is on the output path segment of the first door leading into the controlled building area, indicating that the intruders must be detected by this point on the path for interruption to occur. Now press the [Esc] key to exit this function so that we can see the recommendations for system improvements.

4.5.2 Analyze - Results - Recommendations

Select the Recommendations function and another large window appears on the right side of the screen with suggestions for improvements to the displayed path. This function operates the same way that the Vulnerability function does, allowing you to view the most vulnerable paths for all RFTs in the specified range. For the most vulnerable path and the maximum RFT, the window suggests improving the detectors on the elements that precede the CDP, and increasing delay within the elements after this point. The isolation zone seems to be a likely candidate for improvement. Escape from this function keeping in mind that improving the detection components within the isolation zone is a suggested upgrade for this ASD.

4.5.3 Analyze - Results - Graphs

Before we modify the system, enter the Graphs sub-menu to see the system vulnerabilities presented in a different form. As soon as you select Graphs, the screen makes a dramatic change from the ASD layout, to a graph of analysis results. Notice that the familiar two line menu is still there. Three different graphs can be plotted, each selected from within the Type function.

The graph which you see displayed first is a plot of P(I) and TRI for the most vulnerable paths for a single RFT. This is a concise graphic representation of the information found in the Results-Vulnerability function. Notice that the most vulnerable path (path number 1) has a P(I) of 0.1 as we saw in the Results-Vulnerability function.

You may change the scale from linear to logarithmic if desired using the Scale function, or expand the vertical scale to examine the data more closely by selecting Zoom. These functions can be selected for each of the three graph types. Refer to the Reference Manual for more on these two functions.

Select the Response function to see an animated display of the vulnerability measures for each RFT in the current range. Notice that another pop-up window appears, indicating for which RFT the current graph is plotted. Press the [Home] key to graph the vulnerability data for the minimum RFT (120 seconds). Use the cursor keys to scroll through the entire RFT range. Notice that the system becomes more vulnerable (P(I) decreases) as the response force takes more time to respond. Ensure that the RFT is reset to 300 seconds, and press [Esc] to leave this function.

Now select the Type function to view another graph. Upon selecting Type, a window appears indicating the three graph types which can be displayed. The first type, Vulnerability, is the graph which we have just seen. Select the second graph type, Sensitivity, and a graph of P(I) for the most vulnerable paths

across the entire range of RFTs will be drawn. This graph clearly indicates the system sensitivity to variation in response force time. Notice that for the current ASD, the probability of interrupting an intruder along the most vulnerable path is better than 0.95 (95%) if the response force can respond in 200 seconds or less. However, if the RFT is greater than 200 seconds, the probability of interrupting an intruder along the most vulnerable path drops to 0.1 (10%).

This information can be very helpful in making upgrade decisions. If the response force can guarantee response in 200 seconds or less for our sample facility, the security system might be considered acceptable. On the other hand, if the response force cannot be made to respond any faster, then the PE components must be upgraded. We will assume that the response force in the sample facility may require up to 5 minutes (300 seconds) to respond in some instances.

Before we upgrade the current ASD, return again to the Type function and select the last graph type, Distribution, for a broad view of system performance. This graph displays a histogram of P(I) for all paths through the system. Use this graph to determine what percentage of paths are acceptable. In some cases, a great majority of the paths through a facility are considered acceptable, but the remaining few percent are very vulnerable. This information can give you a feel for the number of paths which might not be adequately secure against intrusion. For the sample facility, you will need to change to a logarithmic scale to see all of the data in this graph. Once you change the scale, notice that over 99% of the paths have a P(I) greater than 0.75 but 0.5% have a P(I) of 0.15 or less.

Escape now from the Graphs sub-menu all the way back to the main menu so that we can upgrade this facility.

4.6 Improving the Protection System

Recalling that SAVI recommended an improvement in the detectors within the isolation zone, select the Define-Component-Settings function so that we can examine the detectors within this element. Highlight the isolation zone PE and select the detection components as suggested.

If we look at the settings of these detection components we find that they appear to be appropriate for a common isolation zone. Notice that the ground detection component ("C") between the fences is selected as multiple sensors with a detection probability of 0.8.

At this point, it should be noted that the personnel portal for this facility spans the isolation zone (see Figure 4.1). However, if we look at the building roof detectors (component "G") within the isolation zone, we notice that the system has been set without any sensors on the roof of the building which spans the isolation zone. Therefore, the intruders would simply climb over the roof of the personnel portal and avoid all probability of being detected while crossing this protection layer. This can be easily corrected by installing roof detectors comparable to the ground sensors which already exist. Select multiple sensors (choice "e") for the building roof detection and escape back to the main menu. You would normally want to modify the title of the ASD at this point to indicate that an upgrade has been implemented.

Select Analyze once again to recalculate path vulnerabilities with the upgrade in place. Once this analysis is complete you may want to save the ASD under a new file name along with the new results to document this upgrade. If you like, you can do this now. Otherwise, select the Results-Vulnerability function to see the effect of your change. Notice that P(I) for the most vulnerable path with the maximum RFT has now improved to 0.775. Select the Graphs functions again to determine if this upgrade is adequate.

At this point, it should be clear to you that making security system upgrades is an iterative process in which you: 1) examine the most vulnerable path for an RFT of concern, 2) modify an appropriate PE's component values to improve the system effectiveness, and 3) re-analyze the system to observe the effects. It is suggested that you continue to upgrade the sample ASD and model other sample facilities to become more familiar with the SAVI package. Refer to Chapter 3 and the Reference Manual for more on fully utilizing the power of SAVI.

Reference Manual

REFERENCE MANUAL

This Reference Manual is written under the assumption that you have read and understand the information which is covered in the SAVI User's Guide. You should be familiar with the main screen display, use of the menu system, and techniques for entering data, as well as understand the basic terms and concepts which underlie vulnerability analysis.

The SAVI menu system is a tree structure, containing sub-menus, or branches, of associated functions. The main menu contains a set of sub-menus which lead to further sub-menus as well as to related functions. Each function is found at the end of a sub-menu branch, and is invoked when selected from the menu. See Figure R-1 for a diagram of the SAVI menu structure. This figure is also found in Chapter 2 of the User's Guide.

Notice that the sequence of selections which lead from the main menu to a particular function forms a string of words which helps describe the function. For example, "Define - Component - Settings" or "Modify - Element - Types". Use this feature to make SAVI functions both easier to remember and easier to find.

All sub-menus and functions are listed here in alphabetical order. Each sub-menu entry lists the sub-menus and functions which it leads to, and each function entry includes a description of capabilities along with instructions for its use. The first letter of each entry is shown in bold text to indicate that any choice can be selected within the menu system by pressing the key which corresponds to the first letter.

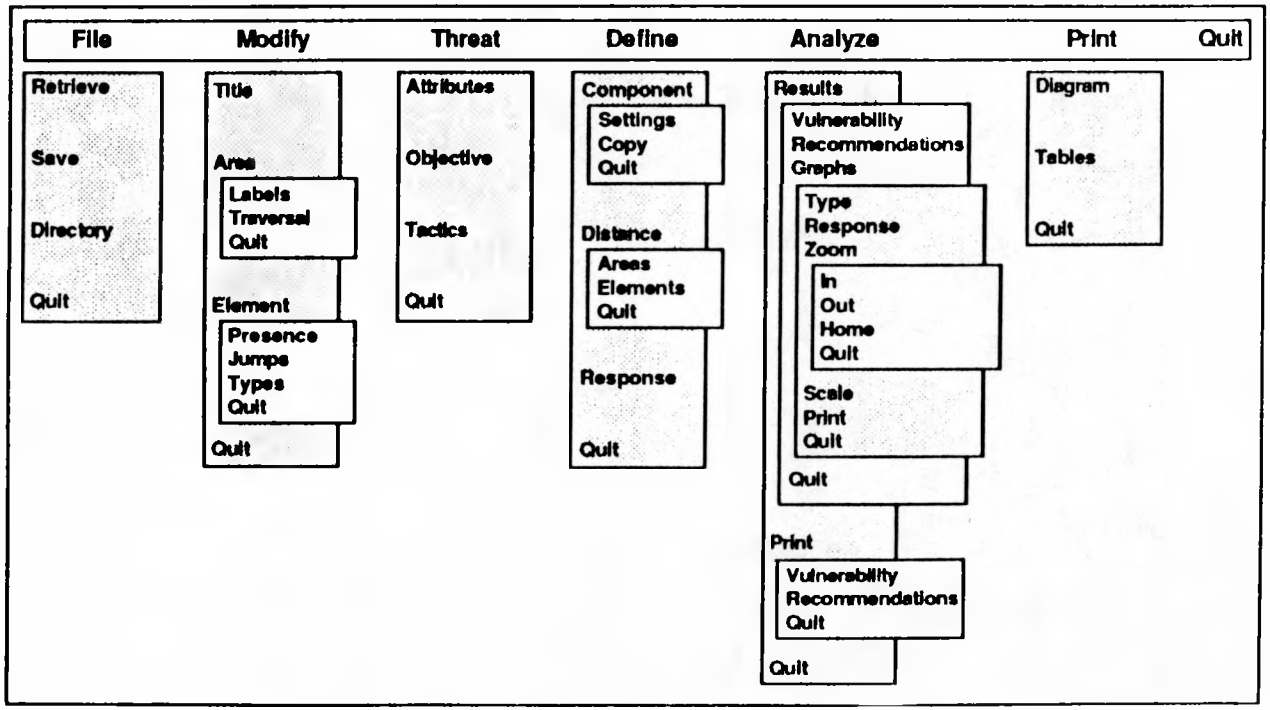


Figure R-1
SAVI Menu Structure

Analyze
Sub-Menu

Description: Calculates the most vulnerable paths through the current ASD and provides access to the Results sub-menu which contains the functions which display the vulnerability diagnostics, improvement recommendations, and analysis graphs. Path vulnerabilities are automatically calculated upon entering this sub-menu if necessary. A "?" is displayed at the right side of the ASD title box to indicate when analysis is required.

Contents:
Results
Print
Quit

Analyze - **P**rint
Sub-Menu

Description: Provides access to the functions which print the results of the vulnerability calculations and system improvement recommendations.

Contents:
Vulnerability
Recommendations
Quit

Analyze - **P**rint - **R**ecommendations
Function

Description: Prints the recommended changes to the delay or detection component values for each PE along the most vulnerable paths for the range of response force times.

Usage: A pop-up window appears displaying the current RFT for which recommendations are to be printed. Use the cursor keys to select a new RFT, if desired. Pressing [↵] enters the selection and begins printing. Press [Esc] at any time to cancel printing and return to the Analyze-Print sub- menu.

Analyze - **P**rint - **V**ulnerability
Function

Description: Prints a table of PEs which lie on the most vulnerable paths and vulnerability diagnostics for each path for a particular RFT from the response force time range. This information includes:

- path rank within most vulnerable paths
- probability of interruption (P(I))
- critical detection point (CDP)
- time remaining after CDP
- time remaining after interruption (TRI)
- response force time (RFT)

If the probability of interruption is zero along any path, diagnostic messages are printed to assist in evaluating the cause.

Usage: A pop-up window appears displaying the current RFT for which vulnerability diagnostics are to be printed. Use the cursor keys to select a new RFT, if desired. Pressing [↵] enters the selection and begins printing. Press [Esc] at any time to cancel printing and return to the Analyze-Print sub- menu.

Analyze - **R**esults
Sub-Menu

Description: Provides access to the functions which display the most vulnerable paths with diagnostics, recommendations for improving the most vulnerable paths, and the sensitivity analysis graphs.

Contents:
Vulnerability
Recommendations
Graphs
Quit

Analyze - Results - Graphs
Sub-Menu

Description: Provides access to the functions which graphically display the results of the vulnerability calculations and print these graphs. When Analyze-Results-Graphs is selected, the SAVI main screen ASD display is replaced by a graph of vulnerability results.

Contents:

Type
Response
Zoom
Scale
Print
Quit

Analyze - **R**esults - **G**raphs - **P**rint
Function

Description: Prints the current graph.

Usage: When selected, this function automatically prints the current graph. The two line menu at the top of the screen is replaced by the ASD title and the current threat settings to further document each printout.

Note - This function will not operate correctly unless a memory resident screen dump utility was loaded prior to running SAVI. The graphic print utility (usually called GRAPHICS.COM or GRAPHICS.EXE) must be capable of printing a high-resolution screen (640x200 pixels) from a CGA compatible display device. Consult your computer system documentation for more on this topic.

Analyze-**R**esults-**G**raphs-**R**esponse Function

Description: Displays the Vulnerability and Distribution graphs for any RFT selected from the response force time range. The current graph information is animated as the user scrolls through the RFT range. This function is not available for the Sensitivity graph, since this graph displays data from the entire RFT range.

Usage: The current display RFT number is displayed in a pop-up window. Use the cursor keys to scroll through the range of RFTs and see the current graph updated for each value. The display RFT can be set directly by pressing [↵] to enter edit mode within the RFT window. Type in the desired RFT number and press [↵]. If desired, you can end editing and revert to the original RFT by pressing [Esc]. Press [Esc] when not in edit mode to exit this function.

Analyze - **R**esults - **G**raphs - **S**cale
Function

Description: Selects a linear or logarithmic scale for the vertical axes of the current graph. The logarithmic scale is useful for displaying data with a large range of magnitudes.

Usage: A pop-up window appears with a pointer indicating the current scale setting. Use the cursor keys to select either scale type and press [↵] to enter the selection. Pressing [Esc] exits the function, leaving the setting where the pointer indicates.

Analyze - **R**esults - **G**raphs - **T**ype
Function

Description: Selects the current graph type. Three types of graphs are available:

- Vulnerability - Plots P(I) and TRI for the most vulnerable paths for any RFT from the current range. This is a graphic display of the results which are presented in the Analyze-Results-Vulnerability function.

- Sensitivity - Plots the P(I) of the most vulnerable path for each RFT in the current response force time range. This graph can be used to find the critical point in an RFT range where P(I) drops below an acceptable level.

- Distribution - Plots the distribution of P(I) for all paths through the current ASD for any RFT in the current range. This graph provides a broad view of the vulnerability of the entire path set.

Usage: A pop-up window appears with a pointer indicating the current graph type. Use the cursor keys to select the desired graph type and press [↵] to make this selection. Pressing [Esc] exits the function, leaving the setting where the pointer indicates.

Analyze - Results - Graphs - Zoom
Functions

Description: The Zoom functions increase or decrease the range of the vertical axis for the current graph so that the vulnerability results can be examined with greater resolution.

Functions:
In
Out
Home
Quit

Usage: When the current graph is first displayed, the vertical range scaling is automatic and is referred to as the home view. In this case the only Zoom function available is Zoom-In. When selected, a dotted frame appears which can be adjusted in height using the cursor keys to set a new range for the vertical axis.

Initially, the top of this frame displays two arrows indicating that it can be moved down to decrease the maximum axis setting. Press the [Space] bar to toggle between control of the top and bottom of the range frame. The bottom of the frame can be moved up to increase the minimum axis setting. Use this capability to frame data in a region of the current graph which you would like to examine more closely. Once you have set the desired range, press [↵] to exit the Zoom-In function and the graph will be redrawn with the new range. You may zoom further into the displayed graph by selecting this function repeatedly as desired.

Analyze - Results - Graphs - Zoom
(continued)

Once the Zoom-In function has been used, the Zoom-Out and Zoom-Home functions become available. Choose Zoom-Out to return to the previous view. The Zoom-Home function returns the current graph to the home view directly.

Analyze-**R**esults-**R**ecommendations
Function

Description: Suggests improvements to the delay or detection values for each PE along the most vulnerable paths for any RFT in the current response force time range.

Usage: When this function is selected, two pop-up windows appear along with a highlighted path. The small window on the left side of the screen identifies the highlighted path by displaying its path number and the associated RFT. The larger window on the right displays the recommended modifications for the highlighted path.

Use the cursor keys to highlight any path by scrolling through the path numbers and RFT range. The left and right arrows are used to change the path number and the up and down arrows scroll through the RFT range. The [Home] and [End] keys can be used to display the most vulnerable and least vulnerable ranked paths respectively. Use [PgUp] and [PgDn] to select the minimum and maximum RFTs in the current range.

Arrows, which indicate the intruder's direction of travel, are displayed on each protection element on the highlighted path. The CDP is displayed as a blinking arrow on the appropriate protection element of each path.

Analyze-Results-Recommendations
(continued)

The sides of each protection element along the highlighted path are displayed with either a solid or broken line to indicate the intrusion tactics that would be used to cross this PE for the current threat settings. A solid line indicates that the PE would be passed through deceit, while a broken line indicates penetration by force. The left and right sides of each PE are associated with entry and exit respectively. For example, a PE with a solid line on the left side and a broken line on the right side indicates traversal by deceit upon entry into the facility, and by force upon exit.

The improvement recommendations are based on the concept of timely detection and show where to improve detection and/or increase delay relative to the critical detection point on the highlighted path. You should upgrade the component settings as appropriate to change a single PEs delay or detection values based on these recommendations and return to the Analyze sub-menu before making further changes. This ensures that the effect of the changes will be determined in an iterative manner.

By repeatedly pressing the [space] bar, the two windows can be toggled on and off in different combinations to permit an unobstructed view of the ASD display. Press [Esc] at any time to exit this function.

Analyze - **R**esults - **V**ulnerability
Function

Description: Displays the most vulnerable paths and vulnerability diagnostics for any RFT in the current range. The diagnostics include:

- path rank within most vulnerable paths
- probability of interruption (P(I))
- time remaining after critical detection point
- time remaining after interruption (TRI)
- response force time (RFT)

If the probability of interruption is zero along any path, diagnostic messages are displayed to assist in evaluating the cause.

Usage: When this function is selected, two pop-up windows appear along with a highlighted path. The small window on the left side of the screen identifies the highlighted path by displaying its path number and the associated RFT. The larger window on the right displays all vulnerability calculations for the highlighted path.

This function operates the same way that the Recommendations function does. Refer to the entry for Analyze-Results-Recommendations for details on displaying a path for a particular RFT and interpreting the highlighted path markings.

Press [Esc] to exit this function.

Define
Sub-Menu

Description: Provides access to functions which define protection system values for the current ASD. Delay and detection components for each protection element may be specified along with the range of response force times and the traversal distances across all PEs and areas.

Contents:
Component
Distance
Response
Quit

Define - Component
Sub-Menu

Description: Provides access to functions which allow setting of delay and detection components for each protection element.

Contents:
Settings
Copy
Quit

Define - Component - Copy
Function

Description: Copies a selected protection element with all of its settings from one PE to another. All PEs in the generic ASD can be used, even those which are not present in the current ASD. This allows PE settings to be copied to an unused PE for later use. All PE settings, including those for non-present PEs, are saved to disk within the File-Save function.

Usage: Use the cursor keys to highlight the protection element to be copied from. A pop-up window appears to display the protection element type and input/output areas. Press [↵] to select the PE. This PE will begin to blink to indicate that it is ready to be copied. Use the cursor keys to highlight the PE which is to be copied to and press [↵] to copy. An exact copy of the blinking PE is made, including all component settings and the element traversal distance. Press [Esc] when finished copying to return to the Define-Component sub-menu.

Define - Component - Settings
Function

Description: Defines the delay and detection component settings within each protection element. This function provides access to the SAVI security component database.

Usage: Use the cursor keys to highlight any protection element to be defined and press [↵]. A pop-up window appears allowing definition of either delay or detection components. Use the cursor keys to choose which type of components are to be defined and press [↵]. Another window pops-up displaying a list of all delay or detection components associated with the highlighted PE. Select each component as desired to see another pop-up window containing the specific component choices available. Note that the current component setting is indicated by a pointer. Use the cursor keys to highlight the desired choice and press [↵] to select it, or simply press the corresponding alpha key.

Any component choice can be cleared by selecting the first choice on the component list, "CLEAR SETTING", or by pressing [?]. Also, the delay or detection value for each component can be set directly by choosing the last choice on the component list, "DIRECT SETTING", or by pressing [#]. When component settings are cleared or directly set, a "?" or "#" will appear as appropriate throughout the component settings windows and on the associated PE itself to indicate this.

If it is possible for a delay component to allow free passage on exit from the facility (ie; a door with a panic bar), a pop-up window will appear to allow this to be specified.

Pressing the [Esc] key repeatedly will close this series of windows and exit this function.

Define - Distance
Sub-Menu

Description: Provides access to functions which define the distances across all areas and protection elements.

Contents:
Areas
Elements
Quit

Define - Distance - Areas
Function

Description: Displays the distance across any area and allows it to be redefined. SAVI uses these distance settings to calculate the time for an intruder to cross each area based on the intruder's mode of transportation and the area traversal limitations. The calculated transit time associated with each area is also displayed.

Usage: Use the cursor keys to highlight the area for which the distance is to be specified. Press [↵] to enter edit mode for this window and enter a new setting. The distance entered should represent the minimum distance across the associated area. Press [↵] again to set the new value. If you like, you can end editing and revert to the original distance setting by pressing [Esc]. When all area distances are set correctly, press [Esc] to exit this function.

Define - Distance - Elements
Function

Description: Displays the distance across any protection element in the current ASD and allows it to be redefined. SAVI uses these distance settings to calculate the time for an intruder to cross each element based on the intruder's mode of transportation and the element type. The calculated transit time associated with each element is also displayed.

Usage: Use the cursor keys to highlight the PE for which the distance is to be specified. Press [↵] to enter edit mode for this window and enter a new setting. The distance entered should represent the minimum distance across the associated PE. Normally this function will only be used for protection elements which have considerable length such as tunnels or wide isolation zones. Enter the appropriate distance and press [↵] to set it. If you like, you can end editing and revert to the original distance setting by pressing [Esc]. When all PE distances are set correctly, press [Esc] to exit this function.

Define - Response
Function

Description: Allows specification of a range of response force times for the current modeled facility. The range is specified by setting the number of RFTs in the range and the minimum and maximum response times. This allows vulnerability analysis results to be examined with respect to variations in the response force time.

Usage: The number of RFTs in the current range is displayed in a pop-up window and may be edited using the cursor keys or by directly entering the desired number. The range can be set to contain up to ten RFTs. Press [↵] to set the number of times and begin editing the minimum and maximum RFT values. If a single RFT is selected, a single RFT value may be entered. Once the RFT value(s) are entered, press [↵] to set these values and exit this function by pressing [Esc].

File
Sub-Menu

Description: Provides access to the functions which retrieve and save ASD disk files.

Contents:
Retrieve
Save
Directory
Quit

File - Directory
Function

Description: Sets the current data disk file directory for the File-Retrieve and Save functions.

Usage: A pop-up window appears displaying the current data file directory. Enter the new file directory and press [↵]. The file directory must conform to DOS path name conventions. When SAVI is started, the data disk file directory is set to the current DOS directory. If you would like ASD files to be stored on a specific disk or directory, use this function to set the directory path. You may exit this function without changing the directory by pressing [Esc] at any time.

File - Retrieve
Function

Description: Replaces the current ASD with a selected ASD retrieved from disk. If analysis results were saved along with the ASD, these will be retrieved as well.

Usage: A pop-up window appears to accept the name of the ASD disk file to be retrieved. Enter the name of the ASD file and press [↵] to retrieve the selected file. You may exit this function without retrieving a new ASD by pressing [Esc] at any time.

File - Save
Function

Description: Saves the current ASD to a specified data disk file. Analysis results are saved along with the ASD if analysis has been completed. A "?" appears at the right side of the ASD title box to indicate when analysis is required. If this mark is not displayed when the ASD is saved, analysis results are available and will be stored along with the ASD settings.

Usage: A pop-up window appears to accept the name of the ASD disk file in which to save the current ASD. Enter the ASD file name, and press [↵] to save the current ASD to this file. If the selected file already exists within the data disk directory, you will be offered the option of replacing it with the current ASD. This function can be utilized to make copies of the current ASD to disk files of different names for future use. You may exit this function without saving by pressing [Esc] at any time.

Modify
Sub-Menu

Description: Provides access to the functions which modify the current ASD display, including setting the ASD title, area labels, protection element types and area connections.

Contents:
Title
Area
Element
Quit

Modify - **A**rea
Sub-Menu

Description: Provides access to functions which modify the current ASD area labels and area traversal settings.

Contents:
Labels
Traversal
Quit

Modify - **A**rea - **L**abels
Function

Description: Modifies the area labels for the current ASD.

Usage: Once this function is selected, the first area label is highlighted and a pop-up window appears displaying the label text. Use the cursor keys to highlight any area label to be modified and press [↵] to edit the label. Enter the new text into the two lines in the window, and press [↵] to set the new label. If you like, you can revert to the original area label by pressing [Esc]. Once all area labels are set, press [Esc] to exit this function.

Modify - Area - Traversal
Function

Description: Modifies the area traversal settings. Each area can be specified as either interior or exterior. Interior areas allow foot traversal only, whereas exterior areas also allow traversal by vehicle. This information is used to calculate the transit time across each area based on the current threat attributes.

Usage: Once this function is selected, the first area label is highlighted and a pop-up window appears displaying its traversal setting. Use the cursor keys to highlight the label for any area and press [↵] to edit the traversal setting. The current traversal setting is indicated by a pointer within the pop-up window. Highlight the desired setting and press [↵] to enter the selection. Notice that interior areas are indicated by a solid line box surrounding the area label, whereas exterior areas are indicated by a dotted line box. Once all area traversal settings are correct, press [Esc] to exit this function.

Modify - Element
Sub-Menu

Description: Provides access to functions which modify protection element types, area connections and element presence in the current ASD.

Contents:
Presence
Jumps
Types
Quit

Modify - Element - Jumps
Function

Description: Modifies the output area connection for any protection element within the current ASD.

Usage: The first protection element is highlighted and a pop-up window appears displaying its type and input/output areas. Use the cursor keys to highlight any protection element to be modified. Press [↵] to select the area into which the output path segment leads. Use the arrow keys to scroll through the possible output area choices and press [↵] to select. If you like, you can revert to the original output area for the highlighted PE by pressing [Esc].

Notice that the PE output segment is displayed as a jump tab when connected to an area other than the area immediately below the PE. The letter on the jump tab corresponds to the letter on the associated output area. Press [Esc] when not modifying a PE to exit this function.

Modify - Element - Presence
Function

Description: Modifies the current ASD by selecting protection elements which are present in the facility to be modeled.

Usage: All protection elements which are available within the current ASD are automatically displayed. Protection elements which are not currently present are displayed with dashed lines. A pop-up window appears to display the highlighted PE's type and input/output areas. Use the cursor keys to highlight any PE which you desire to insert into or delete from the current ASD. Insertion or deletion is accomplished by using the [Ins] or [Del] keys, respectively. The highlighted PE can also be toggled between the inserted and deleted states by pressing [↵].

Two special functions exist to aid in efficient insertion or deletion of entire layers of PEs. To insert or delete all PEs on the layer which the highlighted PE is on, press [•] followed by [Ins] or [Del] as desired.

If all PEs are deleted from a single layer at any time, a protection layer bypass link appears between the two area labels which bracket the layer. This is to indicate free passage between the areas and is displayed as a vertical bar connecting the labels of the areas involved.

Note - The Helicopter Flight Path PE (HEL) cannot be traversed by intruders without a helicopter. Therefore, this type of PE cannot be made present in the current ASD unless the threat attributes include a helicopter.

Press [Esc] at any time to exit this function.

Modify - Element - Types
Function

Description: Modifies the protection element types within the current ASD. Many different PE types are supported including personnel portals (PER), isolation zones (ISO), doors (DOR), surfaces (SUR) and several others.

Usage: The first protection element is highlighted and a pop-up window appears displaying its type and input/output areas. Use the cursor keys to highlight any protection element to be modified. Press [↵] to select the PE type. Use the arrow keys to scroll through all type choices, and press [↵] to select. If you like, you can revert to the original type for the highlighted PE by pressing [Esc]. Press [Esc] when not modifying a PE to exit this function.

Modify - Title
Function

Description: Modifies the title of the current ASD.

Usage: A pop-up window appears displaying the current ASD title. Enter the new title and press [↵] to set it into the system. You may exit this function without changing the ASD title by pressing [Esc] at any time.

Print
Sub-Menu

Description: Provides access to the functions which print the current adversary sequence diagram or the current ASD settings in tabular form.

Contents: Diagram
Tables
Quit

Print-Diagram
Function

Description: Prints the current adversary sequence diagram.

Usage: This function operates automatically when selected. It should be noted that the system printer *must* recognize the IBM Graphic Character Set to produce correct diagrams with this function. Press [Esc] at any time to cancel printing.

Print-Tables
Function

Description: Prints all settings for the current ASD in tabular form. This information includes the threat characteristics, all PE component settings, facility distances, area traversal limitations, and the response force time range.

Usage: This function operates automatically when selected. Press [Esc] at any time to cancel printing.

Quit
Function

Description: Exits SAVI and returns to DOS. If current changes have not been saved, a window will appear offering the option of saving the ASD prior to leaving SAVI.

Usage: Select Yes to exit to DOS. If you do not wish to exit SAVI, select No to return to the main menu.

Threat
Sub-Menu

Description: Provides access to functions which select the threat characteristics.

Contents:
Attributes
Objective
Tactics
Quit

Threat - Attributes
Function

Description: Displays the current threat attributes and allows them to be selected. Three sets of attributes are supported. Each set specifies an outsider threat with metal and explosives. The "metal" attribute indicates that the intruders will be carrying weapons and/or equipment which will be subject to metal detectors. The intruders' "explosives" will be subject to explosives detectors. Each set of attributes differs only in the primary mode of transport, affecting the transit time calculations.

Usage: A pop-up window appears displaying the available threat attributes with a pointer indicating the current selection. Use the cursor keys to select a new set of threat attributes and press [↵] to enter the selection. Pressing [Esc] exits the function leaving the setting where the pointer indicates.

Threat - Objective
Function

Description: Displays the current threat objective and allows it to be redefined. SAVI supports both entry and entry/exit objectives, indicating whether the intruders will be modeled entering the facility up to the target (entry), or entering to the target and attempting to remove the target from the facility (entry/exit).

Usage: A pop-up window appears displaying both threat objectives with a pointer indicating the current objective. Use the cursor keys to select a new threat objective and press [↵] to enter the selection. Pressing [Esc] exits the function leaving the setting where the pointer indicates.

Threat-Tactics
Function

Description: Displays the current threat tactics setting and allows it to be redefined. This setting indicates whether the intruders will simply use force to penetrate each PE (Force Only tactics) or will mix force and deceit tactics along any path (Mixed tactics). If the intruders are restricted to forcibly defeating all security components, for example penetrating surfaces and destroying detection systems, then Force Only tactics should be set. However, if the intruders are also able to minimize detection by deception, for example by falsifying ID badges, then Mixed tactics should be selected.

Usage: A pop-up window appears displaying the threat tactic settings with a pointer indicating the current choice. Use the cursor keys to select the desired threat tactics and press [↵] to enter the selection. Pressing [Esc] exits the function leaving the selection where the pointer indicates.

SAVI
Report Form

Instructions

Use this form to report software bugs, documentation errors, or suggested enhancements. Mail the form to:

SAVI Technical Support
Sandia National Laboratories
Division 5212
Albuquerque, NM 87185 (505) 844-1906

SAVI Software Version Number ☐

Name _____ Title _____

Company _____

Street _____

City _____ State _____ Zip _____

Phone _ ( ) _____ - _____ Date _____

Category

☐ Software Problem ☐ User's Guide Problem ☐ Other

☐ Software Enhancement ☐ Reference Manual Problem _____

Hardware Description

Manufacturer _____ Total RAM _____ KB

Peripherals _____

Problem Description

Describe the problem. Also describe how to reproduce it and your diagnosis or suggested corrections. Attach any related SAVI printouts.

SAVI Technotes

SAVI Technotes

87-1 August 1987

This is the first issue of SAVI Technotes, designed to keep you current on the SAVI software. We are very interested in your feedback for future issues. Please send your ideas, questions or comments to the address listed at the bottom of this page.

SOFTWARE

1 SAVI Version 2.2 was completed and released at the end of May. This newest version provides several functional improvements over Version 1.0 and corrects three errors which were discovered in Version 2.1. The major features of the software are covered along with a complete explanation of these errors.

