# *FINAL DRAFT*

# *CORRECTIONS*
# VULNERABILITY ASSESSMENT (CVA)
# *HANDBOOK*

**Developed with funding provided by the**
**National Institute of Justice, U. S. Department of Justice, to the**
**AMERICAN CORRECTIONAL ASSOCIATION (ACA)**

**Rod Miller, Editor**
**Robert J. Verdeyen**
**J.T. O'Brien**
**Donald Romine**

***Colorado Department of Corrections:***
**Lou Archuleta**
**Mike Fowler**

**Acknowledgements:**

***Sandia National Laboratories Security Systems and Technology Center:***
**Chris E. Robertson**
**Ivan G. Waddoups**
**Michael S. Pacheco**

***Pennsylvania Department of Corrections:***
**Eugene J. Brannigan**
**John Bihun**
**Michael D. Klopotoski**

**Contributors:**
**David Sweetin, Texas**
**Tim LeMaster, New Mexico**
**Pat Keohane, Missouri**
**George Wagner, New Jersey**

**July 2006**

This document was prepared with funding provided by the National Institute of Justice, U. S. Department of Justice (Grant Number: 96-LB-VX-K004). The contents of this document do not necessarily reflect the official position of the National Institute of Justice or the U.S. Department of Justice.

| TABLE OF CONTENTS | Page |
|---|---|
| **PART I: Introduction to Correctional Vulnerability Assessment** | |
| A. What is a VA? | 1 |
| B. What is a CVA? | 1 |
| C. How is CVA Different? | 2 |
| D. Why conduct a CVA? | 3 |
| E. The CVA Process and Methodology | 4 |
| F. A Sample from Colorado | 9 |
| **PART II: Step by Step, the CVA Process** | 13 |
| A. Defining the Threat (Step 1) | 13 |
| B. Characterizing the Institution (Step 2) | 15 |
| C. Defining Inmate Capabilities (Step 3) | 16 |
| D. Characterizing Physical Protection Systems and Operations (Step 4) | 19 |
| E. Analyze PPS and Operations (Data Coll. -Step 5) | 23 |
| F. Create Path Sequence Diagrams and Scenarios (Step 6) | 33 |
| G. Assessing Risk with the EASI Model (Step 7) | 47 |
| H. Acceptability of Risk (Step 8) | 53 |
| I. Using EASI to Reduce Risk (Step 9) | 54 |
| **PART III: A Primer on Physical Protection Systems (PPS)** | 61 |
| **PART III: Planning and Implementing a CVA** | 86 |
| A: Managing the CVA Project | 86 |
| B: The CVA Timeline and Tasks | 86 |
| C. The CVA Report | 92 |
| D: After the CVA Is Complete | 94 |

**APPENDICES**

**Appendix A: Sample PSD's and EASI Results**
**Appendix B: Checklists for Characterizing the Institution (Step 1)**
**Appendix C: Threat Capability Checklists (Step 3)**
**Appendix D: Physical Protection System Checklists (Step 4)**
**Appendix E: Protocols and Practices**
**Appendix F: Data Collection Forms (entry control, delay)**
**Appendix G: Performance Data**
**Appendix H: PSD Checklist**
**Appendix I: Acronyms and Selected EASI Formulas**
**Appendix J: CVA Flowchart**
**Appendix K: A Step-by-Step Guide to Using the EASI Program**
**Appendix L: Sample CVA Report**
**Appendix M: Printouts of Powerpoint Presentations (complete CVA training program)**

**Supplementary CD-ROM:**
Files with handbook, appendices, EASI program, and powerpoint training program.

## Foreword and Acknowledgements

This handbook is the centerpiece of a comprehensive set of materials developed by the National Institute of Justice through a grant to the American Correctional Association. The *Corrections Vulnerability Assessment (CVA)* materials provide correctional facilities with the information, form, guidance and training materials needed to implement a CVA in their own facilities.

In 2001 the National Institute of Justice (NIJ) Office of Science and Technology, recognized the need to help corrections practitioners to assess and analyze vulnerabilities in the increasingly complex context of our nation's prisons and jails. NIJ examined the pioneering work of Sandia National Laboratories (SNL) for the Nuclear Regulatory Commission and other agencies concerned with the safety of nuclear materials, and concluded that this experience could be adapted for correctional settings. At the same time, the Pennsylvania Department of Corrections was working with SNL to explore similar possibilities.

NIJ selected the American Correctional Association (ACA) as the entity that was best positioned to work with SNL to develop, test, and distribute methodologies to provide the field of corrections with new vulnerability assessment and risk management tools. The NIJ, ACA and SNL collaboration began in 2001 and involved participants from eight states.

The evolution of this methodology has required the contributions of many professionals. The first challenge was to transpose the Sandia National Laboratory approach-- which was designed to keep intruders *out*-- for the corrections setting in which our primary concern is keeping people *in.* The Pennsylvania Department of Corrections (PADOC) worked with SNL to adapt this approach for their state correctional facilities. PADOC has invested heavily in the CVA process, developing its own set of policies, procedures and protocols, and a training program. Approximately 70 PADOC staff are currently trained and qualified to participate in vulnerability assessments. Just as SNL helped Pennsylvania to develop a tool for corrections, Pennsylvania shared its expertise with others during a week-long training event in Texas (2005.)

The latest agency to step up to the plate is the Colorado Department of Corrections. After participating in the initial SNL training, and assisting with the Texas training, Colorado officials anchored the final state training event that was held in Ohio, September 2005. Colorado also agreed to be used as our case study for this set of CVA materials, and you will see frequent references to their experiences and innovations.

This document is truly the product of the contributions of many devoted corrections professionals. It is offered to the field as a new tool to promote safety and security in all of our correctional facilities.

Robert J. Verdeyen, Project Director

# PART I. INTRODUCTION TO CORRECTIONS VULNERABILITY ASSESSMENT

## A. What is a Vulnerability Assessment?

Spend a few minutes on the Internet looking up "vulnerability assessment" or "vulnerability analysis" and you will find hundreds of references, many of which address computer systems and their vulnerability to outside intruders. The National Oceanographic and Atmospheric Agency has published a variety of manuals and tools to assist communities in assessing their vulnerability to natural disasters. Similarly, the Environmental Protection Agency has also developed VA tools.

The Sandia National Laboratories methodology is so widespread that you will find references to it throughout the energy, nuclear power and nuclear weapons literature. The SNL approach even appears in the context of local water districts. There is even a college textbook based on the approach.[1]

The risk management and insurance field has used the term for many years, in a variety of contexts.

Vulnerability assessment is a term that is fast becoming overused, and therefore ambiguous. In an effort to distinguish our work from others, we will introduce the term *Corrections* Vulnerability Assessment (CVA) in this handbook. We hope that this new term will become exclusively associated with the specific methodology that is presented in this handbook and its related materials.

## B. What is a *Corrections* Vulnerability Assessment?

We started with the original Sandia National Laboratory definition of vulnerability analysis[2]:

> *Vulnerability* ***analysis*** is a systematic approach used to determine the strengths and weaknesses of facility physical protection systems in place to prevent or mitigate security concerns. The scope of this effort will include characterizing the facility, defining the threat, identifying existing physical protection systems, and evaluating the effectiveness of these systems. This will aid in determining the need for equipment upgrades, or changes in policies and procedures.

In the context of corrections it did not go quite far enough. The initial SNL focus was primarily--and at times *exclusively*--on the physical aspects of security: walls, doors, windows, fences, sensors, cameras, alarms and such.

But in corrections, we know that our actual *practices* are just as important to security as the physical components. A door is not effective if someone forgets to lock it. An alarm is meaningless if someone does not assess it. In the process of adapting the SNL methodology to corrections, we found it necessary to expand the scope of our efforts to include policies,

[1] Mary Lynn Garcia. *The Design and Evaluation of Physical Protection Systems*. Butterworth-Heinemann, 2001.
[2] *Guideline for Conducting a Vulnerability Analysis*, Sandia National Laboratory. 2003.

procedures and practices. Policies and procedures tell us what we *set out* to do, while practices are what we *actually* do.

We suggest that a *corrections vulnerability assessment* (CVA) is:

- A *systematic* evaluation in which…
- Qualitative and quantitative techniques are used…
- To determine the effectiveness of operational and physical protection systems…
- Against specific undesired events or a range of potential threats

In Colorado, the threats of most concern are escapes and the introduction of contraband.

A unique analytical tool-- the Estimate of Adversarial Sequence Interruption (EASI) program-- is central to the implementation of a CVA. The EASI tool actually calculates the odds that an undesired event, such as an escape, will be successful. It also helps point to specific changes in practices, technology, and facilities that might be most effective in reducing the level of risk. The EASI program was developed by Sandia National Laboratories for application in other fields and it has been introduced to the field of corrections largely through the assistance of the National Institute of Justice.

## C. How is CVA different from other types of risk assessments or security audits?

There are many differences between the CVA and other methodologies and approaches because a CVA:

- Considers *three* dimensions of the correctional setting-- physical plant, technology *and* operations
- Provides a variety of perspectives by involving a diverse team
- Examines the correctional setting from all angles
- Connects a series of elements instead of looking at them in isolation
- Puts the elements in motion
- Tests the elements
- Examines the elements under different conditions and at different times
- Quantifies the risk
- Provides a model to test the effectiveness of risk reduction actions

At this point in many of our prior training programs, some participants shake their heads and mumble “heard that one before,” but after seeing the CVA process in action, and working with the results, everyone has become a convert.

In Colorado, officials report that staff involved with the CVA process gained a “new perspective” that they carry with them after the assessment is finished.

A CVA provides a *synthesis* of many elements that contribute to risk. A CVA:

- Connects all of the pieces that combine to achieve security
- Provides a multidimensional view of risk, not just one-dimensional checklists
- Offers a new perspective, often from an inmate's point of view
- Often involves actually testing systems, trying scenarios and measuring time frames

## D. Why Conduct a CVA?

There are many reasons to become involved with the CVA process. Each agency has its own concerns and priorities and the CVA process adapts to provide a new resource. Colorado provides a good case study. Colorado officials have found that the *advantages* of the CVA process include:

- Better decision making
- Understand and address effective threat resolution
- Efficient allocation of resources
- Proven methodology

The goals for the Colorado CVA initiative are:

- Identify and mitigate escape pathways
- Reduce inmate opportunity
- Conduct performance-based testing on existing perimeter intrusion detection system (PIDS) equipment and other physical protection system (PPS)

Colorado officials have found that the CVA process has had a positive impact on other Department of Corrections initiatives, including:

- Manpower surveys (helping to reallocate staff positions and assign priority to requests for additional positions)
- Annual operations inspections
- ACA accreditation process
- Policies and procedures (identifying the need for revisions in procedures)
- Budget priorities (using the EASI model to identify changes that will realize the most benefit for the money)
- Technology (as a supplement, not a solution in itself)

In Colorado, teams of staff and officials work on-site at a facility for a week or more. After the process is completed, the CVA participants find that local facility staff members are impressed with the outcome. For example, in one facility perimeter officers were shown that they were too quick to clear an alarm and that there was too much reliance on physical security.

In response to the effective use of the CVA in Colorado, a variety of actions were taken:

- Procedural issues were corrected
- Repairs to correct physical plant problems were started
- Some repairs involved little or no cost and others were fixed with contingency funds

Colorado officials learned that "not everything takes money" to fix. In fact, 42 out of 45 of the changes that were identified as necessary in their first CVA required no funds. For the few that did need funding, the CVA and its quantified risk outcomes provided the justification needed to secure contingency funds from the central office to make needed changes. The first Colorado facility that volunteered to be the subject of a CVA was rewarded with over $60,000 in contingency funds. The second facility received nearly $50,000. In both cases, the CVA pinpointed the most cost-effective solutions and clearly calculated the level of risk.

## E. The CVA Process and Methodology

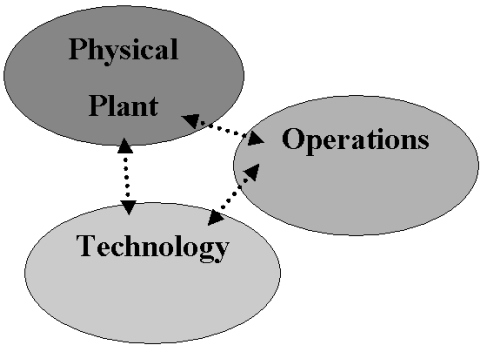
### 1. Safety and Security Principles

Achieving and maintaining safety and security in the correctional setting is a dynamic process that *continuously* demands sufficient staff who are:

- Qualified
- Properly trained
- Directed by policies and procedures
- Supervised, and
- Properly deployed (at the right place, at the right time)

It is difficult, if not impossible, for staff to achieve security without the assistance of the physical plant and technology. Conversely, it is certainly neither feasible nor cost-effective to attempt to secure our correctional facilities through staffing alone. Neither is it appropriate nor feasible to rely solely on our facilities and technology. It takes all three components to achieve and maintain security.

**Figure I.1: Components of Security**

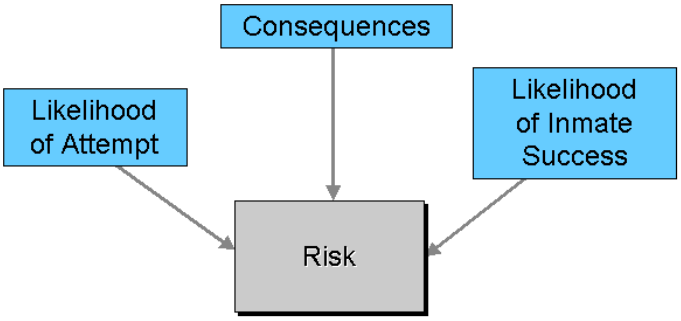


### 2. Risk Concepts

Central to the need for a corrections vulnerability assessment is the concept of risk. Correctional managers are faced with daily decisions that require them to consider how well they are protected, the severity of the consequences if staff and systems fail, and how to balance costs against the potential risk.

Risk is determined by considering how likely it is that an attempt will be made, how likely it is that the attempt would be successful, and the nature and severity of the consequences if the attempt succeeds. The amount of control that administrators and staff have over each element of risk varies.

**Figure I.2: Assessing Risk**




The CVA process described in this handbook will help determine the likelihood of an inmate's (or inmates') success. The methodology will even calculate the *probability* of success, which is an important new management tool. This provides a new, *quantifiable* measure of risk.

### 3. Defining the Threat(s)

Before risk-- or vulnerability-- may be assessed, it is necessary to identify the threat, or threats, that are of concern. The methodology that was developed by Sandia National Laboratories focused on protecting assets, such as nuclear weapons or power plants, from sabotage or theft of materials. Although repelling external assaults might be a threat for some correctional facilities, most of the correctional risks involve *containing* inmates and preventing unwanted inmate behavior.

The CVA process may be applied to just about any type of threat. This handbook uses the prevention of inmate escapes as the threat for training purposes. Colorado has focused on escapes but has also broadened its concerns to prevent the introduction of contraband.

Threats that might be of concern to correctional agencies include, but are not limited to:

- Escapes
- Terrorism
- Riot or mass disturbance
- External assaults
- Assault on staff members
- Introduction of contraband

- Prisoner on prisoner assault
- Creating diversions to aid other inmates to escape or implement an assault

### 4. The CVA Methodology

The steps in the CVA methodology are:

1. Defining the threat(s)
2. Characterizing the institution
3. Defining threat capability
4. Characterizing Physical Protection Systems (PPS) and operations
5. Analyzing PPS and operations
6. Developing Path Sequence Diagrams (PSD)
7. Using the EASI model to assess risk
8. Determining if the risk is acceptable
9. IF NOT, revising the facility design, operations, technology and assumptions

The following diagram shows the steps and provides a brief commentary on each.

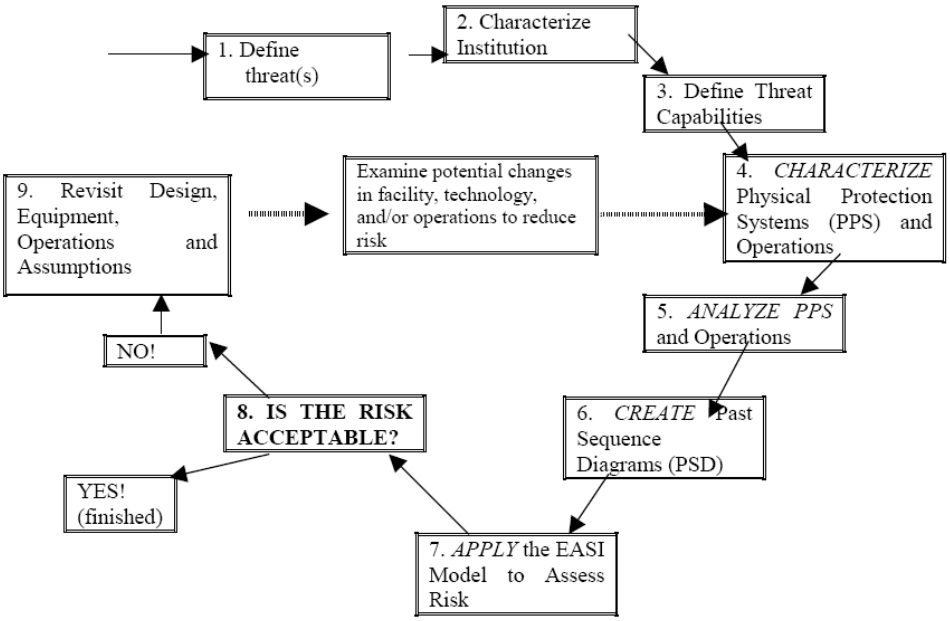
**Figure I.3: CVA Methodology**

| **CVA STEPS** | | ***Comments*** |
|---|---|---|
| 1. Define threat(s) | | Setting the stage by defining the threat |
| 2. Characterize Institution | 3. Define Threat Capability | Describing the setting and considering inmate capabilities in that context |
| 4. *CHARACTERIZE* Physical Protection Systems (PPS) and Operations | | Describing the facility and its operations |
| 5. *ANALYZE PPS* and Operations | | Collecting data and analyzing facilities and operations |
| 6. *CREATE* Past Sequence Diagrams (PSD) | | Determining how a series of steps might allow an inmate(s) to succeed |
| 7. *APPLY* the EASI Model to Assess Risk | | Using the Excel-based tool to predict the likelihood of success |
| **8. ACCEPTABILITY OF THE RISK** | | Determining <u>if</u> something has to be done to reduce the risk |

| | | |
|---|---|---|
| NOT Acceptable! ↓ 9. Revisit Design, Equipment, Operations and Assumptions | Acceptable! (finished) | Using the EASI tool to examine how changes in physical plant, technology and/or operations would affect the likelihood of success. |

It may be helpful to depict the steps of a corrections vulnerability assessment as a *quality circle*, as shown below.

**Figure I.4: The CVA Process as Quality Circle**




In more simplified terms, the process might be described as judging a race between the facility and the inmate, if we are looking at escapes. To determine who wins the race, you must:

- Understand the institution protection system (physical and operational)
- Determine what the inmate can and must do to escape
- Compare the institution protection system with the inmate's actions
- See who wins – look at the time race

The following diagram is drawn from the EASI program, which calculates and draws the timeline and determines how many times the adversary (such as an inmate) will prevail. In Section II-G we show how the EASI program is used. Appendix K provides a more detailed explanation.

In the example below, time passes after the inmate begins the escape process before the first alarm is sounded. More time passes until the alarm is assessed and response actions are

triggered. The response takes less time than the remaining tasks for the inmate, and the inmate is interrupted in his attempt. Various characteristics of the facility, its use of technology, and operations, conspire to "delay" the inmate as he follows the path of tasks that would lead to an escape.

**Figure I.5: Sample Time Line: Inmate Interrupted for Escape is Complete**

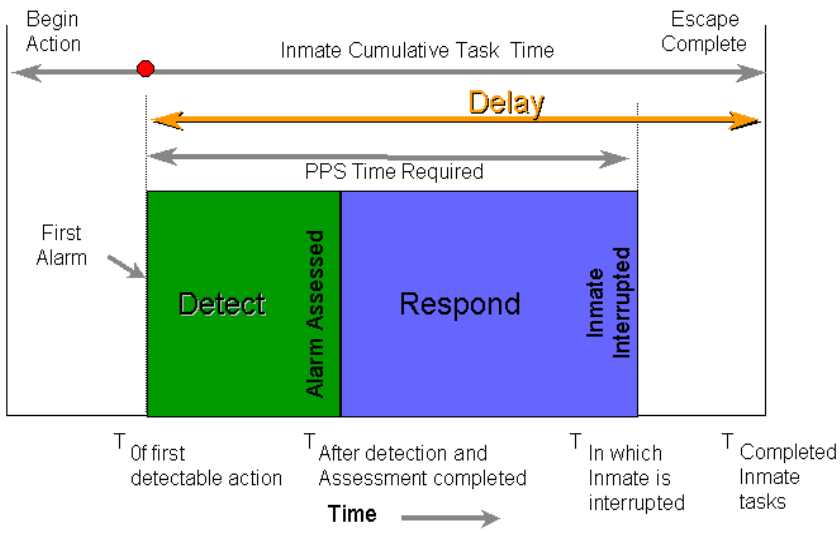
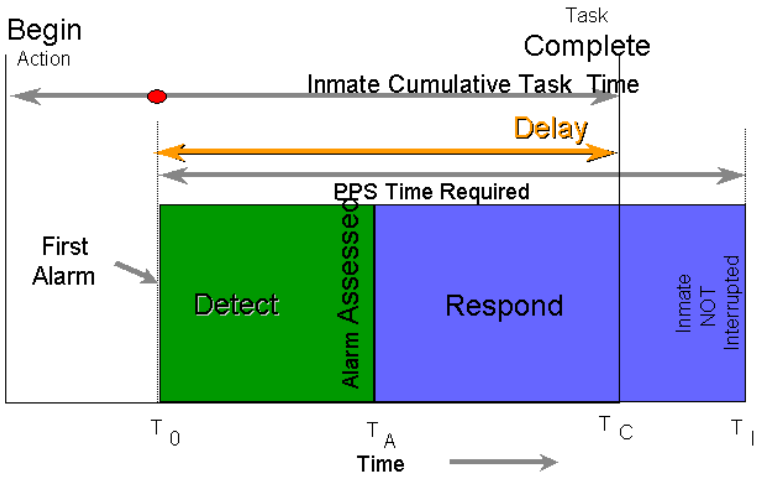



Figure I.6 shows a time line in which the response comes too late and the inmate is able to escape.

**Figure I.6: Sample Time Line: Inmate Completes Escape**



## F. A Sample from Colorado

Before we launch into the detailed process of conducting a corrections vulnerability assessment, let's take a quick look at a completed one from Colorado. Staff and officials from the Colorado Department of Corrections (CDOC) participated in the first vulnerability assessment training event in 2003, and two CDOC officials assisted with the next training event in Texas. These officials anchored the third and final prison training event, held in Lebanon, Ohio in 2005.

CDOC adapted the CVA process for their unique needs and settings by:

- Following the basic CVA handbook but modifying it as needed
- Reducing the scope of the assessment, focusing on specific problem areas of each facility, because time constraints would not allow evaluation of the entire facility
- Focusing on areas where offenders had some element of control
- Briefing each warden before, during and after the CVA
- Learning that every time they tested a system or element at a facility, there had to be an immediate and visible staff response to show the offenders (who were always watching) that they should not try this themselves

The last point is worth further comment. It is virtually impossible to hide many of the CVA activities from offenders. In Colorado, officials were careful to show inmates that staff members are attentive to detection and delay systems. For example, if the CVA team was testing a microwave installation by a fence, they would always call for a visible response from the facility-- whether or not the test triggered the response.

Colorado found that it was important to monitor the facility response to a CVA, and over time CDOC officials developed the following strategies:

- Briefing all staff at roll-calls
- Briefing the Warden daily
- Bringing only immediate threat, life safety, or emergent security concerns to the Warden's attention
- Expecting *initial* staff reactions to be "We already know what's wrong," or "We don't believe in the process," or "Is this a way to embarrass the facility?"
- Meeting with the facility management team to assure them this process was not intended as a "witch hunt"

As staff warmed up to the process and the challenge, the CVA team would often find that problems were being fixed almost immediately after they were identified. While this sometimes complicated the CVA process, it was a healthy and productive response by the facility.

Although we will explore Path Sequence Diagrams and the EASI tool in more detail later, it may be helpful to take a sneak preview here. The following "scenario" was developed by a CVA team at one of the Colorado prisons. The photo below shows the general area that is involved with this scenario.