HARDWARE

4 SAVI was designed to run with a specific set of computer hardware. Although these requirements are discussed briefly in Chapter 1 of the software manual, many users have questions concerning the use of SAVI with various display cards, monitors and printers. These issues are covered more fully, and the correct settings for the Epson FX series printers are given.

QUESTIONS

8 SAVI utilizes an exhaustive path search technique to determine the most vulnerable paths into a particular facility. This ensures that the vulnerability to intrusion is calculated along all paths. However, as many SAVI users know, this can require large amounts of analysis time for complex systems. Techniques are suggested to reduce these analysis times.

IDEAS

11 SAVI users are always discovering new ways to use their software. A simple technique is presented to conveniently store extra Protection Element (PE) settings in non-present PEs by using the Define-Component-Copy function.

• Send all correspondence to • SAVI Technical Support •
• Sandia National Laboratories • Division 5212 •
• Albuquerque, New Mexico • 87185 • (505) 844-1906 •

SOFTWARE

The newest version of SAVI (2.2) offers several new features over those found in earlier versions. SAVI Version 1.0 users will find that although the screens look similar, the menus contain many new functions to support more complex and accurate analyses. The Version 1.0 paper worksheets used to quantify delay and detection values at the path segment level have been replaced with an automated database of security components within the Define-Component-Settings function. Several characteristics of the threat can now be specified including the adversary objective (entry-only or entry/exit). Extensive graphics functions are now included to allow the user to clearly document the calculated path vulnerabilities as well as display the sensitivity to variations in response force time. The major new features include the following:

- Threat Specific Security Component Database.
- Extended Threat Characteristics including Attributes, Objective and Tactics.
- Consideration of Threat Transport Mode to model Traversal Times across specified Area & PE Distances.
- Vulnerabilities calculated for a Range of Response Force Times.
- Analysis Results Automatically Saved with ASD file.
- Graphics functions including three types of graphs and animated display of system vulnerabilities vs. RFT. Support for Zooming and Linear/Logarithmic scaling.

A small group of users received SAVI Version 2.0 at the beginning of 1987. This version was released for beta-test

only, and should not still be in use. If you are a Version 2.1 user, please note that three errors have been discovered in Version 2.1. These errors are explained in detail below and have **all been corrected** in SAVI Version 2.2. It is recommended that you do not use the older versions of the software (2.0 or 2.1). If you do not have a copy of SAVI Version 2.2, send your request to the address listed at the bottom of the front page of these Technotes. For those of you who are interested, the Version 2.1 errors are explained below.

VERSION 2.1 ERRORS

Critical Detection Point Displayed in Wrong Place

The Critical Detection Point (CDP) may be displayed on an incorrect path segment within the Analyze-Results-Vulnerability & Analyze-Results-Recommendations functions. This error only occurs when three specific conditions are met:

1) The Threat Objective is Entry/Exit,
2) The CDP is calculated to lie on the input segment of the Target Task PE on exit,
3) The protection layer preceding the Target Enclosure is bypassed (no PEs present).

Under these circumstances, the CDP is displayed in the wrong place (closer to the start of the path) within the Vulnerability and Recommendations functions in the Analyze-Results sub-menu. The calculated measures of vulnerability (P(I) and TRI) are still accurate for all output including screen printouts and Analysis Graphs. It should be noted that since improvement recommendations are stated relative to the location of the CDP, these suggestions will indicate that detection should be improved prior to the incorrect CDP and delay increased from that point on.

Building Roof Barrier Error

SAVI is designed to model a building roof barrier as impassable by intruders traveling by truck since it is generally not possible to drive a truck over the roof of a building which spans an isolation zone, although it may be possible for an intruder to climb over the roof on foot. SAVI Version 2.1 may incorrectly indicate a path through the building roof barrier within the isolation zone PE as **most** vulnerable on entry for intruders with vehicles. In reality, the building roof barrier is impassable and therefore **least** vulnerable in this case. The resulting vulnerability measures may indicate that isolation zones are more vulnerable than the components would otherwise indicate. This error is only significant when an isolation zone occurs on an identified path after the CDP on entry to the target, since this is when intruder delay is considered.

Analysis Required Indicator Failure

Under certain circumstances, once analysis has been completed on the current ASD, certain component settings can be changed without triggering the analysis required indicator ('?' displayed at the far right of the ASD label box). This error can cause a user to inadvertently associate previous analysis results with modified ASD component settings. The error can occur in two ways, both within the Define-Component-Settings function:

1) A component setting is changed from a discrete lettered choice to a direct setting (#).

2) The [?] key is used to clear a component choice or set of choices.

This error is easy to detect. It **has** occurred if the '?' indicator does not appear once changes have been made to the component settings under the given circumstances. You may force the indicator to appear by simply clearing a component choice and then reselecting the appropriate choice.

HARDWARE

The IBM-PC was one of the first micro-computer systems to be designed with an "open architecture". This allows a world of secondary vendors to produce hardware which will work both inside of and along with PCs and PC compatible machines. Although many experts consider this to be one of the most valuable characteristics of the PC design, it has laid the foundation for a myriad of confusing hardware options for the user. Since there are so many different display cards, display monitors and printers available, systems can easily be assembled which are not compatible with the SAVI software. There are few true "standards" in this area to govern compatibility; however, for display systems and printers, two de-facto standards have emerged.

SAVI Requires a CGA or Compatible Display Device

The oldest and most commonly available display device for the PC is the IBM Color Graphics Adapter (CGA). Although the hardware design is outdated and the display characteristics unimpressive, this card or another vendor's clone of it is the most commonly found display hardware. The CGA can produce 16 colors of text characters in text mode, 320x200 pixels w/ 4 colors or 640x200 pixels in a single color in graphics modes. The main SAVI screen is displayed in 16 color, text mode. The graphs which are produced within the Analyze-Results-Graphs function are produced in 640x200 graphics mode.

This display card can be connected to either a color monitor or to a monitor which can only display a single color (usually green or amber). When the CGA is connected to a single color monitor, the colors can be difficult to differentiate, however the SAVI software was designed so that the colors are not critical to

interpreting the display. There has been some confusion when a CGA is connected to a single color monitor, with a monochrome text-only system. This hardware is not capable of producing graphics. As a result, SAVI will not be able to produce graphs with a monochrome text system.

The IBM Enhanced Graphics Adapter (EGA) is a more powerful display system which was introduced in recent years to improve on the CGA. This system has become very popular, although there are still far fewer installed EGA systems than CGAs. A true EGA device should emulate the functionality of a CGA, thus making it compatible with SAVI. It may be necessary to run a small program from the EGA manufacturer to set it into CGA mode prior to running SAVI. The SAVI software does not automatically set the mode of the display device.

SAVI will run on any PC compatible, including laptops such as the Toshiba T1100 and NEC Multi-Speed. With the recent popularity in laptop computers, it is expected that users will find themselves using SAVI on these machines with their Liquid Crystal Displays (LCD). One problem with an LCD screen, although it supports CGA graphics, is it cannot render colors as shades of gray as a single color monitor on a CGA or EGA can. This can make SAVI difficult to use. However, SAVI can overcome this problem by displaying in a high contrast mode. Simply set your laptop into black&white mode by typing "`MODE BW80`" at the DOS command line prior to running SAVI, and color generation will be suppressed.

SAVI Requires a Printer Which Supports the IBM Graphic Command Language

The most common printer in use with the first IBM PC compatible systems was the Epson FX series. This dot-matrix printer supported a graphic command language which allows bit-mapped graphic output to be produced. Due to the wide spread success of this printer, including distribution under the IBM label, the graphic command language used by this printer has become a practical standard. Most dot-matrix printers on

the market today now support this command language. Consult your printer's user manual to be sure.

Note - a memory resident graphic screen dump utility must be loaded prior to running SAVI if you want to make graphic printouts from the Analyze-Results-Graphs function. The most common screen dump utility is called "GRAPHICS.COM" *or* "GRAPHICS.EXE" *and can be loaded by simply typing* "GRAPHICS" *at the DOS prompt. If you have an EGA display device you will need an EGA screen dump utility which should be provided by the manufacturer.*

SAVI Requires a Printer Which Recognizes the IBM Upper 128 Graphic Character Definitions

The main SAVI screen is composed entirely of text characters. Although the screen includes "graphics" such as boxes and double-lines, these are simply special graphic text characters. The American Standard Code for Information Interchange (ASCII) table defines 128 text characters (numbered 0 through 127) as standard. These characters include the upper and lower-case alphabet, all numbers and common typewriter special characters such as an asterisk and ampersand. Another 128 characters were defined by IBM when the PC was designed, to include special graphic characters for drawing boxes and organizing text on the PC screen. It is this set of characters (numbered 128 through 255) which is used by SAVI on the main screen. The Print-Diagram function requires that your printer recognize these special graphic characters to produce a printout of the SAVI screen. This capability should be discussed in your printer manual as well.

Many users have requested a sample set of printer settings to serve as a guide for setting up their printers. The Epson FX series printers are relatively common, therefore we are providing a discussion of the settings for Epson FX-85/185 printers for your reference.

EPSON FX-85/185 PRINTER SETTINGS

The Epson FX-85/185 printers support the IBM/Epson graphic command language to allow bit-mapped printouts of the SAVI graphs. This capability is true of all Epson FX series printers. However, not all FX series printers support the IBM graphic character set of line drawing text characters, needed to produce copies of Adversary Sequence Diagrams from the Print-Diagram function.

The FX-85 and wide-carriage FX-185 printers will support the IBM graphic character set through DIP switch settings. There are two DIP switch sets on these printers which control various printer functions. DIP switch set 1 has a single switch (#4) which controls the printer mode (Epson or IBM). This switch must be set to IBM mode (OFF) for the printer to recognize the IBM graphic character set. All other switches in DIP switch set 1 control features which will not affect the function of the SAVI software. A single switch (#4) in DIP switch set 2 controls the handling of carriage returns at the end of text lines. This switch should be set OFF to **not** automatically add line feeds to each carriage return sent from the software. If this switch is set ON, all tabular output from SAVI will be incorrectly double-spaced. These are the only switches on this printer which must be set to use SAVI.

If you have experimented with any display devices and/or printer settings and would like to share your success or failure with other SAVI users, please send all information to the address listed on the cover page, and we will publish your findings in future Technotes.

QUESTIONS

Many SAVI users have called us with questions. A commonly asked question is how to reduce analysis time. Analysis time is directly proportional to the complexity of the facility to be analyzed; therefore, if the number of elements can be reduced without affecting the accuracy of the PPS model, analysis time can be reduced. Several techniques to reduce analysis time can be considered:

Install an 8087 Math Co-Processor

Most IBM-PC compatibles support the option of installing an 8087 math co-processor. Once installed, SAVI automatically utilizes the co-processor and can reduce analysis times by up to 1/3 of that required without a co-processor.

Analyze for Entry Only First

SAVI will calculate the most vulnerable paths for both intrusion to the target (entry only) and intrusion to the target and back offsite (entry/exit). This setting is made within the Threat-Objective function. The time for entry/exit analysis requires approximately the square of the time to do entry only analysis. Of course, if a facility can be made secure against entry, it is by definition secure against entry and exit. Therefore, entry only analysis should be done first to determine if the facility is acceptably secure without spending the extra time for entry/exit analysis.

Analyze for Force Only Tactics

If the current threat can be assumed to use force only (no deceit) to defeat the security system, then the force only tactic should be set within the Threat-Tactics function. Selecting force only analysis will reduce calculation time since SAVI will not

consider deceit intrusion when modeling all intrusion paths.

Eliminate Duplicate PEs on Each Protection Layer

Many Physical Protection Systems (PPS) are designed with several identical PEs separating adjacent areas. For example there may be two or more identical doors with the same detectors leading into a building area. Since these doors have the same characteristics and lead between the same areas, they are logically equivalent, and therefore do not need to be modeled separately. A single copy of one of these doors and its component settings is enough to accurately model vulnerability to intrusion through any of these doors into the associated building. Therefore, only one PE with a unique set of components need be modeled on a particular protection layer.

Model Only the Most Vulnerable PEs of Each Type on Each Layer

Since SAVI is designed to model only the most vulnerable intrusion paths, it is possible to eliminate all but the most vulnerable PEs of each type on each layer to reduce the overall complexity of a PPS. This sounds easy, but in reality it can only be done in the simplest cases.

A PE must be determined to be the most vulnerable to intrusion compared to all other PEs of its type on the given layer. The identified PE must have the lowest cumulative probability of detection, and the smallest delay time for all threats. In many cases one PE may be most vulnerable if the intruder is minimizing detection, while another PE on the layer is most vulnerable if the intruder is minimizing delay. In these cases it is not possible to eliminate either PE.

Therefore, be careful to eliminate only those PEs which are less vulnerable (more secure) in **all** cases compared to the PE which is being retained.

For example, consider a facility with two surfaces leading into a building, one of which has a minimum delay of 20 seconds and a minimum detection probability of .2 and the other with a minimum delay of 120 seconds and a minimum detection probability of .8. In this case the first surface is more vulnerable than the second for both detection and delay. If this relationship between the two surfaces holds for all threats both on entry and exit from the facility, then the second surface may be eliminated from the model. If there is any doubt as to the relative vulnerability of two PEs, be sure to include both in the model.

Remove All PEs on Any Layers with "Free Passage"

In some cases it is possible that entry into and out of an area is entirely unrestricted through a particular PE. Although this is clearly a gaping hole in the PPS between the adjacent areas, some facilities have this characteristic during certain operating shifts.

For example, a facility may be operated with an open or unlocked and unmanned door leading between two protected areas. This door might be locked after hours, but if the analysis is concerned with normal operating hours it would be modeled as unsecured. In this case the PPS complexity can be reduced by removing **all** PEs on the protection layer on which this door lies, since all of the most vulnerable paths through the PPS will lead through this door which offers no protection. Of course, if the door is then later locked, all PEs would need to be inserted back onto the layer.

Analyze a Single Path

A single path can be analyzed by removing all PEs except those which lie on a path of interest. Include only those PEs which fall on the entry and/or exit portion of the specific path. Note this will not yield on exhaustive analysis. In this case the analysis will indicate only the vulnerability to intrusion along the chosen path, and not necessarily the most vulnerable path through the facility. However, this will greatly reduce analysis time when necessary.

IDEAS

Store Extra PE Settings in Non-Present PEs

Many SAVI users don't realize that PE settings are always maintained by the software, even when a PE is made non-present within the Modify-Element-Presence function. In other words, a PE's settings will still be available even after a PE has been removed and then re-inserted into the current ASD. This feature combined with the Define-Components-Copy function will allow you to store specific PE settings in unused, non-present PEs within any ASD.

For example, if you have a PE for which you have made all of the component settings, but you would like to modify the PE without throwing away the settings which have already been made, you can simply copy the PE to an unused, non-present PE (indicated by dashed lines) within the Copy function. Then you may change the settings of the PE which you copied from without losing the old settings. Whenever you wish to use the old settings again, you can simply copy them back from the unused PE. All unused PE settings are also saved to disk when you save your ASD, so you can confidently use your non-present PEs as permanent storage for special settings.

SECTION C

SAVI Component Lists

TITLE: _____ **DOOR**

DOR

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. DOOR

	t in seconds
a) Door Not Locked	0
b) Key/Combination Available	0
c) Hollow Core Metal	12
d) Vehicle Rollup - 16 Gauge Metal	42
e) Turnstile - Floor to Ceiling	80
f) 1/2" Steel Plate	84
g) 1" Steel Plate	120
h) Vault - Class V or VI	300
i) Special Door	600
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

B. SECURITY INSPECTOR DELAY

	t in seconds
a) No Inspector	0
b) Unprotected Inspector	5
c) Protected Inspector	30
d) Inspector in Hardened Position	120
SET _____	_____

DETECTION COMPONENTS

A. DOOR POSITION MONITOR

	p
a) No Monitor	0.0
b) Monitor Turned Off	0.0
c) Balanced Magnetic Switch	.99
SET _____	_____

B. DOOR PENETRATION DETECTION

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Grid Mesh	.99
SET _____	_____

C. SECURITY INSPECTOR DETECTION

	p
a) No Inspector	0.0
b) Inspector w/o Duress Alarm	0.0
c) Inspector w/ Duress Alarm	.5
d) Protected Inspector w/ Alarm	.99
SET _____	_____

D. INTERIOR INTRUSION DETECTION

	p
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Motion Sensor	.5
d) Complementary Motion Sensors	.9
SET _____	_____

E. PERSONNEL DETECT DOOR INTRUSION

	p
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

F. IDENTITY CHECK

	p
a) Personnel Not Allowed Through	N/A
b) No ID Check	0.0
c) Picture Badge - Take Home	.1
d) Picture Badge - Exchange	.5
e) Hand Geometry Check	.95
f) Eye Retina Scan	.99
SET _____	_____

G. METAL DETECTION ON PERSON

	p
a) No Metal Detector	0.0
b) Good Detector	.9
c) Excellent Detector	.99
SET _____	_____

H. EXPLOSIVES DETECTION ON PERSON

	p
a) No Explosives Check	0.0
b) Vapor Collection	.1
c) Trained Dog	.1
d) Rigorous Patdown Search	.9
SET _____	_____

TITLE: _____ DOOR

DOR

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONINTUED)

	p
I. SNM DETECTION ON PERSON	
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

	p
J. PACKAGE SEARCH	
a) Packages Not Allowed Through	N/A
b) Packages Allowed - No Search	0.0
c) Visual Check	.1
d) Vapor Collection	.1
e) Trained Dog	.1
f) X-RAY - Metal Only	.9
g) Excellent Metal Detector	.99
h) Rigorous Package Search	.99
SET _____	_____

	p
K. SNM DETECTION IN PACKAGE	
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

TITLE: _____

EVC

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

EVACUATION SHELTER

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. INPUT DOOR

	t in seconds
a) Door Not Locked	0
b) Key/Combination Available	0
c) Hollow Core Metal	12
d) Vehicle Rollup - 16 Gauge Metal	42
e) Turnstile - Floor to Ceiling	80
f) 1/2" Steel Plate	84
g) 1" Steel Plate	120
h) Vault - Class V or VI	300
i) Special Door	600
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

B. INPUT SURFACE

a) Open Port	0
b) Unbarred Window	5
c) Vent, Port, Duct: Standard Louvers	30
d) Vent, Port, Duct: Heavy Grid	60
e) Vent, Port, Duct: Diffusers	120
f) 4" Framed w/ Sheetrock	10
g) 4" Concrete	30
h) 16 Gauge Metal	48
i) 4" Concrete w/ Rebar	84
j) 8" Concrete w/ Rebar	120
k) 2' Earth	120
SET _____	_____

C. OUTPUT DOOR

	t in seconds
a) Door Not Locked	0
b) Key/Combination Available	0
c) Hollow Core Metal	12
d) Vehicle Rollup - 16 Gauge Metal	42
e) Turnstile - Floor to Ceiling	80
f) 1/2" Steel Plate	84
g) 1" Steel Plate	120
h) Vault - Class V or VI	300
i) Special Door	600
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

D. OUTPUT SURFACE

a) Open Port	0
b) Unbarred Window	5
c) Vent, Port, Duct: Standard Louvers	30
d) Vent, Port, Duct: Heavy Grid	60
e) Vent, Port, Duct: Diffusers	120
f) 4" Framed w/ Sheetrock	10
g) 4" Concrete	30
h) 16 Gauge Metal	48
i) 4" Concrete w/ Rebar	84
j) 8" Concrete w/ Rebar	120
k) 2' Earth	120
SET _____	_____

DETECTION COMPONENTS

A. INPUT DOOR POSITION MONITOR

	p
a) No Monitor	0.0
b) Monitor Turned Off	0.0
c) Balanced Magnetic Switch	.99
SET _____	_____

B. INPUT DOOR PENETRATION DETECTION

a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Grid Mesh	.99
SET _____	_____

C. INPUT SURFACE PENETRATION DETECTION

(Select the lowest value surface detection component regardless of the surface delay component selected.)

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

D. PERSONNEL DETECT DOOR INTRUSION

a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

TITLE: _____ **EVACUATION SHELTER**

EVC

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONTINUED)

	p
E. PERSONNEL DETECT SURFACE INTRUSION	
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

	p
F. INTERIOR INTRUSION DETECTION	
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Motion Sensor	.5
d) Complementary Motion Sensors	.9
SET _____	_____

	p
G. OUTPUT DOOR POSITION MONITOR	
a) No Monitor	0.0
b) Monitor Turned Off	0.0
c) Balanced Magnetic Switch	.99
SET _____	_____

	p
H. OUTPUT DOOR PENETRATION DETECTION	
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Grid Mesh	.99
SET _____	_____

I. OUTPUT SURFACE PENETRATION DETECTION

(Select the lowest value surface detection component regardless of the surface delay component selected.)

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

TITLE: _____ **FENCE**

FNC INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. FENCE

	t in seconds
a) No Fence	0
b) 8' Chain Link Fence w/ Outriggers	10
SET _____	_____

B. VEHICLE BARRIER

	t in seconds
a) No Vehicle Barrier	0
b) Aircraft Cable	0
c) Concrete Median or Ditch	0
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

C. SECURITY PATROL DELAY

	t in seconds
a) No Patrol	0
b) Unprotected Patrol	12
c) Protected Patrol	30
d) Inspectors in Tower	30
e) Inspectors in Hardened Position	125
SET _____	_____

DETECTION COMPONENTS

A. FENCE DETECTION

	p
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Fence Intrusion Sensors	.1
SET _____	_____

B. GROUND DETECTION

	p
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Sensor - Not on Fence	.5
d) Multiple Sensors	.8
e) Complementary Sensors	.99
SET _____	_____

C. SECURITY PATROL DETECTION

	p
a) No Patrol	0.0
b) Patrol w/o Duress Alarm	0.0
c) Patrol w/ Duress Alarm	.1
d) Inspector in Tower w/ Duress Alarm	.1
SET _____	_____

TITLE: _____ **GATE**

GAT

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. GATE

	t in seconds
a) Gate Not Locked	0
b) Key/Combination Available	0
c) Gate Locked	10
SET _____	_____

B. VEHICLE BARRIER

a) No Vehicle Barrier	0
b) Aircraft Cable	0
c) Concrete Median or Ditch	0
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

C. SECURITY INSPECTOR DELAY

	t in seconds
a) No Inspector	0
b) Unprotected Inspector	5
c) Protected Inspector	30
d) Inspector in Hardened Position	120
SET _____	_____

DETECTION COMPONENTS

A. GATE DETECTION

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Gate Intrusion Sensor	.1
SET _____	_____

B. GROUND DETECTION

a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Sensor - Not on Fence	.5
d) Multiple Sensors	.8
e) Complementary Sensors	.99
SET _____	_____

C. IDENTITY CHECK

a) Personnel Not Allowed Through	N/A
b) No ID Check	0.0
c) Picture Badge - Take Home	.1
d) Picture Badge - Exchange	.5
e) Hand Geometry Check	.95
f) Eye Retina Scan	.99
SET _____	_____

D. METAL DETECTION ON PERSON

a) No Metal Detector	0.0
b) Good Detector	.9
c) Excellent Detector	.99
SET _____	_____

E. EXPLOSIVES DETECTION ON PERSON

	p
a) No Explosives Check	0.0
b) Vapor Collection	.1
c) Trained Dog	.1
d) Rigorous Patdown Search	.9
SET _____	_____

F. SNM DETECTION ON PERSON

a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

G. PACKAGE SEARCH

a) Packages Not Allowed Through	N/A
b) Packages Allowed - No Search	0.0
c) Visual Check	.1
d) Vapor Collection	.1
e) Trained Dog	.1
f) X-RAY - Metal Only	.9
g) Excellent Metal Detector	.99
h) Rigorous Package Search	.99
SET _____	_____

TITLE: _____ GATE

GAT

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONTINUED)

H. SNM DETECTION IN PACKAGE

	p
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

I. VEHICLE AND CARGO SEARCH

	p
a) Vehicles Not Allowed Through	N/A
b) No Contraband Check	N/A
c) Visual Check	N/A
d) Vapor Collection	N/A
e) Trained Dog	N/A
f) Rigorous Vehicle Inspection	N/A
g) Rigorous Cargo Search	N/A
SET _____	_____

J. SNM DETECTION IN VEHICLE AND CARGO

	p
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

K. SECURITY INSPECTOR DETECTION

	p
a) No Inspector	0.0
b) Inspector w/o Duress Alarm	0.0
c) Inspector w/ Duress Alarm	.5
d) Protected Inspector w/ Alarm	.99
SET _____	_____

TITLE: _____ **GENERIC**

GEN INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. INPUT GENERIC DELAY	t in seconds
a) No Delay	0
SET _____	_____
Does this delay component have a panic bar or allow free passage on exit?	No Yes

B. OUTPUT GENERIC DELAY	t in seconds
a) No Delay	0
SET _____	_____
Does this delay component have a panic bar or allow free passage on exit?	No Yes

DETECTION COMPONENTS

A. INPUT GENERIC DETECTION	p
a) Zero Detection Probability	0.0
SET _____	_____

B. OUTPUT GENERIC DETECTION	p
a) Zero Detection Probability	0.0
SET _____	_____

TITLE: _____ **HELICOPTER FLIGHT PATH**

HEL INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. HELICOPTER UNLOAD DELAY	t in seconds
a) No Delay	0
SET _____	_____

B. HELICOPTER LOAD DELAY	t in seconds
a) No Delay	0
SET _____	_____

DETECTION COMPONENTS

A. HELICOPTER DETECTOR	p
a) No Detector	0.0
b) Fair Detector	.5
c) Good Detector	.9
d) Excellent Detector	.99
SET _____	_____

B. PATROL DETECT HELICOPTER	p
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

C. PERSONNEL DETECT HELICOPTER	p
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

TITLE: _____ **ISOLATION ZONE**

ISO

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. INPUT FENCE

	t in seconds
a) No Fence	0
b) 8' Chain Link Fence w/ Outriggers	10
SET _____	_____

B. INPUT VEHICLE BARRIER

a) No Vehicle Barrier	0
b) Aircraft Cable	0
c) Concrete Median or Ditch	0
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

C. INPUT BUILDING ROOF BARRIER

a) No Building Spans Isolation Zone	N/A
b) No Building Roof Barrier	0
c) 8' Chain Link Fence w/ Outriggers	10
SET _____	_____

D. SECURITY PATROL DELAY

a) No Patrol	0
b) Unprotected Patrol	12
c) Protected Patrol	30
d) Inspectors in Tower	30
e) Inspectors in Hardened Position	125
SET _____	_____

E. OUTPUT FENCE

	t in seconds
a) No Fence	0
b) 8' Chain Link Fence w/ Outriggers	10
SET _____	_____

F. OUTPUT VEHICLE BARRIER

a) No Vehicle Barrier	0
b) Aircraft Cable	0
c) Concrete Median or Ditch	0
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

G. OUTPUT BUILDING ROOF BARRIER

a) No Building Spans Isolation Zone	N/A
b) No Building Roof Barrier	0
c) 8' Chain Link Fence w/ Outriggers	10
SET _____	_____

DETECTION COMPONENTS

A. INPUT FENCE DETECTION

	p
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Fence Intrusion Sensors	.1
SET _____	_____

B. OUTPUT FENCE DETECTION

a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Fence Intrusion Sensors	.1
SET _____	_____

C. GROUND DETECTION

	p
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Sensor - Not on Fence	.5
d) Multiple Sensors	.8
e) Complementary Sensors	.99
SET _____	_____

D. SECURITY PATROL DETECTION

a) No Patrol	0.0
b) Patrol w/o Duress Alarm	0.0
c) Patrol w/ Duress Alarm	.1
d) Inspector in Tower w/ Duress Alarm	.1
SET _____	_____

TITLE: _____

ISO

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

ISOLATION ZONE

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONTINUED)

	p
E. INPUT ROOF FENCE DETECTION	
a) No Building Spans Isolation Zone	N/A
b) No Sensors	0.0
c) Sensors Turned Off	0.0
d) Fence Intrusion Sensors	.1
SET _____	_____

	p
F. OUTPUT ROOF FENCE DETECTION	
a) No Building Spans Isolation Zone	N/A
b) No Sensors	0.0
c) Sensors Turned Off	0.0
d) Fence Intrusion Sensors	.1
SET _____	_____

	p
G. BUILDING ROOF DETECTION	
a) No Building Spans Isolation Zone	N/A
b) No Sensors	0.0
c) Sensors Turned Off	0.0
d) Single Sensor - Not on Fence	.5
e) Multiple Sensors	.8
f) Complementary Sensors	.99
SET _____	_____

TITLE: _____

MAT

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

MATERIAL PORTAL

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. INPUT DOOR

	t in seconds
a) Door Not Locked	0
b) Key/Combination Available	0
c) Hollow Core Metal	12
d) Vehicle Rollup - 16 Gauge Metal	42
e) Turnstile - Floor to Ceiling	80
f) 1/2" Steel Plate	84
g) 1" Steel Plate	120
h) Vault - Class V or VI	300
i) Special Door	600
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

B. INPUT SURFACE

a) Open Port	0
b) Unbarred Window	5
c) Vent, Port, Duct: Standard Louvers	30
d) Vent, Port, Duct: Heavy Grid	60
e) Vent, Port, Duct: Diffusers	120
f) 4" Framed w/ Sheetrock	10
g) 4" Concrete	30
h) 16 Gauge Metal	48
i) 4" Concrete w/ Rebar	84
j) 8" Concrete w/ Rebar	120
k) 2' Earth	120
SET _____	_____

C. SECURITY INSPECTOR DELAY

a) No Inspector	0
b) Unprotected Inspector	5
c) Protected Inspector	30
d) Inspector in Hardened Position	120
SET _____	_____

D. OUTPUT DOOR

	t in seconds
a) Door Not Locked	0
b) Key/Combination Available	0
c) Hollow Core Metal	12
d) Vehicle Rollup - 16 Gauge Metal	42
e) Turnstile - Floor to Ceiling	80
f) 1/2" Steel Plate	84
g) 1" Steel Plate	120
h) Vault - Class V or VI	300
i) Special Door	600
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

E. OUTPUT SURFACE

a) Open Port	0
b) Unbarred Window	5
c) Vent, Port, Duct: Standard Louvers	30
d) Vent, Port, Duct: Heavy Grid	60
e) Vent, Port, Duct: Diffusers	120
f) 4" Framed w/ Sheetrock	10
g) 4" Concrete	30
h) 16 Gauge Metal	48
i) 4" Concrete w/ Rebar	84
j) 8" Concrete w/ Rebar	120
k) 2' Earth	120
SET _____	_____

DETECTION COMPONENTS

A. INPUT DOOR POSITION MONITOR

	p
a) No Monitor	0.0
b) Monitor Turned Off	0.0
c) Balanced Magnetic Switch	.99
SET _____	_____

B. INPUT DOOR PENETRATION DETECTION

a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Grid Mesh	.99
SET _____	_____

C. INPUT SURFACE PENETRATION DETECTION

(Select the lowest value surface detection component regardless of the surface delay component selected.)

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

TITLE: _____

MAT

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

MATERIAL PORTAL

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONTINUED)

D. IDENTITY CHECK

	p
a) Personnel Not Allowed Through	N/A
b) No ID Check	0.0
c) Picture Badge - Take Home	.1
d) Picture Badge - Exchange	.5
e) Hand Geometry Check	.95
f) Eye Retina Scan	.99
SET _____	_____

E. METAL DETECTION ON PERSON

	p
a) No Metal Detector	0.0
b) Good Detector	.9
c) Excellent Detector	.99
SET _____	_____

F. EXPLOSIVES DETECTION ON PERSON

	p
a) No Explosives Check	0.0
b) Vapor Collection	.1
c) Trained Dog	.1
d) Rigorous Patdown Search	.9
SET _____	_____

G. SNM DETECTION ON PERSON

	p
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

H. PACKAGE SEARCH

	p
a) Packages Not Allowed Through	N/A
b) Packages Allowed - No Search	0.0
c) Visual Check	.1
d) Vapor Collection	.1
e) Trained Dog	.1
f) X-RAY - Metal Only	.9
g) Excellent Metal Detector	.99
h) Rigorous Package Search	.99
SET _____	_____

I. SNM DETECTION IN PACKAGE

	p
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

J. INTERIOR INTRUSION DETECTION

	p
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Motion Sensor	.5
d) Complementary Motion Sensors	.9
SET _____	_____

K. SECURITY INSPECTOR DETECTION

	p
a) No Inspector	0.0
b) Inspector w/o Duress Alarm	0.0
c) Inspector w/ Duress Alarm	.5
d) Protected Inspector w/ Alarm	.99
SET _____	_____

L. PERSONNEL DETECT DOOR INTRUSION

	p
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

M. PERSONNEL DETECT SURFACE INTRUSION

	p
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

N. OUTPUT DOOR POSITION MONITOR

	p
a) No Monitor	0.0
b) Monitor Turned Off	0.0
c) Balanced Magnetic Switch	.99
SET _____	_____

TITLE: _____

MATERIAL PORTAL

MAT

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONTINUED)

	p
O. OUTPUT DOOR PENETRATION DETECTION	
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Grid Mesh	.99
SET _____	_____

	p
P. OUTPUT SURFACE PENETRATION DETECTION	
(Select the lowest value surface detection component regardless of the surface delay component selected.)	
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

TITLE: _____

PERSONNEL PORTAL

PER

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. INPUT DOOR

	t in seconds
a) Door Not Locked	0
b) Key/Combination Available	0
c) Hollow Core Metal	12
d) Vehicle Rollup - 16 Gauge Metal	42
e) Turnstile - Floor to Ceiling	80
f) 1/2" Steel Plate	84
g) 1" Steel Plate	120
h) Vault - Class V or VI	300
i) Special Door	600
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

B. INPUT SURFACE

a) Open Port	0
b) Unbarred Window	5
c) Vent, Port, Duct: Standard Louvers	30
d) Vent, Port, Duct: Heavy Grid	60
e) Vent, Port, Duct: Diffusers	120
f) 4" Framed w/ Sheetrock	10
g) 4" Concrete	30
h) 16 Gauge Metal	48
i) 4" Concrete w/ Rebar	84
j) 8" Concrete w/ Rebar	120
k) 2' Earth	120
SET _____	_____

C. SECURITY INSPECTOR DELAY

a) No Inspector	0
b) Unprotected Inspector	5
c) Protected Inspector	30
d) Inspector in Hardened Position	120
SET _____	_____

D. OUTPUT DOOR

	t in seconds
a) Door Not Locked	0
b) Key/Combination Available	0
c) Hollow Core Metal	12
d) Vehicle Rollup - 16 Gauge Metal	42
e) Turnstile - Floor to Ceiling	80
f) 1/2" Steel Plate	84
g) 1" Steel Plate	120
h) Vault - Class V or VI	300
i) Special Door	600
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

E. OUTPUT SURFACE

a) Open Port	0
b) Unbarred Window	5
c) Vent, Port, Duct: Standard Louvers	30
d) Vent, Port, Duct: Heavy Grid	60
e) Vent, Port, Duct: Diffusers	120
f) 4" Framed w/ Sheetrock	10
g) 4" Concrete	30
h) 16 Gauge Metal	48
i) 4" Concrete w/ Rebar	84
j) 8" Concrete w/ Rebar	120
k) 2' Earth	120
SET _____	_____

DETECTION COMPONENTS

A. INPUT DOOR POSITION MONITOR

	p
a) No Monitor	0.0
b) Monitor Turned Off	0.0
c) Balanced Magnetic Switch	.99
SET _____	_____

B. INPUT DOOR PENETRATION DETECTION

a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Grid Mesh	.99
SET _____	_____

C. INPUT SURFACE PENETRATION DETECTION

(Select the lowest value surface detection component regardless of the surface delay component selected.)

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

TITLE: _____ **PERSONNEL PORTAL**

PER

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONTINUED)

D. IDENTITY CHECK

	P
a) Personnel Not Allowed Through	N/A
b) No ID Check	0.0
c) Picture Badge - Take Home	.1
d) Picture Badge - Exchange	.5
e) Hand Geometry Check	.95
f) Eye Retina Scan	.99
SET _____	_____

E. METAL DETECTION ON PERSON

	P
a) No Metal Detector	0.0
b) Good Detector	.9
c) Excellent Detector	.99
SET _____	_____

F. EXPLOSIVES DETECTION ON PERSON

	P
a) No Explosives Check	0.0
b) Vapor Collection	.1
c) Trained Dog	.1
d) Rigorous Patdown Search	.9
SET _____	_____

G. SNM DETECTION ON PERSON

	P
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

H. PACKAGE SEARCH

	P
a) Packages Not Allowed Through	N/A
b) Packages Allowed - No Search	0.0
c) Visual Check	.1
d) Vapor Collection	.1
e) Trained Dog	.1
f) X-RAY - Metal Only	.9
g) Excellent Metal Detector	.99
h) Rigorous Package Search	.99
SET _____	_____

I. SNM DETECTION IN PACKAGE

	P
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

J. INTERIOR INTRUSION DETECTION

	P
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Motion Sensor	.5
d) Complementary Motion Sensors	.9
SET _____	_____

K. SECURITY INSPECTOR DETECTION

	P
a) No Inspector	0.0
b) Inspector w/o Duress Alarm	0.0
c) Inspector w/ Duress Alarm	.5
d) Protected Inspector w/ Alarm	.99
SET _____	_____

L. PERSONNEL DETECT DOOR INTRUSION

	P
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

M. PERSONNEL DETECT SURFACE INTRUSION

	P
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

N. OUTPUT DOOR POSITION MONITOR

	P
a) No Monitor	0.0
b) Monitor Turned Off	0.0
c) Balanced Magnetic Switch	.99
SET _____	_____

TITLE: _____ **PERSONNEL PORTAL**

PER

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONTINUED)

	p
O. OUTPUT DOOR PENETRATION DETECTION	
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Grid Mesh	.99
SET _____	_____

	p
P. OUTPUT SURFACE PENETRATION DETECTION	
(Select the lowest value surface detection component regardless of the surface delay component selected.)	
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

TITLE: _____ **RAIL PORTAL**

RAL — INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. INPUT GATE

	t in seconds
a) Gate Not Locked	0
b) Key/Combination Available	0
c) Gate Locked	10
SET _____	_____

B. INPUT RAIL BARRIER

a) No Rail Barrier	0
b) Concrete Median or Ditch	0
c) Railcar Barrier	0
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

C. SECURITY INSPECTOR DELAY

a) No Inspector	0
b) Unprotected Inspector	5
c) Protected Inspector	30
d) Inspector in Hardened Position	120
SET _____	_____

D. OUTPUT GATE

	t in seconds
a) Gate Not Locked	0
b) Key/Combination Available	0
c) Gate Locked	10
SET _____	_____

E. OUTPUT RAIL BARRIER

a) No Rail Barrier	0
b) Concrete Median or Ditch	0
c) Railcar Barrier	0
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

DETECTION COMPONENTS

A. INPUT GATE DETECTION

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Gate Intrusion Sensor	.1
SET _____	_____

B. DETECTION BETWEEN GATES

a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Sensor - Not on Fence	.5
d) Multiple Sensors	.8
e) Complementary Sensors	.99
SET _____	_____

C. IDENTITY CHECK

a) Personnel Not Allowed Through	N/A
b) No ID Check	0.0
c) Picture Badge - Take Home	.1
d) Picture Badge - Exchange	.5
e) Hand Geometry Check	.95
f) Eye Retina Scan	.99
SET _____	_____

D. METAL DETECTION ON PERSON

	p
a) No Metal Detector	0.0
b) Good Detector	.9
c) Excellent Detector	.99
SET _____	_____

E. EXPLOSIVES DETECTION ON PERSON

a) No Explosives Check	0.0
b) Vapor Collection	.1
c) Trained Dog	.1
d) Rigorous Patdown Search	.9
SET _____	_____

F. SNM DETECTION ON PERSON

a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

TITLE: _____ **RAIL PORTAL**

RAL

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONTINUED)

G. PACKAGE SEARCH

	p
a) Packages Not Allowed Through	N/A
b) Packages Allowed - No Search	0.0
c) Visual Check	.1
d) Vapor Collection	.1
e) Trained Dog	.1
f) X-RAY - Metal Only	.9
g) Excellent Metal Detector	.99
h) Rigorous Package Search	.99
SET _____	_____

H. SNM DETECTION IN PACKAGE

	p
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

I. VEHICLE AND CARGO SEARCH

	p
a) Vehicles Not Allowed Through	N/A
b) No Contraband Check	N/A
c) Visual Check	N/A
d) Vapor Collection	N/A
e) Trained Dog	N/A
f) Rigorous Vehicle Inspection	N/A
g) Rigorous Cargo Search	N/A
SET _____	_____

J. SNM DETECTION IN VEHICLE AND CARGO

	p
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

K. SECURITY INSPECTOR DETECTION

a) No Inspector	0.0
b) Inspector w/o Duress Alarm	0.0
c) Inspector w/ Duress Alarm	.5
d) Protected Inspector w/ Alarm	.99
SET _____	_____

L. PERSONNEL DETECT GATE INTRUSION

a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

M. OUTPUT GATE DETECTION

a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Gate Intrusion Sensor	.1
SET _____	_____

TITLE: _____

SHIPPING AREA

SHP

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. INPUT DOOR

	t in seconds
a) Door Not Locked	0
b) Key/Combination Available	0
c) Hollow Core Metal	12
d) Vehicle Rollup - 16 Gauge Metal	42
e) Turnstile - Floor to Ceiling	80
f) 1/2" Steel Plate	84
g) 1" Steel Plate	120
h) Vault - Class V or VI	300
i) Special Door	600
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

B. INPUT VEHICLE BARRIER

a) No Vehicle Barrier	0
b) Aircraft Cable	0
c) Concrete Median or Ditch	0
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

C. INPUT SURFACE

a) Open Port	0
b) Unbarred Window	5
c) Vent, Port, Duct: Standard Louvers	30
d) Vent, Port, Duct: Heavy Grid	60
e) Vent, Port, Duct: Diffusers	120
f) 4" Framed w/ Sheetrock	10
g) 4" Concrete	30
h) 16 Gauge Metal	48
i) 4" Concrete w/ Rebar	84
j) 8" Concrete w/ Rebar	120
k) 2' Earth	120
SET _____	_____

D. SECURITY INSPECTOR DELAY

a) No Inspector	0
b) Unprotected Inspector	5
c) Protected Inspector	30
d) Inspector in Hardened Position	120
SET _____	_____

E. OUTPUT DOOR

	t in seconds
a) Door Not Locked	0
b) Key/Combination Available	0
c) Hollow Core Metal	12
d) Vehicle Rollup - 16 Gauge Metal	42
e) Turnstile - Floor to Ceiling	80
f) 1/2" Steel Plate	84
g) 1" Steel Plate	120
h) Vault - Class V or VI	300
i) Special Door	600
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

F. OUTPUT VEHICLE BARRIER

a) No Vehicle Barrier	0
b) Aircraft Cable	0
c) Concrete Median or Ditch	0
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

G. OUTPUT SURFACE

a) Open Port	0
b) Unbarred Window	5
c) Vent, Port, Duct: Standard Louvers	30
d) Vent, Port, Duct: Heavy Grid	60
e) Vent, Port, Duct: Diffusers	120
f) 4" Framed w/ Sheetrock	10
g) 4" Concrete	30
h) 16 Gauge Metal	48
i) 4" Concrete w/ Rebar	84
j) 8" Concrete w/ Rebar	120
k) 2' Earth	120
SET _____	_____

TITLE: _____ **SHIPPING AREA**

SHP

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS

A. INPUT DOOR POSITION MONITOR

	p
a) No Monitor	0.0
b) Monitor Turned Off	0.0
c) Balanced Magnetic Switch	.99
SET _____	_____

B. INPUT DOOR PENETRATION DETECTION

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Grid Mesh	.99
SET _____	_____

C. INPUT SURFACE PENETRATION DETECTION

(Select the lowest value surface detection component regardless of the surface delay component selected.)

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

D. IDENTITY CHECK

	p
a) Personnel Not Allowed Through	N/A
b) No ID Check	0.0
c) Picture Badge - Take Home	.1
d) Picture Badge - Exchange	.5
e) Hand Geometry Check	.95
f) Eye Retina Scan	.99
SET _____	_____

E. METAL DETECTION ON PERSON

	p
a) No Metal Detector	0.0
b) Good Detector	.9
c) Excellent Detector	.99
SET _____	_____

F. EXPLOSIVES DETECTION ON PERSON

	p
a) No Explosives Check	0.0
b) Vapor Collection	.1
c) Trained Dog	.1
d) Rigorous Patdown Search	.9
SET _____	_____

G. SNM DETECTION ON PERSON

	p
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

H. PACKAGE SEARCH

	p
a) Packages Not Allowed Through	N/A
b) Packages Allowed - No Search	0.0
c) Visual Check	.1
d) Vapor Collection	.1
e) Trained Dog	.1
f) X-RAY - Metal Only	.9
g) Excellent Metal Detector	.99
h) Rigorous Package Search	.99
SET _____	_____

I. SNM DETECTION IN PACKAGE

	p
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

J. VEHICLE AND CARGO SEARCH

	p
a) Vehicles Not Allowed Through	N/A
b) No Contraband Check	N/A
c) Visual Check	N/A
d) Vapor Collection	N/A
e) Trained Dog	N/A
f) Rigorous Vehicle Inspection	N/A
g) Rigorous Cargo Search	N/A
SET _____	_____

K. SNM DETECTION IN VEHICLE AND CARGO

	p
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

TITLE: _____ SHIPPING AREA

SHP

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONTINUED)

	p
L. INTERIOR INTRUSION DETECTION	
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Motion Sensor	.5
d) Complementary Motion Sensors	.9
SET _____	_____

	p
M. SECURITY INSPECTOR DETECTION	
a) No Inspector	0.0
b) Inspector w/o Duress Alarm	0.0
c) Inspector w/ Duress Alarm	.5
d) Protected Inspector w/ Alarm	.99
SET _____	_____

	p
N. PERSONNEL DETECT DOOR INTRUSION	
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

	p
O. PERSONNEL DETECT SURFACE INTRUSION	
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

	p
P. OUTPUT DOOR POSITION MONITOR	
a) No Monitor	0.0
b) Monitor Turned Off	0.0
c) Balanced Magnetic Switch	.99
SET _____	_____

	p
Q. OUTPUT DOOR PENETRATION DETECTION	
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Grid Mesh	.99
SET _____	_____

R. OUTPUT SURFACE PENETRATION DETECTION

(Select the lowest value surface detection component regardless of the surface delay component selected.)

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

TITLE: _____ **SURFACE**

SUR

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. SURFACE DELAY STAGE 1

(Note: Choices in Stages 1 and 2 Must Be Identical)

	t in seconds
a) Open Port	0
b) Unbarred Window	5
c) Vent, Port, Duct: Standard Louvers	30
d) Vent, Port, Duct: Heavy Grid	60
e) Vent, Port, Duct: Diffusers	120
f) 4" Framed w/ Sheetrock	10
g) 4" Concrete	30
h) 16 Gauge Metal	48
i) 4" Concrete w/ Rebar	84
j) 8" Concrete w/ Rebar	120
k) 12" Concrete w/ Rebar	120
l) 18" Concrete w/ Rebar	120
m) 24" Concrete w/ Rebar	120
n) 36" Concrete w/ Rebar	156
o) 2' Earth	120
p) 3' Earth	120
q) 4' Earth	120
r) 6' Earth	120
s) 10' Earth	156
SET _____	_____

B. SECURITY INSPECTOR DELAY

a) No Inspector	0
b) Unprotected Inspector	5
c) Protected Inspector	30
d) Inspector in Hardened Position	120
SET _____	_____

C. SURFACE DELAY STAGE 2

(Note: Choices in Stages 1 and 2 Must Be Identical)

	t in seconds
a) Open Port	0
b) Unbarred Window	0
c) Vent, Port, Duct: Standard Louvers	0
d) Vent, Port, Duct: Heavy Grid	0
e) Vent, Port, Duct: Diffusers	0
f) 4" Framed w/ Sheetrock	0
g) 4" Concrete	0
h) 16 Gauge Metal	0
i) 4" Concrete w/ Rebar	0
j) 8" Concrete w/ Rebar	0
k) 12" Concrete w/ Rebar	54
l) 18" Concrete w/ Rebar	180
m) 24" Concrete w/ Rebar	384
n) 36" Concrete w/ Rebar	756
o) 2' Earth	0
p) 3' Earth	54
q) 4' Earth	180
r) 6' Earth	384
s) 10' Earth	756
SET _____	_____

DETECTION COMPONENTS

A. SURFACE PENETRATION DETECTION

(Select the lowest value surface detection component regardless of the surface delay component selected.)

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

B. PERSONNEL DETECT SURFACE INTRUSION

a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

C. INTERIOR INTRUSION DETECTION

	p
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Motion Sensor	.5
d) Complementary Motion Sensors	.9
SET _____	_____

D. SECURITY INSPECTOR DETECTION

a) No Inspector	0.0
b) Inspector w/o Duress Alarm	0.0
c) Inspector w/ Duress Alarm	.5
d) Protected Inspector w/ Alarm	.99
SET _____	_____

TITLE: _____

TSK

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

TARGET TASK

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. TARGET TASK DELAY

t in seconds

a) No Delay	0
SET _____	_____

B. SECURITY INSPECTOR DELAY

t in seconds

a) No Inspector	0
b) Unprotected Inspector	5
c) Protected Inspector	30
d) Inspector in Hardened Position	120
SET _____	_____

DETECTION COMPONENTS

A. TARGET TASK DETECTION

p

a) No Detector	0.0
b) Detector Turned Off	0.0
c) Fair Integrity Monitor	.5
d) Fair Presence Monitor	.5
e) Good Integrity Monitor	.9
f) Good Presence Monitor	.9
g) Excellent Integrity Monitor	.99
h) Excellent Presence Monitor	.99
SET _____	_____

B. TWO-PERSON RULE DETECTION

a) No Two-Person Rule	0.0
b) Casual Observation	0.0
c) Dedicated Observation w/ Alarm	.5
d) Protected Dedicated Obsv. w/ Alarm	.95
SET _____	_____

C. INTERIOR INTRUSION DETECTION

p

a) No Sensors	0.0
b) Sensors Turned Off	0
c) Single Motion Sensor	.5
d) Complementary Motion Sensors	9
SET _____	_____

D. SECURITY INSPECTOR DETECTION

a) No Inspector	0.0
b) Inspector w/o Duress Alarm	0.0
c) Inspector w/ Duress Alarm	.5
d) Protected Inspector w/ Alarm	.99
SET _____	_____

TITLE: _____ **TUNNEL**

TUN

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. INPUT TUNNEL BARRIER

	t in seconds
a) Open Tunnel	0
b) Standard Louvers	30
c) Heavy Grid	60
d) Diffusers	120
e) Fence	10
f) 4" Concrete	30
g) 16 Gauge Metal	48
h) 4" Concrete w/ Rebar	84
i) 8" Concrete w/ Rebar	120
j) 2' Earth	120
SET _____	_____

B. OUTPUT TUNNEL BARRIER

	t in seconds
a) Open Tunnel	0
b) Standard Louvers	30
c) Heavy Grid	60
d) Diffusers	120
e) Fence	10
f) 4" Concrete	30
g) 16 Gauge Metal	48
h) 4" Concrete w/ Rebar	84
i) 8" Concrete w/ Rebar	120
j) 2' Earth	120
SET _____	_____

DETECTION COMPONENTS

A. INPUT SURFACE PENETRATION DETECTION

(Select the lowest value surface detection component regardless of the surface delay component selected.)

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

B. INPUT PERSONNEL DETECT SURFACE INTRUSION

	p
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

C. INTERIOR INTRUSION DETECTION

	p
a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Motion Sensor	.5
d) Complementary Motion Sensors	.9
SET _____	_____

D. OUTPUT SURFACE PENETRATION DETECTION

(Select the lowest value surface detection component regardless of the surface delay component selected.)

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Capacitance Sensor	.99
d) Vibration Sensor	.99
e) Grid Mesh	.99
SET _____	_____

E. OUTPUT PERSONNEL DETECT SURFACE INTRUSION

	p
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

TITLE: _____

VEHICLE PORTAL

VEH

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DELAY COMPONENTS

A. INPUT GATE

	t in seconds
a) Gate Not Locked	0
b) Key/Combination Available	0
c) Gate Locked	10
SET _____	_____

B. INPUT VEHICLE BARRIER

a) No Vehicle Barrier	0
b) Aircraft Cable	0
c) Concrete Median or Ditch	0
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

C. SECURITY INSPECTOR DELAY

a) No Inspector	0
b) Unprotected Inspector	5
c) Protected Inspector	30
d) Inspector in Hardened Position	120
SET _____	_____

D. OUTPUT GATE

	t in seconds
a) Gate Not Locked	0
b) Key/Combination Available	0
c) Gate Locked	10
SET _____	_____

E. OUTPUT VEHICLE BARRIER

a) No Vehicle Barrier	0
b) Aircraft Cable	0
c) Concrete Median or Ditch	0
SET _____	_____

Does this delay component have a panic bar or allow free passage on exit? [No] [Yes]

DETECTION COMPONENTS

A. INPUT GATE DETECTION

	p
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Gate Intrusion Sensor	.1
SET _____	_____

B. DETECTION BETWEEN GATES

a) No Sensors	0.0
b) Sensors Turned Off	0.0
c) Single Sensor - Not on Fence	.5
d) Multiple Sensors	.8
e) Complementary Sensors	.99
SET _____	_____

C. IDENTITY CHECK

a) Personnel Not Allowed Through	N/A
b) No ID Check	0.0
c) Picture Badge - Take Home	.1
d) Picture Badge - Exchange	.5
e) Hand Geometry Check	.95
f) Eye Retina Scan	.99
SET _____	_____

D. METAL DETECTION ON PERSON

	p
a) No Metal Detector	0.0
b) Good Detector	.9
c) Excellent Detector	.99
SET _____	_____

E. EXPLOSIVES DETECTION ON PERSON

a) No Explosives Check	0.0
b) Vapor Collection	.1
c) Trained Dog	.1
d) Rigorous Patdown Search	.9
SET _____	_____

F. SNM DETECTION ON PERSON

a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

TITLE: _____ **VEHICLE PORTAL**

VEH

INPUT PATH SEGMENT FROM _____

OUTPUT PATH SEGMENT TO _____

Select the applicable item in each set, or write in component data.

☐ DAYSHIFT ☐ OFFSHIFT

DETECTION COMPONENTS (CONTINUED)

G. PACKAGE SEARCH

	p
a) Packages Not Allowed Through	N/A
b) Packages Allowed - No Search	0.0
c) Visual Check	.1
d) Vapor Collection	.1
e) Trained Dog	.1
f) X-RAY - Metal Only	.9
g) Excellent Metal Detector	.99
h) Rigorous Package Search	.99
SET _____	_____

H. SNM DETECTION IN PACKAGE

a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

I. VEHICLE AND CARGO SEARCH

a) Vehicles Not Allowed Through	N/A
b) No Contraband Check	N/A
c) Visual Check	N/A
d) Vapor Collection	N/A
e) Trained Dog	N/A
f) Rigorous Vehicle Inspection	N/A
g) Rigorous Cargo Search	N/A
SET _____	_____

J. SNM DETECTION IN VEHICLE AND CARGO

	p
a) No SNM Detector	0.0
b) SNM Detector w/o Metal Detector	.1
c) Fair SNM Detector	.5
d) Good SNM Detector	.9
e) Excellent SNM Detector	.99
SET _____	_____

K. SECURITY INSPECTOR DETECTION

a) No Inspector	0.0
b) Inspector w/o Duress Alarm	0.0
c) Inspector w/ Duress Alarm	.5
d) Protected Inspector w/ Alarm	.99
SET _____	_____

L. PERSONNEL DETECT GATE INTRUSION

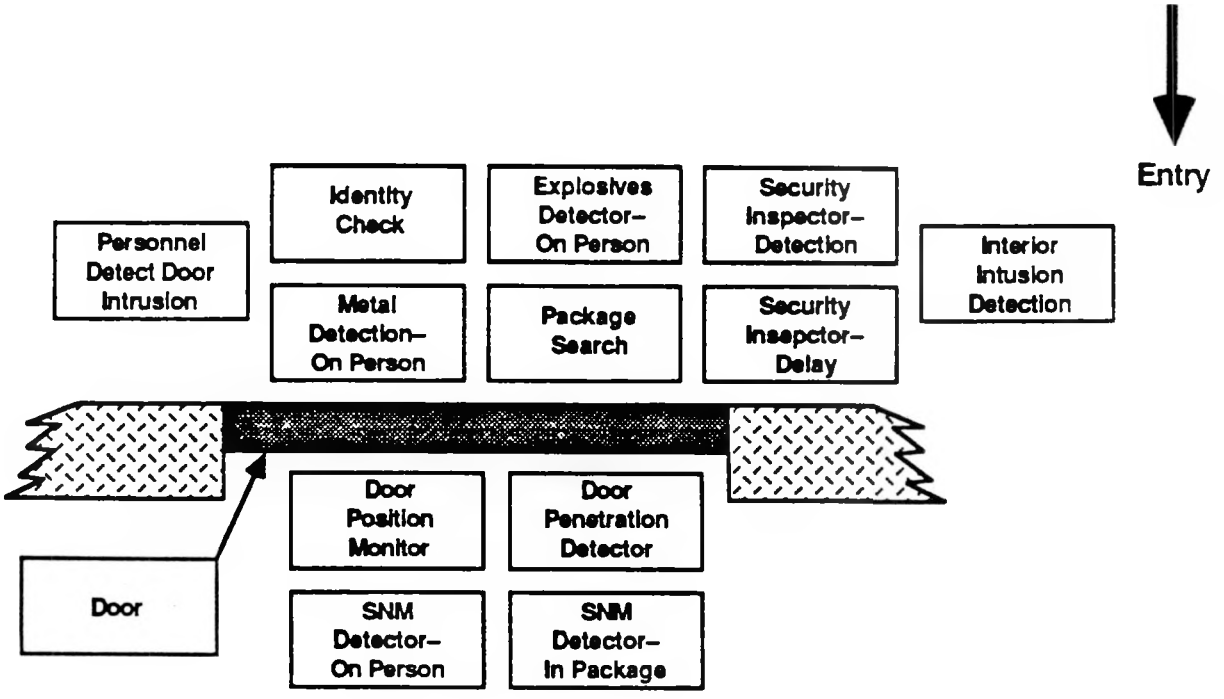
a) Zero Probability	0.0
b) Fair Probability	.5
c) Good Probability	.9
d) Excellent Probability	.99
SET _____	_____

M. OUTPUT GATE DETECTION

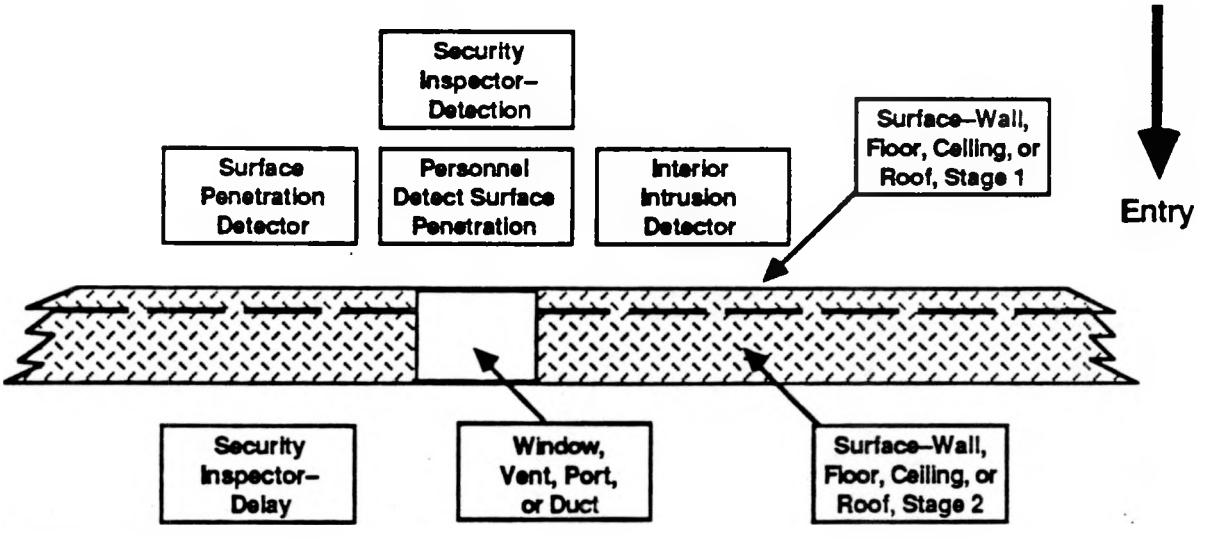
a) No Sensor	0.0
b) Sensor Turned Off	0.0
c) Gate Intrusion Sensor	.1
SET _____	_____