**Figure I.7: Daytime Photo of Escape Scenario Location**

The trailer is a key to this scenario, as it provides an excellent hiding place for the inmates who are attempting to escape. The overall scenario and its assumptions are described in Figure I.8.

**Figure I.8: Summary of Escape Scenario**

Facility tested conditions: Foggy/darkness
Time of Day: Graveyard/Dayshift shift - 0545 – 0615 hrs.
Day of Week: Wednesday
Staffing Level: Full staffing
Participants in the Scenario: Two offender trash workers who have one pair of Lineman's pliers
Summary Description: The morning trash crew picks up trash from each of the living units. Two offenders from the crew are escorted by one staff member through checkpoint to the dock trash compactor. The two offenders have another offender assigned as the "can man" plant a pair of lineman's pliers somewhere near the compactor. They disable the escort officer.
Steps in the Scenario

1. The offenders run from the trash area to the white trailer parked next to the dock sally port fence.
2. One of the offenders cuts the fence, while the other acts as a look out.
3. The offender with the pliers crawls across the Microwave zone to the inner fence. The second offender stays until all fences and wire are breeched.
4. The inner fence is breeched and the first offender crosses the restricted area to the razor ribbon.
5. The first offender breeches the razor ribbon and outer fence.
6. The second offender goes through the dock sally port fence and crosses the Microwave zone.
7. The second offender breeches the inner fence and crosses the restricted area.
8. The second offender goes through the razor ribbon and outer fence.

Time to complete Tasks 1 through 8: 446 seconds (7.4 minutes) for two offenders
Probability of Inmate Success: 78% probability of successful inmate escape.

Wait a minute-- 78% probability of an escape? That's what the EASI tool determined after all of the data was entered into it. And the data was derived from *actual* experience on site, usually as the result of staff repeatedly testing each step and each assumption and timing each test. The CVA team proved that inmates had ready access to lineman pliers. They also demonstrated how well the trailer could hide an inmate, as shown in the daylight photo in Figure I.9 (the CVA team member stuck his hand out only to prove that he was actually there.)

**Figure I.9: Photo Showing How Well Trailer Could Hide an Inmate**

In this scenario, one of the keys is the fact that the offenders have some control. It is the offenders who determine when to empty the garbage container in the facility, which gives them access to the trailer. Figure I.10 shows the EASI worksheet for this scenario. We will explain each element of the worksheet in Part II of this handbook.

**Figure I.10: EASI Worksheet**

| | | | |
|---|---|---|---|
| Foggy, Wednesday, between 5:45 and 6:15 hrs. | Probability of Interruption: | | **0.22400** |
| Inmate collusion - staff hostage -lineman's pliers | | | |

| ***Adversary*** | Alarm | | Response Force Time (in Seconds) | |
|---|---|---|---|---|
| ***Sequence*** | Communi-cation | Pn | Mean | Standard Deviation |
| ***Interruption*** | 0.95 | 1 | 300 | 60 |

| | | | | Delays (in Seconds): | | |
|---|---|---|---|---|---|---|
| Task | Description | | | P(Detection) | Mean: | Standard Deviation |
| 1 | Collect Trash throughout the facility | | | 0.00 | 0 | 0 |
| 2 | Proceed to checkpoint | | | 0.00 | 30 | 15 |
| 3 | Proceed down the corridor to door number | | | 0.00 | 30 | 10 |
| 4 | Exit door number (?) to dock sidewalk | | | 0.00 | 30 | 10 |
| 5 | Proceed to trash compactor to empty trash | | | 0.00 | 60 | 15 |
| 6 | Attack staff member, hide body under compactor and retrieve set of lineman's pliers left by can man | | | 0.05 | 60 | 10 |
| 7 | Cross dock to parked trailer | | | 0.20 | 5 | 2 |
| 8 | Hide between wheels of parked trailer ensuring perimeter vehicle isn't approaching | | | 0.06 | 120 | 15 |
| 9 | First inmate crawls to internal fence and cuts fence utilizing lineman's pliers. | | | 0.07 | 36 | 15 |
| 10 | First inmate crawls through electronic detection zone | | | 0.20 | 38 | 20 |
| 11 | First inmate cuts inner fence while hiding to ensure perimeter vehicle is not approaching | | | 0.27 | 73 | 15 |

| | | | | |
|---|---|---|---|---|
| 12 | First Inmate crawls through restricted area | 0.20 | 2 | 1 |
| 13 | First inmate cuts razor wire utilizing lineman's pliers | 0.20 | 20 | 10 |
| 14 | First inmate cuts outer fence utilizing lineman's pliers | 0.20 | 36 | 10 |
| 15 | Second inmate crawls through internal fence from trailer | 0.07 | 2 | 1 |
| 16 | Second inmate crawls through electronic detection zone | 0.20 | 38 | 10 |
| 17 | Second inmate crawls through inner fence | 0.27 | 2 | 1 |
| 18 | Second inmate crawls through restricted area | 0.20 | 2 | 1 |
| 19 | Second inmate crawls through razor wire | 0.20 | 10 | 5 |
| 20 | Second inmate crawls through outer fence | 0.20 | 2 | 1 |

## PART II. STEP-BY-STEP THROUGH THE CVA PROCESS

This section of the handbook walks you through each step in the CVA process.

Through our training efforts we have found that actual hands-on experience in the facility is necessary to fully understand the CVA methodology. Therefore, we have included several exercises that allow the reader to apply the steps to his/her own facility at each key step in the process.

### A. Defining the Threat (Step 1)

Step 1 requires a careful consideration of the risks that are of concern to you and your colleagues. Although there are many potential threats to the safety, security and order of a correctional facility, it is necessary to limit the number and types of threats that are examined in each CVA.

The following list of potential threats offers a starting point:

- Escape by one or more prisoners
- Unauthorized entry into the facility or movement within the facility
- Introduction of contraband into the facility
- Prisoner assault on staff
- Prisoner assault on another prisoner
- Major disturbance or riot
- Prisoner suicide or attempt
- External attack on the facility
- Terrorism

*For the purpose of this handbook* we will be defining the threat as an escape. This should not limit your approach to this step when you are ready to conduct your own CVA.

Examining data and information may help to identify threats that are most pertinent to your current situation. Facilities that are involved with the accreditation process are familiar with the need to collect and analyze critical incident data, and more recently the expanding series of "outcome measures" that are integral to the new performance-based standards. These sources offer some additional ideas for threat identification, and may also help to assign priority to threats.

**Figure II.1: Outcome Measures[3]**

- Worker compensation claims filed for injuries
- Illnesses
- Physical injuries
- Vehicle accidents
- Emergencies

[3] *from* several Performance-Based Standards books, American Correctional Association, Lanham, Maryland. 2003.

- Times that normal facility operations were suspended due to emergencies
- Injuries requiring medical attention that result from emergencies
- Injuries resulting from fires
- Code violations cited in the past 12 months
- Incidents involving toxic or caustic materials
- Incidents of inventory discrepancies
- Incidents
- Unauthorized inmate absences from the facility
- Instances of unauthorized access to the facility
- Instances in which force was used
- Weapons found in the facility
- Controlled substances found in the facility
- Incidents involving keys
- Incidents involving tools
- Incidents involving culinary equipment
- Incidents involving medical equipment and sharps
- Incidents in which staff were found to have acted in violation of facility policy
- Staff terminated for conduct violations
- Staff substance abuse tests failed

Data and information about the events that are described in the preceding list could help to identify potential threats *and* to determine which threats are of most concern.

Another way to approach threat definition is to consider "undesirable events." In correctional facilities there are several items and/or participants that could be considered in identifying these undesirable events. They include people, important information, vital equipment, weapons, tools, and contraband, as shown in Figure II.2 below.

**Figure II.2: Items and Participants to Consider:**

***People***

1. Inmates
2. Administrative Staff
3. Correctional Officers
4. Contractors/Vendors
5. Visitors

***Important Information***

1. Inmate Records
2. Personnel Records
3. Security Related Documentation, i.e. CO shift changes, assignments
4. Intelligence Information
5. Activity Schedules

***Vital Equipment***

1. Heavy Equipment within the Facility
2. Communication Rooms
3. Security Equipment, i.e. Video cameras, sensors, and transmission mediums
4. Backup Power Source

5. Weapons/Tools

***Contraband***

1. Drugs both legal and illegal
2. Money
3. Alcohol
4. Tools
5. Weapons
6. Electronic Devices

There are obviously a large number of undesirable events that can result from the above items and/or participants. You should tailor your threat definition to your specific needs and priorities. Remember, although this handbook focuses on inmate escape, you should not limit your own threat definition.

## B. Characterizing the Institution (Step 2)

Performing a thorough Corrections Vulnerability Assessment requires a clear understanding of the context in which the CVA is being conduct. By "characterizing" the institution you are identifying building structures, high traffic areas, infrastructure, terrain, weather conditions, historical data, inmate characteristics and other features that could affect the facility's vulnerabilities.

Physical characteristics will require assembling and annotating a variety of documents and plans. The first pages of Appendix B provide a checklist for this physical inventory, including:

B1: Location
B2: Site
B3: Facility Design, Layout and Construction
B4: Video Systems
B5: Alarm and Sensor Systems
B6: Metal and Other Detectors

These checklists with help you to identify key characteristics of the institution and the overall setting. You will start by pulling back from the facility and looking at the broader setting-- it's location and the implications, such as access transportation systems. Moving closer, you will examine the site, also identifying features that have implications for safety and security. From there, the facility design and construction are examined and then attention is given to technical systems. For each of these steps, the checklists prompt you to consider:

- **Proximity and adjacency:** what features on the site pose a threat because they are *near* or *next to* each other?

- **Visibility and Observation:** blind spots, poor lines of sight, obstructions and other features that might pose a threat; environmental conditions-- rain, fog, snow--affect visibility and observation.

- **Continuity:** instances in which continuity of features or systems is interrupted.

- **Condition:** features whose condition pose a potential threat, such as sensors that have not been adequately maintained or control panel lights that do not work.

Operational characteristics are also addressed in Appendix B, Checklist B7 that includes:

1. Manpower surveys, staffing patterns, schedules
2. Historical reports (past/present/future)
3. Site detection/delay/assessment systems
4. Weapons inventory
5. Operational procedures
6. Policy requirements
7. Performance test data, (tests conducted on systems e.g. backup generator)
8. Security inspection results

While it may be tempting to skip this step, or to skimp on it, you will find that the materials you assemble here will save a lot of time later. Also, this process will help you to take a fresh look at the institution, highlighting features that you may have taken for granted but which are of importance to the vulnerability assessment process.

**Exercise 1: Examining the Context**

Pick an area within your facility that you believe is especially vulnerable to potential escapes. You might consider such areas as the kitchen, inmate industries, housing areas, service yards and entrances, or any other location in your facility that poses an obvious risk.

Complete the document entitled "Exercise One: Area Analysis Checklist" at the end of Appendix B while you are examining the area.

## C. Defining Threat Capabilities (Step 3)

In Step 1 you identified the threat (or threats) that will be the focus of your CVA. In this step, you will determine the *capabilities* that the threat participants may bring to bear. By defining the relevant capabilities you will also be able to rule out many capabilities that you do not have to be considered. For example, if you determine for your escape threat that inmates will not have explosives or tools that will enable them to penetrate reinforced concrete, this will simplify the CVA process and allow more time to be spent on real threats.

When defining the threat you should identify those characteristics that are common to a correctional facility, mindful that the goal of the facility is to maintain the safety of the public, staff and inmates. Threat analysis involves a systematic review of the type of incidents that have occurred--not only in the past--but what is happening today, and what might be expected in the future. For our example (escape) the following list provides a starting point for determining the capabilities associated with the threat:

**Institutional Escape History**

1. Identify any past incidents and describe the details of the scenario presented by the inmate(s).

2. Details should include a description of inmate tactics, weapons, escape path elements, tools used, transportation, the time of day, and weather. Was the inmate(s) acting in collusion with anyone from the outside and/or staff?

3. Escape attempts may be accomplished by using either one or all of the following methods: deceit, force, and stealth. The analyst should identify which method(s) was used in the attempt.

4. Examine historical data and information using past records and intelligence information.

This list is drawn from a larger checklist that is presented in Appendix C. Additional threats are addressed there.

The availability of contraband, especially weapons or tools, is a factor. The following list will help you to identify the nature and extent of this threat in your institution:

**Institutional Contraband History**

1. Determine the type of contraband that is being brought into the facility, such as weapons, drugs, money, electronic devices.

2. Identify the means in which the contraband is being introduced into the facility, such as visitor areas, daily deliveries, and staff.

3. Determine the means in which the contraband is being packaged.

4. Determine the ownership of the contraband and if it is associated with a specific group or activity.

5. Examine historical data and information using past records and intelligence information.

Appendix C provides this contraband checklist as well as lists that address suicide and inmate violence threats. Figure II.3 shows a sample threat capability checklist for inmate escapes. It shows the range of issues of consider when defining capabilities, such as:

- Type of inmate
- Assistance (and type)
- Weapons
- Tools
- Vehicles

- Visitors
- Staff
- Other inmates
- Violence

**Figure II.3: Sample Checklist to Define Escape Threat Capabilities**

| **Threat Capabilities Checklist for *Inmate (Escape)*** | ***Check (√) if included in this CVA*** |
|---|---|
| ***Type of Inmate*** | |
| Inmate whose classification does *not* allow him/her outside of the security perimeter. | √ |
| Low security classification inmates escaping from outside the perimeter (i.e. the administration building, warehouse, automotive shop, etc… ) | |
| Low security classification inmates escaping from outside the perimeter on community service jobs | |
| ***Assistance*** | |
| None. | |
| Assistance from one other inmate. | √ |
| Assistance from more than one other inmate. | √ |
| Passive assistance from outsider | √ |
| Active assistance from outsider (e.g. crash into the prison through the gate, disable perimeter vehicle or perimeter patrol officer, etc...) | |
| Passive assistance by staff or contractor | |
| Active assistance by staff or contractor (ignore alarms; leave gate open, erroneous inmate count, etc…) | |
| ***Tools, Weapons*** | |
| Tools allowed within the facility. | √ |
| Restricted tools illegally introduced on site (e.g. thrown over fence) | |
| Weapons legally allowed within the facility. | |
| Restricted weapons illegally introduced on site (e.g. thrown over fence) | |
| ***Vehicles*** | |
| Inmate using a vehicle to forcibly exit the perimeter. | |
| Outsider using vehicle to penetrate perimeter. | |
| ***Visitors*** | |
| Throwing of contraband over the fence into the perimeter | |
| Contraband swallowed or concealed by inmate | √ |
| ***Staff*** | |
| Collusion with multiple staff | |
| ***Inmates (assist in the introduction of contraband)*** | |
| Contraband used while outside the perimeter, or swallowed/concealed to cross the perimeter boundary | |
| ***Inmate Violence*** | |
| Violence toward staff, contractors, other inmates | √ |
| Riots | |

As you develop your threat capability description, remember that inmates have a variety of tactics that may be employed, including:

- Stealth
- Force
- Deceit (such as wearing a uniform, forging a pass)

And be sure not to discount the capabilities of the inmates:

- Knowledge
- Motivation
- Skills
- Abilities

Inmate knowledge often includes a working knowledge of institution procedures and practices. Inmate motivation might be enhanced by a letter from home or another external source, or by a threat from another inmate. Inmates often bring skills from the community such as construction or electronics experience. The Pennsylvania Department of Corrections discovered that they had an inmate who had actually installed exterior sensor systems before he was incarcerated. Some inmates have abilities that may enhance their tactics; an inmate who is a skilled scam artist will be more formidable when using deceit.

*For the purposes of this handbook* , and the supporting training materials, the threat and capabilities are defined as:

1. One or two inmates
2. Primary motive is to escape
3. Can be violent
4. Tools restricted to those available inside facility or brought in with authorization
5. Weapons limited to material found inside facility
6. Staff assistance, if any, is limited to passive actions such as providing information

## D. Characterizing Physical Protection Systems (PPS) and Operations

There are three major components of a physical protection system:

- Detection
- Delay
- Response

In the context of an attempted escape, these functions must be performed in order and within a length of time that is less than the time required for the inmate to complete his/her task (remember the “race” between the inmate and the institution).

For example, an inmate decides on a particular path element to escape from a facility. An effective PPS should detect/delay and provide sufficient response to the situation before the individual is free.

A well-designed system:

- Provides "protection in depth"
- Minimizes the consequences of component failures
- Exhibits balanced protection

Up to this point in the process, we have been characterizing the setting and its systems primarily through inventories. Now we will introduce another, complementary approach: *performance criteria and testing.* By focusing on *performance*, we:

- Determine how each element *really* performs, not what it says on the box or what the vendor told us(performance-based, not feature-based)
- Examine:
    1. Inmate capability
    2. Performance objectives
    3. Effectiveness evaluations
- Make better decisions by--
    - Understanding the system's effectiveness against specific actions
    - Effectively allocating resources

A performance approach will identify operator failures, such as situations in which the system or element is functioning properly but procedures are not followed (or are misguided) and the result of failure. The performance approach will also identify failures caused by properly conceived and executed procedures that are not integrated.

As we evaluate the institution's physical protection system the performance-based approach will require us to test, try and implement many tasks and actions. Appendix D provides a series of checklists that outline PPS elements that must be examined, organized into three sections: detection, delay and response.

Part III of this handbook provides a "Primer" on physical protection systems. Readers are encouraged to review Part III as needed to supplement their understanding of the technical aspects of security systems and components. We continue with our review of the CVA steps here.

**Response**

Response is the final component of physical protection systems (PPS). The checklists in Appendix D provide a good starting point for examining your institution's response capabilities. In the "response" checklist you will be asked to identify and describe:

- The type of communication available to officers and backup types

- Internal communication system for major events, i.e. sirens, duress alarms, public address systems, timely and accurate
- Operator's ability to assess activity, i.e. ergonomics, accessibility to equipment, space availability
- Response timeline and establish timelines in accordance with the threats
- Type of response force plans/training (physical and tactical)/performance tested/ratio of CO's to inmates
- Number and type of primary responders for a given threat and the number of secondary responders should the need arise
- Post and patrol locations and responsibilities in locating / verifying / isolating / containing / evacuating / resolving / de-activating situations
- Compensatory measures that are implemented when the False Alarm Rate (FAR) or Nuisance Alarm Rate (NAR) are excessively high
- Response force armed vs. unarmed, training and checkout procedures. Equipment appropriate for the assigned task
- CO's ability to monitor diversionary tactics, and identify policies in places that address these tactics
- Interview senior CO's and identify additional areas for consideration

You will be concerned with the time frames associated with your answers to the following questions:

- Who responds and from where?
- Are weapons carried at all times by on-duty responders?
- If the responder is also responsible for assessment, how effective is s/he at this function and how long does it take?
- Is the off-site response soon enough to help apprehend the escapees?

It will be necessary to collect data to quantify your response time to specific situations that are elements of the scenarios leading up to the EASI calculations.

**Operations**

In September 2005, project director Robert J. Verdeyen told participants in the week-long CVA training program in Ohio that "The best technology in the world is worthless without trained people doing the right thing."

This handbook has focused largely on physical and technical elements of protection systems up to this point. Now it is time to focus on the staff whose actions will ultimately determine success or failure.

Policies and procedures are a cornerstone for institutional operations. They describe, in advance, what everyone is *expected* to do in hundreds of situations. Policies and procedures provide the basis for post orders, and for the training of institutional staff. But in the final analysis, policies and procedures signal our *intentions* but are do not necessarily reflect what actually happens in the institution-- today and in the future.

Maintaining security is a continuous process. It demands the efforts of sufficient numbers of staff who are:

- Qualified,
- Properly trained,
- Directed by policies and procedures, and
- Supervised
- Properly deployed (at the right place, at the right time)

Appendix E offers resources that will help you to systematically examine you current institutional practices. The exhaustive set of protocols and practices provided in Appendix E portrays sound correctional practices, as defined by experts in the field.

Section II is the centerpiece of Appendix E, providing specific recommended practices that address each of the following topics:

**A. Operations**

- A1. Staffing
- A2. Inmate accountability
- A3. Emergency preparedness
- A4. Intelligence
- A5. Searches
- A6. Institution visiting
- A7. Transportation of inmates (escorted trips)
- A8. Security inspections
- A9. Training

**B. Equipment and technical systems**

- B1. Video systems
- B2. Alarm and sensor systems
- B3. Metal and other detectors
- B4. Physical plant security
- B5. Perimeter security
- B6. Locking systems (key/lock control)
- B7. Control center
- B8. Tool control
- B9. Utilities and mechanical systems
- B10. Toxic/caustics control

**C. Physical plant**

- C1. Location and site
- C2. Building layout and construction
- C3. Entrances and exits in the secure perimeter
- C4. Armory
- C5. Mail room
- C6. Trash collection/disposal

Following each practice, there is a description of:

- protocols (written documentation that is needed to guide the practice)
- process indicators (ways to determine if the practices are being properly implemented)

**Exercise 2: Identifying PPS Elements**

Go back to the area in the facility at which you implemented Exercise 1. Take your notes with you. Describe the following PPS elements while you examine the area in more detail.

Identify and describe all PPS elements, including detection, delay and response. Use the following list to remind you of various elements.

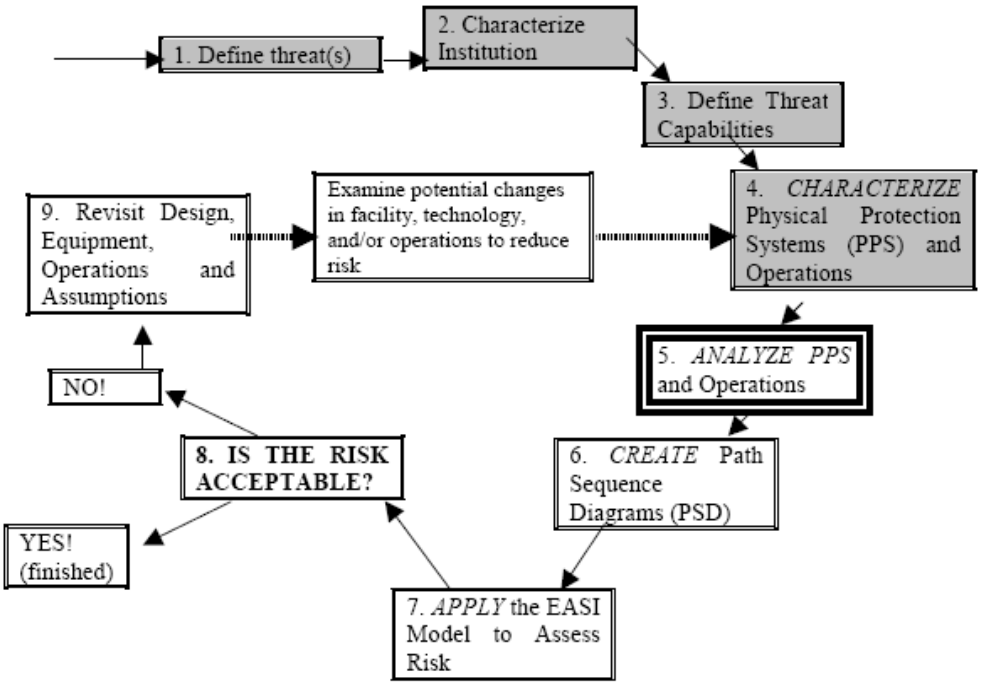
**Key Control.** Key knowledge. Do keys maintained by staff create a pathway in your area?
**Tool Control.** Are tools in the area, which if obtained by an inmate, would assist in creating a pathway?
**Inmate Accountability.** Counts. Movement. Pass System
**Contraband Control (Staff and Inmate).** Are metal or other detectors present and being used? Pat Searches. Property Searches.
**Video, Audio and Other Detection Systems**
**Inmates and Staff.** What numbers and types of inmates are present? When? What are the staffing practices and how do they vary by time of day? Do inmate have control over any aspect of the area (e.g. when to take out trash?)
**Other Observations:** such as condition of elements, operational consistency, etc.

## E. CVA Data Collection-- *Analyzing* Physical Protection Systems (PPS) (Step 5)

With this step in the CVA process we turn a corner from cataloguing and inventorying features of the facility and its operation and start to *analyze* what we have found. Part of the analysis process will require the collection of specific data that will tell us not just what is in place, but also *how it works.*

Figure II.4 shows our current position in the CVA process.

**Figure II.4: The CVA Process as a Quality Circle**




Data collection efforts will focus on three categories:

1. Institutional data
2. Inmate capability and opportunity
3. Performance data

### 1. Institutional Data

The inventory forms in Appendix B provide a format for describing and analyzing the implications of:

1. Location (B1)
2. Site (B2)
3. Facility design, layout and construction (B3)
4. Video systems (B4)
5. Alarm and sensor systems (B5)
6. Metal and other detectors (B6)

Data gathering should include:

- Description of building structures
- High traffic areas
- Infrastructure
- Terrain (topography)
- Weather conditions (fog, heavy rain, snow, high winds)

- Historical data
- Inmate characterizations

The first step i to compile information that depicts everything that could affect the institution's actual *vulnerabilities*, including, but not limited to:

- Policy requirements
- Manpower survey
- Critical incidents
- Security inspection results
- Misconduct information (e.g. serious contraband, escape attempts)
- Other evaluations
- Historical reports (past/present/future)
- Building blueprints and future plans
- Details of detection/delay/assessment systems
- Weapons inventory
- Operational procedures
- Other documents as necessary

Consider routine operations and unusual conditions. For example, most institutions have a list of posts that are vacated when there are budget cuts, limits on overtime, or other situations in which staffing levels are lower.

From the site plan you will be able to extract information that includes:

- Property borders
- Egress and ingress routes
- Previously identified vulnerable areas in facility
- Routes outside the area (railroads, highways, etc.)
- Adjacent parking lots
- Building locations and characteristics (purpose, who is allowed access, operating conditions)

When examining building structures you will want to identify and describe the type of materials that compose:

- Roof
- Walls
- Windows (bars, grilles)
- Floors
- Ventilation ducts
- Sewage
- Water supply

- Extract Information
- Location and type of doors, gates, fences, tunnels, ducts, bars, auxiliary exits

Much of this information will be found in the construction documents for the facility.

***Caution!*** Be careful to look at the "as built" set of construction documents (sometimes called the "register set") because only these will reflect the changes made during construction. Another note of caution: do not make too many assumptions about your facility. Be sure that you know what is actually in place.

In one of the early CVA training classes, an instructor told the class about an escape that was accomplished by an inmate who was able to break through a cinder block wall that was *supposed* to have been filled with concrete and reinforced. It turns out that the contractor failed to fill and reinforce it. The facility learned of this oversight when an inmate exploited it.

When Sandia National Laboratories was conducting one of its first vulnerability assessments in a correctional facility, they asked staff if there were any storm sewers inside the perimeter. The initial response was "no, of course not." But further investigation identified a large sewer opening in an inmate yard. Although construction documents suggested that the sewer pipe was secure, they found it was not. Eventually they determined that an inmate could enter the storm sewer and pass under the perimeter, emerging without visual observation outside.

The physical characteristics of the facility, site and location should have been identified using the inventory forms provided in Appendix B. But in this step it is time to *analyze* these elements to determine if--and how-- they pose a vulnerability for the facility. Your analysis will require you to begin to synthesize various information and elements in order to determine what risks are actually present. For example, a substandard perimeter fence might not pose a risk in a facility that houses low security offenders who have many opportunities to leave the grounds.

Information about operational conditions will include:

- Length and number of day and night shifts
- Deployment of CO's during each shift and holiday
- Availability of special response teams
- Meteorological conditions for region
- Description of adjacent residential areas
- Inmate work details – location, number in workers, who is allowed in and out, etc.
- All instances in which inmates have any control-- such as determining when the trash needs to be taken outside

Be especially alert for situations in which inmates have any amount of control or discretion, when they decide what happens and/or when it happens.

You may want to focus extra attention on inmates who have been designated as the highest risk. How do their conditions of confinement and procedural setting differ from other inmates? What are the procedures associated with their movement outside of their housing units? By posing such questions, potential vulnerabilities will be identified.

By examining procedures you will be able to extract information about:

- Contractor / vendor access
- Inmate transfers
- Inmate activities (privileges, visitors, recreation activities, etc.)
- Access control (including inspection of vehicles and personnel)
- Accountability of inmates
- Correctional officer post orders and operational instructions
- Weapons - issuing and accountability
- Alarm communication (assessment/communication to response forces)
- Extract Information
- Equipment, information and weapons
- Location of vital equipment rooms (power, communication, information, etc.)
- Security of vital information
- Location and type of equipment that can be used by inmates
- Accessibility of weapons used by correctional officers
- Old and outdated equipment and prospect of future upgrades

The data collection forms in Appendix F provide a format to collect information about entry controls and delays. As with the physical aspects of the facility that were discussed earlier in this section, these operational features help to identify potential risks that are posed. For example, vital equipment rooms that are located inside inmate-occupied areas are likely to pose more risk than those that are outside of the secure perimeter.

### 2. Inmate Capability and *Opportunity*

In Step 3 you initially defined inmate capabilities. But at this point in the process, we go into more detail to examine the *specific opportunities* that inmates have to pose threats in the institution. For example, if your facility operates a metal-working industry inside the perimeter its presence will pose significant opportunities that would not be present if the industry were outside the facility, or at another institution.

Past incidents (escapes, escape attempts, contraband introduction, tool control problems, etc.) offer the first source of information. It is important to understand how each incident happened by examining after-incident reviews. It is also necessary to determine if intelligence indicates future activities and how they could be accomplished.

Information that will help to refine the actual capabilities and opportunities that inmates have in your facility may be derived from sources such as:

- Incident reports
- Tool control procedures
- Areas, conditions and times inmates are present
- Lost tool reports

- Lost key reports
- Audit reports
- Internal audit reports

For these and other pertinent sources you should compile and summarize collected information and conduct a systematic review of the type of incidents that have occurred not only in the past, but what is happening today, and what might be expected in the future. You may want to consider "hot" inmates in terms of escape risks. Be sure the describe the details of past incidents, including a description of :

- Inmate tactics
- Weapons
- Escape path elements
- Tools used
- Time of day
- Weather
- If inmate was in collusion with other inmates or staff

Consider the *methods* used in previous escapes or attempts, such as deceit, force or stealth, or a combination.

If you are examining the potential for contraband, be sure to describe:

- Type (e.g. weapons, drugs, money, electronic devices)
- Means of introduction (i.e. visitor areas, daily deliveries, staff)
- Means of packaging
- Ownership of contraband (was it associated with a specific group or activity?)

Remember that for the purposes of this handbook, and the supporting training materials, the threat and capabilities are defined as:

- One or two inmates
- Primary motive is to escape
- May be violent
- Tools restricted to those available inside facility or authorized to be brought in
- Weapons limited to shanks and other material inside facility
- Staff assistance, if any, is limited to passive actions such as providing information

### 3. Performance Data

Collecting and analyzing information from existing sources provides some of the insights needed to assess vulnerability. Now it is time to ask "how do things really work" in the facility. The manufacturer tells us that a door alarm system has certain attributes but the only way to know how the alarm actually functions is to test it.

Performance testing:

- Provides data for our analysis
- Ensures the adequacy, functionality, and reliability of system elements or total systems
- Demonstrates system performance for institution staff with the *need* to know

Performance testing may be done by the institution, by the CVA team, or by both. Many facilities routinely test elements of the physical protect systems. The data from these tests can be invaluable. It is likely, however, that additional testing will invariably have to be accomplished as part of the corrections vulnerability assessment.

There are several ways to collect data, including:

- Field surveys
- Subject matter expert interviews
- Published data (usually provided by the manufacturer)
- Performance tests

Although published data provided by the manufacturer is the easiest to obtain, it is often the least reliable. You must test each system yourself, several times, to ensure that it has been properly installed and maintained, and that it is properly operated.

There are other sources of published data. The Department of Defense has published the results of many tests. Sandia National Labs also publishes some of its findings. Appendix G presents some of this data and identifies specific sources for additional data.

There are two basic types of performance tests:

1. Operability test - confirms that a system element or total system is operating
2. Effectiveness test - confirms that a system element or total system is operating *as intended or required*

If you walk through a metal detector and an alarm sounds, you have determined that it is *operable.* Taking a piece of metal through the detector at different walking speeds, in different locations on your body, will help determine if the equipment is *effective.*

Every time you perform a test, the credibility of your findings goes up. Tests should be conducted at random, at different times and in different locations. Testing is a crucial element that affects the value of the overall credibility of the vulnerability assessment.

Performance test *methods* include limited scope performance tests and full system exercise tests.

The quality of these tests will depend on:

- Detailed planning
- Comprehensiveness

- Conditions
- Recording of results

It is important to *plan* performance tests. Before attempting to test systems and operations you must have a clear plan that addresses safety and security issues.

***Caution!*** The safety of the CVA team and the security of the facility are paramount. You will need to develop specific scenarios for each test, anticipating the circumstances that will be faced and the critical issues associated with testing. One of the issues will be how to handle inmate observation of your activities. Data collection forms should also be developed.

The number of tests that you conduct will affect the reliability of data. Testing levels should be based on importance, time required, cost, and operational impact. You will also need to determine how frequent the tests will be, and under which conditions they will be conducted.

Tests should ideally be conducted under a variety of conditions, including:

- Varying weather (fog, ice, snow, extreme heat, blowing sand, etc.)
- Emergency situations
- Different shifts

Experts should determine the relevant conditions and document the rationale for the conditions that are selected.

Tests should provide a thorough evaluation of areas:

- Detection / assessment
- Delay
- Response

Detection and assessment testing should determine the likelihood of detection for each of the technological sensors. The tests should look for dead spots and use common defeat methods. Tests should determine the effectiveness of personnel in detecting and assessing undesired situations. Tests should be conducted under various work conditions and should simulate situations a number of times--as many times as possible.

Examples of detection criteria testing.

- The perimeter intrusion detection system should be capable of detecting an individual (weighing 35 kg or more) crossing the detection zone walking, crawling, jumping, running, or rolling (at speeds between 0.15 [.5 ft.] and 5 [15 ft.] meters per second), or climbing or cutting the fence at any point in the detection zone with a detection probability of 90 percent at 95 percent confidence

- Probability of detection uses a confidence level, stated as Pd of .9 at 95 % confidence (minimum 30 attempts, 30 detects) to verify

- Percent chance of detection is 9 detects out of 10 attempts

<u>False Alarm Rate Criteria Example</u>

- The false alarm rate for the total perimeter intrusion system should not average more than 1 false alarm per week, per zone, while maintaining proper detection sensitivity
- If the zones can be fully observed at all times, either visually or by CCTV, the false alarm rate can go to 5 alarms, as long as this rate does not result in loss of system confidence by the corrections officers

<u>Microwave Operational Testing Example</u>

- Detection test should be done at average, low, and high intruder velocity limits
- As a minimum, test should be done near cross over points and at the center of each detection zone
- The number of trials (runs, walks, crawls) done at each location should be sufficient to verify the acceptable probability of detection for each velocity of interest

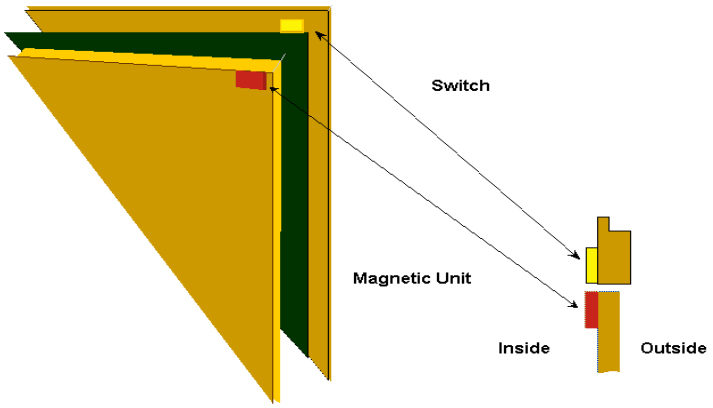
<u>Criteria For Interior Sensors Example</u>

- Should be functionally tested per established procedures at a frequency that is documented. In an Ohio prison, sensors are tested three times daily.
- Volumetric sensors should detect an individual moving at a rate of 1 foot per second or faster within the total field-of-view of the sensor.

<u>Door Switch Criteria Example</u>

- A BMS should initiate an alarm whenever the door is moved 1 inch or more from the jam (see Figure II.5)

**Figure II.5: Door Position Switch**



Delay Data/Testing

- Determine the time involved in defeating the fences and gates surrounding the facility with the inmate capabilities
- Determine the time involved in defeating the walls, windows, doors, roofs, and floors with the inmate capabilities
- Evaluate the use of vehicle barriers to determine times that they are not effective

Response force data/testing measures the time it takes for the institution to react to an identified problem or situation. These tests not only provide a time line, but also identify the steps involved with the response and the physical and technical elements involved. Response force testing will:

- Determine the time required to use the type of communication available to correctional officers
- Determine the timeliness of internal communication systems for major events (sirens, duress alarms, public address systems)
- Verify the number and type of primary and secondary responders
- Include diversionary tactics
- Test all significant elements of the response timeline

It is imperative to accurately and completely record all test results.

Poor recording can:

- Invalidate test
- Cause additional testing
- Portray a false image

There are three basic ways to analyze test results:

- Statistical analysis
- Validated expert judgment
- Expert judgment

**Exercise 3: *Analyzing* PPS Elements**

Go back to the area in the facility at which you implemented Exercises 1 and 2. Take your notes with you, along with this handbook.

Spend some time simply observing operations in your area. Then take a slow and detailed tour through the area, referring to the various elements that were described in the preceding text (1. Institutional Data, 2. Inmate Capability and Opportunity, 3. Performance Data.)

If you are working with a team, divide up these tasks and then compare notes when you are finished.

## F. Step 6: Create Path Sequence Diagrams (PSD) and Scenarios

This is where all of the pieces come together-- the inventory, research, data collection and more. All of the efforts to date combine to provide new insights into the effectiveness of facility systems and operations. As one trainer told the participants in an Ohio session, "this is where it gets down to earth." The abstract and seemingly disconnected findings from previous steps will now be used to build a concrete understanding of vulnerability.

Now it will be even more important to have a team working on this, bringing their individual perspectives, energy and commitment. The team will also be important as a sounding board and a source of debate. *Ideally, all decisions-- big and small-- for the remainder of the CVA process will be made by team consensus.*

### 1. Path Sequence Diagram (PSD)

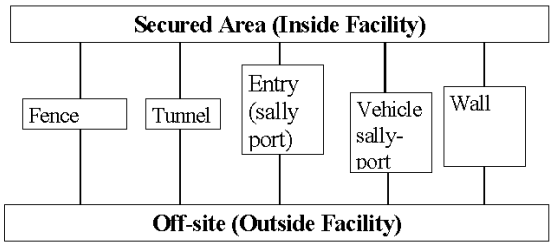
"Path sequence diagram" (PSD) is a fancy name for a map that shows how an inmate might navigate through the facility to affect an escape. A PSD might also show how someone might introduce contraband, or how any number of other defined threats might be implemented.

Path sequence diagrams:

- Provide a graphical model used to help understand the PPS at an institution
- Depict--
  - Paths that inmates can follow
  - PPS elements along the paths
- Assist the CVA team to determine most vulnerable path(s) for specific PPS and inmate
- Are created while touring the institution and by viewing institution information

Figure II.6 depicts a simple PSD.

**Figure II.6: Simple Path Sequence Diagram**




The PSD in Figure II.6 shows the physical elements that lie between an inmate who is inside the facility, and freedom outside the facility.

**<u>Exercise 4</u>: A Simple Diagram**

Take a few minutes to draw a simple diagram of the room in which you are currently sitting. Identify all the elements and the areas that lie on the other side of each element.

Figure II.7 provides a more complex PSD, indicating the path that might be chosen by an inmate to move successfully from a cell to an area outside of the security perimeter. The arrows in the center of the PSD show points at which alarms are raised, and where those alarms are communicated.

**Figure II.7: Path Sequence Diagram**

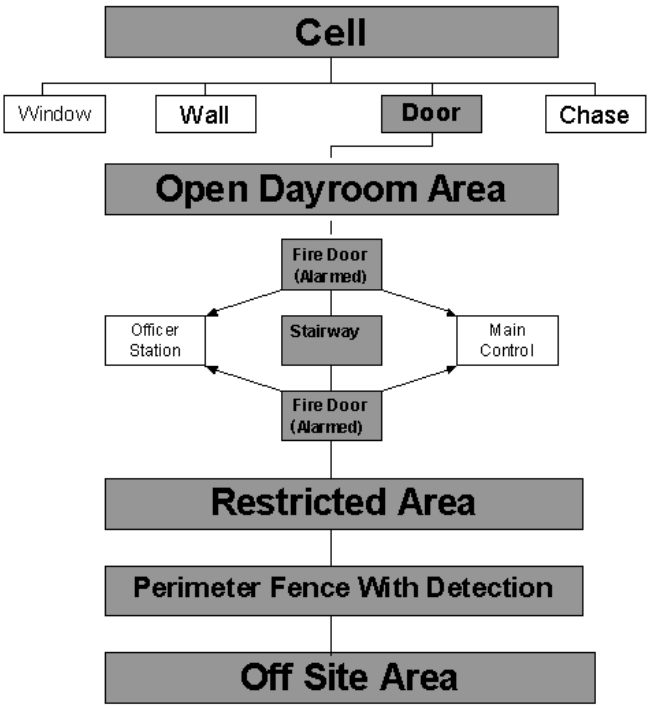
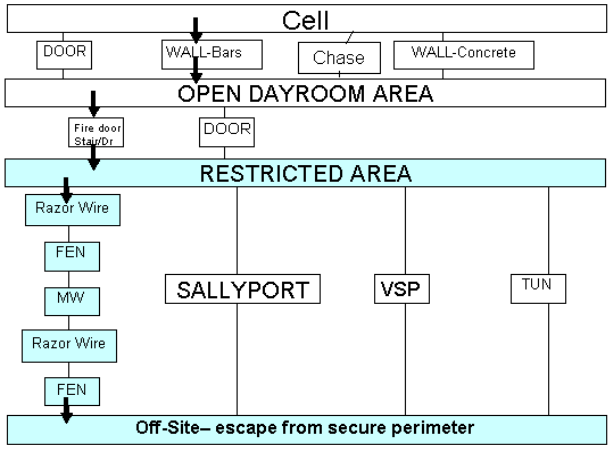



Figure II.7 shows the path of least resistance-- or the path that offers the best chance for success for the inmate. Rather than attempting to exit from the cell by a window, wall or mechanical chase, the inmate selects the door. There are similar choices at each point in the diagram, although this simplified version does not depict them. Alarms are indicated by arrows which show where the alarms are sounded.

Figure II.8 shows the larger context from which one or more PSDs are identified. Note that there are multiple choices to move from the cell block and the open area. This type of larger diagram, from which PSDs are identified, is sometimes called an “Adversary Sequence Diagram” (ASD).

**Figure II.8: Sample Adversary Sequence Diagram (ASD)**




To construct a path sequence diagram for our purposes (inmate escape):

1. Start where the inmate could start an escape – consider a simple diagram or a list to show the places the inmate could start, such as--
    a. Cell
    b. Industry
    c. Recreation yard
2. Identify <u>all</u> the ways the inmate could leave the first area (be sure to look up and down as well as side to side)
3. Go to the area outside that one and identify all the ways the inmate could leave the area
4. Continue until inmate is outside the Institution

When you are looking for starting points, consider the places that inmates usually occupy--housing units, work sites, program and medical areas, and such.

At this early stage of the analysis, be sure to identify *all* of the ways that an inmate could move from one space to another, no matter how futile they might seem. It is important to draw the full picture so that the decisions that the inmate might make are put in context.

When you create a PSD be sure to indicate on the drawing:

- Time of day
- Day of week
- Conditions
- Tools/aids assumed available to inmate

If you are creating a PSD that starts deep inside the facility, it will necessarily include one or more additional PSDs for other areas. Although these additional PSDs will be "subsets" of the inner escape PSD, they might reveal some independent paths of interest in their own right.

Be sure that your PSD includes *all* physical features and represent all the potential ways for an inmate to move from one space to another. In addition to the surfaces, you will be looking at the

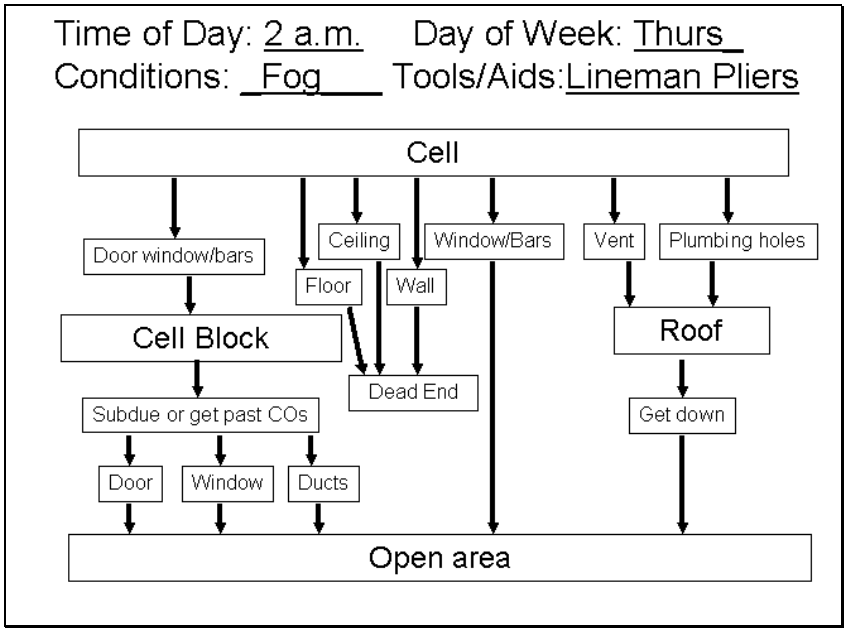
other elements that are present, such as locks. For example, if you are looking for PSD elements from a cell, they might include:

- Walls, ceiling, floors
- Windows, Bars
- Doors, locks, windows, bars
- Ventilation openings
- Fresh and waste water openings

Appendix H provides a tool to help you create your path sequence diagrams. The PSD Checklist in Appendix H prompts you to consider all of the elements in each space, and to record them properly.

Figure II.9 provides a sample of a working PSD document. Note that the time, day of week, tools/aids and conditions are filled in.

**Figure II.9: Sample Worksheet for PSD**



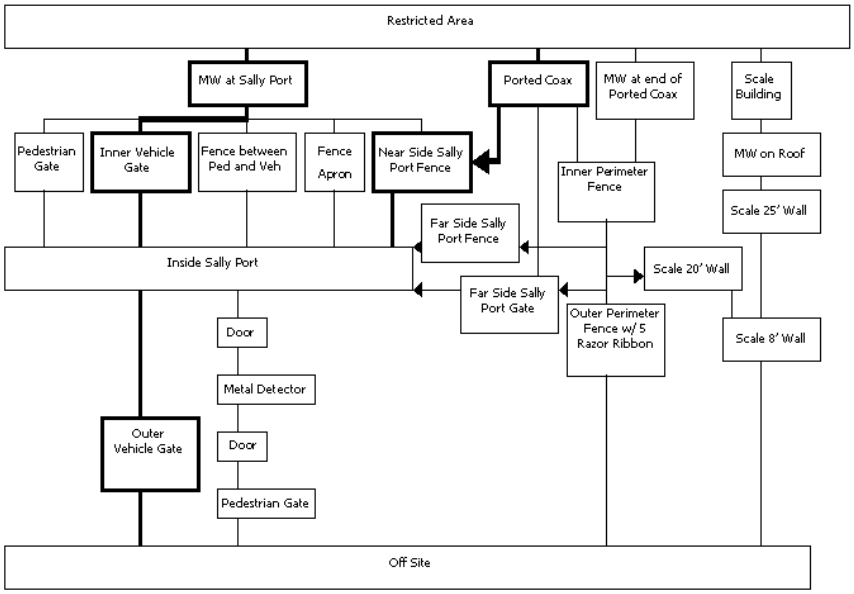

There are several paths that lead to a "dead end" on Figure II.9. There are times when it is simply not possible for a path to continue, under the circumstances for which you are conducting the assessment. When these are encountered, it is appropriate to indicate that a dead end has been reached. Be careful not to be too hasty in reaching this conclusion though, and be sure to seek the advice of your fellow CVA team members before eliminating any avenue. And when you do make a decision to eliminate a path or an element as a dead end, be sure to document this conclusion. It is important to have a clear and concise record of your activities and conclusions. Diagrams that have dead ends will prove that you considered *all* of the potential paths and options.

It is important to revisit each PSD under different times, days, conditions and assumptions (e.g. tools, weapons.) A path that might be readily detectable from an officer's post in daylight might offer a new range of opportunities after dark. Posts that are staffed on weekdays might not be activated on weekends. There are many variations to consider, and your adversary-- the inmate-- has lots of time to process all of them, and to look at all the angles.