SECTION D

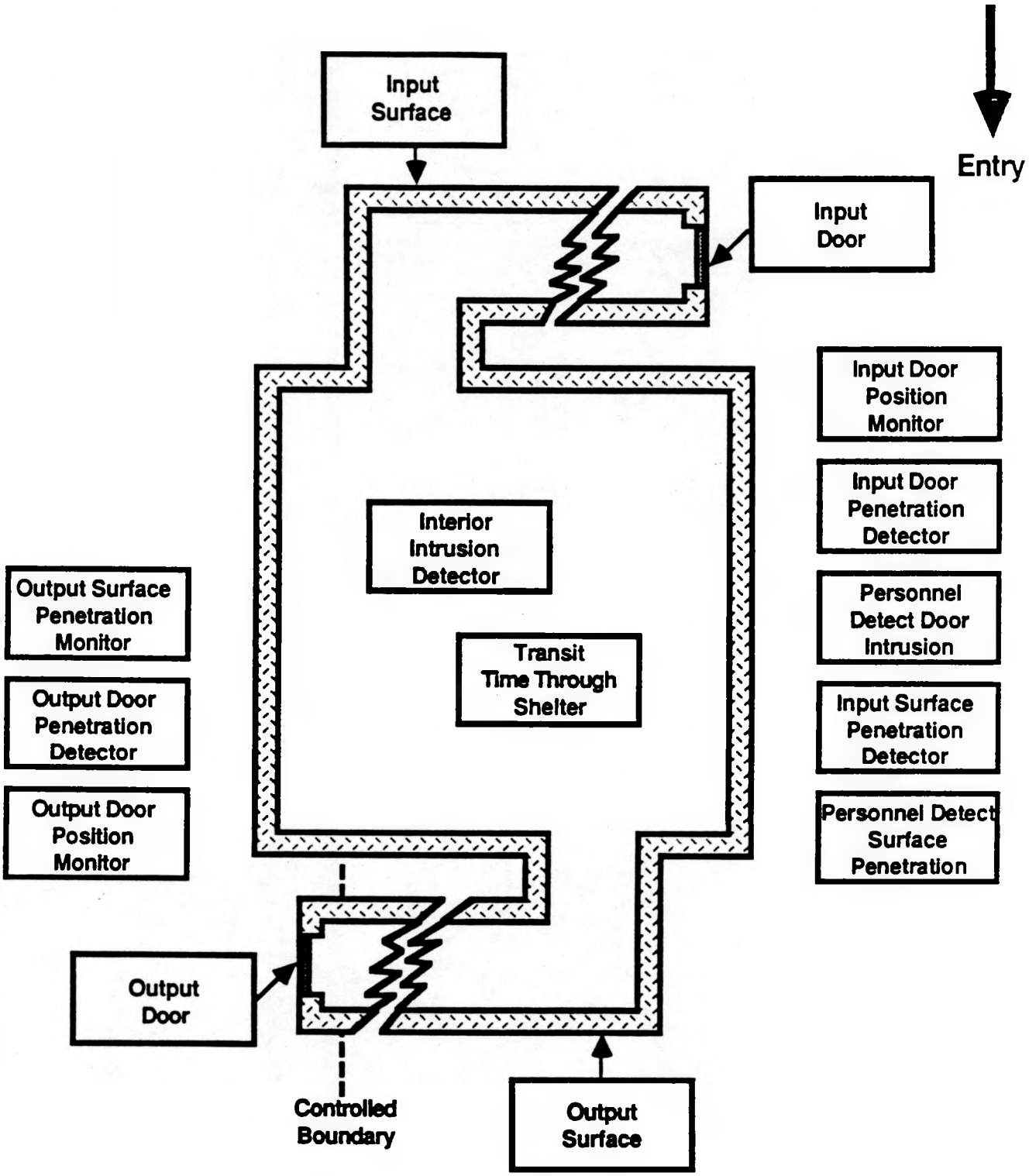
SAVI Protection Element Diagrams



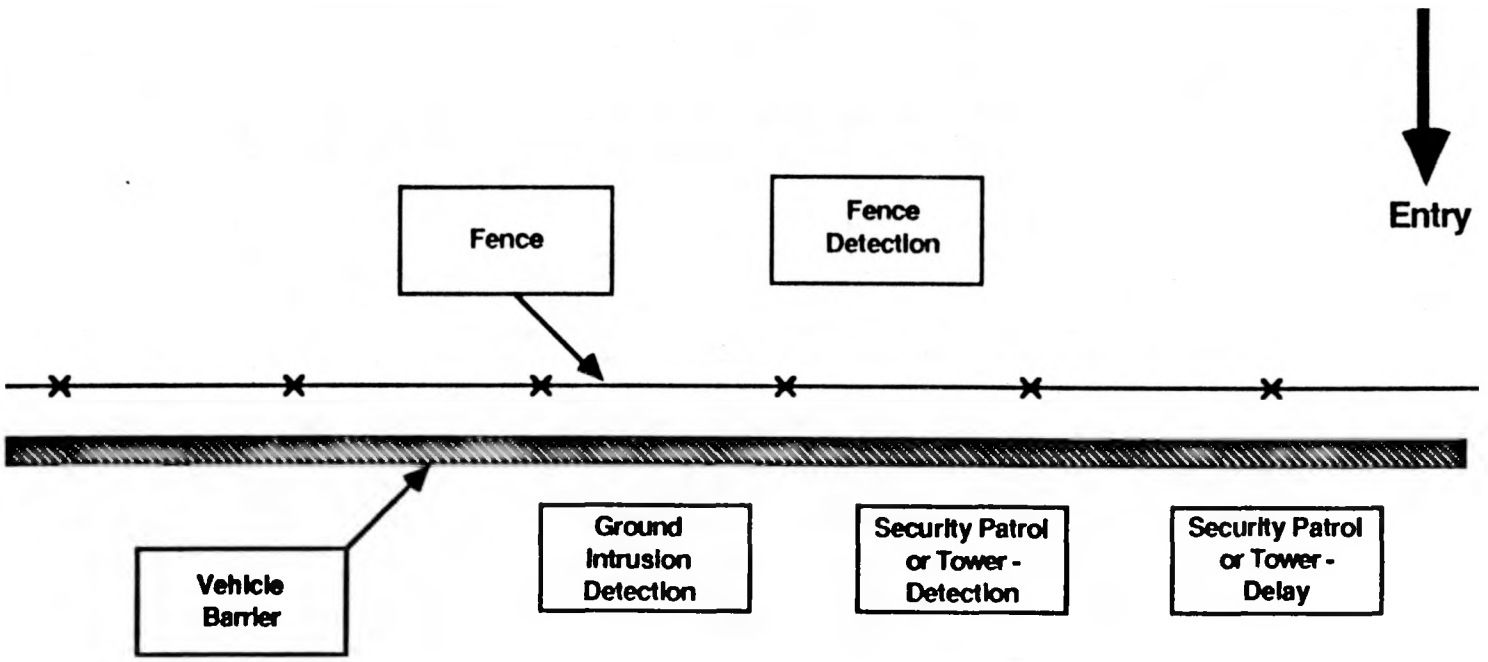
SINGLE DOOR



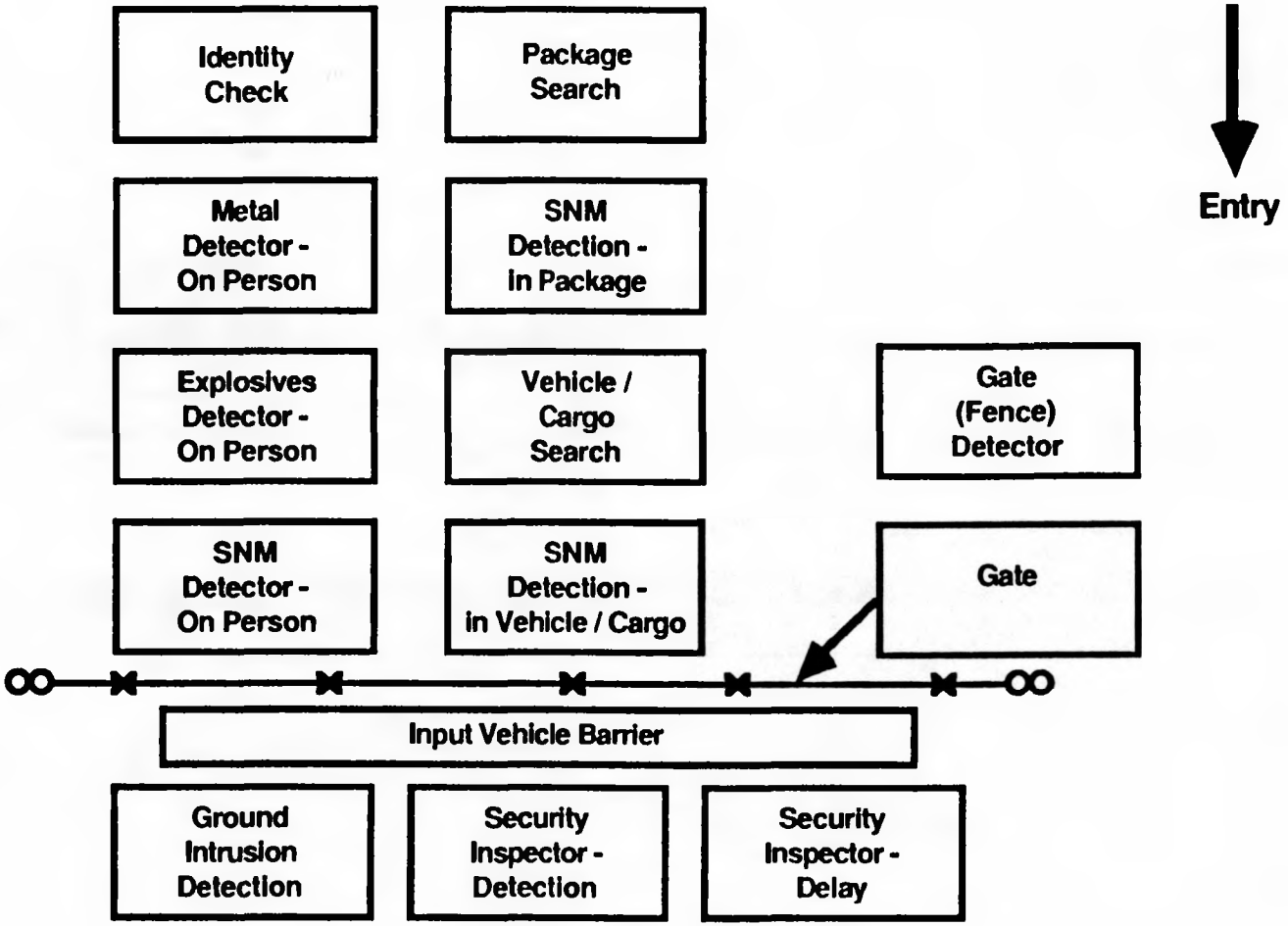
SURFACE



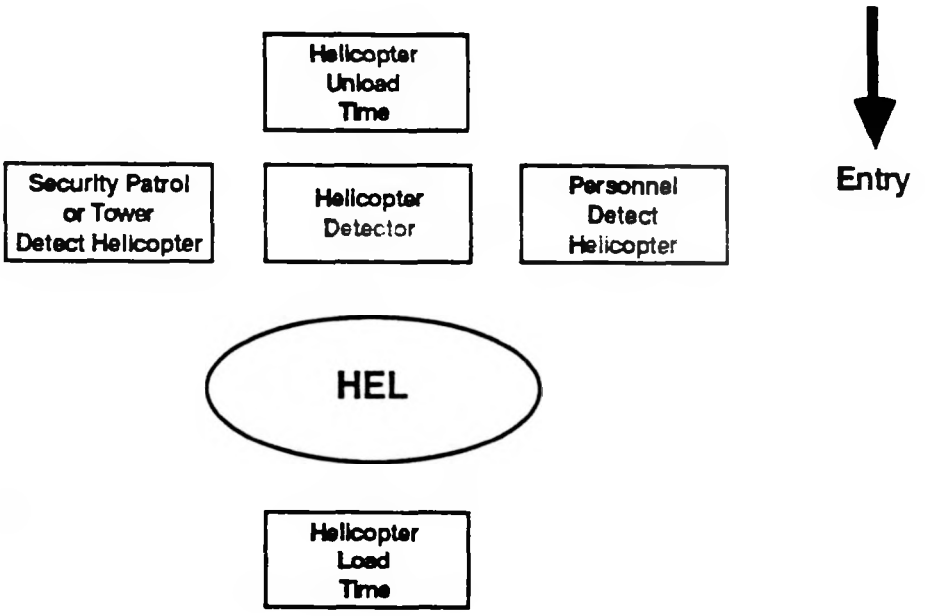
EVACUATION SHELTER


Entry
Fence
Fence Detection
Vehicle Barrier
Ground Intrusion Detection
Security Patrol or Tower - Detection
Security Patrol or Tower - Delay

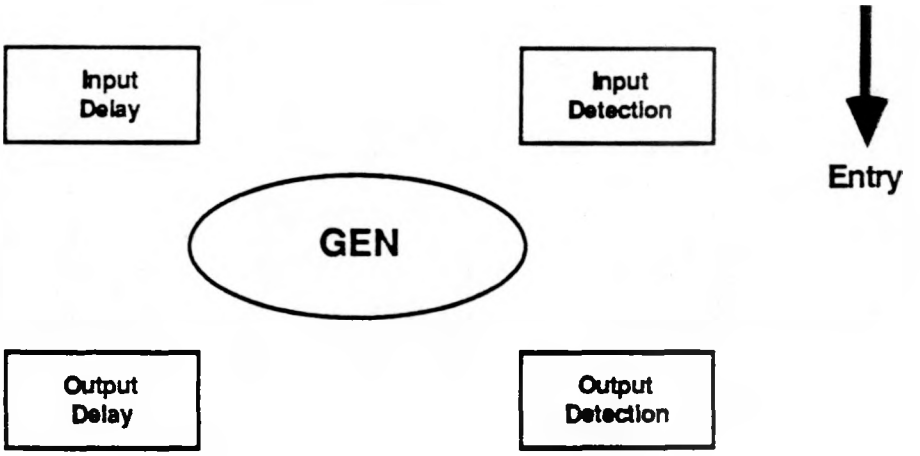
FENCE


Identity Check
Package Search
Entry
Metal Detector - On Person
SNM Detection - In Package
Explosives Detector - On Person
Vehicle / Cargo Search
Gate (Fence) Detector
SNM Detector - On Person
SNM Detection - in Vehicle / Cargo
Gate
Input Vehicle Barrier
Ground Intrusion Detection
Security Inspector - Detection
Security Inspector - Delay

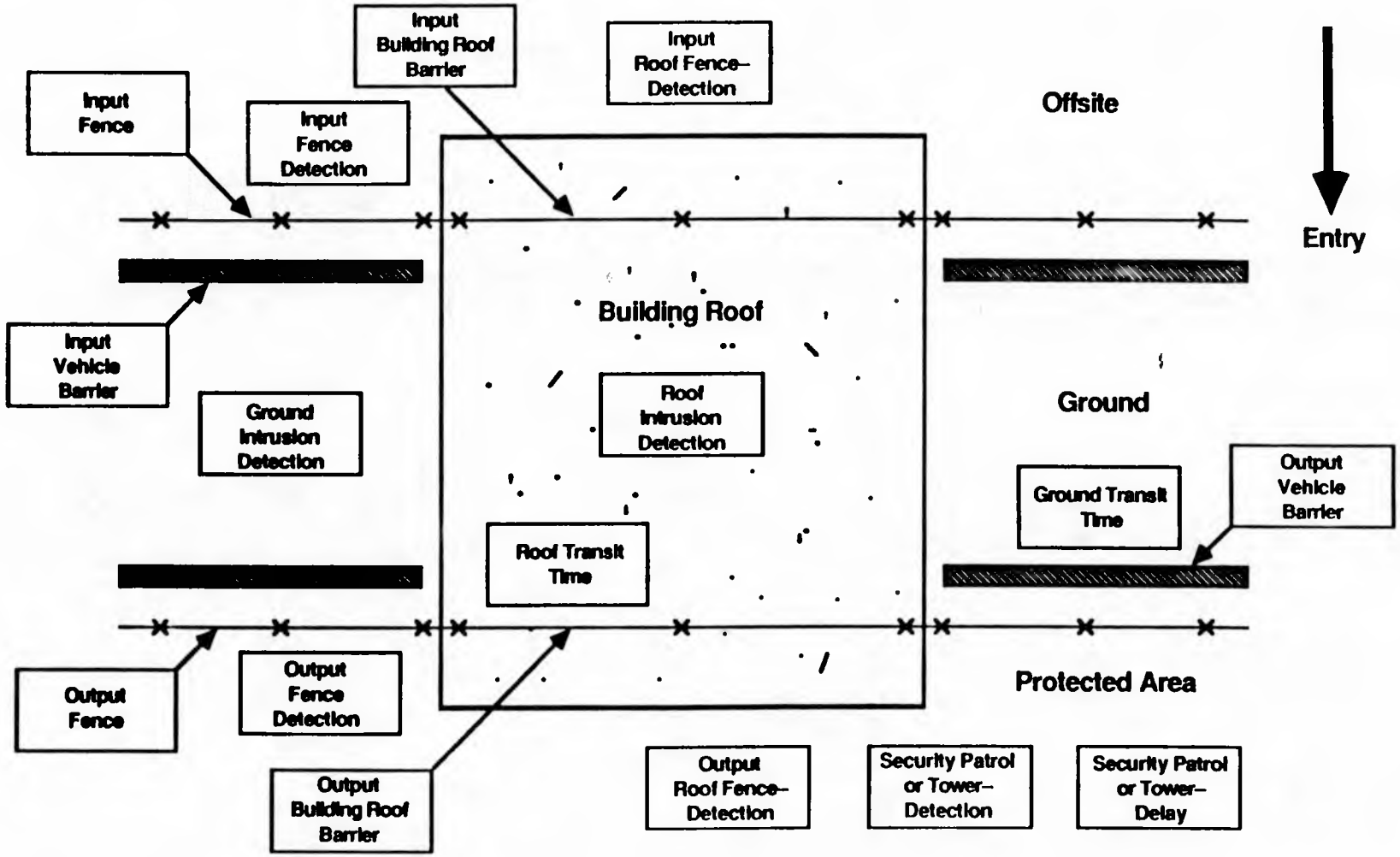
GATE



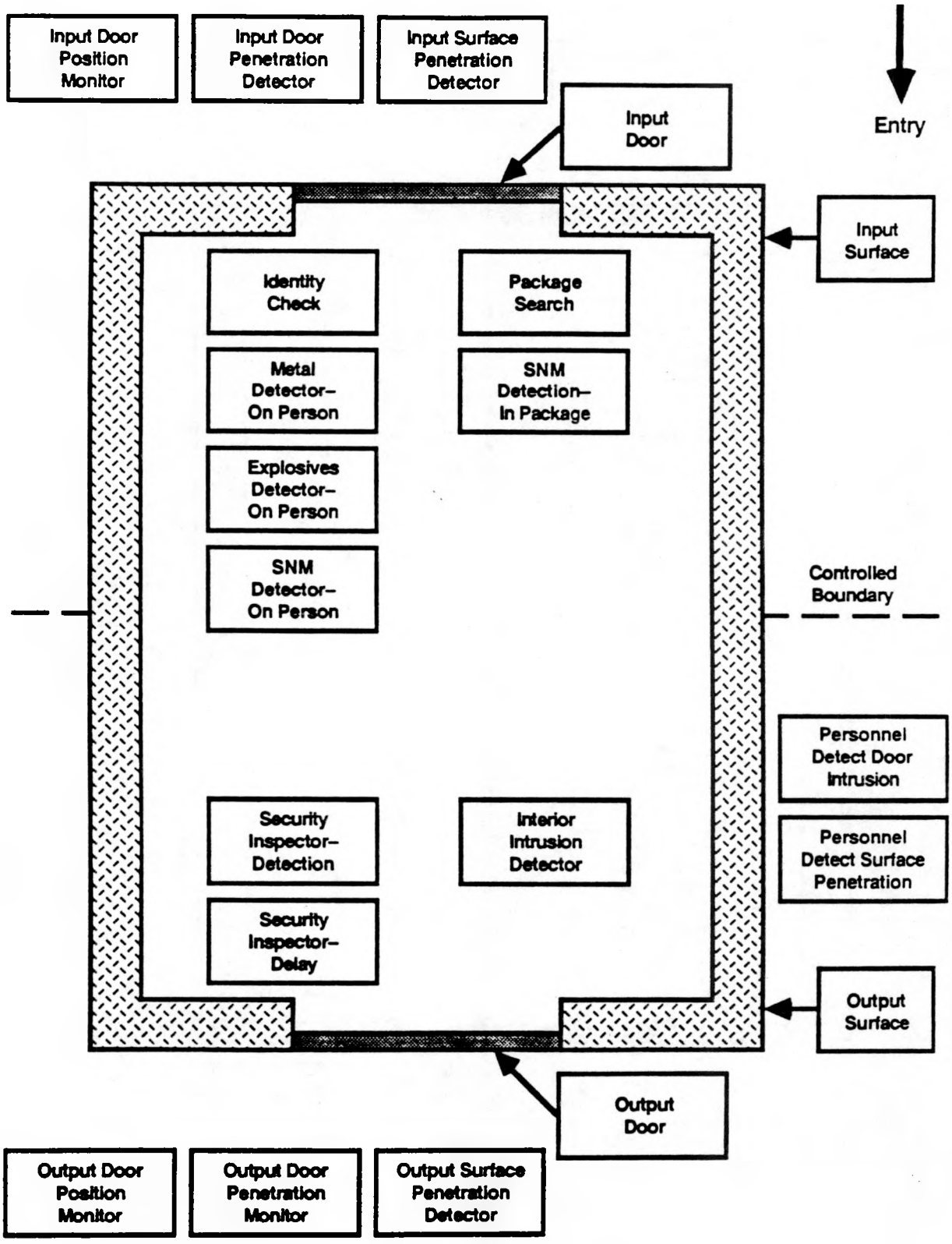
HELICOPTER FLIGHT PATH



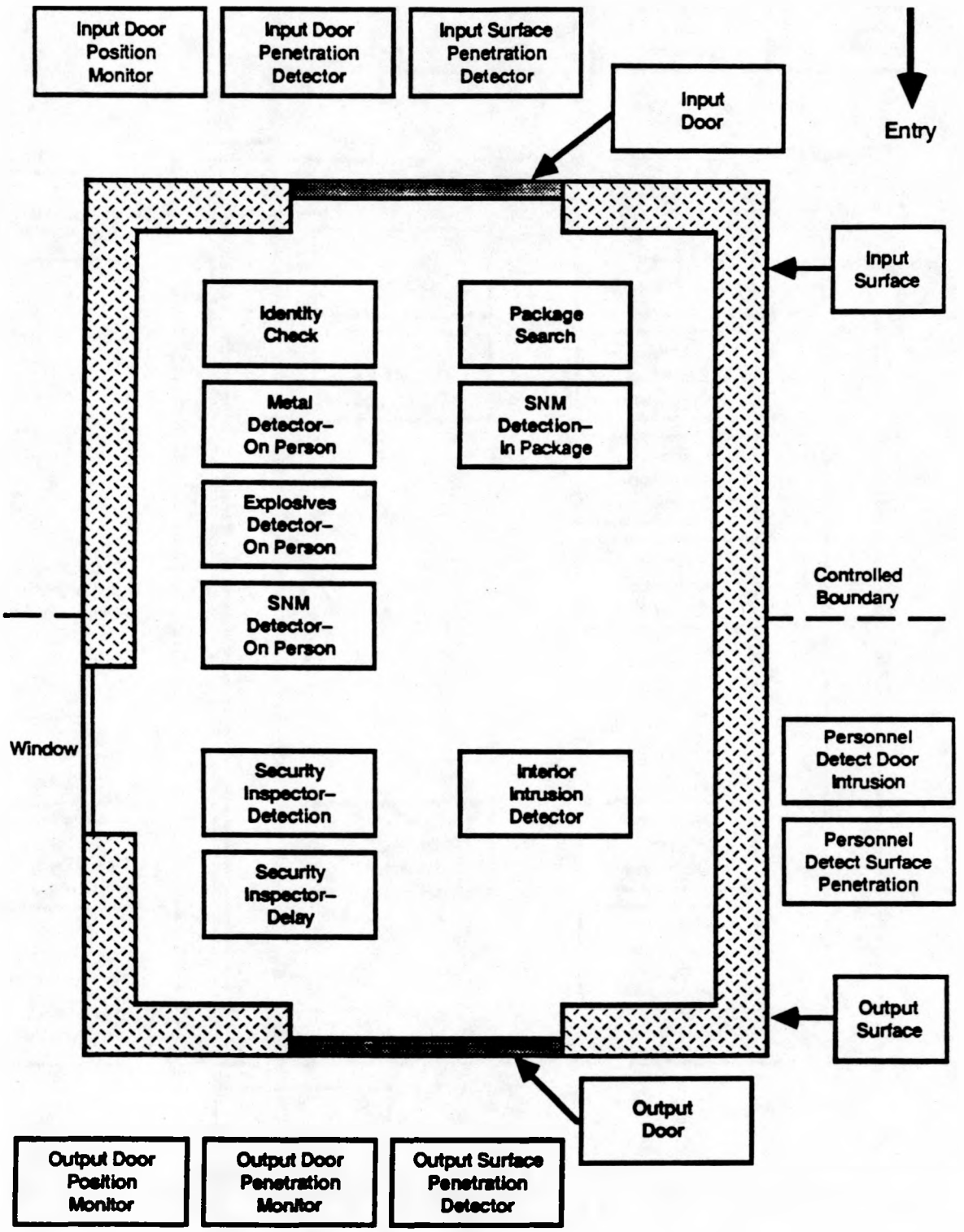
GENERIC



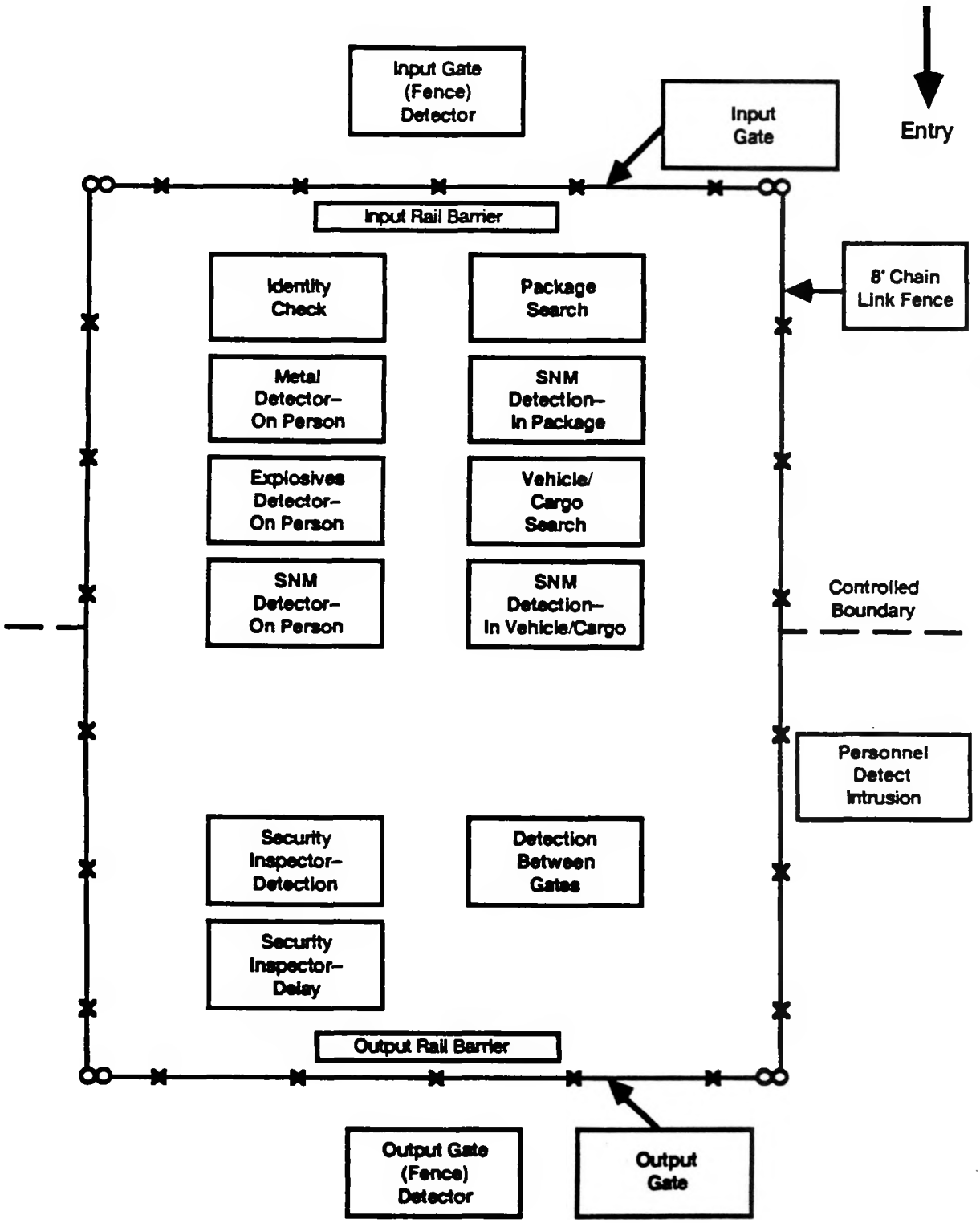
ISOLATION ZONE



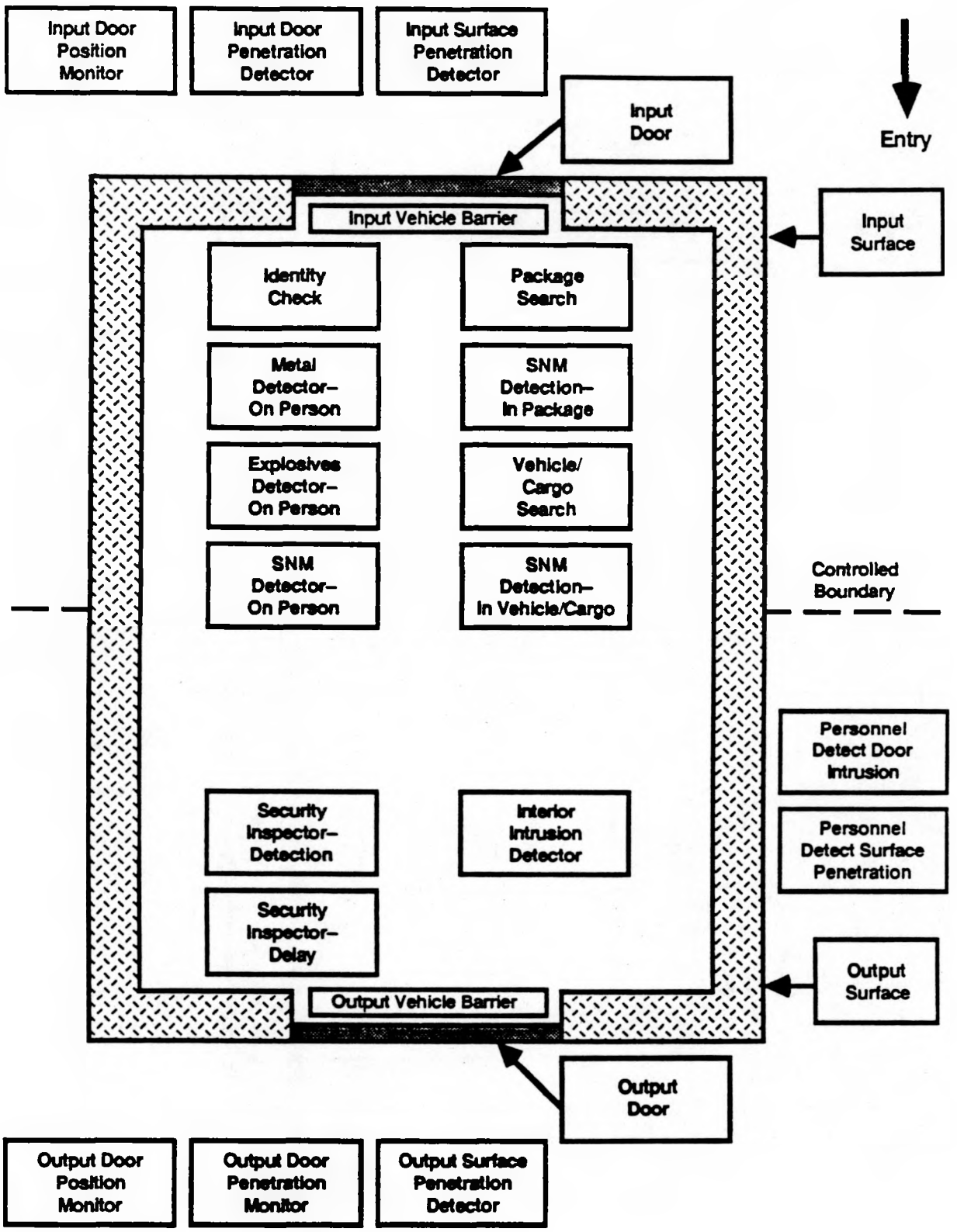
MATERIAL PORTAL



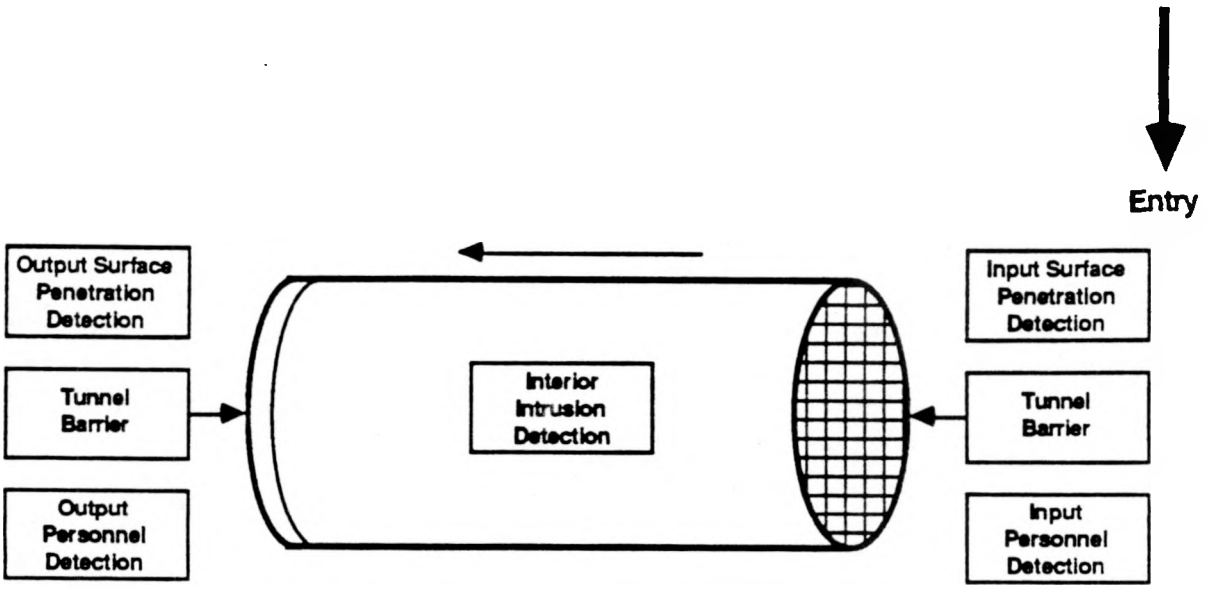
PERSONNEL PORTAL


Input Gate (Fence) Detector
Input Gate
Entry
Input Rail Barrier
8' Chain Link Fence
Identity Check
Package Search
Metal Detector– On Person
SNM Detection– In Package
Explosives Detector– On Person
Vehicle/ Cargo Search
SNM Detector– On Person
SNM Detection– In Vehicle/Cargo
Controlled Boundary
Personnel Detect Intrusion
Security Inspector– Detection
Detection Between Gates
Security Inspector– Delay
Output Rail Barrier
Output Gate (Fence) Detector
Output Gate