You will be identifying and considering the locks, alarms and other features of each space during this initial phase of analysis. Later you will revisit those that pertain to the specific scenarios and you will evaluate their performance.

Figure II.10 presents a PSD for a typical perimeter.

**Figure II.10: Sample Perimeter Path Sequence Diagram (PSD)**




The PSD in Figure II.10 indicates two paths from the restricted area that converge at the inside sally port. From there, both follow the same path out of the facility.

As you and your team identify paths, you will be tempted to identify only the path of "least resistance." Often, this path is fraught with the highest potential for detection. After all, as correctional professionals we know an easy path when we see it, and it is likely that we have already installed systems to make it difficult for an inmate to follow the path without detection. Some paths might involve more time or difficulty overcoming barriers, but also avoid likely detection longer. In other words, inmates will often choose to confront a longer delay instead of facing a higher probability of detection.

As you draw near the end of this step in the process, you will find that you have many path sequence diagrams. It is likely that some of these PSDs have a lot in common. Just as two of the potential paths in Figure II.11 led to the inside sally port, there will be other common points of reference in your PSDs. When the CVA training was conducted in Ohio in 2005, *most* of the viable escape scenarios used the facility roof as a key element. When it was time to consider

ways to effectively and efficiently reduce the likelihood of escape for these paths, participants found that some simple and inexpensive changes in roof security were very effective.

At this point in the process you have assembled a great deal of information, data and insight. You have not yet *discarded* anything. In the next step you will be sifting through your findings and focusing your attention on the most serious and viable threats.

***Caution!*** As you make the transition to the next phase, make a resolve not to *lose* anything that you have assembled or found up to this point in the process. As PSDs are discarded, be sure to keep them as part of the record for the CVA.

Most important, be sure to keep a running list of specific questions, concerns and problems that have been identified-- whether they are connected to an active PSD or not.

**Exercise 5: Develop a PSD for Your Area**

Go back to the area in the facility at which you have implemented Exercises 1, 2 and 3. Take your notes with you, along with this handbook.

Develop an initial PSD for your area. Once you have sketched it out, walk through the area again and be sure it contains all of the elements.

If you are working with a team, consider having each member develop an individual PSD and then compare their findings.

### 2. Developing Scenarios

Now we have another term--"scenario"-- that simply describes writing a script for a series of actions. The dictionary defines a scenario as a "hypothesized chain of events" and that works for our application of the term in the corrections vulnerability assessment process.

Having created a number of path sequence diagrams up to this point in the process, it is time to take each one out in turn and examine it.

The steps for developing scenarios are:

a. Look at each PSD and identify how to defeat each of the security elements.
b. Select the most reasonable defeat or bypass techniques for each of the elements.
c. Define $P_D$ and delay times for each element for each defeat technique.
d. Record this information on the PSD.
e. Evaluate the PSD for paths that have low detection.
f. Identify paths that have low delay times.
g. Select a few scenarios for more detailed evaluation.

To accomplish this task, you will need to tap the data that you collected in Step 6. If you find that you do not have data for a specific element, you will need to find it either as published data, or through performance testing.

***Caution!*** As you go through the scenario development steps, be careful not to throw out any insights that might help improve the overall safety, security or efficiency of the facility.

Keep a running list of findings that you want to be sure to save and report. Although many of these will not be tied your final scenarios. *All* of them will be worth saving and passing along to facility officials.

**a. Look at each PSD and identify how to defeat each of the security elements.**

In Section II-C of this handbook we examined inmate capabilities. Remember that inmates have a variety of tactics that may be employed, including:

- Stealth (such as sneaking)
- Force
- Deceit (such as wearing a uniform, forging a pass)

Be sure not to discount the capabilities of the inmates:

- Knowledge
- Motivation
- Skills
- Abilities

There are many ways that inmates "defeat" us in the correctional setting, including:

- Deceit
- Collusion
- Stealth
- Force
- Knowledge
- Information/intelligence (inmates sell information about the facility to each other)
- Tenure (many inmates have been at the facility longer than the staff members)
- Train us (inmates are sometimes able to alter staff behavior over time)

Here is an example of how various tactics might be employed by an inmate:

*Cell Example*

- Correctional officer (CO) opens the cell and inmate overpowers CO (force), or
- Inmate sneaks past CO (stealth), or
- Inmate gets keys and open the door by appearing authorized to open the door (deceit), or

- Inmate sneaks up on CO and takes them (stealth), or
- Inmate just takes the keys from the officer (force)

**b. Select the most reasonable defeat or bypass techniques for each of the elements.**

After you identify the various ways that an inmate might defeat each element, select the most reasonable defeat method-- or method of "bypassing" the element altogether. Your decision might be based on which is the easiest method, which is most likely to avoid detection, or a combination of the two. It may be helpful to:

- Draw from the details gathered during tours and inspection of documents
- Consider the type and thickness of relevant barriers
- Identify tools that can be used
- Consider detection mechanism likelihood
- Estimate the average time taken to achieve the action at each element

To make these decisions, you will need to list the features at each element for each path. Figure II.11 provides an example of how the features might be described.

**Figure II.11: Sample List of Features for Inmate Cell**

*Inmate Cell Example*

- Wall -12" thick concrete wall with rebar at 6" centers, 4" diameter sewer and water hole, 6"x12" vent with 1/8" grating
- Cell door - two 1/4" steel plates
- Electronic lock
- Open cell door sensor
- 3"x12" Window with one bar
- Personnel generally in vicinity
- Random bed checks by correctional officers

Record your defeat or bypass technique next to each element on the path sequence diagram (PSD).

**<u>Exercise 6</u>: Develop a Scenario**

Go back to "your" area. Take your notes with you, along with this handbook.

Develop an sample scenario for your area, describing a likely (or feasible) series of steps that would lead to an escape.

Draw the path on your PSD diagram from Exercise 5, and then make a written description of the steps.

**c. Define probability of detection ($P_D$) and delay times for each element for each defeat technique.**

Where do you get the information you need to define $P_D$ or estimate delay times?

- Your observations from touring and examining the facility
- Institution documents
- Testing data
- Printed data
- Expert opinion

Remember that all the above data has to be consistent with the defeat approach used by the inmate. You should not transpose data from tests based on one set of assumptions to another context.

**Figure II.12: Sources for Obtaining Detection Probabilities**

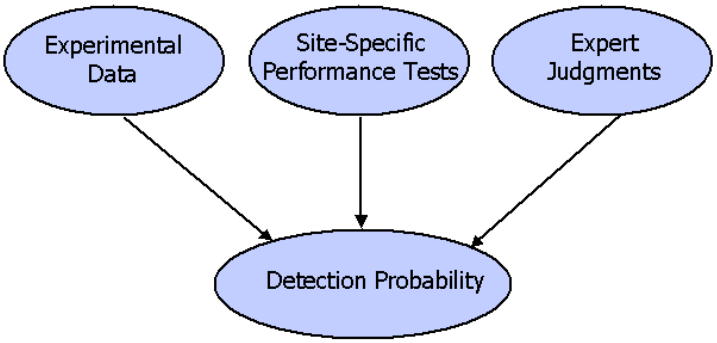



Figure II.13 provides an example of information that might be derived from testing.

**Figure II.13: Example of Data from Testing**

| **Event** | **$P_D$ *OR* Delay Time** |
|---|---|
| Metal core door | 12 second delay per door |
| Climb 14 ft fence | 20 second delay (climbing) |
| Microwave exterior detection system | 0.9 probability of detection |
| 30-cm, reinforced concrete | 3 minute delay |
| Tilt/vibration fence sensor | 0.8 probability of detection |
| 1.6-mm doors (one door into controlled building area and one outside door) | 1 minute delay |
| Officer at post | 0.5 probability of detection |
| Officer at post | 30 second delay |
| Microwave exterior detection system | 0.9 probability of detection |
| Detectors on building doors | 0.99 probability of detection |
| Interior detector | 0.9 probability of detection when on |
| Average guard response time | 60 seconds |
| Standard deviation on all times | 30% of mean |

| | |
|---|---|
| Probability of guard force communication | 0.97 |
| Running | 10 ft / second |

The results shown in Figure II.13 are from testing conducted at Sandia National Laboratories. It is important that you develop your own data to ensure its applicability to your facility.

Figure II.14 provides another example derived from a combination of testing and expert opinion.

**Figure II.14: Example of Data from Testing and Expert Opinion**

| Event | PD and Delay Time |
|---|---|
| People: | |
| CO at post | 0.5 probability of detection |
| CO at post | 30 second delay |
| Average CO response time | 120 seconds |
| Running with equipment | 10 ft / second |

It is important to remember that you are not determining *if* an element can be defeated, but rather how long it takes and how likely the defeat will be detected.

A note about *when* detection occurs. It may not always be clear exactly when detection occurs when an inmate is attempting to defeat an element. The location of the element often determines where detection occurs. For example, if the element is a large yard between a building and a perimeter fence, and a security tower post does not have a field of vision for most of the yard, the detection would not occur until the inmate came within the field of vision.

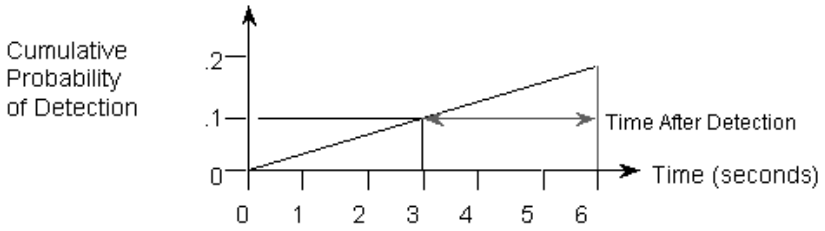
Similarly, the location of a detection element may determine when detection occurs. For example, a door position switch would not register an alarm until the door has been successfully defeated and opened.

In this case, detection occurs at the end of the delay period associated with defeating the door. But if the door has a grill in it, and the inmate removes the grill and passes through the door, the position switch is never triggered and there is no detection.

If you have to estimate the timing of detection, consider that the likelihood of detection often increases in a linear manner along a timeline (therefore in the *middle* of the delay period.) Figure II.15 provides an example of this method of estimating detection.

**Figure II.15: Linear Probability of Detection**

$P_d$ = 0.1, T = 6 seconds, time after detection = 3 seconds
Detection location at middle of delay




In the EASI program, you will be asked to identify when detection occurs during the delay period in terms of the beginning, middle or end (B,M,E).

Remember that the decision-making model for the CVA process is *consensus.* As each element is examined and decisions are made regarding delay, detection, and ultimately whether to discard a path, it is important for all team members to concur.

### d. Record Information on PSD

By recording the data you have collected about detection and delay next to each element, it will be easier for the team to analyze the relative feasibility of each path sequence diagram (PSD).

**Figure II.16: Detection and Delay Recorded on PSD**

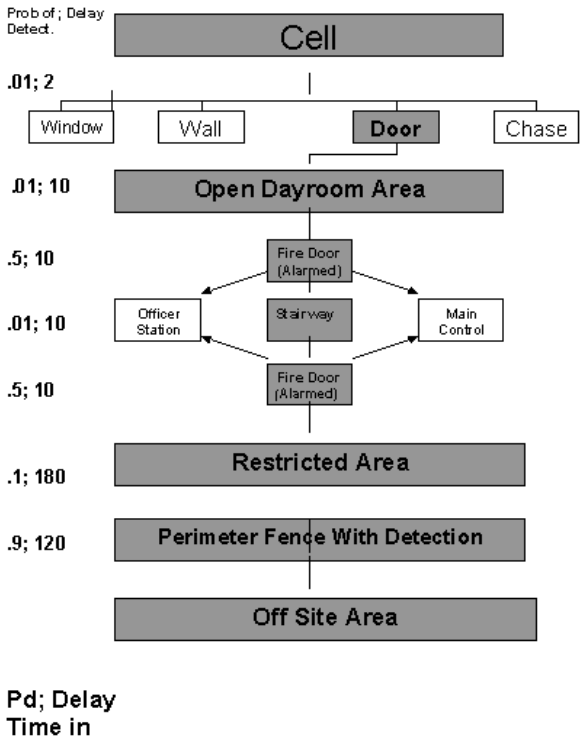
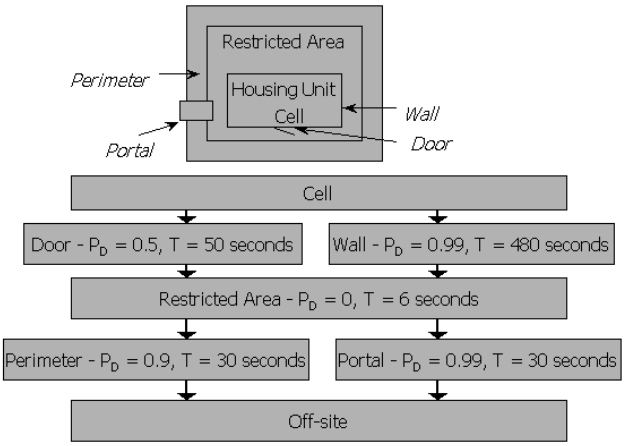



Figure II.17 provides another format for recording PSD and corresponding values.

**Figure II.17: PSD with Detection and Delay Values**




x

**<u>Exercise 7</u>: Add Times and Probabilities to Your Scenario**

Go back to the area in the facility at which you have implemented Exercises 1, 2 and 3. Take your notes with you, along with this handbook.

Spend time identifying the probability of detection for each element of your PSD. Determine the time frame (delay) for each step, and the standard deviation. Record these on your PSD.

### e. Evaluate the PSD for paths that have low *detection*.

The next task is to look at the PSD to identify paths that present a low level of detection. Figure II.16 suggests that the first two steps in the path have an extremely low detection probability (.01, or 1 percent). The alarmed fire doors (steps 3 and 5) have a 50/50 chance of detection, and the probability for the final step--the fence-- is 90 percent. At first glance, it is likely that the inmate will be detected by the time he/she emerges from the second fire door. Examine other PSDs and find those that have the overall lowest likelihood of detection and put them aside for further review.

### f. Evaluate the PSD for paths that have low *delay times.*

As with the previous task, you will look at *all* of the PSDs in terms of delay times. Remember, this is a race between the inmate and the facility. The longer it takes the inmate to complete each step of the path, the more time the facility has to detect, assess and respond.

Looking at Figure II.16 again, the delays are relatively short in the first five steps (a total of 42 seconds.) The path slows considerably at the sixth step (3 minutes), which could be crucial time if the inmate has been detected coming through the fire doors. Another two minutes are required to negotiate the final step.

### g. Select a few scenarios for more detailed evaluation.

Now it is time to narrow your field of vision and focus on a few, or several, specific scenarios. The scenarios have already been sketched out by your previous efforts to identify the defeat or bypass techniques (describe what the inmate will do), calculate the likelihood of detection for each element (or step in the scenario), and estimate the delay time for each step.

A scenario is a step-by-step sequential description of the specific tasks or steps that the inmate will implement to affect an escape. You develop a scenario by piecing together *what* the inmate does, *how* the inmate does it, *how long* each task takes, and *how likely* it is that the inmate will be detected at each step.

Remember to keep a running list of findings that you want to be sure to save and report. Although many of these will not be tied to your final scenarios, *all* of them will be worth saving and passing along to facility officials.

In some instances, an identified problem or deficiency will be so crucial that it must be reported immediately. During the training in Texas, participants identified a shocking problem with keys to emergency hatches for housing unit control centers. This was reported immediately to facility officials, resulting in swift corrective action at the facility and at several other facilities that had similar designs. Another discovery-- a design flaw in several key perimeter locks-- was also reported and system-wide repairs were immediately undertaken.

Figure II.18 provides a sample of a timeline developed by a Pennsylvania CVA team. This is another step toward articulating a scenario. Note that the CVA team concluded that published data about the probability of detection for an alarmed door was higher than the actual conditions in their facility.

**Figure I.18: Sample Timeline with Delay and Detection Probabilities**

**Table 1. Time Line – Escape Via Unit Fire Escape Doors to Rear of Institution**

| Task | Time (seconds) | Accumulated Time (seconds) | $P_D$ |
|---|---|---|---|
| Inmate exits cell via door | 2 | 2 | Low .01 |
| Inmate enters dayroom | 10 | 12 | Low .01 |
| Inmate keys open fire door | 10 | 22 | Medium .5* |
| Inmate moves into stairway | 10 | 32 | Low .01 |
| Inmate keys open fire door | 10 | 42 | Medium .5* |
| Inmate moves across restricted zone | 180 | 222 | Low .1 |
| Inmate attacks perimeter fence | 120 | 342 | Medium .5 |
| Inmate moves to outer fence | 30 | 372 | Medium .5 |
| Inmate attacks perimeter fence | 120 | 492 | High .9 |

***Established data from SNL indicates a Pd of .9 is usually assigned to an alarmed door. However, during the VA it was determined through collective team opinion and actual observations that a Pd of .5 is a more accurate indicator of alarm assessment procedures at Chester.**

At this point you will expand your PSDs and timelines into complete scenarios. These surviving scenarios will be considered the "worst case" scenarios for the facility-- the ones in which the inmate has the highest chances for success. As you elaborate on your scenarios you will need to collect further data and act out each step. You will need to assign "actors" from your team to test each step, coordinating your efforts with administrative staff and security staff.

***Caution!*** Testing scenarios can be very dangerous. Establish clear safety guidelines. Testing scenarios may also, under some circumstances, threaten facility security. Establish clear security guidelines before proceeding.

As you performance test each scenario, be sure to assign CVA team members to serve as observers. Document your actions and findings, and be sure to take photographs to demonstrate what you were doing and how it turned out.

As you performance test scenarios:

- Be sure your testing does not distract an employee from his/her job
- Remember that staff will be on a heightened alert and on their best behavior
- Try to be a "fly on the wall" whenever possible
- Always be aware of safety and security issues
- Remember that inmates will almost always be watching and making their own notes

Figure II.19 displays a format that might prove helpful as you convert PSDs into scenarios, as a prelude to entering your findings into the EASI program for analysis.

**Figure II.19: Format for Developing Scenario Elements**

| Step | Path Element | Task | $P_D$ | Delay (sec.) | Delay After Detection | Equipment |
|---|---|---|---|---|---|---|
| 1 | Door | Penetrate | .5 | 50 | 25 | Hacksaw |
| 2 | Restricted Area | Cross | 0 | 6 | 0 | None |
| 3 | Perimeter | Climb | .9 | 30 | 30 | Climbing aids/blankets |

Note that in the second example in Figure II.19, figures are not provided for the probability of delay. Instead, the CVA team has entered a Low, Medium, or High probability because data could not be generated.

One addition to the preceding format might be a column in which to record the *source(s)* of data that is used.

Appendix A provides several sample PSDs, scenarios and the resulting EASI findings.

## G. Assessing Risk with the EASI Model (Step 7)

At last, after all your hard work, there is a tool that will do much of the remaining work for you. The EASI model (Estimate of Adversarial Sequence Interruption) was created by Sandia National Labs for other applications (military, nuclear weapons, atomic energy plans) and was adapted for correctional settings in the late 1990's.

EASI is provided in an Excel file that it comprised of several worksheets. Appendix I presents the formulas that are embedding in the Excel file for reference.

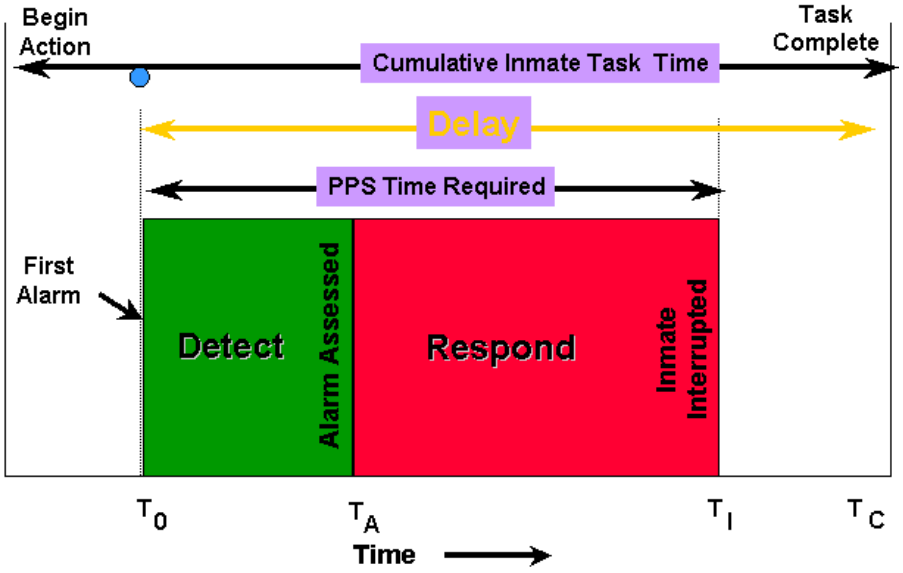
The EASI process starts with the information that you developed in the preceding steps, specifically the scenario with the corresponding delay and detection values. The EASI program requires additional input in the form of:

- response force time calculations
- probability of successful alarm communication
- standard deviations for times (usually entered as 20% unless data proves otherwise)
- location of detection relative to the delay time frames (e.g. beginning, middle, end)

When all of this information is entered into EASI you will be rewarded with a calculation of the "probability of interruption" ($P_I$). In other words, you will have a statistical estimate of the odds that you will be able to win the race with the inmate and prevent the escape (or any other threat that is analyzed.)

Figure II.20 provides an example of an EASI timeline chart in which the inmate is interrupted before the escape time line is complete.

**Figure II.20: Sample EASI Timeline Chart**



In the timeline above, the inmate's actions are depicted on the top line. The actions begin before the first alarm is sounded ($T_O$). More time passes before the alarm is assessed ($T_A$) and the response is initiated. In this example, the cumulative time for detection, assessment and response is *less* than the inmate's total task time, and the inmate is interrupted ($T_I$). Note that the "begin action" time is not calculated. It might have taken four days for the inmate to open a hole in a wall (delay) but the timeline does not get into gear until the first alarm is encountered.

Reponse force time (RFT) is comprised of three elements:

- Alarm assessment time
- Response communication time
- Response deployment time

RFT can vary substantially depending on the scenario that is being evaluated.

Probability of interruption $P_I$) is the cumulative probability that the inmate's actions will be interrupted before the escape succeeds. Put in terms of the inmate's chances for success, the probability of inmate success would be calculated by subtracting $P_I$ from 1. If $P_I$ was determined to be 0.30, it would mean that 30 times out of 100 (30% of the time) the inmate would be interrupted before successfully completing the escape attempt. Expressed as the inmate's chances for success, it would be 0.70 (70 out of 100 times) the inmate would complete the escape. This is also called a measure of the risk.

Consider the following sample scenario:

> *At 1700 hr, an inmate gets to his starting point outside the housing unit undetected. He runs across the outer area to the perimeter fence. Once at the perimeter fence he cuts the razor wire with cutters, cuts the inner fence with cutters, runs across the isolation zone that has a microwave sensor, cuts razor wire on the outer fence, and then cuts through the outer fence.*

A timeline is created for this scenario, in preparation for entry into the EASI worksheet.

**Figure II.21: Timeline for Scenario #1**

| Task Description | PD | Location | Delay time | Cum. time |
|---|---|---|---|---|
| Get outside housing unit | 0 | | | |
| Run across outer area | L | M | 30 | 30 |
| Cut razor ribbon | L | M | 20 | 50 |
| Cut inner fence | H | M | 20 | 70 |
| Run to outer fence | H | M | 0 | 70 |
| Cut outer razor ribbon | L | M | 20 | 90 |
| Cut outer fence | L | M | 20 | 110 |

The following EASI worksheet shows how the EASI program calculates the probability of interruption.

**Figure II.22: Sample EASI Worksheet**

| *Estimate of Adversary Sequence Interruption* | Probability of Alarm Communication | | Response Force Time (in Seconds) Mean | Standard Deviation |
|---|---|---|---|---|
| | 0.9 | | 60 | 5 |

| Task | Description | P (Detection) | Location | Delays (in Seconds): Mean: | Standard Deviation |
|---|---|---|---|---|---|
| 1 | Run across outer area | 0.1 | M | 30 | 5 |
| 2 | Cut Inner Razor Ribbon | 0.1 | M | 20 | 3 |
| 3 | Cut Inner Fence | 0.8 | M | 20 | 4 |
| 4 | Run to outer Fence | 0.9 | M | 0 | 0 |
| 5 | Cut Outer Razor Ribbon | 0.1 | M | 20 | 3 |
| 6 | Cut Outer Fence | 0.1 | M | 20 | 4 |

| Probability of Interruption: | 0.214819151 |
|---|---|

Likelihood of escape is 0.79

In Figure II.22 the "description" column describes each step in the scenario. "Location" refers to the point in the delay time frame in which detection occurs (in the example the "M" stands for middle of delay period.)