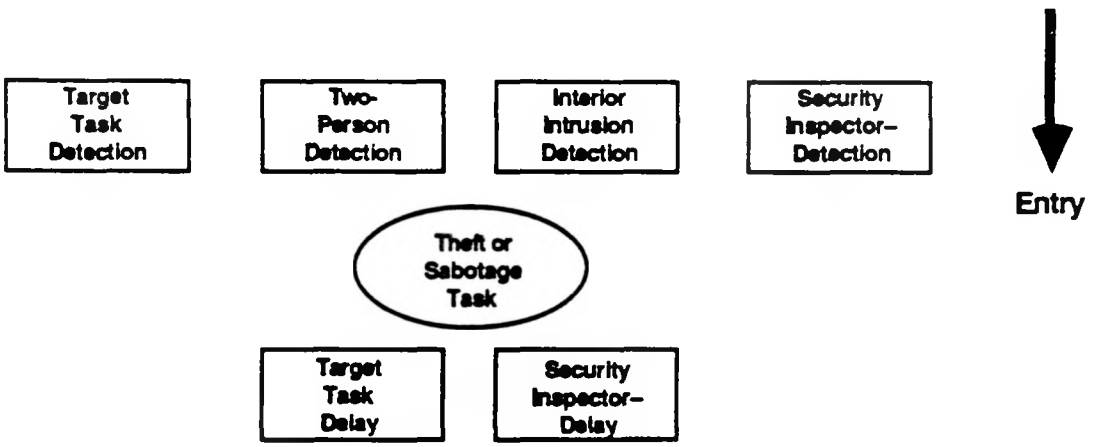
RAIL PORTAL



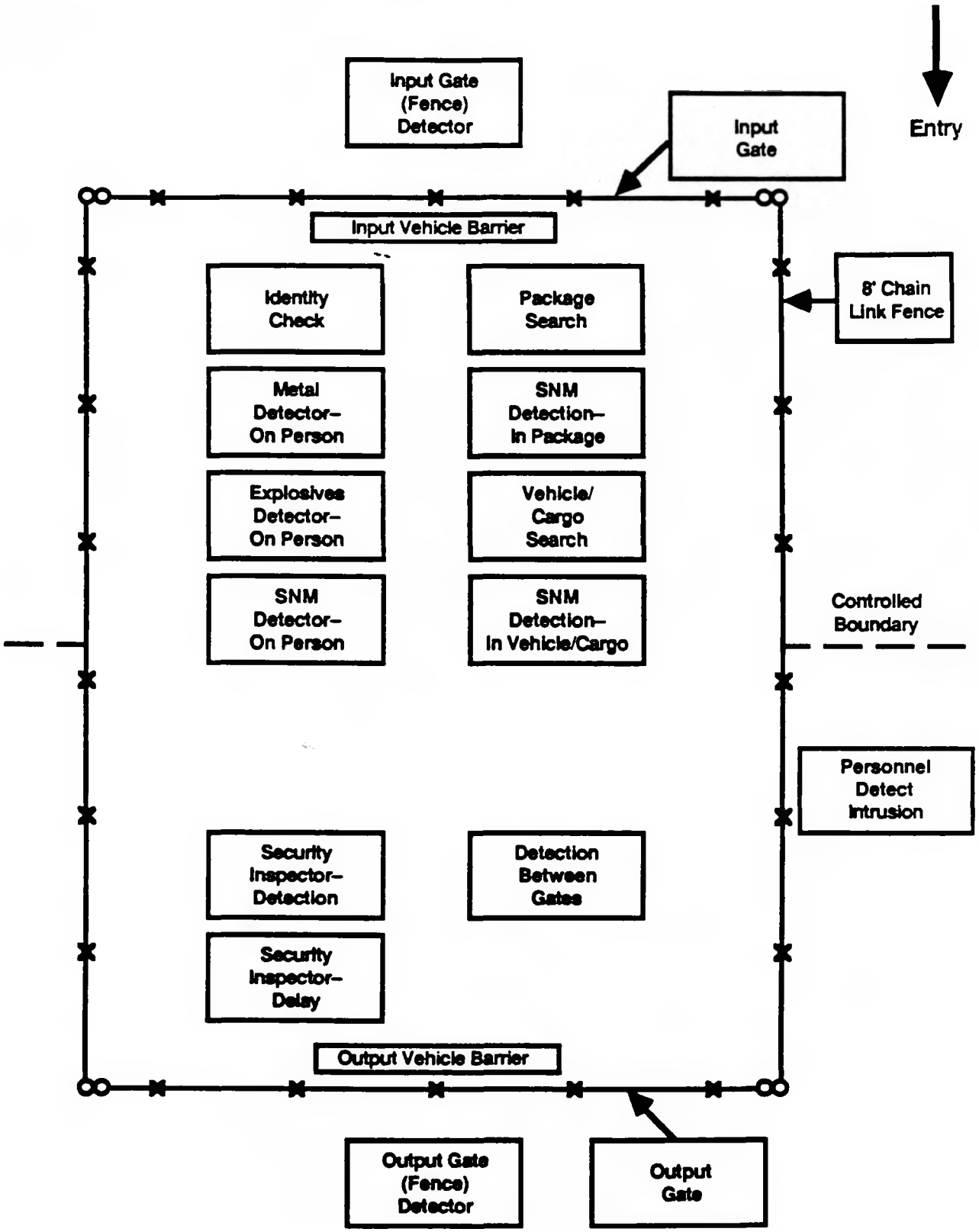
SHIPPING AREA



TUNNEL

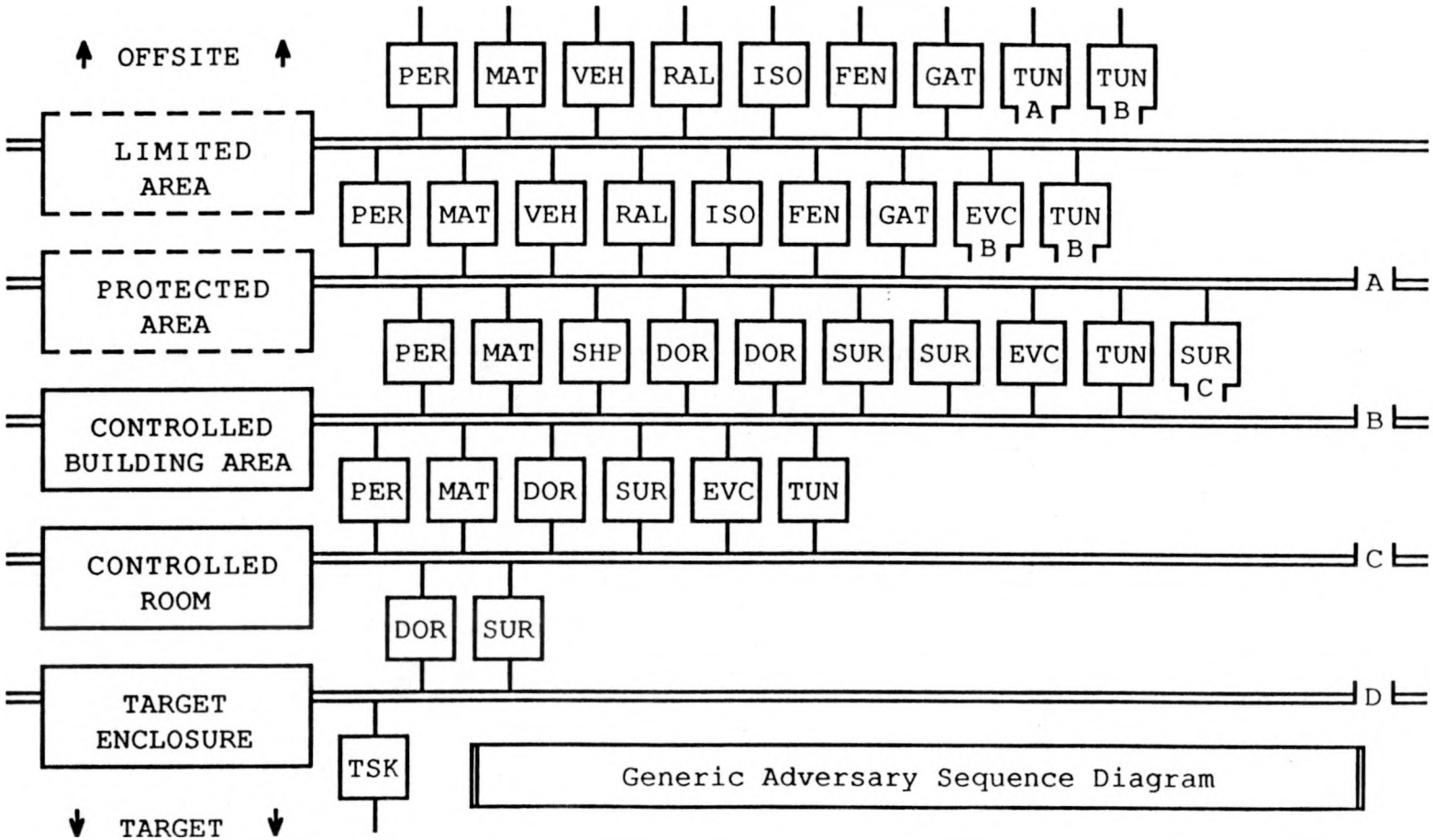


THEFT OR SABOTAGE TASK



VEHICLE PORTAL

Generic Adversary Sequence Diagram



SECTION E

SAVI Algorithm

The SAVI Algorithm

1. Abstract

SAVI (Systematic Analysis of Vulnerability to Intrusion) is a PC-based vulnerability assessment tool for the analysis of physical protection systems. SAVI utililizes an exhaustive path analysis algorithm to identify the most vulnerable path through a facility from offsite to any target of concern; the software can analyze vulnerability to removal of the target from the facility (theft) as well as access to the target (sabotage). All possible paths through the facility are examined and the ten most vulnerable are retained. The vulnerability of a particular path is estimated using the measures of Timely Detection. This is the requirement that an intruder be detected with enough time for the response force to interrupt him before he can complete his mission. Because the analysis is exhaustive, complex facilities can take a long time to analyze and some paths are considered illogical or inappropriate. Paths are pruned where possible to mitigate these problems.

2. Terms and Concepts

The complex nature of vulnerability analysis has caused the development of a large dialect of terms to simplify the concepts behind the SAVI methodology. A portion of the SAVI dialect is reproduced below as a convenience to the reader. These terms are the minimum required to understand the description of the SAVI algorithm.

Area - A physical area at a facility separated from other areas by layers of protection. The SAVI model assumes that all points inside a given area are equally accessible to an intruder.

ASD - Adversary Sequence Diagram. A graphic representation of a physical protection system comprised of protection elements connecting physical areas.

CDP - Critical Detection Point. The last point on a given path where detection must occur if the response force is to have enough time to interrupt the adversary before he completes his mission.

Delay Leg - The portion of a path where an adversary minimizes the time it takes to complete his mission.

Detection Leg - The portion of a path where an adversary minimizes his chances of being detected.

Entry Leg - The sequence of areas and elements traversed by an intruder from offsite to the target.

Exit Leg - The sequence of areas and elements traversed by an intruder from the target to offsite (only considered in the case of theft analysis).

Invalid Path - A path generated during theft analysis where the intruder forces his way through an element on entry and attempts to deceive his way through the same element on exit.

P(I) - Probability of Interruption. The probability that the response force will interrupt the adversary prior to completion of his mission.

Parasite Path - One of several path scenarios for a given path which is not the most vulnerable scenario.

Path - A specific route through the facility consisting of a sequence of physical areas and protection elements that an adversary traverses to accomplish his mission.

Path Scenario - A specific sequence of force or deceit actions that an adversary may use to defeat each protection element on a path. A path scenario differs from a path in that it contains traversal mode information.

PE - Protection Element. The basic building block of a physical protection system consisting of components which detect and delay the adversary.

PPS - Physical Protection System. The collective interaction of delay, detection, assessment and communication components, plus security and response force personnel that provide protection for facility targets.

Protection Layer - A set of protection elements which separate two physical areas in a physical protection system.

Redundant Path - A path scenario with deceit traversal on the delay leg of the path.

RFT - Response Force Time. The assessment, communication, and deployment time expended by the response force in order to reach a specified interruption point after receiving the first alarm.

Timely Detection - A security system requirement which states that the adversary must be detected in time for the response force to interrupt him before he completes his mission.

TR - Time Remaining after CDP. The minimum time required for an adversary to complete his mission from the Critical Detection Point on a given path.

Traversal Mode - The tactics employed by the adversary to penetrate a protection layer. The two tactics currently supported by SAVI are force and deceit.

TRI - Time Remaining after Interruption. The time remaining on a path after interruption occurs. This is the difference in the time remaining after CDP and the response force time.

The SAVI Algorithm - 2

3. SAVI Overview

The SAVI software package is a vulnerability assessment code developed under contract to Sandia National Laboratories with Department of Energy funding to support the effective design and analysis of Physical Protection Systems (PPSs) at facilities that handle special nuclear materials. SAVI represents a PPS as a connected graph of areas and elements in a structure called an Adversary Sequence Diagram (ASD). As an adversary penetrates a PPS he moves from area to area within the facility and submits himself to an ordered sequence of protection layers arranged in 'concentric' shells of protection. The ASD is therefore a series of areas separated by protection layers through which the adversary must pass in order to successfully complete his mission. Each layer of protection is comprised of Protection Elements (PEs) which correspond to the physical elements providing security at the facility: portals, surfaces, isolation zones, etc. Each element is a collection of components which act to detect or delay an intruder during his assault on the facility: metal detectors, walls, doors, etc. The adversary must traverse a PE in order to move from one area to another one deeper in the facility, and he must pay a price in doing so. If the intruder has not yet been detected, the cost is the chance that he will be detected attempting to penetrate this particular layer of security. If he *has* been detected, then the cost is the amount of time that the PE delays him in his race to complete his mission before being interrupted by the response force. All detection probabilities in SAVI are chosen assuming no previous detection has taken place while all delays are chosen assuming the adversary has been previously detected. A PE is modelled as an input segment and an output segment, providing a simple and flexible structure to describe a large variety of elements. Each segment is assigned detection probabilities and delay times as costs associated with traversing that segment. There are 6 costs associated with each segment: probabilities of non-detection and delays for entry, exit, and dependent exit. These costs are explained in greater detail below.

Any sequence of elements from offsite to the target or mission end point of concern is a potential path for the intruder to take in his assault on the system. SAVI identifies the paths which are most vulnerable to intrusion. These are the paths that are the most advantageous from the adversary's point of view. The SAVI model is conceptually very simple. The concept of Timely Detection is used to quantify the vulnerability of a legitimate path through the ASD. Timely Detection is a security system requirement that an intruder must be detected with enough time left to interrupt him. The crafty intruder minimizes his chances of being detected until the amount of delay time remaining before completion of his mission is less than the Response Force Time (RFT). After the adversary has passed this point

there is no longer any chance of detecting him with enough delay in the system to allow the response force to interrupt him. This point, the Critical Detection Point (CDP), is therefore the last chance to detect the adversary before he beats the system. The probability of interruption, P(I), is the cumulative probability of detection from the entry point through CDP. The difference between Time Remaining after CDP (TR) and the Response Force Time is the Time Remaining after Interruption (TRI) and is a measure of how close the adversary gets to mission completion assuming he is detected at CDP. The Timely Detection concept is illustrated graphically as shown in Figure 1.

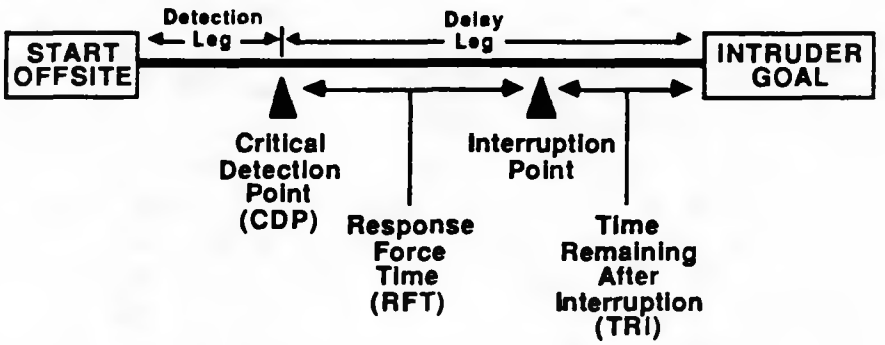


Figure 1. Timely Detection Event Sequence

SAVI allows the security analyst to specify the tactics that an adversary will use to defeat a given security system, i.e. whether he will simply force his way through each PE or attempt to deceive his way through when appropriate. If the adversary forces his way through a PE, destroying barriers or detectors in the process, the protection offered by that PE on the intruder's return trip has been compromised. If the adversary *deceives* his way through a PE, the safeguards in the PE are still available to hinder the intruder should he return through the same element on exit. The SAVI analysis engine handles the different traversal modes by splitting each deceivable PE into a force-only and deceit-only counterpart (or clone). Each cloned element increases the number of possible paths in the facility geometrically.

Consider a unique chain of elements comprising a path from offsite to the target. Cloning a single element into a force/deceit pair will produce two new paths (at the cloned element the adversary may choose to traverse in a force manner or in a deceit manner). If another element along the path is cloned, the number of paths is doubled again for a total of four paths. If the facility is being analyzed for vulnerability to theft, then there is an exit leg corresponding to each entry leg and the number of paths increases to the square of the number of entry paths. But the cloning process is simply the approach used by the engine to track the traversal tactics used by the adversary in his assault on each element. The SAVI analyst

doesn't care about the extra paths since he is concerned only with the unique chain of elements used by the intruder. Thus the total number of paths generated by the SAVI engine is a superset of the set of all paths represented by the analyst's ASD. These extra 'paths' actually contain information about which elements were traversed and the tactics used to traverse them. These 'paths' are called path scenarios to distinguish them from actual paths, which are unique chains of PEs.

Handling paths in this fashion has several interesting side effects. SAVI can produce the ten most vulnerable paths for a given RFT, but if mixed tactics are used, it may be that these ten paths are the same set of PEs with different traversal modes (i.e. different path scenarios). Such paths are called parasite paths; they are useless information for the analyst who is interested in the optimal traversal of a unique path. Therefore, any path which is actually a different scenario of a path that has been found previously is discarded unless it is the more vulnerable of the two. Each of the ten most vulnerable paths is a unique chain of elements and represents the most vulnerable path scenario for that chain of elements.

The second side effect of the cloning process is the production of a type of path called a 'redundant path'. After the adversary has passed the CDP, detection is unimportant since the guards cannot respond fast enough to interdict him. Therefore the delay times for traversing a segment are the same whether the traversal tactic is force or deceit. This means that the force and deceit clones created from a deceivable element both have the same delay values. We are therefore only interested in force-traversal clones on the delay leg of the path. Note that redundant paths would be taken care of in the removal of parasite paths, but we discard them as soon as we are aware that they are redundant in order to save calculation time.

The last side effect of the cloning process is the production of 'invalid paths'. This type of path only appears when the analysis is for theft. If the adversary forces a particular PE, blowing up the door and killing the guard for example, it is illogical to model deceit through the same PE on exit. Therefore, any time a deceit-only clone appears on the exit leg, a check is made to see if its force counterpart appears on the entry leg. If so, the path is discarded.

4. SAVI ASD Tree Structure

The SAVI ASD can be thought of as a tree structure, and all PEs that an intruder might use to leave an area can be thought of as a branch in the tree. The SAVI engine uses two data structures to find the set of paths through an ASD. These are the adjacency array and the stack. The adjacency array represents the ASD tree structure while the stack is a list of segments representing a single path. The

elemental unit in this representation is the vertex, or path segment. A vertex has a one to one correspondence to the segments which make up Protection Elements. The time it takes an intruder to cross an area is accumulated into the input segment of a PE and the time it takes to cross a PE accumulated into the output segment. Each vertex has an associated structure or record that contains all the information about its corresponding segment on the graph. The structure contains a pointer to the next structure, a visited field, and information specific to the given ASD. There are six pieces of information maintained for each path segment describing the costs associated with crossing that segment:

- Probability of non-detection on entry
- Probability of non-detection on exit (independent)
- Dependent probability on exit (assuming entry through this segment)
- Time delay on entry
- Time delay on exit (independent)
- Dependent delay on exit (assuming entry through this segment)

These values are determined in the following manner: the entry and exit detection probabilities are the sets of detection components which have the lowest cumulative probability across that segment upon traversal. The dependent values are set to 0.0 if the segment represents delay or detection associated with traversal by force on entry. If it is not a forced entry (i.e. the current element is the deceit-only clone of a deceivable element), then the dependent value is the same as the independent exit value. In addition, there are 3 fields which identify this vertex, and its adjacent vertex:

- Vertex number, a unique identifier for this vertex
- Adjacent number, an identifier for the adjacent vertex
- Clone number, an identifier for Force/Deceit vertices.

The tree structure is implemented in the SAVI engine as an array of linked lists. Each path segment in the ASD appears as an item in the array. For each vertex in the array there is a linked list of all vertices adjacent to that vertex (leading *from* that vertex). Figure 2 shows a simple ASD and the adjacency array representing it. Note that vertex 5 is the target and since it does not connect to any further nodes, vertex 5 has a null pointer.

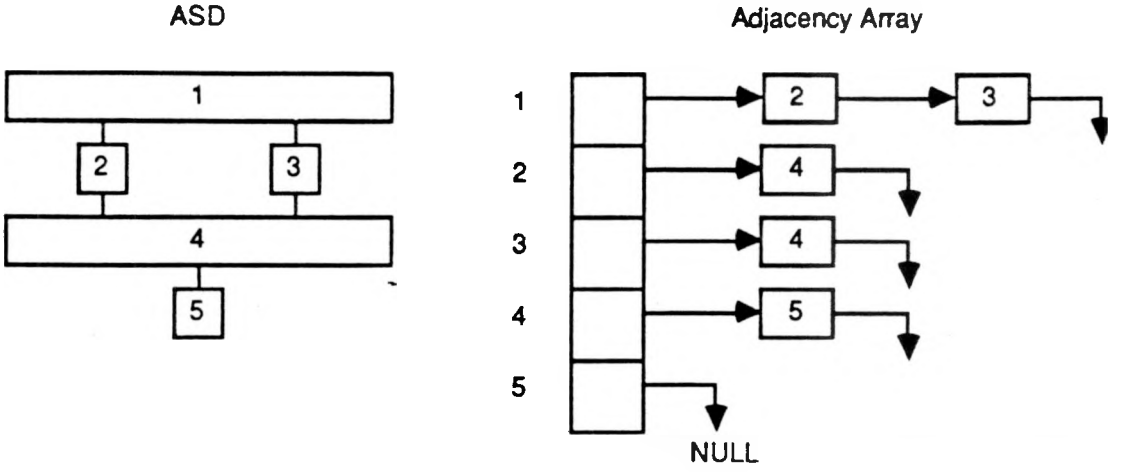


Figure 2. SAVI Tree Structure for Entry Analysis

The tree is built by inspecting the connectivity of each element in the ASD. For each element a pointer to that path segment is inserted into the linked list for that vertex in the Adjacent Array. In addition to all the values in the structure, the vertex identification number is assigned, and the adjacent number is the number of the area that the Protection Element is connected to. If this element is entered in a Force manner, that node is inserted again with its clone number as its vertex identification number.

If the analysis is for the theft case (see Figure 3), the adjacency array is expanded to model the vertices separately on exit. The destination now becomes the origin; the traversal is origin to target to origin. The identification number of all the vertices from the target back to the origin are aliased by adding an offset which is the actual target's index number. The identification number of the destination in the example is 6 (obtained by adding the origin identification number, 1, to the alias offset, 5). Hence, the path from 1 -> 2 -> 4 -> 5 -> 4 -> 2 -> 1 is represented as 1 -> 2 -> 4 -> 5 -> 9 -> 7 -> 6.

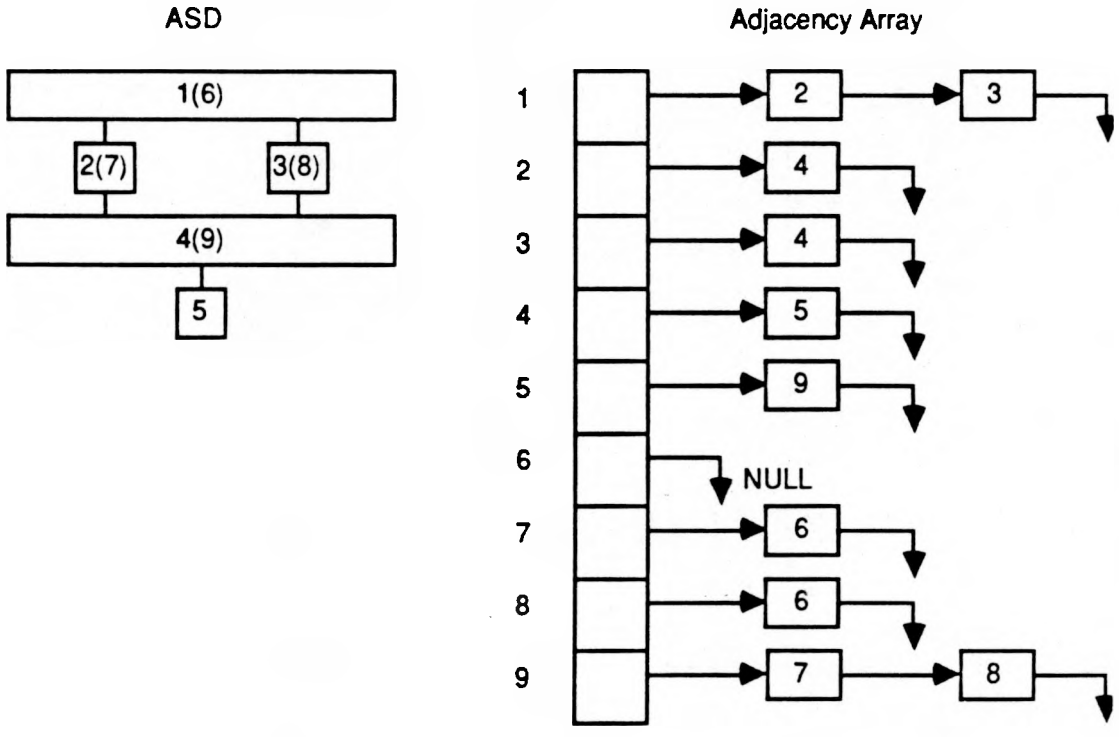


Figure 3. SAVI Tree Structure for Entry/Exit Analysis

5. Finding a path

The SAVI engine employs an exhaustive tree traversal algorithm called a 'depth first search'. The algorithm operates on vertices as follows:

The first vertex from the origin is marked visited. Then the next adjacent or connecting unvisited vertex from the previous vertex is marked visited and the depth first search is initiated again. This continues until a destination vertex is reached. At this point the algorithm 'back-tracks'. We back up to the last vertex which has an unvisited vertex adjacent to it, and then we can initiate the depth first search once again. The entire search terminates when no unvisited vertices can be reached from any of the visited ones (and therefore every branch of the tree has been traversed). The following is a pseudo-code representation of the 'depth first search' employed by SAVI:

```
Procedure Depth_First
    Vertex = Adjacent[origin]
    push(stack,Vertex)
```

```
while not empty(stack)
        begin
                // find a path //
                while adjacent[Vertex] not NULL
                        begin
                                // find next connection //
                                Vertex = Adjacent[Vertex]
                                push(stack,Vertex)
                                set Vertex visited
                        end
                // path has been found. Display, perform analysis, etc. //
                // get next path from the the stack //
                backtrack(Vertex)
        end

Procedure Backtrack(Vertex)
   begin
        Vertex = pop(stack)          // remove target //
        while Adjacent[Vertex] = NULL
                pop(stack)           // pop stack until a vertex is found with //
                                     // other connections //
        while Adjacent[Vertex] is visited and Adjacent[Vertex] not NULL
                Vertex = next Vertex      // now that a connection is found, //
                                          // skip to next unvisited connection //
        return(Vertex)
   end
```

The algorithm can be described in the following manner:

Initialize all vertices to unvisited.

Path Finding Algorithm:
Starting with the origin, or first vertex, set it to visited, save this vertex on the stack. Get its next connection from the Adjacency array and set it visited. Continue until the destination is encountered, or there are no further connections in the adjacency array. An entire path has been found and can be viewed and used for analysis at this point.

The backtrack algorithm is employed to find any other routes to the destination from each vertex:

Backtrack Algorithm:
Pop the target from the stack and check if there are any other unvisited vertices in the adjacency array. If so, push it onto the stack and return to the path finding algorithm. If not, and there are no other connections from this vertex, pop the next vertex from the stack and search for an unvisited vertex. This continues until either a vertex is found, or the origin is encountered, meaning all vertices have been seen.

6. Quantifying a path

Once a path is identified it is quantified and ranked by its vulnerability. The path finding algorithm produces a string of segments representing the path taken by the adversary from offsite to his goal. The target is the goal in the case of sabotage analysis and offsite via the target is the goal in the case of theft analysis. The path is scanned once before quantification begins in order to prepare the quantify algorithm. The target is located on the stack to identify the entry and exit legs of the path in the theft case. The entry and exit sides are compared to identify dependent elements. Any element appearing in the exit side of the path after having appeared in the entry side is said to be dependent. All dependent elements are marked. If force/deceit analysis is requested, the path is checked for validity during this first pass. If a deceit-only clone is found on the exit side of the path then the entry side of the path is checked for a corresponding force-only clone. If the force-only element is found, the path is considered invalid, quantification of this path ends, and the path is discarded. At this point the quantify algorithm is ready to analyze the current path. If multiple RFTs are requested, then the path is analyzed once for each RFT.

The quantify algorithm begins at the top of the path stack and grabs the vertex it finds there (offsite in the theft case and the target in the sabotage case) and begins its analysis. Since the adversary is being backtracked from his goal, the CDP has not been located and we are on the delay leg of the path. Therefore, if the current vertex is a deceit-only element, then the path is a redundant path and we stop analyzing for this particular RFT. Since the CDP can change with RFT, we cannot assume this path is redundant for *all* RFTs. If the path is still legitimate, the delay offered to the intruder is added into the total delay value for this path. If we are still on the exit side of the path then the exit delay value is used unless this vertex has been marked as a dependent element. If a dependency exists the exit-dependent delay value is used. If the current vertex is on the entry side of the path, the entry delay value is used. The new total delay value for this path is now compared against the current RFT. If the total delay is greater than RFT, the entire delay leg is found and we have fixed CDP. If the total delay is less than or equal to RFT then we are still working on the delay leg and we grab the next vertex from the stack and

do it all again. If the CDP is never found, there is not enough delay in the entire system to prevent the intruder from completing his mission; the response force is too slow or the barriers protecting the target or preventing the adversary's escape are insufficient.

Once CDP is located for a given RFT we calculate the Probability of Interruption for the current path. The probabilities of nondetection for each vertex from CDP to the bottom of the stack are accumulated according to the following equation:

$$P(I) = 1 - \prod_{k}(PNDk)$$

where PNDk is the Probability of Nondetection for the kth vertex.