The "mean" is the average number of seconds of delay that is associated with each step, and the standard deviation expresses the number of seconds (plus or minus) that the actual delay will vary from the mean.

For example, the first task, "run across outer perimeter" could be expected to take 25 to 35 seconds.

Another EASI worksheet is provided in Figure II.23, depicting substantially different conclusions.

**Figure II.23: Sample EASI Worksheet**

***Estimate of Adversary Sequence Interruption***

| Probability of Alarm Communication | Response Force Time (in Seconds) Mean | Standard Deviation |
|---|---|---|
| 0.9 | 75 | 15 |

| Task | Description | P(Detection) | Location | Delays (in Seconds): Mean: | Standard Deviation |
|---|---|---|---|---|---|
| 1 | Penetrates Exterior Cell Wall | 0.5 | B | 60 | 12 |
| 2 | Drop to Restricted Area | 0.2 | B | 10 | 2 |
| 3 | Move to Containment Fence | 0.2 | M | 20 | 4 |
| 4 | Climb Containment Fence | 0.2 | M | 10 | 2 |
| 5 | Move to Inner Perimeter | 0.2 | M | 10 | 2 |
| 6 | Cut Shaker Wire | 0.3 | M | 150 | 30 |
| 7 | Cut Inner Perimeter Fence | 0.1 | M | 300 | 60 |
| 8 | Move through MW Zone | 0.8 | M | 150 | 30 |
| 9 | Cut Outer Perimeter Fence | 0.4 | E | 205 | 41 |

| Probability of Interruption: | 0.953746421 |
|---|---|

Likelihood of escape is 0.05

In this example, the inmate will be interrupted before his escape 95% of the time. The inmate is interrupted early in his escape path in the second scenario, as shown in the EASI timeline in Figure II.24.

**Figure II.24: EASI Timeline for Second Scenario, Early Interruption**

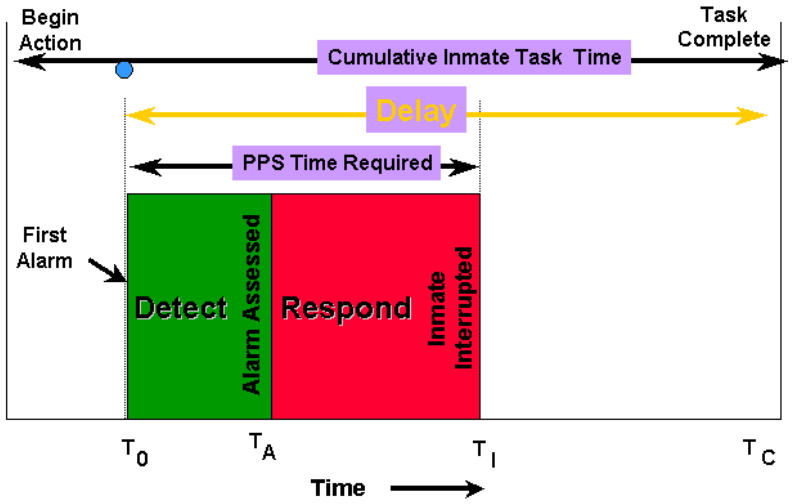
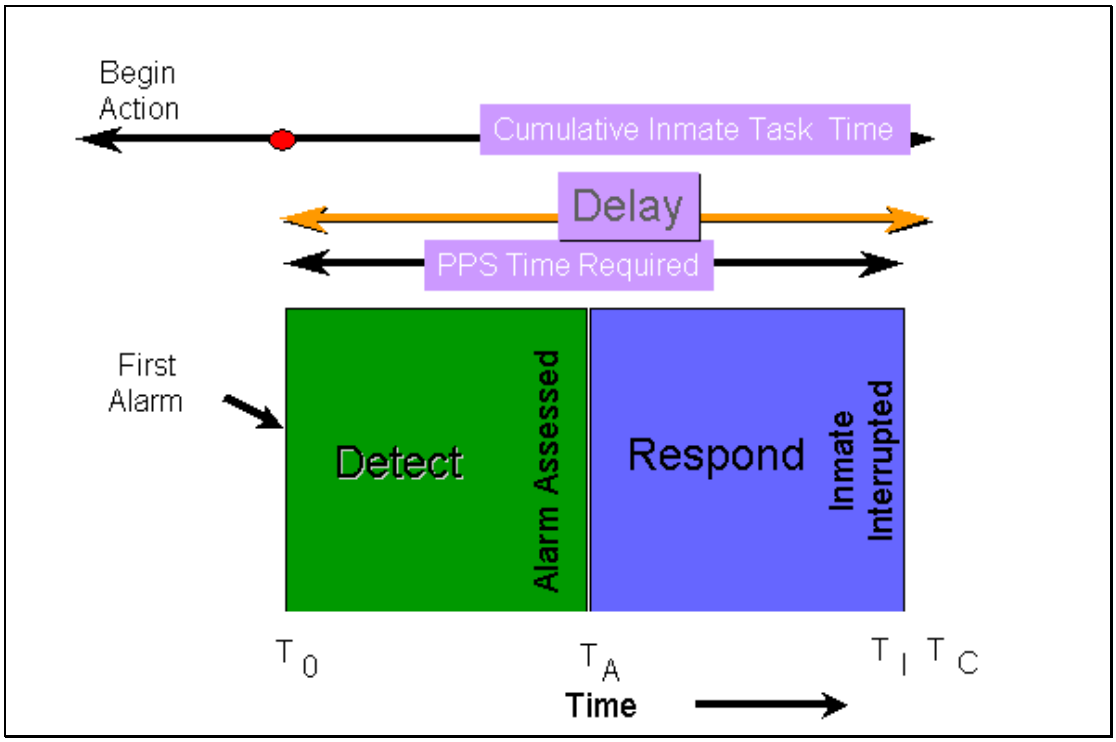



Figure II.25 shows a timeline in which the inmate is interrupted very late in his timeline.

**Figure II.25: EASI Timeline, Late Interruption**




## Neutralization

An element of "interrupting" an escape attempt (or other threat) requires that an inmate actually be stopped or defeated prior to completion of escape. This is called "neutralization" and as you might expect by now, there is a probability for neutralization ($P_N$).

As you might have guessed, the term "neutralization" comes from the military. As we use it hear, it means to stop or interrupt the inmate before successfully accomplishing his/her objective.

Estimating $P_N$ is often estimated based on experience, and may be difficult to determine. There are many parameters to consider, and of course live exercises are usually out of the question.

Figure II.26 displays an "engagement" timeline. This type of diagram helps to focus on the manner in which the facility responds to an assessed alarm and engages the inmate.

The time it takes to respond to an alarm is called "response force time" (RFT).

There is a method that may be used to calculate $P_N$ under some circumstances. When you consider any type of engagement between an inmate and facility staff, there will be situations in which one side or the other has an advantage. For example, an inmate hiding and waiting to attack an officer will often have an advantage of surprise. Similarly, the number of officers compared to the number of inmates will often indicate an advantage for one side or the other.

**Figure II.26: Engagement Timeline**

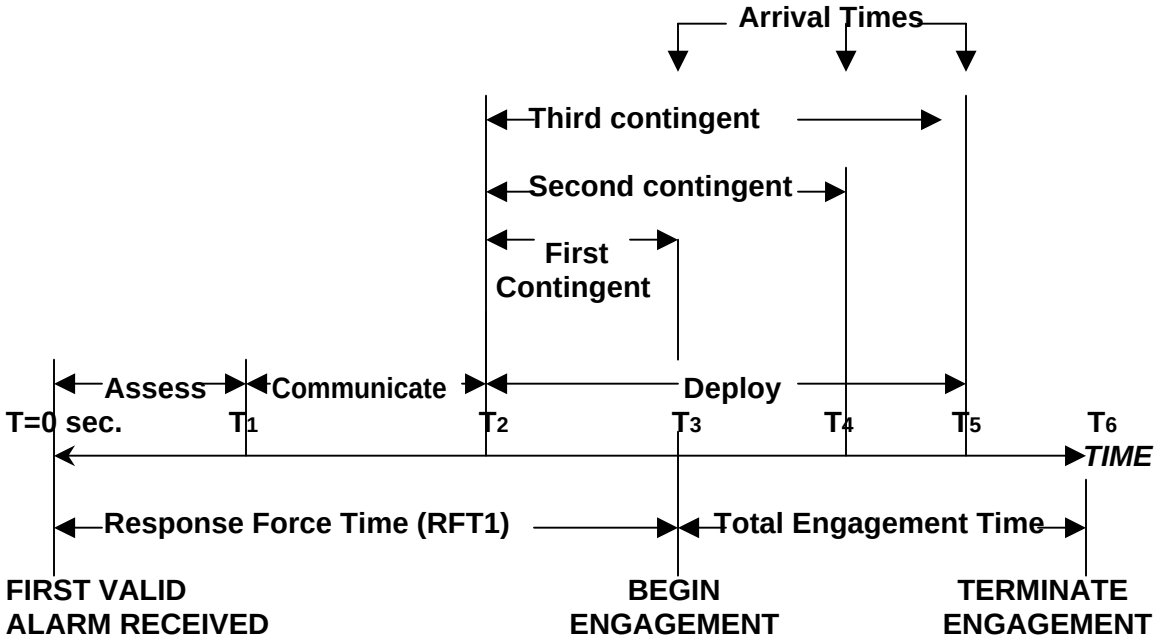
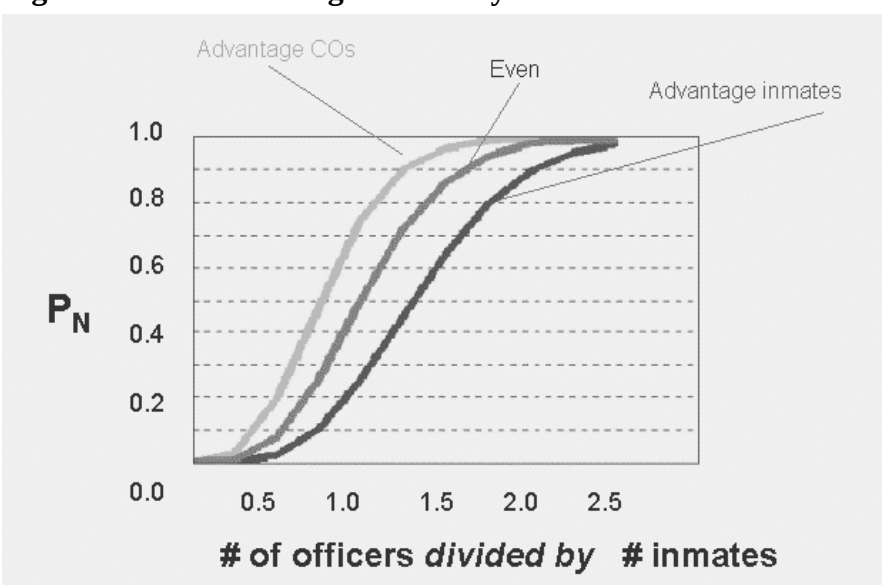



Figure II.27 provides a method for calculating the $P_N$ in situations that involved more than one inmate or officer.

**Figure II.27: Calculating Probability of Neutralization**




In Figure II.27, assume we have one officer and one inmate at the intercept point. The ratio of officers to inmates (one divided by one) is 1.0. Moving up the graph to the value lines, the curve has three values depending on who has the advantage. If an officer is armed and the inmate is not, we use the "Advantage COs" line. The $P_N$ is about 0.75, meaning that the officer will win 75% of the time. Conversely, if the inmate has an element of surprise, you would use the "advantage inmates" line, and find a $P_N$ of about 0.20, suggesting that the officer will win only 20% of the time. Of course, if you have better data, use it!

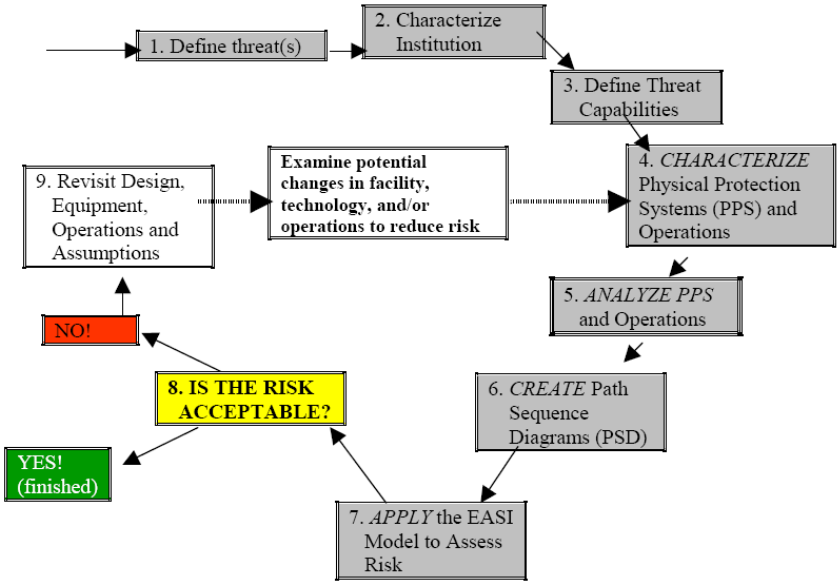
After you have used the EASI methodology for each of your "worst case" scenarios, assemble your findings for comparison and further analysis. In the next step you will determine if the risk is acceptable.

> **Exercise 8: Use EASI to Evaluate Your Scenario**
>
> Take the scenario, PSD and values that you have developed for your area. Enter the information into the EASI program and examine the results. Be sure to look at the timeline and other features of the EASI program.

## H. Acceptability of Risk (Step 8)

As the CVA process description in Figure II.28 shows, you have now arrived at a crucial decision point.

**Figure II.28: CVA Quality Circle, Step 8**




Consider each one of the scenarios that you have evaluated. Compare the probability of interruption ($P_I$) for each and then look at them as a whole. Taken together, the results for these worst-case scenarios are an indicator of the overall effectiveness of your physical protection system. The scenarios with the lowest probability of interruption are the most important indicators of our vulnerability.

**Figure II.29: Sample Summary of Worst Case Scenarios**

| | **Scenario** | **Probability of Interruption ($P_I$)** | **"Risk"** (1.0 minus $P_I$) | **Acceptable?** |
|---|---|---|---|---|
| 1 | Cell to roof, side yard, over fence | 0.85 | 0.15 | N |
| 2 | Cell to roof, vehicle sallyport | 0.27 | 0.73 | N |
| 3 | Medical unit to vehicle sallyport | 0.55 | 0.45 | N |
| 4 | Medical unit to front entry | 0.67 | 0.33 | N |
| 5 | Industry to yard to corner fence | 0.18 | 0.82 | N |
| 6 | Gymnasium to yard to perimeter fence | 0.06 | 0.94 | N |
| 7 | Classroom to mechanical space, storm sewer | 0.92 | 0.08 | Y |
| 8 | Kitchen to ventilation duct, side yard, fence | 0.44 | 0.56 | N |
| 9 | Kitchen to trash bin, garbage truck | 0.83 | 0.17 | N |

Figure II.29 shows a sample summary of worst case scenarios and their corresponding probabilities of interruption. In this sample, only one of the scenarios (#7) had a risk level that was acceptable.

Decide if the probability of interruption is acceptable for any of the scenarios. If any are acceptable, you may put them aside and focus your attention of the remaining scenarios.

After you have sorted through your findings, you will take your unacceptable scenarios into Step 9.

## I. Step 9: Using EASI to Reduce Risk

*First a reminder*: don't forget to keep all of those stray observations and findings that you have discovered in the CVA process to this point. Many findings will not be part of the scenarios that are ultimately evaluated, but it is imperative to lose *nothing*. You should have been keeping a running log or list of these items, such as equipment problems, staff training issues, and procedures that fall short, and more. Be sure that each of these is included in your final report, and that no loose ends are left to hamper operations after you are finished with the CVA.

In this step, you will find that EASI is a versatile tool that will help you to identify ways to reduce risk, and to model the impact of changes on the bottom line risk level for each scenario.

At this point in the process, for each scenario that has an unacceptable level of risk, you will:

- Determine the reason(s) for the high level of risk
- Evaluate potential options to reduce risk
- Consider the cost associated with solutions compared with the benefits

In many cases, you will find that there are "root causes" for high-risk scenarios. These might include, but are not limited to:

- Inappropriate *policies* (setting out to do the wrong thing)
- Inadequate *procedures* (not attempting to do it the right way)
- Training *deficiencies* (not arming staff with the knowledge, skills and abilities they need)
- *Staffing* issues (insufficient staff, wrong type of staff assigned, inadequate deployment, etc.)
- *Equipment* shortcomings (the wrong equipment for the application, poor installation, failure to maintain the equipment, etc.)
- *Physical plant* problems (poor design, improper construction, inadequate maintenance, etc.)

As you look for root causes, you need to expand your perspective beyond just the high-risk scenarios. You should:

- Consider the entire inmate range of inmates and their risk levels
- Examine scenarios and situations that are tied into, or which parallel the high-risk scenarios
- Identify critical components of the PPS and the extent to which there is defense-in-depth

When it comes to considering *systems,* there might be upgrades available for your consideration. If so, you-- or the person who analyzes these systems-- must understand:

- System strengths and weaknesses for *all* types of inmates that will be affected
- Safeguards that could potentially enhance protection
- Ways to identify and group alternatives to facilitate the meaningful analysis of their benefits
- Costs and operational impacts of these upgrade packages

When examining potential upgrades, consider that:

- Some vulnerabilities can be solved with “quick fixes”
- Combinations of hardware and procedures may be needed
- Procedural upgrades are often cheaper than hardware
- Hardware fixes can be expensive and difficult to implement
- Combinations of upgrades might increase effectiveness uniformly

**Using EASI to Identify *and* Test Potential Solutions**

In the following charts we will use one of the Colorado scenarios (see Appendix A) to demonstrate various ways in which the EASI tool may be used to identify strategies to reduce risk and to measure the impact of potential changes.

Figure II.30 presents the EASI table and the probability of interruption ($P_I$), which is very low. Without any changes, the inmate will succeed four out of five times.

**Figure II.30: Sample EASI Scenario and Table**

| | | | | Delays (in Seconds): | | |
|---|---|---|---|---|---|---|
| Task | Description | P(Detection) | Location | Mean: | Standard Deviation | |
| 1 | Arrive at Maintenance, retrieve tools including lineman's pliers, attack/secure staff member | 0.2 | | 120 | 30 | |
| 2 | Exit door -SV-32 | 0.1 | | 5 | 2 | |
| | Run across dock to parked trailer | 0.2 | | 11 | 5 | |
| 4 | Hide between wheels on trailer | 0.03 | | 120 | 30 | |
| 5 | Run to internal fence and cut utilizing lineman's pliers | 0.07 | | 36 | 15 | |
| 6 | Crawl through electronic detection zone (microwave) | 0.2 | | 38 | 20 | |
| 7 | Cut fence with lineman's pliers ensuring perimeter vehicle does not detect. | 0.27 | | 73 | 30 | |
| 8 | Cross restricted area | 0.2 | | 2 | 1 | |
| 9 | Cut razor wire utilizing lineman's pliers | 0.2 | | 20 | 5 | **Probability of Interruption** |
| 10 | Cut fence with lineman's pliers | 0.2 | | 36 | 10 | **0.19123999** |

### a. Removing Tool from Scenario

The underlined words in the table identify a common tool that is critical to the success of the scenario-- lineman's pliers. One of the first potential solutions to consider would be to decrease the ability of inmates to gain access to this tool, by improving tool control procedures, changing the classification of the tool, increasing the security measures that control the tool, or other methods. Depriving inmates of this critical tool could result in the abandonment of the plan by the inmates. If not, it would at least make it more difficult to cut through the fences.

Figure II.31 shows the impact of increasing the time it takes to cut the fences by a factor of two, which might happen if the lineman's pliers were not available. The impact on the risk is to reduce it from 80% success for the inmate, to 60% for the inmate.

**Figure II.31: Eliminating Access to Tool, Increasing Time to Cut Fences**

| | | | | Delays (in Seconds): | |
|---|---|---|---|---|---|
| Task | Description | P(Detection) | Location | Mean: | Standard Deviation |
| 1 | Arrive at Maintenance, retrieve tools, attack/secure staff member | 0.2 | | 120 | 30 |
| 2 | Exit door -SUV-32 | 0.1 | | 5 | 2 |
| 3 | Run across dock to parked trailer | 0.2 | | 11 | 5 |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Hide between wheels on trailer | 0.03 | | 120 | 30 |
| 5 | Run to internal fence and cut | 0.07 | | 72 | 15 |
| 6 | Crawl through electronic detection zone (microwave) | 0.2 | | 38 | 20 |
| 7 | Cut fence ensuring perimeter vehicle does not detect. | 0.27 | | 146 | 30 |
| 8 | Cross restricted area | 0.2 | | 2 | 1 |
| 9 | Cut razor wire | 0.2 | | 20 | 5 |
| 10 | Cut fence | 0.2 | | 72 | 10 |

### b. Eliminating the Trailer

What about the trailer, which is used by the inmates to hide them from detection during the escape? Using EASI, you can determine the impact of removing the trailer from the yard. For example, if you determine that removing the trailer would increase the probability of detection for steps 3 and 4 to 0.5, the EASI program will recalculate the Probability of Interruption. In this example, $P_I$ is hardly affected, increased by only 1 percent (from 19% to 20%.) While moving the trailer might be a good idea, EASI shows that it is not the magic bullet that will foil this escape scenario.

### c. Increasing the Probability of Detection

What if we increase the <u>probability of detection</u> for other steps? Use EASI to help you determine if there is a critical step at which detection would change the odds substantially. Experiment with different probability of detection values and you will find that:

- Increasing $P_D$ in Step 1 from 0.2 to 0.5 would increase $P_I$ to .594
- Increasing $P_D$ in Step 2 from 0.1 to 0.5 would increase $P_I$ to .626
- Increasing $P_D$ in any of the subsequent steps 0.5 would not increase $P_I$ by even 1%!

Why would changes in detection early in the scenario yield such strong results, while comparable changes later in the sequence would have virtually no impact? Because, when it comes to detection, the major impact will be made at the earliest steps in the scenario. In this example, better detection later in the process is simply “too little, too late.”

### d. Improving Response Time

Can we make a difference if we <u>improve response time</u>? Once again, use EASI to determine the answer. The response time for Figures 74 and 75 is 341 seconds, with a standard deviation of 70 seconds. If the response time is *reduced*, the impact on the probability of interruption would be:

- Reduce response time to 300 seconds and $P_I$ is 0.269
- Reduce response time to 240 seconds and $P_I$ is 0.368
- Reduce response time to 200 seconds and $P_I$ is 0.423
- Reduce response time to 100 seconds and $P_I$ is 0.567

Clearly, reducing response time may have a significant impact on the probability of interruption, but it may not be, by itself, the solution that makes the odds acceptable.

Tip: Instead of using a "trial and error" approach to determine the impact of changes in detection probabilities, delay, or response time, use the buttons on the top of the EASI worksheet. For example, if you click on the value for "mean response time" and then click on the button "analyze response" you will be taken to the worksheet entitled "response" which has a table and graph. The table shows you the impact on $P_I$ for various new values of response time.

Similarly, you may click on any of the values for $P_D$ and then on the "analyze $P_D$ " button and you will be taken to the worksheet entitled "PDs" where you will find a table and chart showing the impact of changes in $P_D$ on the $P_I$ .

The same process works for any cell containing a delay value and the "Analyze DELAY" button.

To move back to the home page for EASI, just click on the worksheet tab entitled "XL EASI" at the bottom of the screen.

Using EASI you are able to examine each element of the scenario, enter new values, and immediately determine the impact on the probability of interruption. This will lead you to the critical element(s) that could reduce risk if you can find a way to change the detection, delay or response.

Similarly, you may examine two or more changes using EASI to determine the cumulative effect on risk. For example, increasing detection probabilities for Steps 1 and 2 to 0.5, along with reducing response time to 200 seconds, would produce a probability of interruption of .804, reversing the odds in favor of the facility.

The preceding examples are only a hint of the power that EASI offers as an analytical tool. By experimenting with changes in detection, delay and response, the impact on risk is instantly recalculated.

Every time you recalculate the probability of interruption you may also have EASI redraw the timeline. If you click on "draw timeline" you will be taken to the timeline worksheet and a message will appear asking if you want permanently delete the selected sheet. If you answer "OK" then the old timeline will be removed, making room for your new one.

Costs and Benefits

As you identify promising solutions, you will need to consider the costs compared with the benefits. In some instances, you might prepare an actual "cost benefit analysis" or even a "life cycle cost analysis." In the latter case, you will be putting the initial costs for a solution into the broader context of the ongoing costs.

For example, one solution to a problem might involve adding a post and staffing it around the clock. Another approach to the same problem might involve the installation of new technology that costs $700,000 and has an annual maintenance cost of $20,000. A life cycle cost analysis looks at annual costs over a period of several years. In this example, the first year cost of the post

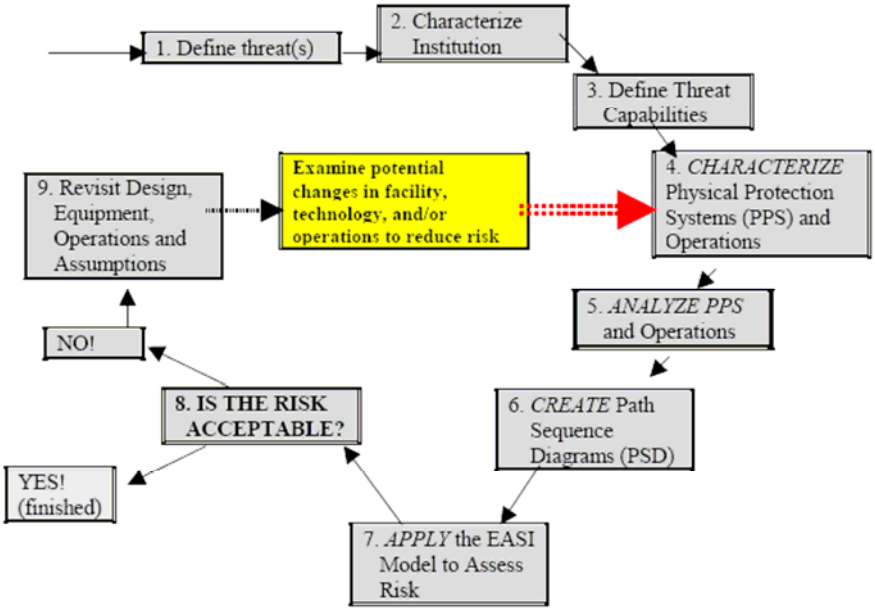
might be $400,000, but the staffing cost continues and actually grows (with staff pay increases) every year. The technology solution, while initially more expensive, would prove less costly at the end of the second year, and would realize substantially savings every year thereafter. Officials sometimes pale at the initial costs associated with physical and technical solutions, but total costs over time often show that staffing solutions are almost always the most costly.

Usually the least expensive solutions involve changes in policies, procedures and/or practices. It may be prudent to focus your initial attention on such no- or low-cost solutions. But remember that these often require initial efforts in the form of training, and ongoing efforts to ensure that staff implement the changes consistently over time.

Fixing One Problem Might Cause Another

As you formulate plans to reduce risk, the changes you make in practices, technology and facilities might have their own implications. After you have assembled your changes, sometimes referred to as "solution sets," you will need to go back through the CVA quality circle process to ensure that you have not created new problems, as shown in Figure II.32.

**Figure II.32: CVA Quality Circle, Final Steps**




**<u>Exercise 9</u>: Use EASI to Analyze Alternatives**

Using the scenario that you entered into EASI, take some time to experiment with changes in detection, delay and response times. Record the changes in overall risk (Probability of Interruption) for each variation, and save the EASI Excel file under a new name each time you make a change (for reference.)

Pulling It All Together

When you have finished your re-check, and you are sure that your proposed solutions do not cause additional problems or risk, it is time to pull all of your findings and recommendations together and implement them.

Part IV of this handbook examines the logistics the overall CVA process, including report-writing. Implementation tips are also offered.

Part III provides a “primer” that reviews the technical aspects of physical protection systems.

# PART III: A PRIMER ON PHYSICAL PROTECTION SYSTEMS (PPS)

The following pages provide a primer on detection systems, in an effort to give all participants in the CVA process a common understanding of the basics. We will identify the resources needed to provide detailed evaluations of detection capabilities.

Why? So you will be able to calculate the "probability of detection" for elements of the physical protection system. Probability of detection (expressed as $P_D$) is one of the critical components of the EASI model that determines the overall probability of success or failure.

## 1. Interior and Exterior Detection Systems

This section of the handbook will provide the following:

- Introduction
- Sensor fundamentals
- Exterior sensor technologies
- Interior sensor technologies
- System considerations
- Summary

### a. Introduction

Detection occurs when an event is assessed by an authorized person. The typical sequence of events is:

**Alarm + Assessment = Detection**

Assessment is usually-- but not always-- preceded by an alarm. For example, an officer might discover an inmate who is out of place during his/her rounds. In this instance there is no alarm, but the officer assessed the situation and determines that an unauthorized event is occurring, which means the event has been detected.

Another detection sequence might look like this:

1. Motion detector is triggered by an inmate who is in an unauthorized area. (Alarm)
2. Control center sends an officer to investigate. (Assessment)
3. Officer discovers inmate and reports it to the control center. (Detection)

A variation of the preceding might eliminate the need for the officer to investigate. The control center officer might have the ability to view the inmate using closed circuit television, allowing assessment to occur and detection to be accomplished.

There are countless detection scenarios, but all of them have the following in common: w**ithout assessment, there is no detection.**

Where does detection occur in the following set of activities?

1. Perimeter sensor alarm signal is generated
2. Alarm signal is transmitted to console
3. Operator is alerted by incoming alarm
4. Operator scans detection zone of alarming sensor for cause (either visually or with CCTV)
5. In searching for cause of alarm, operator observes an unauthorized person in that area
6. Operator notifies response force, identifying nature and location of intrusion
7. Response force interdicts intruder or escapee

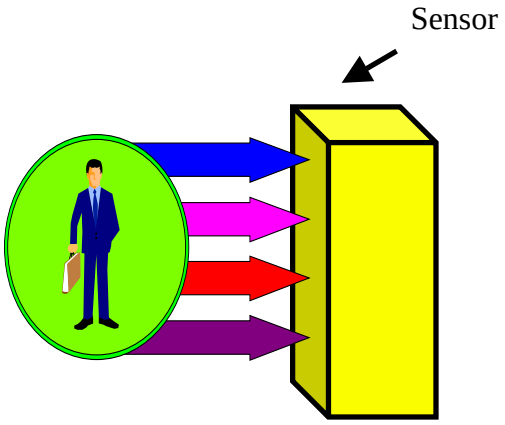
It is not until #5 (operator observes an unauthorized person) that detection occurs.

There are several physical components that are often involved with detection. These include:

- Exterior intrusion alarm
- Interior intrusion alarm
- Alarm communication and display
- Assessment
- Entry control

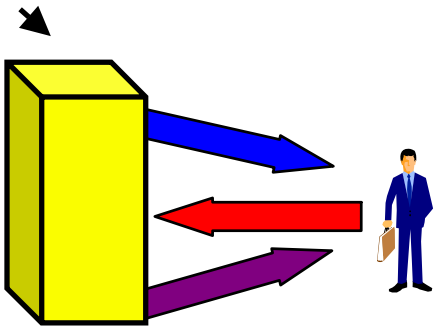
There are two types of sensors: active and passive. A passive sensor has a receiver that detects vibration, heat (infrared), sound or capacitance (electrical charge). In a passive system, the sensor receives input from the target, as shown below.

**Figure III.1: Passive Sensor**




An active sensor has a transmitter and a receiver. It sends a signal and detects a target by analyzing the return (see Figure III.2 below.) Active sensors include microwave, infrared, RF (radio frequency) and other technologies.

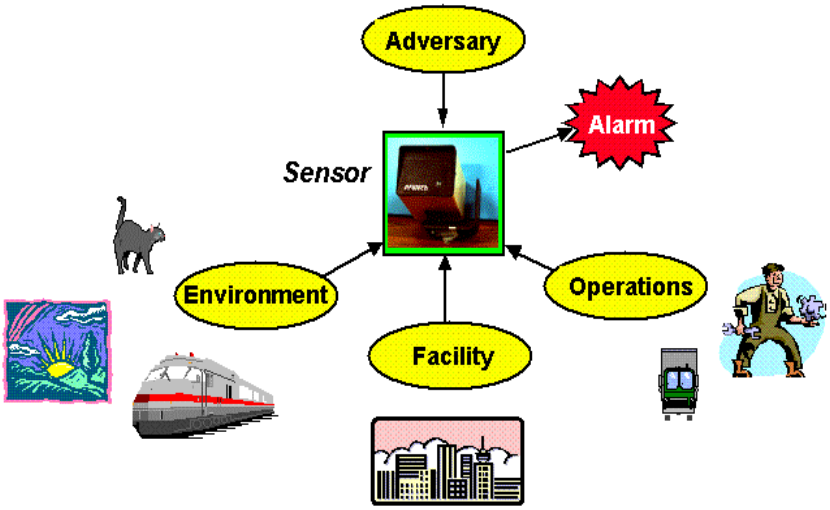
**Figure III.2: Active Sensor**



You may hear a sensor referred to as "bi-static." This simply means that it has a transmitter and a receiver.

Sensors are designed to interact with the setting around them. Unfortunately, you are not able to control what a sensor detects, which may lead to some difficulties. As Figure III.3 suggests, there are many targets and events that might trigger an alarm.

**Figure III.3: Sensor Interactions**




Several factors will determine how well a sensor performs, including:

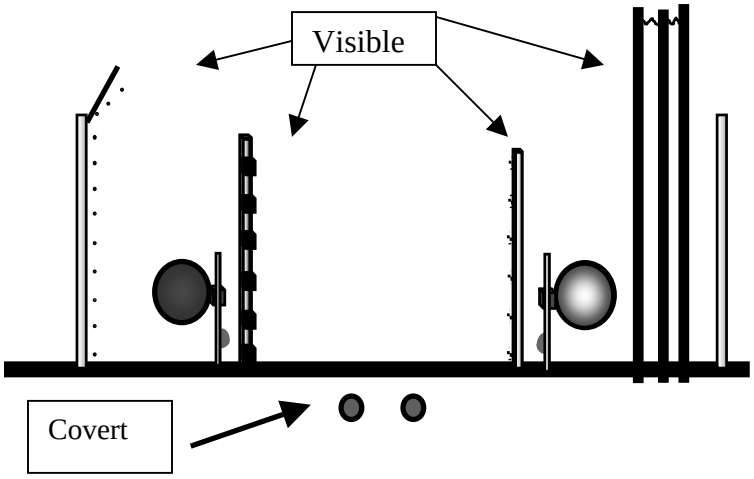
- Sensor characteristics
- Sensor condition (maintenance)
- Probability of detection (does the sensor alarm when it is supposed to?)
- Nuisance alarm rate (NAR)
- False alarm rate (FAR)
- Vulnerability to defeat

The probability of detection is also conditioned on:

- Target size and speed
- Sensor hardware
- Installation conditions
- Sensitivity setting
- Weather conditions
- Maintained condition
- Method of intrusion
  - Walking
  - Jumping
  - Tunneling

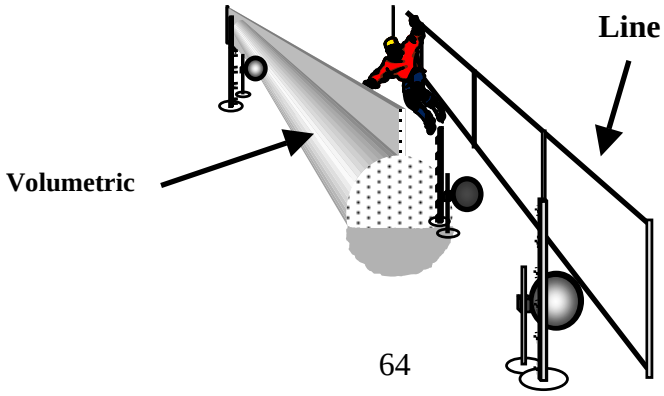
Covert systems are not easy to see, while visible systems are easily viewed. Obviously, covert sensors are more difficult for an intruder to detect. Visible systems are easier to install and maintain, though.

**Figure III.4: Visible and Covert Systems**




Volumetric sensors provide detection in a volume of space and their detection area is not usually visible. Line sensors provide detection along a line and the detection zone is usually easy to identify.

**Figure III.5: Volumetric and Line Sensors**



### b. Exterior Alarm Systems

There are several types of intrusion sensor technologies:

- Microwave
- Active infrared
- Passive infrared
- Buried cable
- Vibration
- Sensor coil
- Taut Wire
- Video motion detectors
- Ultrasonic
- Sonic

Exterior microwave systems have several characteristics. They are:

- Active (send a signal)
- Visible (are readily apparent to the observer)
- Line-of-sight (must have unobstructed field of vision)
- Freestanding
- Volumetric
- Two classes of sensors
  - Bistatic (transmitter and receiver)
  - Monostatic (receiver only)

Exterior microwave systems have very specific site requirements. It is important to understand these requirements to ensure that systems are properly installed and maintained. The requirements include:

- Sensor bed-- The surface over which the microwave passes must be very flat-- no more than 6 inches of variation. Obstructions in the surface will create voids behind which the microwave will not be effective.
- Antenna height-- 18 to 24 inches above the sensor bed surface to the center of the cone
- Slope of plane- No more than a one inch elevation change in 10 feet from any point on the surface of the plane (note that this does not necessarily mean that the field has to be level, but it must be a continuous plane with little variation if it is on a slope)

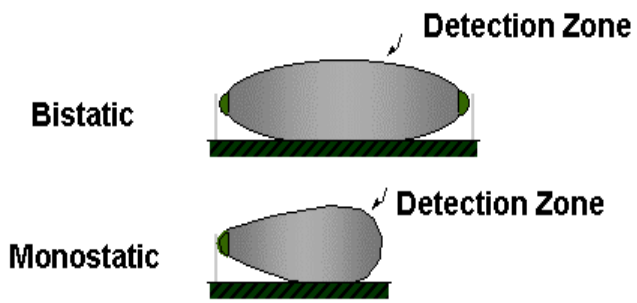
Performance characteristics for exterior microwave systems vary. The probability of detection ($P_d$) varies with:

- Direction of movement-- the system is most sensitive to movement across the field-of-view (perpendicular to the line between of the signal)

- Velocity of the intruder (a slow crawl may sometimes defeat it)
- Height and angle of installation

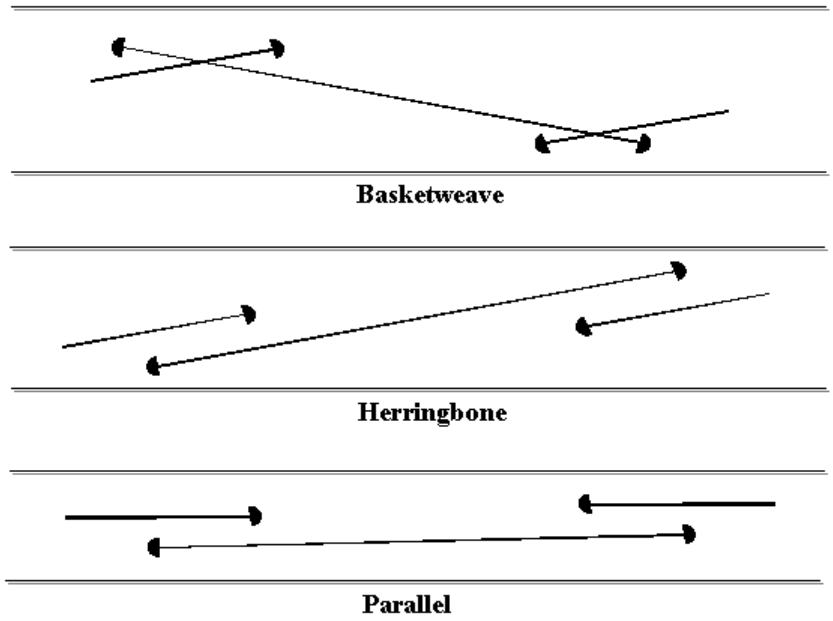
Figure III.6 shows the detection zones for the two types of microwave systems. Note that these detection zones are volumetric (e.g. shaped like a cigar, three-dimensional).

**Figure III.6: Detection Zones for Microwave Systems**




To respond to the detection zones, there are several types of installation patterns (see Figure III.7).

**Figure III.7: Microwave Installation Patterns**



Fence disturbance sensors come in many forms. They have the following characteristics in common:

- Passive
- Visible
- Terrain-following
- Normally installed on existing fence
- Line sensors
- Detect penetration or climbing of fence
- Types
  - Mechanical
  - Sensor Coil
  - Strain sensitive cable
  - Fiber optic

Some may be defeated by a very slow climb. These systems essentially turn the fence into a microphone. The system is "tuned" to alarm to specific types of input, such as the signature of a tool cutting a chain link, or a series of two or more vibrations. It is important to know the specifications of such systems, and to train persons who are testing these systems to use the right techniques.

Taut wire sensors may be freestanding or attached to the fence. These sensors are:

- Passive
- Visible
- Terrain-following
- Freestanding or attached to fence
- Line sensors
- Sensor fence section
- Types
  - Mechanical switch
  - Strain gauge / piezoelectric device

These sensors work on several operational principles: motion (often a mercury switch which is tripped by the low frequency movement of the fence; shock (detection is usually by a mechanical means); and analog (piezoelectric crystals, fence mounted geophones, electric or fiber optic cable.) Performance is affected by fabric tension, processor settings, rigidity of the fence, factors affecting noise coupling of the fence, and aids used by the intruder.

Video motion detectors (VMD) are being employed more frequently as the technology is refined and as costs decline. VMDs are:

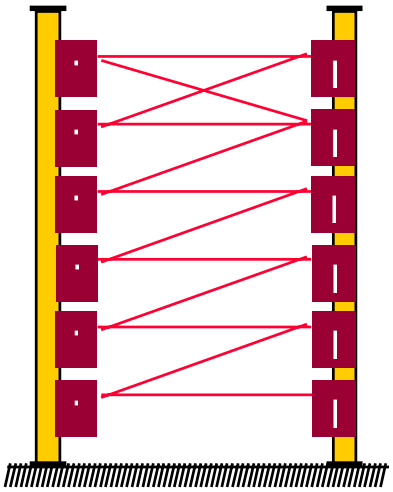
- Passive
- Covert
- Line-of-sight / terrain-following
- Installed with other video assessment equipment
- Line sensor / volumetric

Active Infrared (AIR) systems have the following characteristics:

- Active
- Visible
- Line-of-sight
- Detection zone (basically a vertical plane)
- Single or multiple beam systems

The probability of detection for AIR systems can be very high for multiple beam sensors, but the detection zone is usually narrow, high, and is not in contact with the ground.

**Figure III.8: Detection Zone for Active Infrared Sensors**

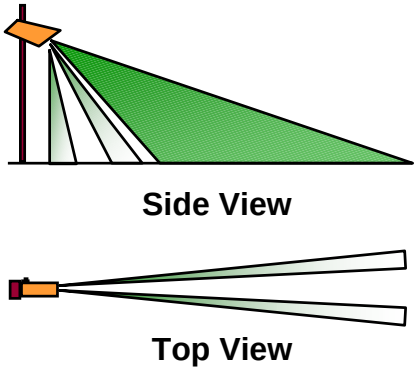


Passive Infrared (PIR) have the following characteristics:

- Passive
- Visible
- Line-of-sight
- Free-standing
- Volumetric
- Detect changes in infrared radiation within a specific field-of-view

PIR is most sensitive to movement across the field of view, and is sensitive to the velocity of the intruder (slow speed might evade detection.) The height and angle of the installation affect the probability of detection greatly.

**Figure III.9: Passive Infrared (PIR) Detection Zone**




Ported coaxial cable sensors are installed underground. The sensor is an electromagnetic sensor using 2-3 coaxial cables buried parallel to each other and a processor.

Ported coaxial cable sensors are:

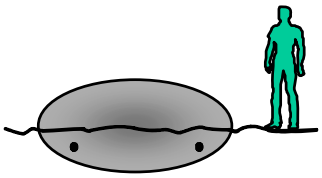
- Active
- Covert
- Terrain-following
- Volumetric
- Types
  - Pulsed
  - Continuous wave

Performance is affected by:

- Processor settings
- Orientation of intruder
- Soil characteristics (clay, sand, iron)
- Presence of metallic objects

Figure III.10 shows the detection zone for this type of sensor.

**Figure III.10: Ported Coaxial Cable Detection Zone**



Sandia National Labs has determined the relative probability of detection for these exterior sensor systems, as shown in Figure III.11.

**Figure III.11: Relative Probability of Detection- Exterior Sensor Systems**

| Intruder | Electric Field | Microwave | Active Infrared | Passive Infrared | Fence Motion | Taut - Wire | Ported Coax | VMD |
|---|---|---|---|---|---|---|---|---|
| Walking | VH | VH | VH | VH | N/A | N/A | VH | VH |
| Slow Walk | VH | H | VH | H | N/A | N/A | H | H |
| Running | VH | H | VH | H | N/A | N/A | VH | VH |
| Rolling | H | M-H | M-H | M-H | N/A | N/A | VH | VH |
| Crawling | VH | M-H | M-H | M-H | N/A | N/A | VH | VH |
| Jumping | VH | M-H | H | M-H | VH | VH | H | H |
| Tunneling | VH | VL | VL | VL | L | VL | M | M |
| Trenching | L | L-M | L | L | L | VL | VH | VH |
| Bridging | L | L | VL | L | VL | VL | L | L |
| Cutting | H | N/A | N/A | N/A | M-H | H | N/A | N/A |
| Climbing | H | N/A | N/A | N/A | H | H | N/A | N/A |

Key: VL - Very Low
L - Low
M - Medium
H - High
VH - Very High
N/A - Not Applicable

Source: Sandia National Laboratories

SNL has also estimated the susceptibility of each system to various types of nuisance alarms.

**Figure III.12: Relative Susceptibility to Nuisance Alarms**

| Environment | Electric Field | Microwave | Active Infrared | Passive Infrared | Fence Motion | Taut - Wire | Ported Coax | VMD |
|---|---|---|---|---|---|---|---|---|
| Wind<47km/h | L | VL | VL | VL | L | VL | VL | L-M |
| Wind 47-115km/h | M | L | L | L | H | VL | VL | L-M |
| Wind>115km/h | M | L-M | L-M | L-M | VH | L | VL | M |
| Rain | L-H | L | L | L-M | M | VL | M | L |
| Snow | M | L-M | M | L-M | L | VL | L | M |
| Fog | VL | L | M | L | VL | VL | VL | L-M |
| Small Animals (Rabbits) | M | M-H | M | M-H | VL | VL | VL | M |
| Large Animals (Dogs) | VH | VH | VH | VH | L | L | M | M-H |
| Small Birds | L | VL | L | L | L | VL | VL | M-H |
| Large Birds | M | M | M | M | L | VL | VL | M |
| Lightning | M | L-M | L | L | L | VL | M | L-M |

Key: VL - Very Low
L - Low
M - Medium
H - High
VH - Very High
N/A - Not Applicable

### c. Interior Alarm Systems

There are even more sensor technologies available for interior applications than there are for exterior use. Interior systems include:

- Balanced magnetic switches
- Glass break
- Photoelectric
- Microwave
- Ultrasonic
- Passive infrared
- Video motion detection
- Capacitive
- Fiber optics
- Vibration

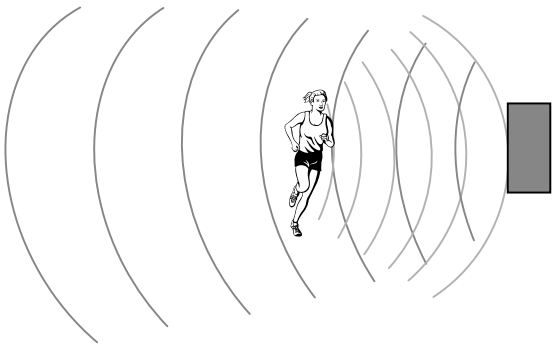
Boundary penetration sensors include magnetic switches (such as a door position indicator), glass break sensors, and photoelectric sensors. Photoelectric sensors provide line of sight protection and have a relatively long range. They are active systems that have low false alarm rates (FAR). The major types of glass break sensors are shock, frequency, shock/stress, and passive audio.