After the path is quantified it is checked against each of the top ten most vulnerable paths currently stored for this RFT to determine if it is a parasite of one of the top ten paths. If the path is a parasite path, its vulnerability is checked against that of the stored path and the less vulnerable path is discarded. If the current path is not a parasite path then it is compared against the other most vulnerable paths and kept or discarded based on vulnerability. If the current path is kept, it is inserted into the list of top ten paths.

Summary

The algorithms utilized by SAVI to identify and quantify the most vulnerable paths through a physical protection system are fairly straight forward. The implementation of fast, powerful algorithms was considered secondary to the development of a mathematically defendable modelling methodology. Work is proceeding on new algorithms which should provide considerable improvements over those presented in this document.

References

1. A. E. Winblad, "The SAVI Vulnerability Assessment Model", Volume XVI, Proceedings of the 28th Annual Meeting of the Institute for Nuclear Materials Management, July 12-15, 1987.

2. R. J. McAniff, W. K. Paulus, B. Key, B. Simpkins, "The SAVI Vulnerability Analysis Software Package", Volume XVI, Proceedings of the 28th Annual Meeting of the Institute for Nuclear Materials Management, July 12-15, 1987.

SECTION F

SAVI Element Scenario Equations

SAVI - 2 ELEMENT SCENARIO EQUATIONS

Entry		Exit	
Input	Output	Input	Output
DOR - SINGLE DOOR			
UNAUTHORIZED: Delay			
ZDEL	DR + SID	DR + SID	ZDEL
UNAUTHORIZED: Detection			
INT*SIA	DP*PHD + DG*PHD	DP*PHD*INT*SIA + DG*PHD*INT*SIA	ZDET
AUTHORIZED: Detection			
IDEND*MET*EXP + IDEND*PKG	ZDET	ZDET	SNMP + SNMPK
EVC - EVACUATION SHELTER			
UNAUTHORIZED: Delay			
DR' SURF'	DR' SURF'	DR' SURF'	DR' SURF'
UNAUTHORIZED: Detection			
DP'*INT*PHD + DG'*INT*PHD + DIS'*INT*PHS	DP' + DG' + DIS'	DP' + DG' + DIS'	DP'*INT*PHD + DG'*INT*PHD + DIS'*INT*PHS
FEN - FENCE			
UNAUTHORIZED: Delay			
ZDEL	FN + VB + PTD	FN + VB + PTD	ZDEL
UNAUTHORIZED: Detection			
PTA	DF*DEP	DF	PTA*DEP

SAVI ELEMENT SCENARIO EQUATIONS

Entry		Exit	
Input	Output	Input	Output
	GAT - GATE		
	UNAUTHORIZED: Delay		
ZDEL	GT + VB + SID	GT + VB + SID	ZDEL
	UNAUTHORIZED: Detection		
SIA	GD*DEP	GD	SIA*DEP
	AUTHORIZED: Detection		
IDEND*MET*EXP + IDEND*PKG + IDEND*VSRC	ZDET	ZDET	SNMP + SNMPK + SNMV
	GEN - GENERIC PROTECTION ELEMENT		
	UNAUTHORIZED: Delay		
GDEL'	GDEL'	GDEL'	GDEL'
	UNAUTHORIZED/AUTHORIZED: Detection		
GDET'	GDET'	GDET'	GDET'
	HEL - HELICOPTER FLIGHT PATH		
	UNAUTHORIZED: Delay		
ZDEL	UHDEL	LHDEL	ZDEL
	UNAUTHORIZED: Detection		
HDET*PHH*PTHH	ZDET	ZDET	HDET*PHH*PTHH
	ISO - ISOLATION ZONE		
	UNAUTHORIZED: Delay		
FN' + VB' PB'	FN' + VB' + PTD PB' + PTD	FN' + VB' + PTD PB' + PTD	FN' + VB' PB'
	UNAUTHORIZED: Detection		
DF'*DEP*PTA + DRF'*PBDET*PTA	DF' + DRF'	DF' + DRF'	DF'*DEP*PTA + DRF'*PBDET*PTA

SAVI ELEMENT SCENARIO EQUATIONS

Entry		Exit	
Input	Output	Input	Output
MAT - MATERIAL PORTAL			
UNAUTHORIZED: Delay			
DR' SURF'	DR' + SID SURF' + SID	DR' + SID SURF' + SID	DR' SURF'
UNAUTHORIZED: Detection			
DP'*INT*PHD*SIA + DG'*INT*PHD*SIA + DIS'*INT*PHS*SIA	DP' + DG' + DIS'	DP' + DG' + DIS'	DP'*INT*PHD*SIA + DG'*INT*PHD*SIA + DIS'*INT*PHS*SIA
AUTHORIZED: Detection			
IDEND*MET*EXP + IDEND*PKG	ZDET	ZDET	SNMP + SNMPK
PER - PERSONNEL PORTAL			
UNAUTHORIZED: Delay			
DR' SURF'	DR' + SID SURF' + SID	DR' + SID SURF' + SID	DR' SURF'
UNAUTHORIZED: Detection			
DP'*INT*PHD*SIA + DG'*INT*PHD*SIA + DIS'*INT*PHS*SIA	DP' + DG' + DIS'	DP' + DG' + DIS'	DP'*INT*PHD*SIA + DG'*INT*PHD*SIA + DIS'*INT*PHS*SIA
AUTHORIZED: Detection			
IDEND*MET*EXP + IDEND*PKG	ZDET	ZDET	SNMP + SNMPK

SAVI ELEMENT SCENARIO EQUATIONS

Entry		Exit	
Input	Output	Input	Output
RAL - RAIL PORTAL			
UNAUTHORIZED: Delay			
GT' + VBR'	GT' + VBR' + SID	GT' + VBR' + SID	GT' + VBR'
UNAUTHORIZED: Detection			
GD'*DTE*PHG*SIA	GD'	GD'	GD'*DTE*PHG*SIA
AUTHORIZED: Detection			
IDEND*MET*EXP + IDEND*PKG + IDEND*VSRC	ZDET	ZDET	SNMP + SNMPK + SNMV
SHP - SHIPPING AREA			
UNAUTHORIZED: Delay			
DR' + VB' SURF'	DR' + VB' + SID SURF' + SID	DR' + VB' + SID SURF' + SID	DR' + VB' SURF'
UNAUTHORIZED: Detection			
DP'*INT*PHD*SIA + DG'*INT*PHD*SIA + DIS'*INT*PHS*SIA	DP' + DG' + DIS'	DP' + DG' + DIS'	DP'*INT*PHD*SIA + DG'*INT*PHD*SIA + DIS'*INT*PHS*SIA
AUTHORIZED: Detection			
IDEND*MET*EXP + IDEND*PKG + IDEND*VSRC	ZDET	ZDET	SNMP + SNMPK + SNMV
SUR - SURFACE			
UNAUTHORIZED: Delay			
WLA	WLB + SID	WLB + SID	WLA
UNAUTHORIZED: Detection			
DIS'*INT*PHS*SIA	ZDET	INT	DIS'*PHS*SIA

SAVI ELEMENT SCENARIO EQUATIONS

Entry		Exit	
Input	Output	Input	Output
TSK - TARGET TASK			
UNAUTHORIZED: Delay			
ZDEL	TSKTIM + SID	ZDEL	ZDEL
UNAUTHORIZED: Detection			
TSKDET*INT*2PR*SIA	ZDET	ZDET	ZDET
TUN - TUNNEL			
UNAUTHORIZED: Delay			
TUN'	TUN'	TUN'	TUN'
UNAUTHORIZED: Detection			
DIS'*INT*PHS'	DIS'*PHS'	DIS'*PHS'	DIS'*INT*PHS'
VEH - VEHICLE PORTAL			
UNAUTHORIZED: Delay			
GT' + VB'	GT' + VB' + SID	GT' + VB' + SID	GT' + VB'
UNAUTHORIZED: Detection			
GD'*DTE*PHG*SIA	GD'	GD'	GD'*DTE*PHG*SIA
AUTHORIZED: Detection			
IDEND*MET*EXP + IDEND*PKG + IDEND*VSRC	ZDET	ZDET	SNMP + SNMPK + SNMV

Key:

' Different input and output values

SAVI ELEMENT SCENARIO EQUATIONS

COMPONENT TYPES

DELAYS

PB	Building Roof Barrier
DR	Door
FN	Fence
GT	Gate
GDEL	Generic Delay
LHDEL	Helicopter Load Delay
UHDEL	Helicopter Unload Delay
VBR	Rail Barrier
SID	Security Inspector Delay
PTD	Security Patrol Delay
SURF	Surface
WLA	Surface Delay Stage 1
WLB	Surface Delay Stage 2
TSKTIM	Target Task Time
TUN	Tunnel Barrier
VB	Vehicle Barrier
ZDEL	Zero Delay

DETECTION, UNAUTHORIZED ACTS (FORCE)

PBDET	Building Roof Detection
DTE	Detection Between Gates
DG	Door Penetration Detection
DP	Door Position Monitor
DF	Fence Detection
GD	Gate Detection
GDET	Generic Detection
DEP	Ground Detection
HDET	Helicopter Detector
INT	Interior Intrusion Detection
PTHH	Patrol Detect Helicopter
PHD	Personnel Detect Door Intrusion
PHG	Personnel Detect Gate Intrusion
PHH	Personnel Detect Helicopter
PHS	Personnel Detect Surface Intrusion
SIA	Security Inspector Detection
PTA	Security Patrol Detection
DIS	Surface Penetration Detection
TSKDET	Target Task Detection
2PR	Two-Person Rule Detection
ZDET	Zero Probability of Detection

SAVI ELEMENT SCENARIO EQUATIONS

DETECTION, AUTHORIZED ACTS (DECEIT)

EXP	Explosives Detection on Person
IDEND	Identity Check
MET	Metal Detection on Person
PKG	Package Search
SNMPK	SNM Detection in Package
SNMP	SNM Detection on Person
SNMV	SNM Detection in Vehicle and Cargo
VSRC	Vehicle and Cargo Search

SECTION G

SAVI Component Assignments and Component Performance Values for Protection Elements

***** Protection Element #1 Specifications *****
PERSONNEL PORTAL : PER
Authorized Passage is Possible
Interior Element

Delay Component List :
A) INPUT DOOR
B) INPUT SURFACE
C) SECURITY INSPECTOR DELAY
D) OUTPUT DOOR
E) OUTPUT SURFACE

Detection Component List :
A) INPUT DOOR POSITION MONITOR
B) INPUT DOOR PENETRATION DETECTION
C) INPUT SURFACE PENETRATION DETECTION
D) IDENTITY CHECK
E) METAL DETECTION ON PERSON
F) EXPLOSIVES DETECTION ON PERSON
G) SNM DETECTION ON PERSON
H) PACKAGE SEARCH
I) SNM DETECTION IN PACKAGE
J) INTERIOR INTRUSION DETECTION
K) SECURITY INSPECTOR DETECTION
L) PERSONNEL DETECT DOOR INTRUSION
M) PERSONNEL DETECT SURFACE INTRUSION
N) OUTPUT DOOR POSITION MONITOR
O) OUTPUT DOOR PENETRATION DETECTION
P) OUTPUT SURFACE PENETRATION DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
DOOR
****
SURFACE
****

Unauthorized Delay Traversal Equations :

Output Entry Components
****
DOOR
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
DOOR
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
DOOR
****
SURFACE
****

Unauthorized Detection Traversal Equations :

Input Entry Components
****
DOOR POSITION MONITOR
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
DOOR PENETRATION DETECTION
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
INTERIOR INTRUSION DETECTION
SECURITY INSPECTOR DETECTION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
DOOR POSITION MONITOR
****
DOOR PENETRATION DETECTION
****
SURFACE PENETRATION DETECTION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
DOOR POSITION MONITOR
****
DOOR PENETRATION DETECTION
****
SURFACE PENETRATION DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
DOOR POSITION MONITOR
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
DOOR PENETRATION DETECTION
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
INTERIOR INTRUSION DETECTION
SECURITY INSPECTOR DETECTION
****

Authorized Delay Traversal Equations :

Input Entry Components
****
DOOR
****
SURFACE
****

Authorized Delay Traversal Equations :

Output Entry Components
****
DOOR
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Input Exit Components
****
DOOR
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Output Exit Components
****
DOOR
****
SURFACE
****

Authorized Detection Traversal Equations :

Input Entry Components
****
IDENTITY CHECK
EXPLOSIVES DETECTION ON PERSON
METAL DETECTION ON PERSON
****
IDENTITY CHECK
PACKAGE SEARCH
****

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
SNM DETECTION ON PERSON
****
SNM DETECTION IN PACKAGE
****

***** Protection Element #2 Specifications *****
MATERIAL PORTAL : MAT
Authorized Passage is Possible
Interior Element

Delay Component List :
A) INPUT DOOR
B) INPUT SURFACE
C) SECURITY INSPECTOR DELAY
D) OUTPUT DOOR
E) OUTPUT SURFACE

Detection Component List :
A) INPUT DOOR POSITION MONITOR
B) INPUT DOOR PENETRATION DETECTION
C) INPUT SURFACE PENETRATION DETECTION
D) IDENTITY CHECK
E) METAL DETECTION ON PERSON
F) EXPLOSIVES DETECTION ON PERSON
G) SNM DETECTION ON PERSON
H) PACKAGE SEARCH
I) SNM DETECTION IN PACKAGE
J) INTERIOR INTRUSION DETECTION
K) SECURITY INSPECTOR DETECTION
L) PERSONNEL DETECT DOOR INTRUSION
M) PERSONNEL DETECT SURFACE INTRUSION
N) OUTPUT DOOR POSITION MONITOR
O) OUTPUT DOOR PENETRATION DETECTION
P) OUTPUT SURFACE PENETRATION DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
DOOR
****
SURFACE
****

Unauthorized Delay Traversal Equations :

Output Entry Components
****
DOOR
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
DOOR
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
DOOR
****
SURFACE
****

Unauthorized Detection Traversal Equations :

Input Entry Components
****
DOOR POSITION MONITOR
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
DOOR PENETRATION DETECTION
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
INTERIOR INTRUSION DETECTION
SECURITY INSPECTOR DETECTION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
DOOR POSITION MONITOR
****
DOOR PENETRATION DETECTION
****
SURFACE PENETRATION DETECTION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
DOOR POSITION MONITOR
****
DOOR PENETRATION DETECTION
****
SURFACE PENETRATION DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
DOOR POSITION MONITOR
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
DOOR PENETRATION DETECTION
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
INTERIOR INTRUSION DETECTION
SECURITY INSPECTOR DETECTION
****

Authorized Delay Traversal Equations :

Input Entry Components
****
DOOR
****
SURFACE
****

Authorized Delay Traversal Equations :

Output Entry Components
****
DOOR
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Input Exit Components
****
DOOR
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Output Exit Components
****
DOOR
****
SURFACE
****

Authorized Detection Traversal Equations :

Input Entry Components
****
IDENTITY CHECK
EXPLOSIVES DETECTION ON PERSON
METAL DETECTION ON PERSON
****
IDENTITY CHECK
PACKAGE SEARCH
****

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
SNM DETECTION ON PERSON
****
SNM DETECTION IN PACKAGE
****

***** Protection Element #3 Specifications *****
VEHICLE PORTAL : VEH
Authorized Passage is Possible
Exterior Element

Delay Component List :
A) INPUT GATE
B) INPUT VEHICLE BARRIER
C) SECURITY INSPECTOR DELAY
D) OUTPUT GATE
E) OUTPUT VEHICLE BARRIER

Detection Component List :
A) INPUT GATE DETECTION
B) DETECTION BETWEEN GATES
C) IDENTITY CHECK
D) METAL DETECTION ON PERSON
E) EXPLOSIVES DETECTION ON PERSON
F) SNM DETECTION ON PERSON
G) PACKAGE SEARCH
H) SNM DETECTION IN PACKAGE
I) VEHICLE AND CARGO SEARCH
J) SNM DETECTION IN VEHICLE AND CARGO
K) SECURITY INSPECTOR DETECTION
L) PERSONNEL DETECT GATE INTRUSION
M) OUTPUT GATE DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
GATE
VEHICLE BARRIER
****

Unauthorized Delay Traversal Equations :

Output Entry Components
****
GATE
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
GATE
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
GATE
VEHICLE BARRIER
****

Unauthorized Detection Traversal Equations :

Input Entry Components
****
PERSONNEL DETECT GATE INTRUSION
SECURITY INSPECTOR DETECTION
GATE DETECTION
DETECTION BETWEEN GATES
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
GATE DETECTION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
GATE DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
PERSONNEL DETECT GATE INTRUSION
SECURITY INSPECTOR DETECTION
GATE DETECTION
DETECTION BETWEEN GATES
****

Authorized Delay Traversal Equations :

Input Entry Components
****
GATE
VEHICLE BARRIER
****

Authorized Delay Traversal Equations :

Output Entry Components
****
GATE
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Input Exit Components
****
GATE
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Output Exit Components
****
GATE
VEHICLE BARRIER
****

Authorized Detection Traversal Equations :

Input Entry Components
****
IDENTITY CHECK
EXPLOSIVES DETECTION ON PERSON
METAL DETECTION ON PERSON
****
IDENTITY CHECK
PACKAGE SEARCH
****
IDENTITY CHECK
VEHICLE AND CARGO SEARCH
****

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
SNM DETECTION ON PERSON
****
SNM DETECTION IN PACKAGE
****
SNM DETECTION IN VEHICLE AND CARGO
****

***** Protection Element #4 Specifications *****
RAIL PORTAL : RAL
Authorized Passage Is Possible
Exterior Element

Delay Component List :
A) INPUT GATE
B) INPUT RAIL BARRIER
C) SECURITY INSPECTOR DELAY
D) OUTPUT GATE
E) OUTPUT RAIL BARRIER

Detection Component List :
A) INPUT GATE DETECTION
B) DETECTION BETWEEN GATES
C) IDENTITY CHECK
D) METAL DETECTION ON PERSON
E) EXPLOSIVES DETECTION ON PERSON
F) SNM DETECTION ON PERSON
G) PACKAGE SEARCH
H) SNM DETECTION IN PACKAGE
I) VEHICLE AND CARGO SEARCH
J) SNM DETECTION IN VEHICLE AND CARGO
K) SECURITY INSPECTOR DETECTION
L) PERSONNEL DETECT GATE INTRUSION
M) OUTPUT GATE DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
GATE
RAIL BARRIER
****

Unauthorized Delay Traversal Equations :

Output Entry Components
****
GATE
RAIL BARRIER
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
GATE
RAIL BARRIER
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
GATE
RAIL BARRIER
****

Unauthorized Detection Traversal Equations :

Input Entry Components
****
PERSONNEL DETECT GATE INTRUSION
SECURITY INSPECTOR DETECTION
GATE DETECTION
DETECTION BETWEEN GATES
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
GATE DETECTION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
GATE DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
PERSONNEL DETECT GATE INTRUSION
SECURITY INSPECTOR DETECTION
GATE DETECTION
DETECTION BETWEEN GATES
****

Authorized Delay Traversal Equations :

Input Entry Components
****
GATE
RAIL BARRIER
****

Authorized Delay Traversal Equations :

Output Entry Components
****
GATE
RAIL BARRIER
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Input Exit Components
****
GATE
RAIL BARRIER
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Output Exit Components
****
GATE
RAIL BARRIER
****

Authorized Detection Traversal Equations :

Input Entry Components
****
IDENTITY CHECK
EXPLOSIVES DETECTION ON PERSON
METAL DETECTION ON PERSON
****
IDENTITY CHECK
PACKAGE SEARCH
****
IDENTITY CHECK
VEHICLE AND CARGO SEARCH
****

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
SNM DETECTION ON PERSON
****
SNM DETECTION IN PACKAGE
****
SNM DETECTION IN VEHICLE AND CARGO
****

***** Protection Element #5 Specifications *****
SHIPPING AREA : SHP
Authorized Passage is Possible
Interior Element

Delay Component List :
A) INPUT DOOR
B) INPUT VEHICLE BARRIER
C) INPUT SURFACE
D) SECURITY INSPECTOR DELAY
E) OUTPUT DOOR
F) OUTPUT VEHICLE BARRIER
G) OUTPUT SURFACE

Detection Component List :
A) INPUT DOOR POSITION MONITOR
B) INPUT DOOR PENETRATION DETECTION
C) INPUT SURFACE PENETRATION DETECTION
D) IDENTITY CHECK
E) METAL DETECTION ON PERSON
F) EXPLOSIVES DETECTION ON PERSON
G) SNM DETECTION ON PERSON
H) PACKAGE SEARCH
I) SNM DETECTION IN PACKAGE
J) VEHICLE AND CARGO SEARCH
K) SNM DETECTION IN VEHICLE AND CARGO
L) INTERIOR INTRUSION DETECTION
M) SECURITY INSPECTOR DETECTION
N) PERSONNEL DETECT DOOR INTRUSION
O) PERSONNEL DETECT SURFACE INTRUSION
P) OUTPUT DOOR POSITION MONITOR
Q) OUTPUT DOOR PENETRATION DETECTION
R) OUTPUT SURFACE PENETRATION DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
DOOR
VEHICLE BARRIER
****
SURFACE
****

Unauthorized Delay Traversal Equations :

Output Entry Components
****
DOOR
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
DOOR
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
DOOR
VEHICLE BARRIER
****
SURFACE
****

Unauthorized Detection Traversal Equations :

Input Entry Components
****
DOOR POSITION MONITOR
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
DOOR PENETRATION DETECTION
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
INTERIOR INTRUSION DETECTION
SECURITY INSPECTOR DETECTION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
DOOR POSITION MONITOR
****
DOOR PENETRATION DETECTION
****
SURFACE PENETRATION DETECTION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
DOOR POSITION MONITOR
****
DOOR PENETRATION DETECTION
****
SURFACE PENETRATION DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
DOOR POSITION MONITOR
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
DOOR PENETRATION DETECTION
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
****
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
INTERIOR INTRUSION DETECTION
SECURITY INSPECTOR DETECTION
****

Authorized Delay Traversal Equations :

Input Entry Components
****
DOOR
VEHICLE BARRIER
****
SURFACE
****

Authorized Delay Traversal Equations :

Output Entry Components
****
DOOR
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Input Exit Components
****
DOOR
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****
SURFACE
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Output Exit Components
****
DOOR
VEHICLE BARRIER
****
SURFACE
****

Authorized Detection Traversal Equations :

Input Entry Components
****
IDENTITY CHECK
EXPLOSIVES DETECTION ON PERSON
METAL DETECTION ON PERSON
****
IDENTITY CHECK
PACKAGE SEARCH
****
IDENTITY CHECK
VEHICLE AND CARGO SEARCH
****

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
SNM DETECTION ON PERSON
****
SNM DETECTION IN PACKAGE
****
SNM DETECTION IN VEHICLE AND CARGO
****

***** Protection Element #6 Specifications *****
ISOLATION ZONE : ISO
Exterior Element

Delay Component List :
A) INPUT FENCE
B) INPUT VEHICLE BARRIER
C) INPUT BUILDING ROOF BARRIER
D) SECURITY PATROL DELAY
E) OUTPUT FENCE
F) OUTPUT VEHICLE BARRIER
G) OUTPUT BUILDING ROOF BARRIER

Detection Component List :
A) INPUT FENCE DETECTION
B) OUTPUT FENCE DETECTION
C) GROUND DETECTION
D) SECURITY PATROL DETECTION
E) INPUT ROOF FENCE DETECTION
F) OUTPUT ROOF FENCE DETECTION
G) BUILDING ROOF DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
FENCE
VEHICLE BARRIER
****
BUILDING ROOF BARRIER
****

Unauthorized Delay Traversal Equations :

Output Entry Components
****
FENCE
VEHICLE BARRIER
SECURITY PATROL DELAY
****
BUILDING ROOF BARRIER
SECURITY PATROL DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
FENCE
VEHICLE BARRIER
SECURITY PATROL DELAY
****
BUILDING ROOF BARRIER
SECURITY PATROL DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
FENCE
VEHICLE BARRIER
****
BUILDING ROOF BARRIER
****

Unauthorized Detection Traversal Equations :

Input Entry Components
****
FENCE DETECTION
GROUND DETECTION
SECURITY PATROL DETECTION
****
ROOF FENCE DETECTION
BUILDING ROOF DETECTION
SECURITY PATROL DETECTION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
FENCE DETECTION
****
ROOF FENCE DETECTION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
FENCE DETECTION
****
ROOF FENCE DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
FENCE DETECTION
GROUND DETECTION
SECURITY PATROL DETECTION
****
ROOF FENCE DETECTION
BUILDING ROOF DETECTION
SECURITY PATROL DETECTION
****

Authorized Delay Traversal Equations :

Input Entry Components
****
No Components

Authorized Delay Traversal Equations :

Output Entry Components
****
No Components

Authorized Delay Traversal Equations :

Input Exit Components
****
No Components

Authorized Delay Traversal Equations :

Output Exit Components
****
No Components

Authorized Detection Traversal Equations :

Input Entry Components
****
No Components

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
No Components

***** Protection Element #7 Specifications *****
EVACUATION SHELTER : EVC
Interior Element

Delay Component List :
A) INPUT DOOR
B) INPUT SURFACE
C) OUTPUT DOOR
D) OUTPUT SURFACE

Detection Component List :
A) INPUT DOOR POSITION MONITOR
B) INPUT DOOR PENETRATION DETECTION
C) INPUT SURFACE PENETRATION DETECTION
D) PERSONNEL DETECT DOOR INTRUSION
E) PERSONNEL DETECT SURFACE INTRUSION
F) INTERIOR INTRUSION DETECTION
G) OUTPUT DOOR POSITION MONITOR
H) OUTPUT DOOR PENETRATION DETECTION
I) OUTPUT SURFACE PENETRATION DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
DOOR
****
SURFACE
****

Unauthorized Delay Traversal Equations :

Output Entry Components
****
DOOR
****
SURFACE
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
DOOR
****
SURFACE
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
DOOR
****
SURFACE
****

Unauthorized Detection Traversal Equations :

Input Entry Components
****
DOOR POSITION MONITOR
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
****
DOOR PENETRATION DETECTION
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
****
SURFACE PENETRATION DETECTION
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
DOOR POSITION MONITOR
****
DOOR PENETRATION DETECTION
****
SURFACE PENETRATION DETECTION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
DOOR POSITION MONITOR
****
DOOR PENETRATION DETECTION
****
SURFACE PENETRATION DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
DOOR POSITION MONITOR
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
****
DOOR PENETRATION DETECTION
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT DOOR INTRUSION
****
SURFACE PENETRATION DETECTION
INTERIOR INTRUSION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
****

Authorized Delay Traversal Equations :

Input Entry Components
****
No Components

Authorized Delay Traversal Equations :

Output Entry Components
****
No Components

Authorized Delay Traversal Equations :

Input Exit Components
****
No Components

Authorized Delay Traversal Equations :

Output Exit Components
****
No Components

Authorized Detection Traversal Equations :

Input Entry Components
****
No Components

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
No Components

***** Protection Element #8 Specifications *****
TUNNEL : TUN
Interior Element

Delay Component List :
A) INPUT TUNNEL BARRIER
B) OUTPUT TUNNEL BARRIER

Detection Component List :
A) INPUT SURFACE PENETRATION DETECTION
B) INPUT PERSONNEL DETECT SURFACE INTRUSION
C) INTERIOR INTRUSION DETECTION
D) OUTPUT SURFACE PENETRATION DETECTION
E) OUTPUT PERSONNEL DETECT SURFACE INTRUSION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
TUNNEL BARRIER
****

Unauthorized Delay Traversal Equations :

Output Entry Components
****
TUNNEL BARRIER
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
TUNNEL BARRIER
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
TUNNEL BARRIER
****

Unauthorized Detection Traversal Equations :

Input Entry Components
****
INTERIOR INTRUSION DETECTION
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
INTERIOR INTRUSION DETECTION
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
****

Authorized Delay Traversal Equations :

Input Entry Components
****
No Components

Authorized Delay Traversal Equations :

Output Entry Components
****
No Components

Authorized Delay Traversal Equations :

Input Exit Components
****
No Components

Authorized Delay Traversal Equations :

Output Exit Components
****
No Components

Authorized Detection Traversal Equations :

Input Entry Components
****
No Components

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
No Components

***** Protection Element #9 Specifications *****
SURFACE : SUR
Interior Element

Delay Component List :
A) SURFACE DELAY STAGE 1
B) SECURITY INSPECTOR DELAY
C) SURFACE DELAY STAGE 2

Detection Component List :
A) SURFACE PENETRATION DETECTION
B) PERSONNEL DETECT SURFACE INTRUSION
C) INTERIOR INTRUSION DETECTION
D) SECURITY INSPECTOR DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
SURFACE DELAY STAGE 1
****

Unauthorized Delay Traversal Equations :

Output Entry Components
****
SURFACE DELAY STAGE 2
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
SURFACE DELAY STAGE 2
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
SURFACE DELAY STAGE 1
****

Unauthorized Detection Traversal Equations :

Input Entry Components
****
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
INTERIOR INTRUSION DETECTION
SECURITY INSPECTOR DETECTION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
No Components

Unauthorized Detection Traversal Equations :

Input Exit Components
****
INTERIOR INTRUSION DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
SURFACE PENETRATION DETECTION
PERSONNEL DETECT SURFACE INTRUSION
SECURITY INSPECTOR DETECTION
****

Authorized Delay Traversal Equations :

Input Entry Components
****
No Components

Authorized Delay Traversal Equations :

Output Entry Components
****
No Components

Authorized Delay Traversal Equations :

Input Exit Components
****
No Components

Authorized Delay Traversal Equations :

Output Exit Components
****
No Components

Authorized Detection Traversal Equations :

Input Entry Components
****
No Components

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
No Components

***** Protection Element #10 Specifications *****
DOOR : DOR
Authorized Passage is Possible
Interior Element

Delay Component List :
A) DOOR
B) SECURITY INSPECTOR DELAY

Detection Component List :
A) DOOR POSITION MONITOR
B) DOOR PENETRATION DETECTION
C) SECURITY INSPECTOR DETECTION
D) INTERIOR INTRUSION DETECTION
E) PERSONNEL DETECT DOOR INTRUSION
F) IDENTITY CHECK
G) METAL DETECTION ON PERSON
H) EXPLOSIVES DETECTION ON PERSON
I) SNM DETECTION ON PERSON
J) PACKAGE SEARCH
K) SNM DETECTION IN PACKAGE

Unauthorized Delay Traversal Equations :

Input Entry Components
****
No Components

Unauthorized Delay Traversal Equations :

Output Entry Components
****
DOOR
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
DOOR
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
No Components

Unauthorized Detection Traversal Equations :

Input Entry Components
****
INTERIOR INTRUSION DETECTION
SECURITY INSPECTOR DETECTION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
DOOR POSITION MONITOR
PERSONNEL DETECT DOOR INTRUSION
****
DOOR PENETRATION DETECTION
PERSONNEL DETECT DOOR INTRUSION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
DOOR POSITION MONITOR
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
INTERIOR INTRUSION DETECTION
****
DOOR PENETRATION DETECTION
PERSONNEL DETECT DOOR INTRUSION
SECURITY INSPECTOR DETECTION
INTERIOR INTRUSION DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
No Components

Authorized Delay Traversal Equations :

Input Entry Components
****
No Components

Authorized Delay Traversal Equations :

Output Entry Components
****
DOOR
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Input Exit Components
****
DOOR
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Output Exit Components
****
No Components

Authorized Detection Traversal Equations :

Input Entry Components
****
IDENTITY CHECK
EXPLOSIVES DETECTION ON PERSON
METAL DETECTION ON PERSON
****
IDENTITY CHECK
PACKAGE SEARCH
****

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
SNM DETECTION ON PERSON
****
SNM DETECTION IN PACKAGE
****

***** Protection Element #11 Specifications *****
FENCE : FEN
Exterior Element

Delay Component List :
A) FENCE
B) VEHICLE BARRIER
C) SECURITY PATROL DELAY

Detection Component List :
A) FENCE DETECTION
B) GROUND DETECTION
C) SECURITY PATROL DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
No Components