Interior motion sensors have a broader range of detection than boundary penetration sensors because motion sensors have volumetric detection zones. There are several types of interior motion sensors:

- Microwave
- Ultrasonic
- Video motion
- Sonic
- Infrared

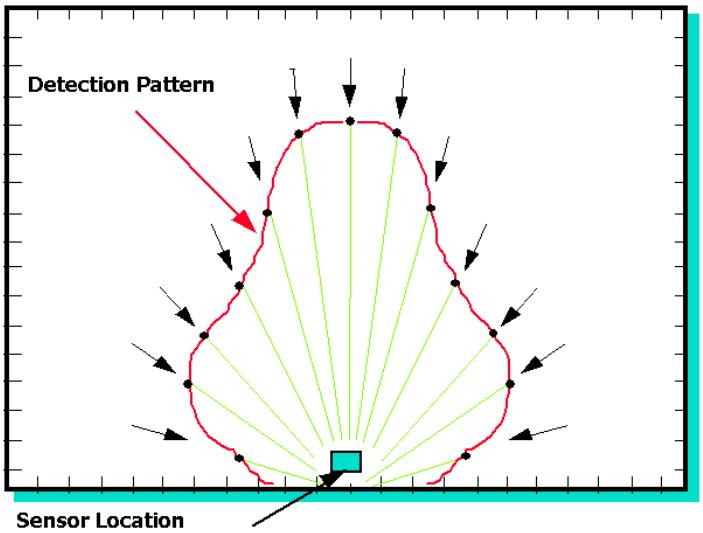
Microwave sensors transmit energy and monitor the return through a receiver. The motion of an intruder alters the pattern and frequency of the "return" and causes a shift in the frequency. If there is sufficient amplitude change and duration time, an alarm is sounded.

**Figure III.13: Microwave Sensor**



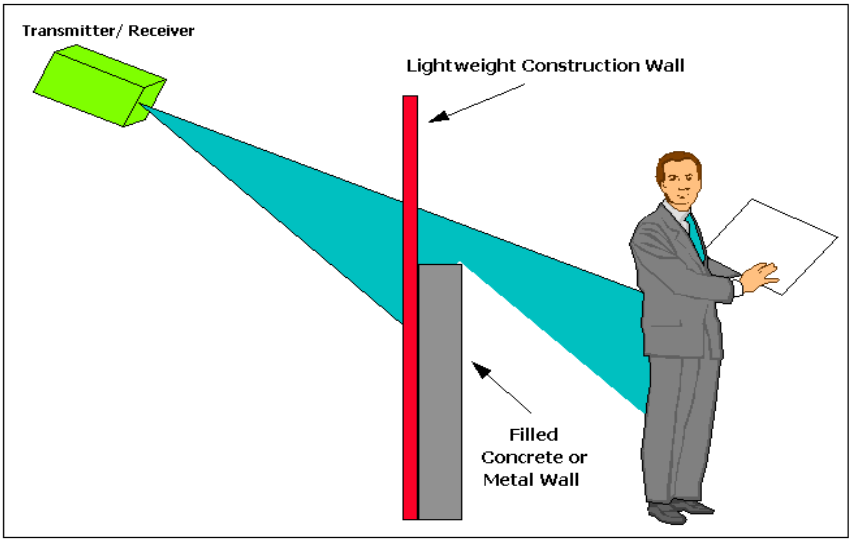
The detection pattern for a microwave sensor is shown in Figure III.14, which demonstrates for doppler effect.[4] The effectiveness of detection will vary with the direction an intruder is moving. For example, if an intruder is moving left to right on the diagram below, detection will be higher than if the intruder is moving in a line toward the sensor. And as with exterior microwave applications, time and mass trigger the alarm and a low fast crawl may sometimes defeat it.

**Figure III.14: Microwave (Monostatic) Doppler Detection Pattern**




A word of caution about monostatic microwave sensors: microwaves will *penetrate* walls and other barriers that are of light construction. This may result in false alarms when there is movement in an adjacent space. Figure III.15 depicts this characteristic.

**Figure III.15: Monostatic Microwave Penetration**

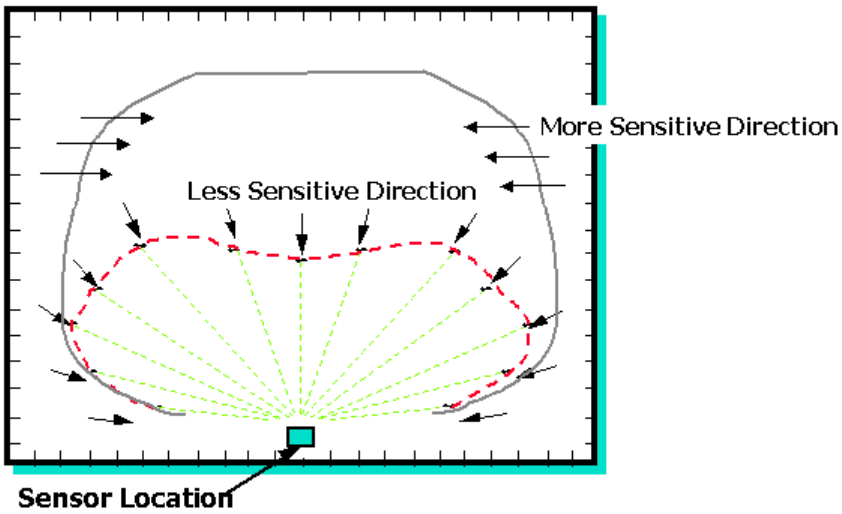



[4] The "doppler effect" means that the frequency and wavelength of an electromagnetic field is affected by relative motion.

Ultrasonic motion sensors are used in an active system that also provides true volumetric protection. The surveillance area for ultrasonic systems is defined by the walls, floor, ceiling and windows.

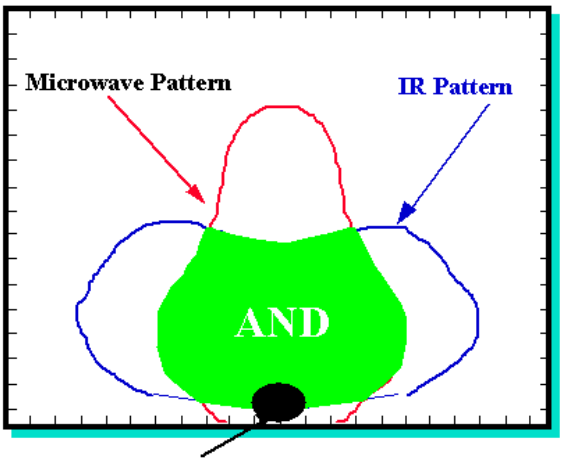
Passive infrared (PIR) detects by receiving infrared energy from objects. Ceilings, walls, floors, furniture and other objects emit infrared energy that is proportionate to their temperature. Motion is detected by measuring changes in the received infrared energy. Figure III.16 provides an example of the PIR detection pattern. As with the microwave sensors, detection is more sensitive for intruders moving across the detection area (left and right on the diagram below), while the least sensitive direction would be a path moving straight toward the sensor.

**Figure III.16: Sample Passive Infrared (PIR) Detection Pattern (walking at 1 foot per second)**




Combination sensors systems usually employ microwave *and* infrared. These systems allow for a higher sensitivity setting and reduce the incidence of false alarms (FAR). But the probability of detection is lower for these systems because the intrusion must be detected *twice*-- once by each type of sensor. Figure III.17 shows the detection pattern for a typical combination sensor system.

**Figure III.17: Combination Sensor System Detection Pattern**



**So many choices...which is "right?"**

There are no absolute right or wrong answers when considering detection systems. The goal is to find the system that works best for each unique application. It is also important to understand what each system can, and *cannot* do. Figure III.18 provides a comparison of the features of the various systems.

Another consideration in selection of the right system(s) is the consequence of component failure. A system that becomes inoperable when one component fails is less reliable than one that has redundant systems or equipment that can take over when a component fails. In some systems, aid from sources outside the institution is required to restore the component to a functioning condition.

**Figure III.18: Interior Sensor Selection**

| Applications | Operating Principle | Detection | | | | | Conditions for Unreliable Detection | Typical Defeat Methods | Major Causes of Nuisance Alarms | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Portal Opening | Breaking Through Wall, Floor, Ceiling | Radial Motion | Transverse Motion | Touching Object | | | Air, Humidity, Temperature | Localized Heating | Movement Outside Area | Fluorescent Lights | Loose Fitting Doors | Mount Vibration | Ambient Acoustic Noise | Rodents, Animals | Radio Freq Interference |
| Boundary Penetration | Balance Magnetic | + | | | | | Improper Installation | Stay-Behind Intruder or Entry Through Unprotected Area | | | | | - | | | | |
| | Vibration | | + | | | | | | | | - | | | - | | | |
| | Intrasonic | + | + | | | | | | - | | | | - | | | | |
| Interior Motion | Sonic | + | | + | + | | | | - | | | | | - | - | - | |
| | Ultrasonic | + | | + | | | Air Movement | Cover When Sensor is in Access Mode | - | | | | | - | - | - | |
| | Microwave | + | | + | | | RFI | | | | - | - | | - | | - | - |
| | Infrared | | | | + | | Variable Thermal Background | | | - | | | | - | | - | - |
| Proximity | Capacitance | | | | | + | Given Changes in Humidity, Temperature, or Pressure | Disable Electronics | - | | | | | | | - | |
| | Pressure Mat | | | | | + | | | | | | | | | | - | |

Source: Sandia National Laboratories

A good system for your application would have the following characteristics:

- *High* probability of detection ($P_D$)
- *Low* nuisance alarm rate (NAR)
- *Low* vulnerability
- *Fast* communication system
- *Good* lighting/assessment system
- *Balance* - a system approach
- *No* single point/component failure
- *Good* protection in depth

A *balanced* physical protection system provides adequate protection along *all* possible paths. Failing to consider all paths is like installing a highly secure lock on the front door of your house, but leaving the back door open.

The realities of institutional operations require that a balance is achieved between:

- Cost
- Safety
- Structural integrity

The EASI tool, introduced in Section II of this handbook, provides an excellent resource for modeling the impact of enhancements and improvements in your physical protection systems. EASI will help you to determine which approaches and systems reduce risk the most. Unfortunately, many of the upgrades provided for our institutions are prompted by tragedy and are funded in an effort to throw money at the problem rather than consider the complete picture. The EASI tool provides a more rational approach to system improvements.

### 2. Alarm Communication and Display

The preceding pages addressed methods and sensor systems that may be employed to detect intruders or other undesired events. For true "detection" to occur, each of the following steps must be complete.

**Figure III.19: Elements of Detection**

Several performance measures may be applied to the detection process, including:

- Probability of detection
- Time for communication and assessment
- Frequency of nuisance alarms
- Frequency of false alarms

Remember, alarm without assessment is not *detection*.

A sensor is useless if it is not able to communicate an alarm to the appropriate person or people. Figure III.20 presents a diagram of a typical traditional annunciator panel system, identifying the function of each component.

**Figure III.20: Traditional Annunciator Panel System**

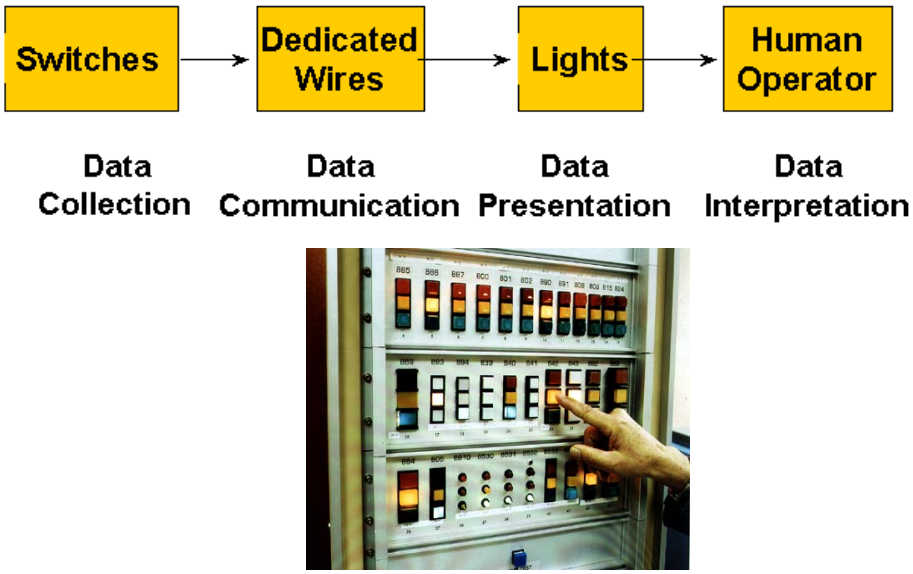



Figure III.21 shows the more modern integrated system.

**Figure III.21: Integrated Display and Assessment Systems**

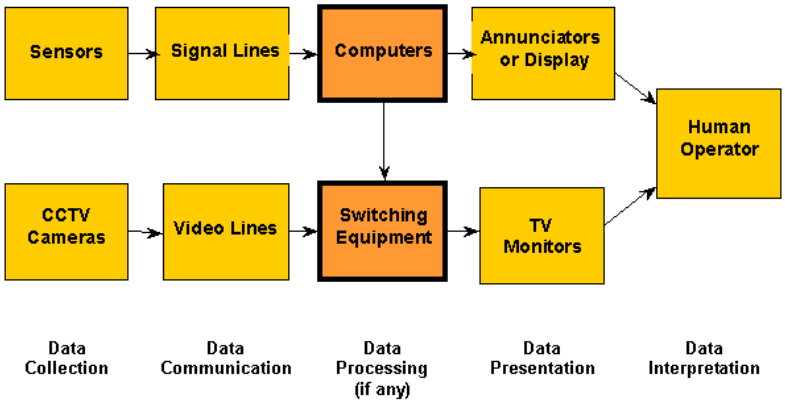



Figure III.22 provides a whimsical portrayal of what *not* to do. In this situation, which is often encountered in correctional facilities, the operator often turns off some of the alarms.

**Figure III.22: Alarm Overload**

What are the characteristics of a good alarm communication system? The preferred features include:

- Fast reporting time
- Supervision of all cables (cables not easily tampered with)
- Easy and quick discovery of single-point failure – redundancy
- Isolation and control of sensor
- Expansion flexibility

Common sense tells us that cables should be not be placed on the "threat side" of a sensor, where an intruder may have easy access to it. Similarly, alarms should be triggered if a cable or other communicating element, such as a cable, is disabled. Of course, redundancy is important whenever it is feasible.

There are many options available, and the choices are expanding as technology evolves. It is important to understand the unique characteristics of your site and installation.

Video systems are found in almost every institution, although there are many variations in their application and technology. The major components of a video system are:

- Camera, lens and mount
- Lighting system
- Transmission system
- Video switching equipment
- Video recorder (often digital now)
- Video monitor
- Video controller

A video system has many potential uses, including:

- Confirming that an electronic alarm is real
- Providing identification of what caused the alarm
- Providing general surveillance of an area
- Identifying people in the area
- Identifying unusual activity of any kind in the area

Consoles also vary, but usually display the following information:

- Zone status (secure, access, alarm)
- Assessment information
- Procedural instructions
- System status
- Alarm history

Information may be displayed as text, graphics, or as a combination. Many new systems use touch screens or a computer mouse.

Typical operator functions include:

- Start and end assessment of alarms
- Set individual sensors into access or secure
- Open and close doors/buildings
- Display system status
- Request procedural instructions
- Assign CCTV cameras to video monitors
- Start and stop recording
- Examine system log

As with sensors, *redundancy* is important. This might involve backup equipment and procedures or duplicate consoles. Emergency power supply and an uninterruptible power supply for computers are essential.

### 3. Entry Control and Contraband Detection

The following text and diagrams provides an overview of entry *and exit* control and contraband detection systems, explores various types of badges, and examines the characteristics of contraband detectors.

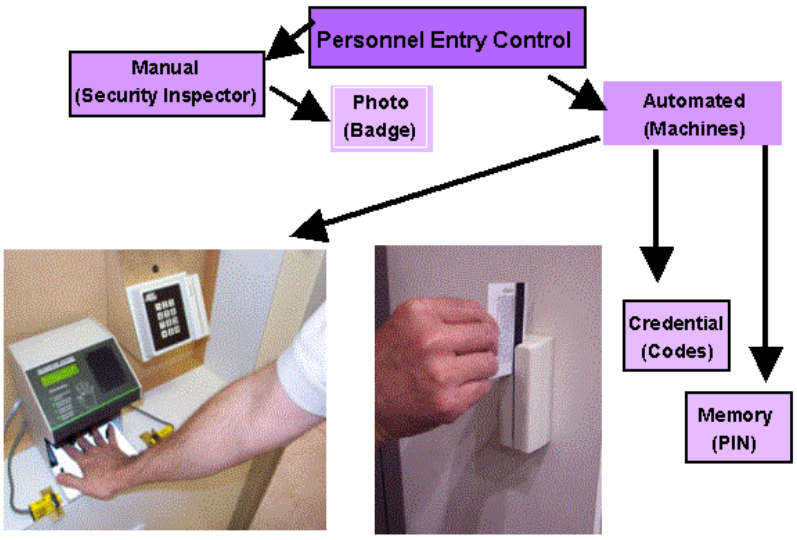
The purpose of entry control is to:

| | |
|---|---|
| To allow entry of: | authorized people<br>authorized material |

| | |
|---|---|
| To allow exit of: | authorized people<br>authorized material |
| To prevent entry of: | unauthorized people<br>weapons and other contraband |
| To prevent exit of: | unauthorized people |

Figure III.23 shows the various types of entry control systems.

**Figure III.23: Entry Control Systems**




Several types of badge technologies may be found in correctional institutions, including:

- Photo identification badge
- Bar code technology
- Magnetic stripe technology
- Wiegand technology[5]
- Proximity card technology
- Smart card technology

Any badge system is concerned with the ability to counterfeit. Figure III.24 describes the ease of counterfeiting for several types of coded badges.

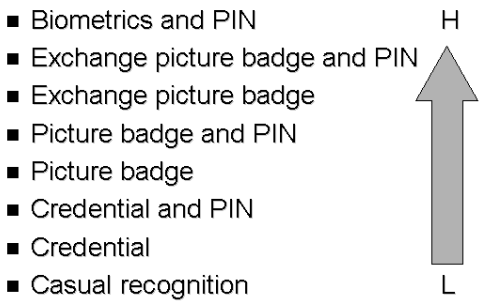
[5] Wiegand technology is a proprietary card system that is very difficult to duplicate

**Figure III.24: Ease of Counterfeiting Coded Badges**

- Proximity read ↓ difficult
- Direct read
  - Magnetic stripe ↓ easy to difficult
  - Bar code ↓ easy
  - Wiegand wire ↓ average
  - Smart card ↓ difficult

Similarly, the probability of detection for counterfeit badges has been calculated by Sandia National Laboratories.

**Figure III.25: Relative Probability of Detection of Counterfeits**




Biometric systems include hand, thumbprint, facial, retinal and iris scan technologies. A PIN is a personal identification number that is assigned to an individual. In a Texas institution, persons wishing to enter the facility are required to pass their identification and credentials into a control center to be examined by a staff member. One institution in Ohio has a video camera system that projects an image of each ID badge onto a 13-inch monitor, making it easier to identify counterfeits. All too often, the persons responsible for checking identification are so busy that they give only a cursory glance, or sometimes do not even look at all.

There is often a temptation for personnel to move fast. When lines get long and visitors and personnel become impatient, it is only natural to try to speed up the identification process. While speed was an ally when it came to communicating alarms, it is an adversary to proper entry and exit security practices. Personnel must know that they have permission, or better yet are *expected*, to take the necessary time to ensure the proper identification of every person who enters and exits the institution. Good security is not necessarily *convenient*.

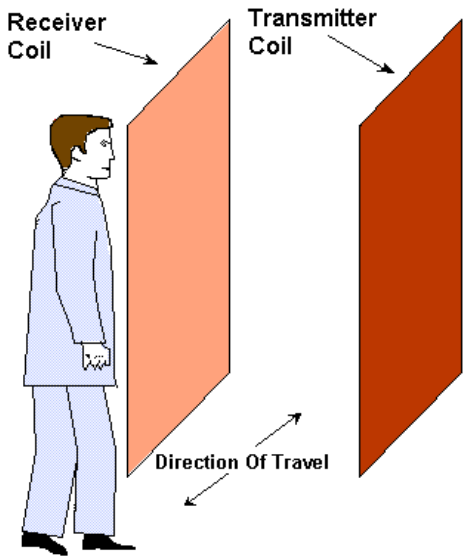
<u>Contraband detection systems</u> fall into three major categories:

- Metal detectors
- X-ray techniques
- Emerging “sniffer” technologies

Selecting contraband detection systems, and specific devices, requires consideration of their corresponding principles of operation, sensitivity factors, and placement considerations.

Metal detectors have a transmitter coil and a receiver coil, as shown in Figure III.26.

**Figure III.26: Coil Geometry for Typical Pulsed Field Metal Detector**



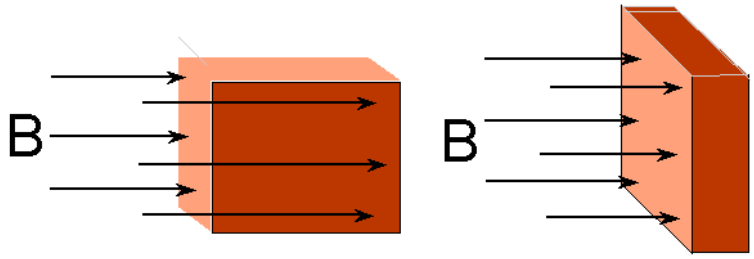

Many factors have an influence on the effectiveness of metal detectors.

- **Detector itself** (how it is programmed, its settings)
- **Objects** (weapons, personal possessions)
- **Object characteristics** (size and shape, orientation to coil, type of metal)
- **Subject walking through** (velocity, location of object on the person)
- **Environment/setting** (nearby metal, electromagnetic background such as flourescent lights, floor buffer)

Metal detectors are often defeated, deliberately and accidentally. Unfortunately, inmates often watch as the detectors are defeated. It is important that personnel who operate metal detectors are thoroughly trained and are closely supervised.

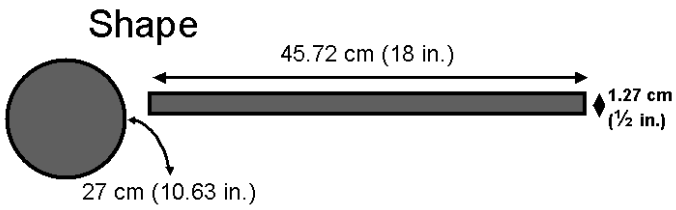
It may help to think of the metal detector as a series of arrows that go from the transmitter coil to the receiver coil. The amount of *area* that is presented to the detector will influence how well the object is detected. In Figure III.27 shows six imaginary “arrows” that represent the direction of the field in a metal detector. When the box on the left is passed through the field only three of the arrows “hit” it because it is turned sideways. But all six arrows hit the box when it is turned to face the field, as shown on the right.

**Figure III.27: Importance of Orientation of Object**



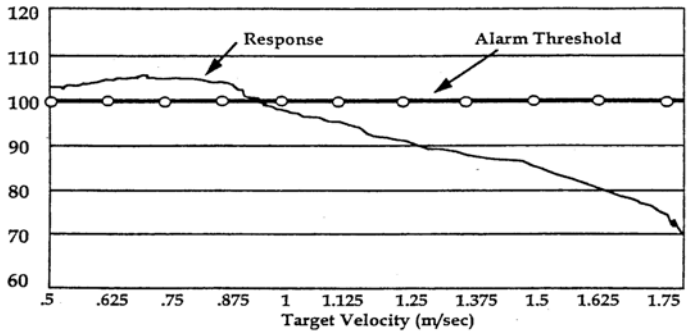

Similarly, the *shape* of an object will have a significant effect on the probability of detection. Figure III.28 shows two objects that have equal areas. But the circle is three-times easier to detect because of the shape it presents to the detector.

**Figure III.28: Effect of Shape on Detection**




Finally, the *velocity* at which an object passes through metal detector will also affect the probability that it is detected. Figure III.29 shows the relationship between the speed at which an object passes through a detector and its ability to be detected. The graph shows that once an object is traveling at about 1 meter per second or more, it is unlikely that it will be detected. Some persons will try to defeat a metal detector by taking a "big step" into it and moving through quickly. In response to these attempts to evade detection, some institutions require subjects to turn around while in the detector.