Unauthorized Delay Traversal Equations :

Output Entry Components
****
FENCE
VEHICLE BARRIER
SECURITY PATROL DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
FENCE
VEHICLE BARRIER
SECURITY PATROL DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
No Components

Unauthorized Detection Traversal Equations :

Input Entry Components
****
SECURITY PATROL DETECTION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
FENCE DETECTION
GROUND DETECTION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
FENCE DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
SECURITY PATROL DETECTION
GROUND DETECTION
****

Authorized Delay Traversal Equations :

Input Entry Components
****
No Components

Authorized Delay Traversal Equations :

Output Entry Components
****
No Components

Authorized Delay Traversal Equations :

Input Exit Components
****
No Components

Authorized Delay Traversal Equations :

Output Exit Components
****
No Components

Authorized Detection Traversal Equations :

Input Entry Components
****
No Components

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
No Components

***** Protection Element #12 Specifications *****
GATE : GAT
Authorized Passage is Possible
Exterior Element

Delay Component List :
A) GATE
B) VEHICLE BARRIER
C) SECURITY INSPECTOR DELAY

Detection Component List :
A) GATE DETECTION
B) GROUND DETECTION
C) IDENTITY CHECK
D) METAL DETECTION ON PERSON
E) EXPLOSIVES DETECTION ON PERSON
F) SNM DETECTION ON PERSON
G) PACKAGE SEARCH
H) SNM DETECTION IN PACKAGE
I) VEHICLE AND CARGO SEARCH
J) SNM DETECTION IN VEHICLE AND CARGO
K) SECURITY INSPECTOR DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
No Components

Unauthorized Delay Traversal Equations :

Output Entry Components
****
GATE
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
GATE
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
No Components

Unauthorized Detection Traversal Equations :

Input Entry Components
****
SECURITY INSPECTOR DETECTION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
GATE DETECTION
GROUND DETECTION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
GATE DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
SECURITY INSPECTOR DETECTION
GROUND DETECTION
****

Authorized Delay Traversal Equations :

Input Entry Components
****
No Components

Authorized Delay Traversal Equations :

Output Entry Components
****
GATE
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Input Exit Components
****
GATE
VEHICLE BARRIER
SECURITY INSPECTOR DELAY
****

Authorized Delay Traversal Equations :

Output Exit Components
****
No Components

Authorized Detection Traversal Equations :

Input Entry Components
****
IDENTITY CHECK
EXPLOSIVES DETECTION ON PERSON
METAL DETECTION ON PERSON
****
IDENTITY CHECK
PACKAGE SEARCH
****
IDENTITY CHECK
VEHICLE AND CARGO SEARCH
****

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
SNM DETECTION ON PERSON
****
SNM DETECTION IN PACKAGE
****
SNM DETECTION IN VEHICLE AND CARGO
****

***** Protection Element #13 Specifications *****
HELICOPTER FLIGHT PATH : HEL
Exterior Element
This is the Helicopter Element

Delay Component List :
A) HELICOPTER UNLOAD DELAY
B) HELICOPTER LOAD DELAY

Detection Component List :
A) HELICOPTER DETECTOR
B) PATROL DETECT HELICOPTER
C) PERSONNEL DETECT HELICOPTER

Unauthorized Delay Traversal Equations :

Input Entry Components
****
No Components

Unauthorized Delay Traversal Equations :

Output Entry Components
****
HELICOPTER UNLOAD DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
HELICOPTER LOAD DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
No Components

Unauthorized Detection Traversal Equations :

Input Entry Components
****
HELICOPTER DETECTOR
PATROL DETECT HELICOPTER
PERSONNEL DETECT HELICOPTER
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
No Components

Unauthorized Detection Traversal Equations :

Input Exit Components
****
No Components

Unauthorized Detection Traversal Equations :

Output Exit Components
****
HELICOPTER DETECTOR
PATROL DETECT HELICOPTER
PERSONNEL DETECT HELICOPTER
****

Authorized Delay Traversal Equations :

Input Entry Components
****
No Components

Authorized Delay Traversal Equations :

Output Entry Components
****
No Components

Authorized Delay Traversal Equations :

Input Exit Components
****
No Components

Authorized Delay Traversal Equations :

Output Exit Components
****
No Components

Authorized Detection Traversal Equations :

Input Entry Components
****
No Components

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
No Components

***** Protection Element #14 Specifications *****
GENERIC PROTECTION ELEMENT : GEN
Interior Element

Delay Component List :
A) INPUT GENERIC DELAY
B) OUTPUT GENERIC DELAY

Detection Component List :
A) INPUT GENERIC DETECTION
B) OUTPUT GENERIC DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
GENERIC DELAY
****

Unauthorized Delay Traversal Equations :

Output Entry Components
****
GENERIC DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
GENERIC DELAY
****

Unauthorized Delay Traversal Equations :

Output Exit Components
****
GENERIC DELAY
****

Unauthorized Detection Traversal Equations :

Input Entry Components
****
GENERIC DETECTION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
GENERIC DETECTION
****

Unauthorized Detection Traversal Equations :

Input Exit Components
****
GENERIC DETECTION
****

Unauthorized Detection Traversal Equations :

Output Exit Components
****
GENERIC DETECTION
****

Authorized Delay Traversal Equations :

Input Entry Components
****
No Components

Authorized Delay Traversal Equations :

Output Entry Components
****
No Components

Authorized Delay Traversal Equations :

Input Exit Components
****
No Components

Authorized Delay Traversal Equations :

Output Exit Components
****
No Components

Authorized Detection Traversal Equations :

Input Entry Components
****
No Components

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
No Components

***** Protection Element #19 Specifications *****
TARGET TASK : TSK
Interior Element

Delay Component List :
A) TARGET TASK DELAY
B) SECURITY INSPECTOR DELAY

Detection Component List :
A) TARGET TASK DETECTION
B) TWO-PERSON RULE DETECTION
C) INTERIOR INTRUSION DETECTION
D) SECURITY INSPECTOR DETECTION

Unauthorized Delay Traversal Equations :

Input Entry Components
****
No Components

Unauthorized Delay Traversal Equations :

Output Entry Components
****
TARGET TASK DELAY
SECURITY INSPECTOR DELAY
****

Unauthorized Delay Traversal Equations :

Input Exit Components
****
No Components

Unauthorized Delay Traversal Equations :

Output Exit Components
****
No Components

Unauthorized Detection Traversal Equations :

Input Entry Components
****
INTERIOR INTRUSION DETECTION
SECURITY INSPECTOR DETECTION
TARGET TASK DETECTION
TWO-PERSON RULE DETECTION
****

Unauthorized Detection Traversal Equations :

Output Entry Components
****
No Components

Unauthorized Detection Traversal Equations :

Input Exit Components
****
No Components

Unauthorized Detection Traversal Equations :

Output Exit Components
****
No Components

Authorized Delay Traversal Equations :

Input Entry Components
****
No Components

Authorized Delay Traversal Equations :

Output Entry Components
****
No Components

Authorized Delay Traversal Equations :

Input Exit Components
****
No Components

Authorized Delay Traversal Equations :

Output Exit Components
****
No Components

Authorized Detection Traversal Equations :

Input Entry Components
****
No Components

Authorized Detection Traversal Equations :

Output Entry Components
****
No Components

Authorized Detection Traversal Equations :

Input Exit Components
****
No Components

Authorized Detection Traversal Equations :

Output Exit Components
****
No Components

***** Delay Component #0 Specifications *****
GENERIC DELAY
Panic Bar Capable
a) No Delay

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

***** Delay Component #1 Specifications *****
DOOR
Panic Bar Capable
a) Door Not Locked

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

b) Key/Combination Available

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

c) Hollow Core Metal

12.000	12.000	12.000	12.000	48.000	12.000	INFINITY	12.000

d) Vehicle Rollup - 16 Gauge Metal

42.000	42.000	42.000	42.000	42.000	60.000	INFINITY	42.000

e) Turnstile - Floor to Ceiling

80.000	80.000	80.000	80.000	80.000	190.000	INFINITY	80.000

f) 1/2" Steel Plate

84.000	84.000	84.000	84.000	84.000	192.000	INFINITY	84.000

g) 1" Steel Plate

120.000	120.000	120.000	120.000	120.000	275.000	INFINITY	120.000

h) Vault - Class V or VI

300.000	300.000	300.000	300.000	INFINITY	INFINITY	INFINITY	300.000

i) Special Door

600.000	600.000	600.000	600.000	INFINITY	INFINITY	INFINITY	600.000

***** Delay Component #2 Specifications *****
SURFACE
a) Open Port
0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
b) Unbarred Window
5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000
c) Vent, Port, Duct: Standard Louvers
30.000 30.000 30.000 30.000 30.000 30.000 INFINITY 30.000
d) Vent, Port, Duct: Heavy Grid
60.000 60.000 60.000 60.000 60.000 130.000 INFINITY 60.000
e) Vent, Port, Duct: Diffusers
120.000 120.000 120.000 120.000 120.000 240.000 INFINITY 120.000
f) 4" Framed w/ Sheetrock
10.000 10.000 10.000 10.000 10.000 10.000 INFINITY 10.000
g) 4" Concrete
30.000 30.000 30.000 30.000 30.000 30.000 INFINITY 30.000
h) 16 Gauge Metal
48.000 48.000 48.000 48.000 48.000 60.000 INFINITY 48.000
i) 4" Concrete w/ Rebar
84.000 84.000 84.000 84.000 INFINITY 240.000 INFINITY 84.000
j) 8" Concrete w/ Rebar
120.000 120.000 120.000 120.000 INFINITY INFINITY INFINITY 120.000
k) 2' Earth
120.000 120.000 120.000 120.000 INFINITY INFINITY INFINITY 120.000

***** Delay Component #3 Specifications *****
GATE
a) Gate Not Locked
0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
b) Key/Combination Available
0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
c) Gate Locked
10.000 10.000 10.000 10.000 10.000 10.000 10.000 10.000

***** Delay Component #4 Specifications *****
VEHICLE BARRIER
Panic Bar Capable
a) No Vehicle Barrier
0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
b) Aircraft Cable
0.000 20.000 0.000 0.000 0.000 0.000 0.000 0.000
c) Concrete Median or Ditch
0.000 125.000 0.000 0.000 0.000 0.000 0.000 0.000

***** Delay Component #5 Specifications *****
SECURITY INSPECTOR DELAY
a) No Inspector

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

b) Unprotected Inspector

5.000	5.000	5.000	5.000	INFINITY	5.000	INFINITY	5.000

c) Protected Inspector

30.000	30.000	30.000	30.000	INFINITY	30.000	INFINITY	30.000

d) Inspector in Hardened Position

120.000	120.000	120.000	120.000	INFINITY	120.000	INFINITY	120.000

***** Delay Component #6 Specifications *****
RAIL BARRIER
Panic Bar Capable
a) No Rail Barrier

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

b) Concrete Median or Ditch

0.000	125.000	0.000	0.000	0.000	0.000	0.000	0.000

c) Railcar Barrier

0.000	125.000	0.000	0.000	0.000	0.000	0.000	0.000

***** Delay Component #7 Specifications *****
HELICOPTER UNLOAD DELAY
a) No Delay

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

***** Delay Component #8 Specifications *****
FENCE
a) No Fence

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

b) 8' Chain Link Fence w/ Outriggers

10.000	10.000	10.000	10.000	10.000	10.000	10.000	10.000

***** Delay Component #9 Specifications *****
BUILDING ROOF BARRIER
a) No Building Spans Isolation Zone

INFINITY	INFINITY	INFINITY	INFINITY	INFINITY	INFINITY	INFINITY	INFINITY

b) No Building Roof Barrier

0.000	INFINITY	INFINITY	0.000	0.000	0.000	INFINITY	0.000

c) 8' Chain Link Fence w/ Outriggers

10.000	INFINITY	INFINITY	10.000	10.000	10.000	INFINITY	10.000

***** Delay Component #10 Specifications *****
SURFACE DELAY STAGE 1

a) Open Port

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

b) Unbarred Window

5.000	5.000	5.000	5.000	5.000	5.000	5.000	5.000

c) Vent, Port, Duct: Standard Louvers

30.000	30.000	30.000	30.000	30.000	30.000	INFINITY	30.000

d) Vent, Port, Duct: Heavy Grid

60.000	60.000	60.000	60.000	60.000	130.000	INFINITY	60.000

e) Vent, Port, Duct: Diffusers

120.000	120.000	120.000	120.000	120.000	240.000	INFINITY	120.000

f) 4" Framed w/ Sheetrock

10.000	10.000	10.000	10.000	10.000	10.000	INFINITY	10.000

g) 4" Concrete

30.000	30.000	30.000	30.000	30.000	30.000	INFINITY	30.000

h) 16 Gauge Metal

48.000	48.000	48.000	48.000	48.000	60.000	INFINITY	48.000

i) 4" Concrete w/ Rebar

84.000	84.000	84.000	84.000	INFINITY	240.000	INFINITY	84.000

j) 8" Concrete w/ Rebar

120.000	120.000	120.000	120.000	INFINITY	INFINITY	INFINITY	120.000

k) 12" Concrete w/ Rebar

120.000	120.000	120.000	120.000	INFINITY	INFINITY	INFINITY	120.000

l) 18" Concrete w/ Rebar

120.000	120.000	120.000	120.000	INFINITY	INFINITY	INFINITY	120.000

m) 24" Concrete w/ Rebar

120.000	120.000	120.000	120.000	INFINITY	INFINITY	INFINITY	120.000

n) 36" Concrete w/ Rebar

156.000	156.000	156.000	156.000	INFINITY	INFINITY	INFINITY	156.000

o) 2' Earth

120.000	120.000	120.000	120.000	INFINITY	INFINITY	INFINITY	120.000

p) 3' Earth

120.000	120.000	120.000	120.000	INFINITY	INFINITY	INFINITY	120.000

q) 4' Earth

120.000	120.000	120.000	120.000	INFINITY	INFINITY	INFINITY	120.000

r) 6' Earth

120.000	120.000	120.000	120.000	INFINITY	INFINITY	INFINITY	120.000

s) 10' Earth

156.000	156.000	156.000	156.000	INFINITY	INFINITY	INFINITY	156.000

***** Delay Component #11 Specifications *****
SURFACE DELAY STAGE 2

a) Open Port

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

b) Unbarred Window

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

c) Vent, Port, Duct: Standard Louvers

0.000	0.000	0.000	0.000	0.000	0.000	INFINITY	0.000

d) Vent, Port, Duct: Heavy Grid

0.000	0.000	0.000	0.000	0.000	0.000	INFINITY	0.000

e) Vent, Port, Duct: Diffusers

0.000	0.000	0.000	0.000	0.000	0.000	INFINITY	0.000

f) 4" Framed w/ Sheetrock

0.000	0.000	0.000	0.000	0.000	0.000	INFINITY	0.000

g) 4" Concrete

0.000	0.000	0.000	0.000	0.000	0.000	INFINITY	0.000

h) 16 Gauge Metal

0.000	0.000	0.000	0.000	0.000	0.000	INFINITY	0.000

i) 4" Concrete w/ Rebar

0.000	0.000	0.000	0.000	INFINITY	0.000	INFINITY	0.000

j) 8" Concrete w/ Rebar

0.000	0.000	0.000	0.000	INFINITY	INFINITY	INFINITY	0.000

k) 12" Concrete w/ Rebar

54.000	54.000	54.000	54.000	INFINITY	INFINITY	INFINITY	54.000

l) 18" Concrete w/ Rebar

180.000	180.000	180.000	180.000	INFINITY	INFINITY	INFINITY	180.000

m) 24" Concrete w/ Rebar

384.000	384.000	384.000	384.000	INFINITY	INFINITY	INFINITY	384.000

n) 36" Concrete w/ Rebar

756.000	756.000	756.000	756.000	INFINITY	INFINITY	INFINITY	756.000

o) 2' Earth

0.000	0.000	0.000	0.000	INFINITY	INFINITY	INFINITY	0.000

p) 3' Earth

54.000	54.000	54.000	54.000	INFINITY	INFINITY	INFINITY	54.000

q) 4' Earth

180.000	180.000	180.000	180.000	INFINITY	INFINITY	INFINITY	180.000

r) 6' Earth

384.000	384.000	384.000	384.000	INFINITY	INFINITY	INFINITY	384.000

s) 10' Earth

756.000	756.000	756.000	756.000	INFINITY	INFINITY	INFINITY	756.000

***** Delay Component #12 Specifications *****
TUNNEL BARRIER
a) Open Tunnel

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

b) Standard Louvers

30.000	30.000	30.000	30.000	30.000	30.000	INFINITY	30.000

c) Heavy Grid

60.000	60.000	60.000	60.000	60.000	130.000	INFINITY	60.000

d) Diffusers

120.000	120.000	120.000	120.000	120.000	240.000	INFINITY	120.000

e) Fence

10.000	10.000	10.000	10.000	10.000	10.000	INFINITY	10.000

f) 4" Concrete

30.000	30.000	30.000	30.000	30.000	30.000	INFINITY	30.000

g) 16 Gauge Metal

48.000	48.000	48.000	48.000	48.000	60.000	INFINITY	48.000

h) 4" Concrete w/ Rebar

84.000	84.000	84.000	84.000	INFINITY	INFINITY	INFINITY	84.000

i) 8" Concrete w/ Rebar

120.000	120.000	120.000	120.000	INFINITY	INFINITY	INFINITY	120.000

j) 2' Earth

120.000	120.000	120.000	120.000	INFINITY	INFINITY	INFINITY	120.000

***** Delay Component #13 Specifications *****
TARGET TASK DELAY
a) No Delay

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

***** Delay Component #14 Specifications *****
SECURITY PATROL DELAY
a) No Patrol

0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

b) Unprotected Patrol

12.000	12.000	12.000	12.000	INFINITY	12.000	INFINITY	12.000

c) Protected Patrol

30.000	30.000	30.000	30.000	INFINITY	30.000	INFINITY	30.000

d) Inspectors in Tower

30.000	30.000	30.000	30.000	INFINITY	30.000	INFINITY	30.000

e) Inspectors in Hardened Position

125.000	125.000	125.000	125.000	INFINITY	125.000	INFINITY	125.000

***** Delay Component #15 Specifications *****
HELICOPTER LOAD DELAY
a) No Delay
0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000

***** Detection Component #0 Specifications *****
GENERIC DETECTION
a) Zero Detection Probability
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000

***** Detection Component #1 Specifications *****
DOOR POSITION MONITOR
a) No Monitor
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Monitor Turned Off
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Balanced Magnetic Switch
0.010 0.010 0.010 0.010 0.010 0.010 0.010 0.010

***** Detection Component #2 Specifications *****
DOOR PENETRATION DETECTION
a) No Sensor
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Sensor Turned Off
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Grid Mesh
0.010 0.010 0.010 0.010 0.010 0.010 0.010 0.010

***** Detection Component #3 Specifications *****
INTERIOR INTRUSION DETECTION
a) No Sensors
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Sensors Turned Off
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Single Motion Sensor
0.500 0.500 0.500 0.500 0.500 0.500 0.500 0.500
d) Complementary Motion Sensors
0.100 0.100 0.100 0.100 0.100 0.100 0.100 0.100

***** Detection Component #4 Specifications *****
PERSONNEL DETECT DOOR INTRUSION
a) Zero Probability

1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000

b) Fair Probability

0.500	0.500	0.500	0.500	0.500	0.500	0.500	0.500

c) Good Probability

0.100	0.100	0.100	0.100	0.100	0.100	0.100	0.100

d) Excellent Probability

0.010	0.010	0.010	0.010	0.010	0.010	0.010	0.010

***** Detection Component #5 Specifications *****
SECURITY INSPECTOR DETECTION
a) No Inspector

1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000

b) Inspector w/o Duress Alarm

1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000

c) Inspector w/ Duress Alarm

0.500	0.500	0.500	0.500	0.500	0.500	0.500	0.500

d) Protected Inspector w/ Alarm

0.010	0.010	0.010	0.010	0.010	0.010	0.010	0.010

***** Detection Component #6 Specifications *****
SURFACE PENETRATION DETECTION
a) No Sensor

1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000

b) Sensor Turned Off

1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000

c) Capacitance Sensor

0.010	0.010	0.010	0.010	0.010	0.010	0.010	0.010

d) Vibration Sensor

0.010	0.010	0.010	0.010	0.010	0.010	0.010	0.010

e) Grid Mesh

0.010	0.010	0.010	0.010	0.010	0.010	0.010	0.010

***** Detection Component #7 Specifications *****
PERSONNEL DETECT SURFACE INTRUSION
a) Zero Probability
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Fair Probability
0.500 0.500 0.500 0.500 0.500 0.500 0.500 0.500
c) Good Probability
0.100 0.100 0.100 0.100 0.100 0.100 0.100 0.100
d) Excellent Probability
0.010 0.010 0.010 0.010 0.010 0.010 0.010 0.010

***** Detection Component #8 Specifications *****
IDENTITY CHECK
a) Personnel Not Allowed Through
0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
b) No ID Check
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Picture Badge - Take Home
0.900 0.900 0.900 1.000 1.000 1.000 1.000 1.000
d) Picture Badge - Exchange
0.500 0.500 0.500 1.000 1.000 1.000 1.000 1.000
e) Hand Geometry Check
0.050 0.050 0.050 1.000 1.000 1.000 1.000 0.050
f) Eye Retina Scan
0.010 0.010 0.010 1.000 1.000 1.000 1.000 0.010

***** Detection Component #9 Specifications *****
EXPLOSIVES DETECTION ON PERSON
a) No Explosives Check
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Vapor Collection
0.900 0.900 0.900 0.900 0.900 1.000 1.000 0.900
c) Trained Dog
0.900 0.900 0.900 0.900 0.900 1.000 1.000 0.900
d) Rigorous Patdown Search
0.100 0.100 0.100 0.100 0.100 1.000 1.000 0.100

***** Detection Component #10 Specifications *****
METAL DETECTION ON PERSON
a) No Metal Detector
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Good Detector
0.100 0.100 0.100 0.100 1.000 0.100 1.000 0.100
c) Excellent Detector
0.010 0.010 0.010 0.010 1.000 0.010 1.000 0.010

***** Detection Component #11 Specifications *****
PACKAGE SEARCH
a) Packages Not Allowed Through
0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
b) Packages Allowed - No Search
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Visual Check
0.900 0.900 0.900 0.900 0.900 1.000 1.000 0.900
d) Vapor Collection
0.900 0.900 0.900 0.900 0.900 1.000 1.000 0.900
e) Trained Dog
0.900 0.900 0.900 0.900 0.900 1.000 1.000 0.900
f) X-RAY - Metal Only
0.100 0.100 0.100 0.100 1.000 0.100 1.000 0.100
g) Excellent Metal Detector
0.010 0.010 0.010 0.010 1.000 0.010 1.000 0.010
h) Rigorous Package Search
0.010 0.010 0.010 0.010 0.010 0.010 1.000 0.010

***** Detection Component #12 Specifications *****
SNM DETECTION ON PERSON
SNM Detector
a) No SNM Detector
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) SNM Detector w/o Metal Detector
0.900 0.900 0.900 0.900 0.900 0.900 0.900 0.900
c) Fair SNM Detector
0.500 0.500 0.500 0.500 0.500 0.500 0.500 0.500
d) Good SNM Detector
0.100 0.100 0.100 0.100 0.100 0.100 0.100 0.100
e) Excellent SNM Detector
0.010 0.010 0.010 0.010 0.010 0.010 0.010 0.010

***** Detection Component #13 Specifications *****
SNM DETECTION IN PACKAGE
SNM Detector
a) No SNM Detector

1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000

b) SNM Detector w/o Metal Detector

0.900	0.900	0.900	0.900	0.900	0.900	0.900	0.900

c) Fair SNM Detector

0.500	0.500	0.500	0.500	0.500	0.500	0.500	0.500

d) Good SNM Detector

0.100	0.100	0.100	0.100	0.100	0.100	0.100	0.100

e) Excellent SNM Detector

0.010	0.010	0.010	0.010	0.010	0.010	0.010	0.010

***** Detection Component #14 Specifications *****
SNM DETECTION IN VEHICLE AND CARGO
SNM Detector
a) No SNM Detector

1.000	1.000	1.000	0.000	0.000	0.000	0.000	0.000

b) SNM Detector w/o Metal Detector

0.900	0.900	0.900	0.000	0.000	0.000	0.000	0.000

c) Fair SNM Detector

0.500	0.500	0.500	0.000	0.000	0.000	0.000	0.000

d) Good SNM Detector

0.100	0.100	0.100	0.000	0.000	0.000	0.000	0.000

e) Excellent SNM Detector

0.010	0.010	0.010	0.000	0.000	0.000	0.000	0.000

***** Detection Component #15 Specifications *****
HELICOPTER DETECTOR
a) No Detector

0.000	0.000	1.000	0.000	0.000	0.000	0.000	0.000

b) Fair Detector

0.000	0.000	0.500	0.000	0.000	0.000	0.000	0.000

c) Good Detector

0.000	0.000	0.100	0.000	0.000	0.000	0.000	0.000

d) Excellent Detector

0.000	0.000	0.010	0.000	0.000	0.000	0.000	0.000

***** Detection Component #16 Specifications *****
PATROL DETECT HELICOPTER
a) Zero Probability
0.000 0.000 1.000 0.000 0.000 0.000 0.000 0.000
b) Fair Probability
0.000 0.000 0.500 0.000 0.000 0.000 0.000 0.000
c) Good Probability
0.000 0.000 0.100 0.000 0.000 0.000 0.000 0.000
d) Excellent Probability
0.000 0.000 0.010 0.000 0.000 0.000 0.000 0.000

***** Detection Component #17 Specifications *****
PERSONNEL DETECT HELICOPTER
a) Zero Probability
0.000 0.000 1.000 0.000 0.000 0.000 0.000 0.000
b) Fair Probability
0.000 0.000 0.500 0.000 0.000 0.000 0.000 0.000
c) Good Probability
0.000 0.000 0.100 0.000 0.000 0.000 0.000 0.000
d) Excellent Probability
0.000 0.000 0.010 0.000 0.000 0.000 0.000 0.000

***** Detection Component #18 Specifications *****
FENCE DETECTION
a) No Sensors
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Sensors Turned Off
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Fence Intrusion Sensors
0.900 0.100 0.900 0.900 0.900 0.900 0.900 0.900

***** Detection Component #19 Specifications *****
DETECTION BETWEEN GATES
a) No Sensors
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Sensors Turned Off
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Single Sensor - Not on Fence
0.500 0.100 0.500 0.500 0.500 0.500 0.500 0.500
d) Multiple Sensors
0.200 0.010 0.200 0.200 0.200 0.200 0.200 0.200
e) Complementary Sensors
0.010 0.001 0.010 0.010 0.010 0.010 0.010 0.010

***** Detection Component #20 Specifications *****
VEHICLE AND CARGO SEARCH
a) Vehicles Not Allowed Through
0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
b) No Contraband Check
0.000 1.000 0.000 0.000 0.000 0.000 0.000 0.000
c) Visual Check
0.000 0.900 0.000 0.000 0.000 0.000 0.000 0.000
d) Vapor Collection
0.000 0.900 0.000 0.000 0.000 0.000 0.000 0.000
e) Trained Dog
0.000 0.900 0.000 0.000 0.000 0.000 0.000 0.000
f) Rigorous Vehicle Inspection
0.000 0.100 0.000 0.000 0.000 0.000 0.000 0.000
g) Rigorous Cargo Search
0.000 0.010 0.000 0.000 0.000 0.000 0.000 0.000

***** Detection Component #21 Specifications *****
GROUND DETECTION
a) No Sensors
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Sensors Turned Off
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Single Sensor - Not on Fence
0.500 0.010 0.500 0.500 0.500 0.500 0.500 0.500
d) Multiple Sensors
0.200 0.010 0.200 0.200 0.200 0.200 0.200 0.200
e) Complementary Sensors
0.010 0.001 0.010 0.010 0.010 0.010 0.010 0.010

***** Detection Component #22 Specifications *****
SECURITY PATROL DETECTION
a) No Patrol
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Patrol w/o Duress Alarm
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Patrol w/ Duress Alarm
0.900 0.900 0.900 0.900 0.900 0.900 0.900 0.900
d) Inspector in Tower w/ Duress Alarm
0.900 0.900 0.900 0.900 0.900 0.900 0.900 0.900

***** Detection Component #23 Specifications *****
NOT CURRENTLY USED
a) No Choices
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000

***** Detection Component #24 Specifications *****
BUILDING ROOF DETECTION
a) No Building Spans Isolation Zone -
0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
b) No Sensors
1.000 0.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Sensors Turned Off
1.000 0.000 1.000 1.000 1.000 1.000 1.000 1.000
d) Single Sensor - Not on Fence
0.500 0.000 0.500 0.500 0.500 0.500 0.500 0.500
e) Multiple Sensors
0.200 0.000 0.200 0.200 0.200 0.200 0.200 0.200
f) Complementary Sensors
0.010 0.000 0.010 0.010 0.010 0.010 0.010 0.010

***** Detection Component #25 Specifications *****
TARGET TASK DETECTION
a) No Detector
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Detector Turned Off
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Fair Integrity Monitor
0.500 0.500 0.500 0.500 0.500 0.500 0.500 0.500
d) Fair Presence Monitor
0.500 0.500 0.500 0.500 0.500 0.500 0.500 0.500
e) Good Integrity Monitor
0.100 0.100 0.100 0.100 0.100 0.100 0.100 0.100
f) Good Presence Monitor
0.100 0.100 0.100 0.100 0.100 0.100 0.100 0.100
g) Excellent Integrity Monitor
0.010 0.010 0.010 0.010 0.010 0.010 0.010 0.010
h) Excellent Presence Monitor
0.010 0.010 0.010 0.010 0.010 0.010 0.010 0.010

***** Detection Component #26 Specifications *****
TWO-PERSON RULE DETECTION
a) No Two-Person Rule
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Casual Observation
1.000 1.000 1.000 1.000 0.900 1.000 0.900 1.000
c) Dedicated Observation w/ Alarm
0.500 0.500 0.500 0.500 0.500 0.500 0.500 0.500
d) Protected Dedicated Obsv. w/ Alarm
0.050 0.050 0.050 0.050 0.050 0.050 0.050 0.050

***** Detection Component #27 Specifications *****
NOT USED

***** Detection Component #28 Specifications *****
PERSONNEL DETECT GATE INTRUSION
a) Zero Probability
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Fair Probability
0.500 0.500 0.500 0.500 0.500 0.500 0.500 0.500
c) Good Probability
0.100 0.100 0.100 0.100 0.100 0.100 0.100 0.100
d) Excellent Probability
0.010 0.010 0.010 0.010 0.010 0.010 0.010 0.010

***** Detection Component #29 Specifications *****
ROOF FENCE DETECTION
a) No Building Spans Isolation Zone
0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
b) No Sensors
1.000 0.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Sensors Turned Off
1.000 0.000 1.000 1.000 1.000 1.000 1.000 1.000
d) Fence Intrusion Sensors
0.900 0.000 0.900 0.900 0.900 0.900 0.900 0.900

***** Detection Component #30 Specifications *****
GATE DETECTION
a) No Sensor
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
b) Sensor Turned Off
1.000 1.000 1.000 1.000 1.000 1.000 1.000 1.000
c) Gate Intrusion Sensor
0.900 0.100 0.900 0.900 0.900 0.900 0.900 0.900

SECTION H

SAVI Data File Structure

SAVI Version 2.2 Data File Structure

This document specifies the format of the Physical Protection System (PPS) data files which are used by the SAVI software, version 2.2. These files are both created and read by SAVI and carry the MS-DOS filename extension '.ASD'. Data files with this extension are referred to as 'ASD files'. The data in ASD files are stored in a serial binary format, with the interpretation of all information based upon the specific data type of each field; for example a string of single byte ASCII characters or a two byte integer. Each data file is divided into two logical parts; the PPS definition which contains all data specific to a facility security system, followed by the vulnerability analysis results. If analysis results were not available at save time, this part does not exist. The presence of the analysis results at the end of the file is indicated by a flag field within the PPS definition part. The data fields are listed below in the order in which they are stored in an ASD file. Information concerning interpretation of the content as well as specification of the size of each field in bytes is included. The numeric data types Float and Integer refer to the interpretation as defined by Microsoft C Version 4.0. The String type is an array of single byte ASCII characters with a terminating null byte at the end of the string. The null byte is included in the byte count.