**Figure III.29: Velocity of Object vs. Detection**

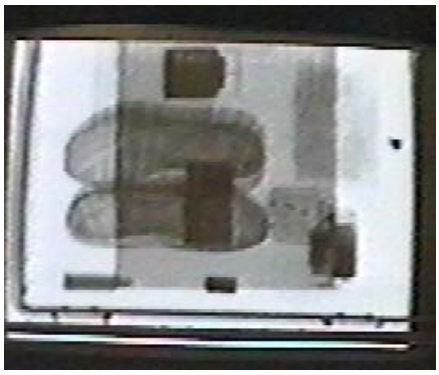



The location of the object on the person will also affect the chances it will be detected. Metal detectors may be adjusted to focus more on certain areas. It is not unusual to find that little

detection occurs in the lower area of the field. Smugglers have been known to tape metal tins with drugs to their ankles in an effort to evade detection. Similarly, weapons such as small guns or knives are often less detectible if carried very low.

X-Ray machines provide another resource for contraband detection. X-rays may be used to detect other objects, in addition to metal. For example, the two images in Figure III.30 are of the same bag. The one of the right uses backscatter technology, and it identifies explosives in the back as light colored areas on the screen.

**Figure III.30: Backscatter X-Ray Image**

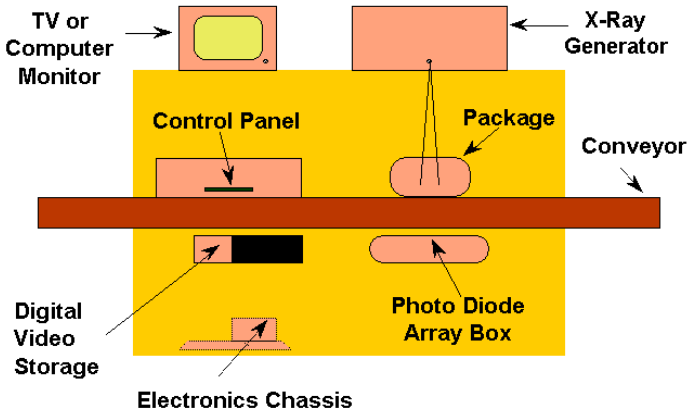


Regular X-ray

Backscatter X-ray image

A typical X-ray package search system is shown in Figure III.31. X-ray machines are capable of imaging a 26-gauge wire hidden in a test wedge, when properly operated. Personnel who operate this equipment must be well-trained and should have short duty periods to prevent loss of detection efficiency due to fatigue.

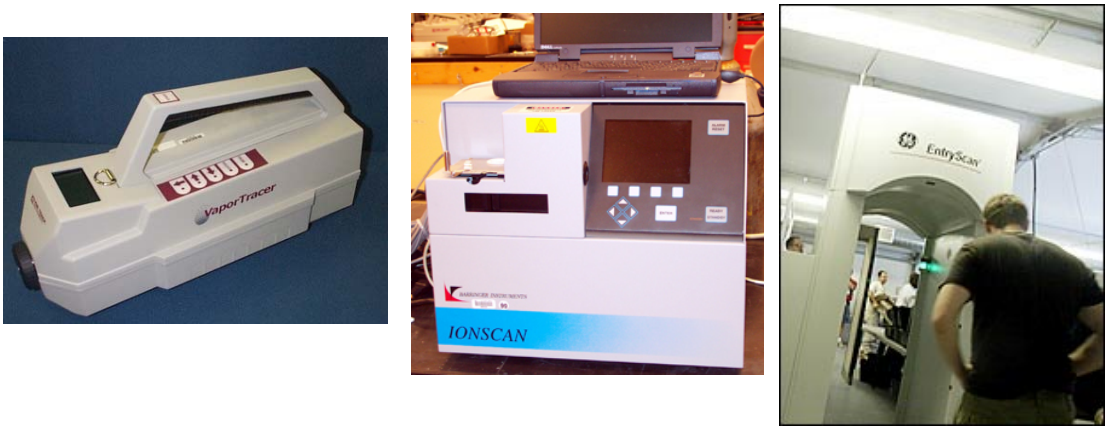
**Figure III.31: Typical X-Ray Package Search System**




Sniffer detectors represent a fast-evolving technology that is appearing in airports and other locations. Hand-held sniffers were initially developed for field applications. A bench model version may often be seen in airports, where personnel use a pad to wipe down surfaces of a

traveler's baggage and then insert the pad for analysis. Several airports now have sniffer "portals" that look somewhat like telephone booths. The subject steps into the portal and the doors close. The portal employs a "preconcentrator" that works by drawing in a large volume of air, collecting heavy organic compounds from the air stream onto a filter, then vaporizing these organics into a smaller parcel of air that is delivered to a commercial explosives or drug detector. Figure III.32 shows the three types of sniffers.

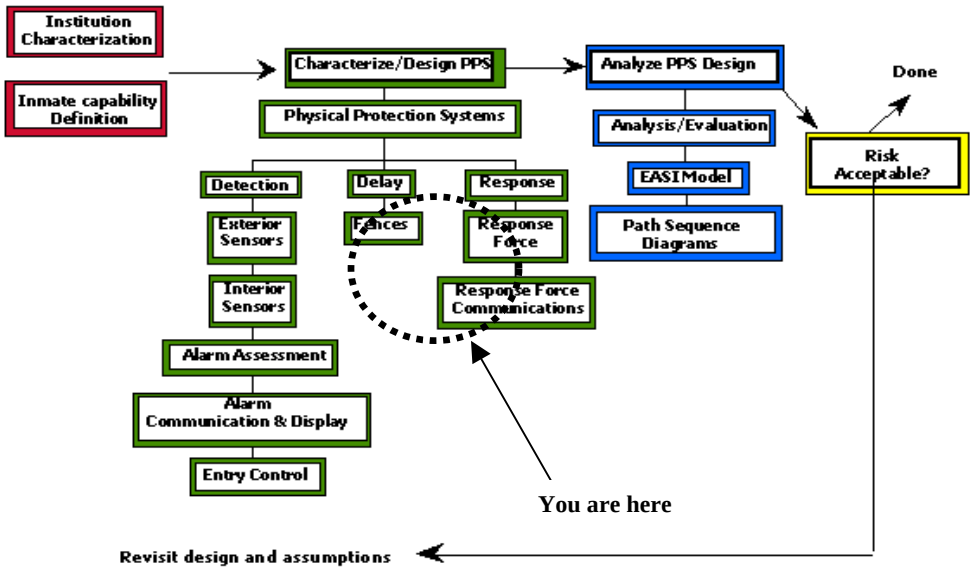
**Figure III.32: Three Types of Detectors Using "Sniffer" Technology**




## 4. Delay

Having examined detection methods and technologies in some detail, it is time to turn to the next two elements of physical protections systems (PPS). Figure III.33 shows the overall risk evaluation process and highlights our current position.

**Figure III.33: Risk Evaluation Process**



The checklists in Appendix D help to identify the delay features in your institution. These include, but are not limited to:

- Fences and gates surrounding the facility
- Vehicle barriers
- Construction of walls/windows/doors/roofs/floors
- Areas where detection is not provided before delay
- Areas where there are multiple layers of delay exist, i.e. locks, windows, walls, distance, fences, and razor wire

Sandia National Laboratories has tested a variety of delay and detection systems. Their findings are integrated into the EASI program spreadsheets, as a "lookup" function. Figure III.34 provides sample of their findings.

**Figure III.34: Sample of Data Collected for Physical Protection System Components.**

| General Task | $P_D$ and Delay Time |
|---|---|
| Climb 14 ft. fence | 20 second delay (climbing) |
| Running with equipment | 10 feet per second |
| Cut 1 ¾" carbon steel bar with hacksaw | 30 seconds per bar |
| Cut hardened bars with hacksaw | 60 minutes per bar |
| Penetrate cell door without tools | Infinite |
| Penetrate Metal core door | 12 second delay per door |
| Microwave exterior detection system | 0.9 probability of detection |
| Tilt / vibration fence sensor | 0.8 probability of detection |
| Detectors on building doors | 0.99 probability of detection |
| Interior detector | 0.9 probability of detection |
| Standard deviation on all times | 30% of mean |

# PART IV. PLANNING AND IMPLEMENTING A CVA

## A. Managing the CVA Project

It is important to remember that a corrections vulnerability assessment is a *project*. A successful project requires:

- An understanding of organizational requirements
- A specific goal
- Objectives to achieve each goal
- A defined scope
- A work structure

This handbook is built on the concept of a team approach to the CVA. This approach:

- Ensures delegation of responsibility
- Provides a diversity of knowledge, skills and experience
- Provides the levels of expertise needed
- Promotes ownership (especially when local facility staff are on the team)
- Speeds up the process

As you plan the CVA you will need to answer the following questions:

- Who are the clients?
- Why is the cva being requested?
- What improvements are needed?
- Are there sufficient resources to conduct a CVA (staff time, equipment, etc.)?

Conducting an effective CVA requires a strong commitment from to top down. It will demand a great deal of effort from the core team and the on-site team. Facility staff will be required to assemble a great deal of information and data. Staff efforts will be needed throughout the on-site stage of the CVA.

In addition to the considerable personnel costs that can be expected, there will also be transportation and travel expenses, and possibly funds for the acquisition of needed equipment and supplies.

While considering the costs and commitment associated with a CVA it will be necessary to determine the scope of the activity (e.g. the entire facility or only a few selected units). Scheduling will also be a consideration, to ensure adequate time for the site visit, analysis, report generation, and post-CVA activities.

## B. The CVA Timeline and Tasks

Conducting a corrections vulnerability assessment in the context of a state corrections department offers many opportunities and benefits. The Pennsylvania Department of Corrections pioneered the application of the EASI methodology in corrections, developing and implementing

the use of CVA's throughout the state. Colorado was the second state to embrace the CVA tool. The Colorado Department of Corrections benefited from the Pennsylvania experience, but also developed its own variations and innovations.

Appendix J presents a detailed flowchart that describes all of the elements of a CVA conducted in a state corrections department. The chart shows the tasks, their relationships and timing.

The process is divided into three major phases:

1. Pre-site visit activities
2. Site visit
3. Post-site visit activities

Phase One: Pre-Site Visit Activities

There are several tasks that must be implemented before the CVA site visit. These are described in Figure IV.1. The Phase One tasks involve:

- Defining the scope of the assessment
- Visiting the target site to make preparations
- Creating the CVA team
- Starting the information and data collection process
- Defining the threat

The "core team" refers to a small group of corrections officials who have been trained and authorized to schedule and implement corrections vulnerability assessments. "Local site contacts" are individuals at the target correctional facility who have been designated to coordinate with the CVA team. This team is usually based in the department's central office, or at least has one member at that location.

"Local site personnel" are other individuals at the target correctional facility that will directly and indirectly contribute information and assistance to the process.

**Figure IV.1: Phase One, Pre-Site Visit Activities**

| **What?** | **Who?** | **When?** | ***Resources* Needed** |
|---|---|---|---|
| **PHASE 1** | | | |
| Initial Definition of Assessment | Core team | After initial site visit | -Sample definition report<br>-Checklist of issues to be considered<br>- Identifying stakeholders, including legal/risk managers, others |
| Evaluation of Resources | Core team<br>Corrections officials | After definition has been submitted | - Determine if a CVA is feasible |

| | | | |
|---|---|---|---|
| Initial site visit to facility (reconnaissance) | Core team<br>Local site contacts | After it has been determined that there are sufficient resources (staff, equipment, etc.) | - Site visit checklist<br>- Guidelines for scheduling (how long to prepare, how much time to plan on site) |
| Create assessment team | Core team | Following site reconnaissance | |
| Orient assessment team | Core team | As soon as members are confirmed | -Orientation materials for non-core assessment team members |
| Create Pre-Assessment Data Collection Lists and Instructions | Core team | ASAP after recon visit | -Guidelines, checklists and tips for pre-site visit preparations |
| Define Primary Threat | Core team | Prior to site visit | - How to define threat(s)<br>- Sample threat definitions |
| Site Data Collection and Preparations | Local site personnel | Prior to site visit, after list received | - Tailored list of data and information from core team<br>- Samples and instructions for generic activities (NAR, FAR and such) |
| <u>Assemble Materials and Prepare for Site Visit</u><br>- Assemble materials provided by site<br>- Develop battle plan/assignments<br>- Develop checklists and aids | Core team | Prior to site visit | - Guidelines for preparing for site visits<br>- Sample site visit schedules and plans<br>- Tips and contingencies |

Many of the resources needed for Phase One are provided in Appendix B. Other resources are found throughout the text of this workbook.

A key element of the Phase One involves what is sometimes called a "scoping briefing." The purpose of this briefing is to:

- Reach an understanding and general agreement on the scope of the CVA and major assumptions, and
- Ensure that all parties concur with the "framework" of the CVA

The briefing should involve all of the major CVA stakeholders. It will necessarily address the assumptions associated with CVA, including:

- What is and what is not included in the analysis
- The "snapshot in time" to be used for the analysis

- How dynamic events will be factored in

These assumptions should be clearly documented.

Phase Two: Site Visit

The site visit is the most complex phase of the CVA. It involves a great deal of coordination among all of the team members. As Figure IV.2 shows, there are several "rounds" of assessment activity. With each round of site work, the team narrows its focus and deepens its examination.

**Figure IV.2: Phase Two, Site Visit**

| What? | Who? | When? | Resources Needed |
|---|---|---|---|
| **PHASE 2: Site Visit** | | | |
| Assessment team initial meeting, prior to going to the site (as needed) to meet each other, receive training and orientation, identify strategies and issues | Core team and all assessment team members | Before going to site (meet near site at hotel or similar neutral location) | All site assessment protocols, schedules, lists, and materials |
| Initial meeting on site.<br>Go over logistics, authorizations, identification, and such | All assessment team members<br>Key facility officials and personnel | First day on site | Initial meeting checklist and guidelines<br>Potential contingencies and solutions |
| Assessment team meeting on site.<br>Create task groups, give out assignments and materials<br>Provide orientation and training as needed | First day on site | Assessment team | Task group assignments<br>Task group assessment materials<br>Guidelines for creating task groups and conducting initial assessment activities<br>Contingencies and solutions |
| ROUND ONE: Task groups conduct initial research and diagramming in their assigned areas<br>Map each assigned area to identify ALL logical paths, prepare path sequence diagrams (PSD) for each potential path, identifying descriptors of conditions (time of day, events such as lock down, etc.)<br>Identify variations for each PSD (don't focus on feasibility at this point--just be sure to identify all | Each task group | Afternoon of first day, or morning of second day | Protocols and instructions for each task group<br>Instructions for mapping paths and samples<br>Checklists and shopping lists to assist in defining conditions and variations |

| | | | |
|---|---|---|---|
| potential paths<br>Be skeptical-- "humor me- let's take a look" | | | |
| <u>Initial processing</u> of PSDs<br>Describe each PSD, and evaluate as a full team<br>Identify missing paths, missing information<br>Discard, with justification, PSD as appropriate based on team evaluation | Entire assessment team | Second day on site | Guidelines for initial critique of PSDs.<br>Samples of PSDs and variations<br>Checklist of questions to ask about PSDs |
| ROUND TWO:<br>Task groups go back into the field to further evaluate PSDs that are still under consideration according to the full team<br>Task groups identify and describe, in detail, the actual characteristics of every element of surviving PSDs--<br>- what is actually there, e.g. doors, locks, times to traverse, methods of detection<br>* detection (and reliability)<br>* delays (and time frames)<br>* assessment/ID (accuracy)<br>Identify weakest points/routes | Each task group | Second day on site | Guidelines for describing characteristics of PSDs<br>Checklists<br>Samples-- lots of samples |
| <u>Further processing of PSDs.</u><br>Full team reviews findings of each task group. Evaluates each and identifies additional PSDs to discard, missing data, variations to consider | Full team | Third day on site | Guidelines for evaluating PSDs<br>Potential criteria for analyzing and improving PSD |
| ROUND THREE<br>Each task group returns to the field to further refine surviving PSDs<br>Conduct testing as needed<br>Collect further data as needed | Each task group | Third day on site | Instructions for conducting testing on site<br>Samples of tests and results<br>Benchmark values for generic features (fences, walls, etc.) |
| <u>Final Processing of PSDs</u><br>Full team reviews each task group's findings, evaluates and discards as appropriate<br>Group works on surviving PSDs<br>Worse case scenarios selected<br>Probability of success is | Full team | Fourth day on site | Guidelines for selecting worse case scenarios<br>Formulas and instructions for calculating probability of success (or interruption)<br>Samples |

| | | | |
|---|---|---|---|
| calculated, as possible<br>*(if needed, additional field work is conducted until the full team is confident in findings)* | | | |
| Identify and describe full range of measures that could be implemented to reduce risk (operations, technology, facilities). As needed, describe "solution sets" of related measures that are interdependent.<br>Identify cost/benefits as possible | Full team | Fourth day on site | Shopping list of potential solutions<br>Checklist of considerations<br>Samples, including solution sets |
| Assemble draft assessment report | Full team | Fifth day on site | Guidelines for creating assessment report<br>Sample report<br>Checklist of elements and considerations |
| Conduct close out meeting with facility officials and staff | Full team<br>Local officials and staff | Fifth day on site | Guidelines for conducting a closeout meeting<br>Contingencies and solutions |
| Final full team meeting<br>Assign final report responsibilities<br>Debrief and self-evaluate<br>Identify deficiencies, needs, improvements for the next time | Full team | Fifth day on site (before leaving site--could be off site in hotel or other neutral location) | Debriefing and self evaluation guidelines and tips |

As the CVA process narrows its focus to a few scenarios, it is important to ensure that none of the findings are discarded, even if they do not refer to the final scenarios. Throughout the site visit, team members should identify *all* concerns and keep a running log of them. Why? Because many serious issues are identified apart from the scenarios. Also, something that might not be a part of a viable scenario day could become a part of a future scenario.

During one CVA training session, several serious safety and security issues were identified. Many of these were not reflected in the final scenarios, but they were highlighted by the team as part of the final report. For example, the team discovered that certain type of entry lock may be disabled by an inmate while he/she is walking by it. This was called out as a separate finding in the report and the facility made immediate changes in response.

Phase 3: Post Site Visit

It will be tempting to take a rest after your arduous days on site, but the momentum should not be allowed to slow. The core team will need to press forward to complete the final report.

## C. CVA Report

The core team should refer to the sample report that is provided in Appendix L. Much of the text from this handbook might also prove useful, and readers are encouraged to draw from it, with attribution.

The final report should be submitted to the department, as determined when the initial CVA was planned. Of course the facility should receive a copy, preferably at the same time. In some instances, the facility administrator might be offered the opportunity to review the final report first, or even to review a draft.

Colorado's CVA Report Format

In Colorado, the CVA report consists of eight segments that describe the "systematic evaluation" of observations made by the Assessment Team, conclusions reached, and obtainable recommendations to correct or resolve an issue. Their reports include:

1. **C**over
2. Introduction Letter
3. Executive Summary
4. Project Description
5. Facility Overview
6. Scenarios
7. Observations and Suggestions
8. Conclusion

The cover indicates the state and facility where the assessment was conducted, the dates of the assessment, and the names of the individuals who contributed to the reporting process.

The introductory letter includes the date, the assessment team members (who should be the authors of the letter), the date, and the name of the target facility. It should be addressed to appropriate executive staff and should indicate all of the entities who initially received copies of the report.

The Executive Summary provides a list of tasks the Team completed. For example:

- Executive staff selects a team leader and assigns team members from various facilities.
- The CVA Team visits the site to conduct a preliminary meeting with the facility's management team to understand and define the project objectives and to become acquainted with the facilities policies, procedures and areas of concerns.
- The Team leader assigns tasks and roles to the team members.
- The Team members disperse throughout the site and observe the areas and complete their tasks.

- The CVA Team gathers together and discusses their observations, writes the observations, documents the observations and creates path sequence diagrams that describe how offenders could defeat the existing security system.
- The CVA Team defines the scenarios that could result in offender escapes.
- The CVA Team conducts a limited scope exercise to test specific features of the Physical Protection system and to gather additional pertinent information. The objective is to simulate parts of the scenario and to attempt to defeat the security system in selected vulnerable areas without interrupting security or safety requirements.
- The CVA Team analyzes the results of the scenarios.

The project description provides specific details of the objectives of the Assessment Team, such as:

- Access and egress points
- Ttool control
- Detection systems
- Perimeter fences

The facility overview describes the facility, identifies the procedures and operations reviewed during the CVA, describes the perimeter description and other areas observed, and includes many illustrative photographs.

The section on scenarios provides a detailed account of each scenario conducted, including:

- Conditions
- Analysis
- Copy of an EASI file

The section on observations and suggestions provides a detailed description of each observation from the Team. It should also provide a suggested resolution to each and every observation from the Team. In Colorado, an observation from the Team is *never* reported without a corresponding suggestion as to how the facility may correct or address any issue. It may also be advisable to note that many-- if not most-- of the suggested solutions and improvements may be implemented at no- or low-cost.

In the conclusion, the process should be described, including comments that:

- Acknowledge that the process designed to focus on the negative
- Affirm that the CVA is used as a tool to detect, analyze, evaluate and correct deficiencies
- Describe how the Team perceived the facility and the offender population
- Commend staff who performed in an exceptional manner
- Identify ways in which staff are recognized for exemplary performance
- Identify concerns already being addressed by facility staff
- Compliments the facility appropriately

## D. After the CVA Is Complete

In many ways, completion of the CVA and submission of the report is only the beginning. The facility, working in concert with the regional/central office, should develop an action plan that identifies the steps that will be taken to address the issues identified in the CVA, and to implement lasting solutions to identified problems.

### Liability

The liability discussed earlier in this section should be a continuing concern. Failing to effectively address identified problems will increase liability. Every official, at all levels, should do everything within his/her power to act effectively to make improvements. The facility should be sure to address *every* issue and vulnerability that was identified through the CVA. These will include the elements of the scenarios, and also the various findings and observations that were not attached to specific scenarios.

### Policies and Procedures

The CVA will likely identify instances in which current facility policies and procedures are inadequate. In some instances the procedures will be incorrect; in others, procedures might not go far enough. The need for additional policies and procedures will also be identified through the CVA. One of the first steps after completion of the CVA is to examine all policies and procedures, to make revisions as necessary, and to develop new ones as needed.

### Training

The CVA benefits training in several ways. First, everyone who was directly involved with the CVA will have received invaluable training and insights. It is likely that their perspectives will be changed for the better. Second, facility staff members who observed CVA activities and learned about the findings will also benefit and they will be more receptive to subsequent training activities. Finally, the CVA findings should be incorporated into ongoing facility training activities. Many of the deficiencies that will be identified by a CVA may be addressed by enhanced staff training.

### Supervision

Just as many deficiencies may be addressed through training, most of these and possibly additional deficiencies, may be addressed by improved supervision activities. The American Correctional Association (ACA) has recently developed important new tools through the creation of “performance-based” standards and practices. The ACA performance-based template has several elements associated with each “expected practice.” These include:

- *Protocols,* such as policies and procedures, training curricula, that describe in writing what is to be done
- *Process indicators* that identify methods to determine, on an ongoing basis, if practices are being properly implemented (an excellent supervisory tool)
- *Outcome measures* that guide the collection and analysis of data and information to determine if practices are producing the desired results

The ACA process indicators are an excellent resource to help improve continuing efforts to supervise correctional staff.

Data and Information

The CVA will have benefited from the collection and analysis of various types of data and information. After the CVA, data collection activities should at least continue, if not expand. Also, there were likely many instances in which data and information were not available, and the CVA was diminished as a result. These should be addressed as part of the post-CVA activities. The ACA outcome measures should also be considered as a new tool to help determine the extent to which desired results are being realized.

Testing

The CVA will spotlight the need to improve ongoing efforts to test elements of the physical protection system. The lessons from the CVA should be translated into improved testing practices.

Audits

Finally, the CVA will suggest ways in which audits may be enhanced to be more comprehensive and effective.

Summary

The benefits of a CVA are many and varied. While improvements might be made during, and immediately after the CVA process, the real value of a CVA will be measured in the changes that are made and implemented over the long term.

==========

# APPENDICES

**Appendix A: Sample PSD's and EASI Results**

**Appendix B: Checklists for Characterizing the Institution (Step 1)**

**Appendix C: Threat Capability Checklists (Step 3)**

**Appendix D: Physical Protection System Checklists (Step 4)**

**Appendix E: Protocols and Practices**

**Appendix F: Data Collection Forms (entry control, delay)**

**Appendix G: Performance Data**

**Appendix H: PSD Checklist**

**Appendix I: Acronyms and Selected EASI Formulas**

**Appendix J: CVA Flowchart**

**Appendix K: A Step-by-Step Guide to Using the EASI Program**

**Appendix L: Sample CVA Report**

**Appendix M: Printouts of Powerpoint Presentations (complete CVA training program)**

## Supplementary CD-ROM:

Files with handbook, appendices, EASI program, and the complete powerpoint training program.