Attached to this document are listings of the catalogs which define the SAVI Protection Elements, Delay Components and Detection Components.

Field Count	Field Name	Byte Count	Type	Interpretation
1	Version Number	- 4	Float	File Format Version # (ex: 2.2)
1	ASD Label	- 49	String	User specified label (ex: "Generic ASD")
5	Area Transit Distance	- 2	Integer	Distance across each area in whole meters. Range from 0 to 9999.
5	Area Type	- 2	Integer	Indicates whether vehicle traversal is possible or not for the associated area. Vehicle traversal is possible for Exterior areas only which is indicated by an integer value of 1. Interior areas are indicated by a 0 in this field.
5	Area Label	- 28	2 Strings	The first 14 bytes contain a string representing the first line of text within the area label. The second 14 bytes contain the second line of text. (ex: "Limited" followed by "Area")

Protection Element Structures

Fifty-six (56) Protection Element (PE) Structures follow. These structures represent the data specific to each PE within the ASD. The PE structures are stored left to right across each layer beginning with the top layer which leads from Offsite. There are five (5) protection layers with eleven (11) PEs on each layer. The 56th PE corresponds to the Target Task PE which permanently leads between the last area and the target.

Field Count	Field Name	Byte Count	Type	Interpretation
1	Present Flag	- 2	Integer	This field indicates whether or not this PE will be included in vulnerability analysis. Note that SAVI always maintains space for all 56 PEs with associated data. This field is set TRUE (integer value of 1) if the associated PE is present and is set FALSE (0) if non-present.
1	PE Type	- 2	Integer	Number of the PE type from the PE catalog. (ex: 1 = Personnel Portal)
4	Unused Field	- 4	N/A	Skip over these bytes when reading file.

Component Choice Structures

Twenty (20) component choice structures occur at this point within each PE structure. The order corresponds to the order of the delay and detection components as specified in the PE catalog. For example, the second delay component within a Vehicle Portal (PE Type 3) is the 'Input Vehicle Barrier'. If there are less than 20 delay or detection components for a particular PE type, the extra data within the file should be ignored.

Field Count	Field Name	Byte Count	Type	Interpretation
1	Delay Component Choice	- 2	Integer	This field indicates the choice for a particular delay component. If the user has made no choice then this field is set to Clear (integer value of -1). If the user has chosen to directly set a delay value then this field is set to Direct (-2). Any other positive value corresponds to the component choice within the delay component catalog. Note that the first choice in a list is choice 0. (ex: choice 2 for a 'Vehicle Barrier' component is 'Concrete Median or Ditch')

1	Delay Direct Setting	-	4	Float	Direct setting of delay in whole seconds. Range from 0 to 5999. This value is only used when the corresponding choice is set to Direct (-2).
1	Panic Bar Setting	-	2	Integer	Indicates for those components which are panic bar capable, whether this instance allows free passage on exit. This field is set TRUE (1) if free passage is possible on exit and set FALSE (0) otherwise. Components which are panic bar capable are indicated as such in the delay component catalog.
1	Detection Component Choice	-	2	Integer	This field indicates the choice for a particular detection component. If the user has made no choice then this field is set to Clear (integer value of -1). If the user has chosen to directly set a detection value then this field is set to Direct (-2). Any other positive value corresponds to the component choice within the detection component catalog. Note that the first choice in a list is choice 0. (ex: choice 2 for a 'Door Position Monitor' component is 'Balanced Magnetic Switch')
1	Detection Direct Setting	-	4	Float	Direct setting of probability of detection. Range from 0.0 to1.0. This value is only used when the corresponding choice is set to Direct (-2).
1	Unused Field	-	2	N/A	Skip over these bytes when reading file.

End Component Choice Structures

Field Count	Field Name	Byte Count		Type	Interpretation
1	Input Area #	-	2	Integer	Number of area which corresponding PE leads from. Range from 0 to 5. Offsite area is number 0.
1	Output Area #	-	2	Integer	Number of area which corresponding PE leads to. Range from 1 to 6.
1	Transit Distance	-	2	Integer	Distance across PE in whole meters. Range from 0 to 9999.

End Protection Element Structures

Field Count	Field Name	Byte Count	Type	Interpretation
5	Layer Bypass	- 2	Integer	Indicates whether the corresponding protection layer contains any present PEs. TRUE (1) if no PEs are present on a layer and FALSE (0) otherwise.
1	Analysis Results Follow	- 2	Integer	Set TRUE if analysis results are present at the end of this file. FALSE (0) if analysis results were not appended.
10	Response Force Time	- 2	Integer	Response Force Time (RFT) in whole seconds. Range from 0 to 5999.
1# of Specified RFTs		- 2	Integer	Number of RFTs which are real within above list. Range from 0 to 10. The specified RFTs are at the beginning of the list. Note that the RFTs increase from the smallest to the largest in equal steps.
1	Unused Field	- 4	N/A	Skip over these bytes when reading file.
1	Threat Attributes Set #	- 2	Integer	Number of selected set of Threat Attributes. Range from 0 to 2. (ex: 0 corresponds to 'Outsiders with Metal /Explosives on Foot')
1	Threat Objective	- 2	Integer	Threat Objective setting. A setting of 0 corresponds to Entry Only Analysis, and 1 corresponds to Entry/Exit.
1	Threat Tactics	- 2	Integer	Threat Tactics setting. 0 indicates Force Only. 1 indicates Mixed Force/Deceit tactics.

Analysis Results begin here if previous 'Analysis Results Follow' field is set TRUE. Note that twelve (12) bytes of workspace data appear at the beginning of the results data. These bytes should be skipped when reading the file.

Field Count	Field Name	Byte Count	Type	Interpretation
6	Work Space Field	- 2	Integer	Skip over these bytes when reading file.

The calculated most vulnerable paths through the ASD follow. This information is stored unsorted within ten (10) path structures for each RFT in the range specified above. Therefore, there are '# of Specified RFTs'*10 path structures written here. The path ordering information is stored in index structures which follow the path structures. It should be noted that although ten path structures are stored for each specified RFT, some paths may be garbage data if there are less than ten paths through the ASD for a given RFT. The number of path structures which contain valid path data is determined from the '# of Valid Paths' field which also follows.

Begin Most Vulnerable Path Structures

Field Count	Field Name	Byte Count	Type	Interpretation
1	Probability of Non-Detection	- 4	Float	Probability of Non-Detection of intruders of specified Threat type up to and including the critical detection point on path.
1	Time Remaining after CDP	- 2	Integer	Time remaining on path from CDP to goal.
1	CDP Node	- 2	Integer	Index of node in node list which CDP falls on. Note that if this node is an area then the CDP falls on the preceding PE on the path.
1	# of Nodes on Path	- 2	Integer	Number of nodes which exist on path.
25	Node Numbers	- 2	Integer	The encoded node numbers of all nodes which appear on the path in order of traversal from offsite to goal. Note that only the first '# of Nodes on Path' values contain valid node numbers. The Node Numbering System is explained at the end of this document.
25	Work Space Field	- 2	Integer	Skip over these bytes when reading file.

End Most Vulnerable Path Structures

Ten (10) path sort index structures follow. Only the first '# of Specified RFTs' structures contain real data.

Begin Path Sort Index Structures

Field Count	Field Name	Byte Count	Type	Interpretation
10	Path Index	- 2	Integer	Index of Path in Path structure list sorted by relative vulnerability. The most vulnerable path is first. The primary criteria for the vulnerability sort is by Probability of Interruption (P(I)) which is the inverse of the non-detection probability found in the path structures. The path with the smallest P(I) is considered most vulnerable. The Time Remaining on a path is used as a secondary sort criteria for ordering paths with equal P(I). Note that the number of paths in the most vulnerable list for a given RFT may be less than ten (10). If the '# of Valid Paths' field which follows contains a value less than 10, then this is the number of paths which are sorted by this index structure. If the indicated number of valid paths is greater than or equal to ten (10) then all 10 paths in the path structure list for the corresponding RFT are valid.

End Path Sort Index Structures

Field Count	Field Name	Byte Count	Type	Interpretation
10	# of Valid Paths	- 4	Float	Number of paths in the path structure list which are valid for the corresponding RFT. Note that only the first '# of Specified RFTs' values are real.

Ten (10) frequency distribution structures follow. This data includes the percentage distribution of path vulnerabilities in bins of 0.05 probability points. There are ten (10) distribution structures, although only the first '# of Specified RFTs' structures contain real data.

Begin Frequency Distribution Structures

Field Count	Field Name	Byte Count	Type	Interpretation
20	Frequency Bin	4	Float	Percentage of all paths which have a Probability of Interruption (P(I)) within the corresponding frequency bin. Note that the first bin contains the percentage of paths which have a P(I) between 0 and 0.05. The second bin contains the percentage of paths which have a P(I) between 0.05 and 0.10 and so on.

End Frequency Distribution Structures

Two analysis specific, SAVI work space bytes appear at the end of the file. These should be ignored.

Field Count	Field Name	Byte Count	Type	Interpretation
1	Work Space Field	- 2	Integer	Ignore these bytes at the end of the file.

Node Numbering System

Both Areas and PEs along a path are assigned a node number which is used to reference the traversal of a path. The numbering system guarantees a unique number for each Area and PE within an ASD. Areas are numbered from 0 beginning at offsite and increase in steps of 60; therefore, offsite is number 0, the next area is 60 followed by 120, 180 etc. PEs begin numbering at one (1) greater than the preceding area number and increase by one (1), left to right across the protection layer. PEs which may also be traversed by deceit (ie: marked 'Authorized Passage is Possible' within the PE catalog) are 'cloned' to model both force and deceit traversal of these elements. The deceit clone node numbers are calculated by adding 25 to the base PE node number. For example: the node representing force traversal of the first PE on the second layer of the ASD is always numbered 61; if this PE may also be traversed using deceit tactics, then the node representing deceit traversal of this PE is 61+25 = 86. Attention must be paid to this numbering system to accurately indicate the elements and areas which appear on a vulnerable path, as well as the intrusion tactics which apply.

SAVI Protection Element Catalog

***** Protection Element #1 Specifications *****
PERSONNEL PORTAL : PER
Authorized Passage is Possible
Interior Element

Delay Component List :
A) INPUT DOOR
B) INPUT SURFACE
C) SECURITY INSPECTOR DELAY
D) OUTPUT DOOR
E) OUTPUT SURFACE

Detection Component List :
A) INPUT DOOR POSITION MONITOR
B) INPUT DOOR PENETRATION DETECTION
C) INPUT SURFACE PENETRATION DETECTION
D) IDENTITY CHECK
E) METAL DETECTION ON PERSON
F) EXPLOSIVES DETECTION ON PERSON
G) SNM DETECTION ON PERSON
H) PACKAGE SEARCH
I) SNM DETECTION IN PACKAGE
J) INTERIOR INTRUSION DETECTION
K) SECURITY INSPECTOR DETECTION
L) PERSONNEL DETECT DOOR INTRUSION
M) PERSONNEL DETECT SURFACE INTRUSION
N) OUTPUT DOOR POSITION MONITOR
O) OUTPUT DOOR PENETRATION DETECTION
P) OUTPUT SURFACE PENETRATION DETECTION

***** Protection Element #2 Specifications *****
MATERIAL PORTAL : MAT
Authorized Passage is Possible
Interior Element

Delay Component List :
A) INPUT DOOR
B) INPUT SURFACE
C) SECURITY INSPECTOR DELAY
D) OUTPUT DOOR
E) OUTPUT SURFACE

Detection Component List :
A) INPUT DOOR POSITION MONITOR
B) INPUT DOOR PENETRATION DETECTION
C) INPUT SURFACE PENETRATION DETECTION
D) IDENTITY CHECK
E) METAL DETECTION ON PERSON
F) EXPLOSIVES DETECTION ON PERSON
G) SNM DETECTION ON PERSON
H) PACKAGE SEARCH
I) SNM DETECTION IN PACKAGE
J) INTERIOR INTRUSION DETECTION
K) SECURITY INSPECTOR DETECTION
L) PERSONNEL DETECT DOOR INTRUSION
M) PERSONNEL DETECT SURFACE INTRUSION
N) OUTPUT DOOR POSITION MONITOR
O) OUTPUT DOOR PENETRATION DETECTION
P) OUTPUT SURFACE PENETRATION DETECTION

***** Protection Element #3 Specifications *****
VEHICLE PORTAL : VEH
Authorized Passage is Possible
Exterior Element

Delay Component List :
A) INPUT GATE
B) INPUT VEHICLE BARRIER
C) SECURITY INSPECTOR DELAY
D) OUTPUT GATE
E) OUTPUT VEHICLE BARRIER

Detection Component List :
A) INPUT GATE DETECTION
B) DETECTION BETWEEN GATES
C) IDENTITY CHECK
D) METAL DETECTION ON PERSON
E) EXPLOSIVES DETECTION ON PERSON
F) SNM DETECTION ON PERSON
G) PACKAGE SEARCH
H) SNM DETECTION IN PACKAGE
I) VEHICLE AND CARGO SEARCH
J) SNM DETECTION IN VEHICLE AND CARGO
K) SECURITY INSPECTOR DETECTION
L) PERSONNEL DETECT GATE INTRUSION
M) OUTPUT GATE DETECTION

***** Protection Element #4 Specifications *****
RAIL PORTAL : RAL
Authorized Passage is Possible
Exterior Element

Delay Component List :
A) INPUT GATE
B) INPUT RAIL BARRIER
C) SECURITY INSPECTOR DELAY
D) OUTPUT GATE
E) OUTPUT RAIL BARRIER

Detection Component List :
A) INPUT GATE DETECTION
B) DETECTION BETWEEN GATES
C) IDENTITY CHECK
D) METAL DETECTION ON PERSON
E) EXPLOSIVES DETECTION ON PERSON
F) SNM DETECTION ON PERSON
G) PACKAGE SEARCH
H) SNM DETECTION IN PACKAGE
I) VEHICLE AND CARGO SEARCH
J) SNM DETECTION IN VEHICLE AND CARGO
K) SECURITY INSPECTOR DETECTION
L) PERSONNEL DETECT GATE INTRUSION
M) OUTPUT GATE DETECTION

***** Protection Element #5 Specifications *****
SHIPPING AREA : SHP
Authorized Passage is Possible
Interior Element

Delay Component List :
A) INPUT DOOR
B) INPUT VEHICLE BARRIER
C) INPUT SURFACE
D) SECURITY INSPECTOR DELAY
E) OUTPUT DOOR
F) OUTPUT VEHICLE BARRIER
G) OUTPUT SURFACE

Detection Component List :
A) INPUT DOOR POSITION MONITOR
B) INPUT DOOR PENETRATION DETECTION
C) INPUT SURFACE PENETRATION DETECTION
D) IDENTITY CHECK
E) METAL DETECTION ON PERSON
F) EXPLOSIVES DETECTION ON PERSON
G) SNM DETECTION ON PERSON
H) PACKAGE SEARCH
I) SNM DETECTION IN PACKAGE
J) VEHICLE AND CARGO SEARCH
K) SNM DETECTION IN VEHICLE AND CARGO
L) INTERIOR INTRUSION DETECTION
M) SECURITY INSPECTOR DETECTION
N) PERSONNEL DETECT DOOR INTRUSION
O) PERSONNEL DETECT SURFACE INTRUSION
P) OUTPUT DOOR POSITION MONITOR
Q) OUTPUT DOOR PENETRATION DETECTION
R) OUTPUT SURFACE PENETRATION DETECTION

***** Protection Element #6 Specifications *****
ISOLATION ZONE : ISO
Exterior Element

Delay Component List :
A) INPUT FENCE
B) INPUT VEHICLE BARRIER
C) INPUT BUILDING ROOF BARRIER
D) SECURITY PATROL DELAY
E) OUTPUT FENCE
F) OUTPUT VEHICLE BARRIER
G) OUTPUT BUILDING ROOF BARRIER

Detection Component List :
A) INPUT FENCE DETECTION
B) OUTPUT FENCE DETECTION
C) GROUND DETECTION
D) SECURITY PATROL DETECTION
E) INPUT ROOF FENCE DETECTION
F) OUTPUT ROOF FENCE DETECTION
G) BUILDING ROOF DETECTION

***** Protection Element #7 Specifications *****
EVACUATION SHELTER : EVC
Interior Element

Delay Component List :
A) INPUT DOOR
B) INPUT SURFACE
C) OUTPUT DOOR
D) OUTPUT SURFACE

Detection Component List :
A) INPUT DOOR POSITION MONITOR
B) INPUT DOOR PENETRATION DETECTION
C) INPUT SURFACE PENETRATION DETECTION
D) PERSONNEL DETECT DOOR INTRUSION
E) PERSONNEL DETECT SURFACE INTRUSION
F) INTERIOR INTRUSION DETECTION
G) OUTPUT DOOR POSITION MONITOR
H) OUTPUT DOOR PENETRATION DETECTION
I) OUTPUT SURFACE PENETRATION DETECTION

***** Protection Element #8 Specifications *****
TUNNEL : TUN
Interior Element

Delay Component List :
A) INPUT TUNNEL BARRIER
B) OUTPUT TUNNEL BARRIER

Detection Component List :
A) INPUT SURFACE PENETRATION DETECTION
B) INPUT PERSONNEL DETECT SURFACE INTRUSION
C) INTERIOR INTRUSION DETECTION
D) OUTPUT SURFACE PENETRATION DETECTION
E) OUTPUT PERSONNEL DETECT SURFACE INTRUSION

***** Protection Element #9 Specifications *****
SURFACE : SUR
Interior Element

Delay Component List :
A) SURFACE DELAY STAGE 1
B) SECURITY INSPECTOR DELAY
C) SURFACE DELAY STAGE 2

Detection Component List :
A) SURFACE PENETRATION DETECTION
B) PERSONNEL DETECT SURFACE INTRUSION
C) INTERIOR INTRUSION DETECTION
D) SECURITY INSPECTOR DETECTION

***** Protection Element #10 Specifications *****
DOOR : DOR
Authorized Passage is Possible
Interior Element

Delay Component List :
A) DOOR
B) SECURITY INSPECTOR DELAY

Detection Component List :
A) DOOR POSITION MONITOR
B) DOOR PENETRATION DETECTION
C) SECURITY INSPECTOR DETECTION
D) INTERIOR INTRUSION DETECTION
E) PERSONNEL DETECT DOOR INTRUSION
F) IDENTITY CHECK
G) METAL DETECTION ON PERSON
H) EXPLOSIVES DETECTION ON PERSON
I) SNM DETECTION ON PERSON
J) PACKAGE SEARCH
K) SNM DETECTION IN PACKAGE

***** Protection Element #11 Specifications *****
FENCE : FEN
Exterior Element

Delay Component List :
A) FENCE
B) VEHICLE BARRIER
C) SECURITY PATROL DELAY

Detection Component List :
A) FENCE DETECTION
B) GROUND DETECTION
C) SECURITY PATROL DETECTION

***** Protection Element #12 Specifications *****
GATE : GAT
Authorized Passage is Possible
Exterior Element

Delay Component List :
A) GATE
B) VEHICLE BARRIER
C) SECURITY INSPECTOR DELAY

Detection Component List :
A) GATE DETECTION
B) GROUND DETECTION
C) IDENTITY CHECK
D) METAL DETECTION ON PERSON
E) EXPLOSIVES DETECTION ON PERSON
F) SNM DETECTION ON PERSON
G) PACKAGE SEARCH
H) SNM DETECTION IN PACKAGE
I) VEHICLE AND CARGO SEARCH
J) SNM DETECTION IN VEHICLE AND CARGO
K) SECURITY INSPECTOR DETECTION

***** Protection Element #13 Specifications *****
HELICOPTER FLIGHT PATH : HEL
Exterior Element
This is the Helicopter Element

Delay Component List :
A) HELICOPTER UNLOAD DELAY
B) HELICOPTER LOAD DELAY

Detection Component List :
A) HELICOPTER DETECTOR
B) PATROL DETECT HELICOPTER
C) PERSONNEL DETECT HELICOPTER

***** Protection Element #14 Specifications *****
GENERIC PROTECTION ELEMENT : GEN
Interior Element

Delay Component List :
A) INPUT GENERIC DELAY
B) OUTPUT GENERIC DELAY

Detection Component List :
A) INPUT GENERIC DETECTION
B) OUTPUT GENERIC DETECTION

***** Protection Element #19 Specifications *****
TARGET TASK : TSK
Interior Element

Delay Component List :
A) TARGET TASK DELAY
B) SECURITY INSPECTOR DELAY

Detection Component List :
A) TARGET TASK DETECTION -
B) TWO-PERSON RULE DETECTION
C) INTERIOR INTRUSION DETECTION
D) SECURITY INSPECTOR DETECTION

SAVI Delay Component Catalog

***** Delay Component #0 Specifications *****
GENERIC DELAY
Panic Bar Capable
a) No Delay

***** Delay Component #1 Specifications *****
DOOR
Panic Bar Capable
a) Door Not Locked
b) Key/Combination Available
c) Hollow Core Metal
d) Vehicle Rollup - 16 Gauge Metal
e) Turnstile - Floor to Ceiling
f) 1/2" Steel Plate
g) 1" Steel Plate
h) Vault - Class V or VI
i) Special Door

***** Delay Component #2 Specifications *****
SURFACE
a) Open Port
b) Unbarred Window
c) Vent, Port, Duct: Standard Louvers
d) Vent, Port, Duct: Heavy Grid
e) Vent, Port, Duct: Diffusers
f) 4" Framed w/ Sheetrock
g) 4" Concrete
h) 16 Gauge Metal
i) 4" Concrete w/ Rebar
j) 8" Concrete w/ Rebar
k) 2' Earth

***** Delay Component #3 Specifications *****
GATE
a) Gate Not Locked
b) Key/Combination Available
c) Gate Locked

***** Delay Component #4 Specifications *****
VEHICLE BARRIER
Panic Bar Capable
a) No Vehicle Barrier
b) Aircraft Cable
c) Concrete Median or Ditch

***** Delay Component #5 Specifications *****
SECURITY INSPECTOR DELAY
a) No Inspector
b) Unprotected Inspector
c) Protected Inspector
d) Inspector in Hardened Position

***** Delay Component #6 Specifications *****
RAIL BARRIER
Panic Bar Capable
a) No Rail Barrier
b) Concrete Median or Ditch
c) Railcar Barrier

***** Delay Component #7 Specifications *****
HELICOPTER UNLOAD DELAY
a) No Delay

***** Delay Component #8 Specifications *****
FENCE
a) No Fence
b) 8' Chain Link Fence w/ Outriggers

***** Delay Component #9 Specifications *****
BUILDING ROOF BARRIER
a) No Building Spans Isolation Zone
b) No Building Roof Barrier
c) 8' Chain Link Fence w/ Outriggers

***** Delay Component #10 Specifications *****
SURFACE DELAY STAGE 1
a) Open Port
b) Unbarred Window
c) Vent, Port, Duct: Standard Louvers
d) Vent, Port, Duct: Heavy Grid
e) Vent, Port, Duct: Diffusers
f) 4" Framed w/ Sheetrock
g) 4" Concrete
h) 16 Gauge Metal
i) 4" Concrete w/ Rebar
j) 8" Concrete w/ Rebar
k) 12" Concrete w/ Rebar
l) 18" Concrete w/ Rebar
m) 24" Concrete w/ Rebar
n) 36" Concrete w/ Rebar
o) 2' Earth
p) 3' Earth
q) 4' Earth
r) 6' Earth
s) 10' Earth

***** Delay Component #11 Specifications *****
SURFACE DELAY STAGE 2
a) Open Port
b) Unbarred Window
c) Vent, Port, Duct: Standard Louvers
d) Vent, Port, Duct: Heavy Grid
e) Vent, Port, Duct: Diffusers
f) 4" Framed w/ Sheetrock
g) 4" Concrete
h) 16 Gauge Metal
i) 4" Concrete w/ Rebar
j) 8" Concrete w/ Rebar
k) 12" Concrete w/ Rebar
l) 18" Concrete w/ Rebar
m) 24" Concrete w/ Rebar
n) 36" Concrete w/ Rebar
o) 2' Earth
p) 3' Earth
q) 4' Earth
r) 6' Earth
s) 10' Earth

***** Delay Component #12 Specifications *****
TUNNEL BARRIER
a) Open Tunnel
b) Standard Louvers
c) Heavy Grid
d) Diffusers
e) Fence
f) 4" Concrete
g) 16 Gauge Metal
h) 4" Concrete w/ Rebar
i) 8" Concrete w/ Rebar
j) 2' Earth

***** Delay Component #13 Specifications *****
TARGET TASK DELAY
a) No Delay

***** Delay Component #14 Specifications *****
SECURITY PATROL DELAY
a) No Patrol
b) Unprotected Patrol
c) Protected Patrol
d) Inspectors in Tower
e) Inspectors in Hardened Position

***** Delay Component #15 Specifications *****
HELICOPTER LOAD DELAY
a) No Delay

SAVI Detection Component Catalog

***** Detection Component #0 Specifications *****
GENERIC DETECTION
a) Zero Detection Probability

***** Detection Component #1 Specifications *****
DOOR POSITION MONITOR
a) No Monitor
b) Monitor Turned Off
c) Balanced Magnetic Switch

***** Detection Component #2 Specifications *****
DOOR PENETRATION DETECTION
a) No Sensor
b) Sensor Turned Off
c) Grid Mesh

***** Detection Component #3 Specifications *****
INTERIOR INTRUSION DETECTION
a) No Sensors
b) Sensors Turned Off
c) Single Motion Sensor
d) Complementary Motion Sensors

***** Detection Component #4 Specifications *****
PERSONNEL DETECT DOOR INTRUSION
a) Zero Probability
b) Fair Probability
c) Good Probability
d) Excellent Probability

***** Detection Component #5 Specifications *****
SECURITY INSPECTOR DETECTION
a) No Inspector
b) Inspector w/o Duress Alarm
c) Inspector w/ Duress Alarm
d) Protected Inspector w/ Alarm

***** Detection Component #6 Specifications *****
SURFACE PENETRATION DETECTION
a) No Sensor
b) Sensor Turned Off
c) Capacitance Sensor
d) Vibration Sensor
e) Grid Mesh

***** Detection Component #7 Specifications *****
PERSONNEL DETECT SURFACE INTRUSION
a) Zero Probability
b) Fair Probability
c) Good Probability
d) Excellent Probability

***** Detection Component #8 Specifications *****
IDENTITY CHECK
a) Personnel Not Allowed Through
b) No ID Check
c) Picture Badge - Take Home
d) Picture Badge - Exchange
e) Hand Geometry Check
f) Eye Retina Scan

***** Detection Component #9 Specifications *****
EXPLOSIVES DETECTION ON PERSON
a) No Explosives Check
b) Vapor Collection
c) Trained Dog
d) Rigorous Patdown Search

***** Detection Component #10 Specifications *****
METAL DETECTION ON PERSON
a) No Metal Detector
b) Good Detector
c) Excellent Detector

***** Detection Component #11 Specifications *****
PACKAGE SEARCH
a) Packages Not Allowed Through
b) Packages Allowed - No Search
c) Visual Check
d) Vapor Collection
e) Trained Dog
f) X-RAY - Metal Only
g) Excellent Metal Detector
h) Rigorous Package Search

***** Detection Component #12 Specifications *****
SNM DETECTION ON PERSON
SNM Detector
a) No SNM Detector
b) SNM Detector w/o Metal Detector
c) Fair SNM Detector
d) Good SNM Detector
e) Excellent SNM Detector

***** Detection Component #13 Specifications *****
SNM DETECTION IN PACKAGE
SNM Detector
a) No SNM Detector
b) SNM Detector w/o Metal Detector
c) Fair SNM Detector
d) Good SNM Detector
e) Excellent SNM Detector

***** Detection Component #14 Specifications *****
SNM DETECTION IN VEHICLE AND CARGO
SNM Detector
a) No SNM Detector
b) SNM Detector w/o Metal Detector
c) Fair SNM Detector
d) Good SNM Detector
e) Excellent SNM Detector

***** Detection Component #15 Specifications *****
HELICOPTER DETECTOR
a) No Detector
b) Fair Detector
c) Good Detector
d) Excellent Detector

***** Detection Component #16 Specifications *****
PATROL DETECT HELICOPTER
a) Zero Probability
b) Fair Probability
c) Good Probability
d) Excellent Probability

***** Detection Component #17 Specifications *****
PERSONNEL DETECT HELICOPTER
a) Zero Probability
b) Fair Probability
c) Good Probability
d) Excellent Probability

***** Detection Component #18 Specifications *****
FENCE DETECTION
a) No Sensors
b) Sensors Turned Off
c) Fence Intrusion Sensors

***** Detection Component #19 Specifications *****
DETECTION BETWEEN GATES
a) No Sensors
b) Sensors Turned Off
c) Single Sensor - Not on Fence
d) Multiple Sensors
e) Complementary Sensors

***** Detection Component #20 Specifications *****
VEHICLE AND CARGO SEARCH
a) Vehicles Not Allowed Through
b) No Contraband Check
c) Visual Check
d) Vapor Collection
e) Trained Dog
f) Rigorous Vehicle Inspection
g) Rigorous Cargo Search

***** Detection Component #21 Specifications *****
GROUND DETECTION
a) No Sensors
b) Sensors Turned Off
c) Single Sensor - Not on Fence
d) Multiple Sensors
e) Complementary Sensors

***** Detection Component #22 Specifications *****
SECURITY PATROL DETECTION
a) No Patrol
b) Patrol w/o Duress Alarm
c) Patrol w/ Duress Alarm
d) Inspector in Tower w/ Duress Alarm

***** Detection Component #23 Specifications *****
NOT USED

***** Detection Component #24 Specifications *****
BUILDING ROOF DETECTION
a) No Building Spans Isolation Zone
b) No Sensors
c) Sensors Turned Off
d) Single Sensor - Not on Fence
e) Multiple Sensors
f) Complementary Sensors

***** Detection Component #25 Specifications *****
TARGET TASK DETECTION
a) No Detector
b) Detector Turned Off
c) Fair Integrity Monitor
d) Fair Presence Monitor
e) Good Integrity Monitor
f) Good Presence Monitor
g) Excellent Integrity Monitor
h) Excellent Presence Monitor

***** Detection Component #26 Specifications *****
TWO-PERSON RULE DETECTION
a) No Two-Person Rule
b) Casual Observation
c) Dedicated Observation w/ Alarm
d) Protected Dedicated Obsv. w/ Alarm

***** Detection Component #27 Specifications *****
NOT USED

***** Detection Component #28 Specifications *****
PERSONNEL DETECT GATE INTRUSION
a) Zero Probability
b) Fair Probability
c) Good Probability
d) Excellent Probability

***** Detection Component #29 Specifications *****
ROOF FENCE DETECTION
a) No Building Spans Isolation Zone
b) No Sensors
c) Sensors Turned Off
d) Fence Intrusion Sensors

***** Detection Component #30 Specifications *****
GATE DETECTION
a) No Sensor
b) Sensor Turned Off
c) Gate Intrusion Sensor

DISTRIBUTION:

1 Tom Cousins
DP-341.3
U.S. Department of Energy
19900 Germantown Rd.
Germantown, MD 20874

1 Rokaya Al-Ayat
NSS/Safeguards Program Manager
Lawrence Livermore National Laboratory
7000 East Ave.
Mail Stop L-195
Livermore, CA 94550

1 Science & Engineering Associates, Inc.
Attn: Richard DeFuria
6100 Uptown Blvd., N.E.
Albuquerque, NM 87110

1	2614	A. A. Elsbernd
5	3141	S. A. Landenberger
8	3141-1	C. L. Ward
3	3151	W. I. Klein
1	5210	C. C. Hartwigsen
1	5211	E. R. Hoover
1	5211	W. K. Paulus
1	5211	M. K. Snell
1	5211	A. E. Winblad
1	5212	J. C. Matter
5	5212	S. E. Jordan
1	5240	D. S. Miyoshi
1	8524	J. A. Wackerly