SAN098-2408C

Assessing the Security Vulnerabilities of Correctional Facilities

Debra S. Spencer[a], G. Steve Morrison[b]

[a]Sandia National Laboratories, P.O. Box 5800, Albuquerque, NM 87185-0762
[b]National Law Enforcement and Corrections Technology Center, Southeast Region, 7325 Peppermill Parkway, N. Charleston, SC 29418

ABSTRACT

The National Institute of Justice has tasked their Satellite Facility at Sandia National Laboratories and their Southeast Regional Technology Center in Charleston, South Carolina to devise new procedures and tools for helping correctional facilities to assess their security vulnerabilities. Thus, a team is visiting selected correctional facilities and performing vulnerability assessments. A vulnerability assessment helps to identify the easiest paths for inmate escape, for introduction of contraband such as drugs or weapons, for unexpected intrusion from outside of the facility, and for the perpetration of violent acts on other inmates and correctional employees. In addition, the vulnerability assessment helps to quantify the security risks for the facility. From these initial assessments will come better procedures for performing vulnerability assessments in general at other correctional facilities, as well as the development of tools to assist with the performance of such vulnerability assessments.

Keywords: vulnerability assessment, correctional facility, detection, security.

1. INTRODUCTION

The National Institute of Justice (NIJ) has an interest in devising better procedures and tools for helping correctional facilities assess their security vulnerabilities. Under this charter, Sandia National Laboratories (SNL) in Albuquerque, New Mexico and NIJ's National Law Enforcement and Corrections Technology Center, Southeast Region (NLECTC-SE) in Charleston, South Carolina are visiting selected correctional facilities and performing security-related vulnerability assessments. This paper will describe this process and the lessons being learned.

2. ACKNOWLEDGEMENTS

Both SNL and NLECTC-SE are supported in the efforts described in this document by NIJ. NLECTC-SE is supported under Cooperative Agreement #97-MU-MU-K020 between the Department of Justice and the South Carolina Research Authority. SNL is supported under Interagency Agreement #97-LB-R-004 between the Department of Justice and the Department of Energy.

3. PARTICIPANTS

3.1 NLECTC-SE

The National Institute of Justice, responding to recommendations of the law enforcement and corrections communities, established the National Law Enforcement and Corrections Technology Center (NLECTC) System in 1994 as a component of NIJ's Office of Science and Technology. NLECTC's goal, like NIJ's, is to offer support, research findings, and technological expertise to help state and local law enforcement and corrections personnel.

NIJ's NLECTC system consists of facilities located across the country. Each facility is co-located with an organization or agency that specializes in one or more specific areas of research and development. Although each of the NLECTC facilities has a different technology focus, they work together to form a seamless web of support, technology development, and information to help the law enforcement and corrections communities do their job more safely and efficiently.

The NLECTC-SE region has the primary corrections technology thrust for NIJ and during the past several years has been involved in projects such as the following.

DISCLAIMER

- Corrections Vendor Database: Currently under development, this database will provide corrections officials with a source of information about products and services. The database will highlight vendors' capabilities, whether their products have been tested by a national laboratory or in a pilot test at a correctional facility. It will also identify at least five correctional agencies that currently use the product or service, complete with agency name, telephone number, and a point of contact at the facility. This provides the potential user with the opportunity to talk to someone at a correctional facility that has used the product or service and to ask questions to ensure it meets their expectations.

- Medical and Pharmaceutical Information System (MAPIS): Under an NIJ grant, the Battelle Corporation and the Ohio Department of Rehabilitation and Correction have developed a smart card system that tracks inmate medication dispensing and medical services. The smart card system is a three-media credit-card-sized identification card with bar code, magnetic stripe, and an 8kb embedded computer chip. Inmates wear this card as an identification card. When they report to medical for medication, the card is inserted into a reader, automatically updated, and all services received are recorded on the chip. The use of this card has cut the time of processing each inmate from 30-40 seconds to 3-5 seconds. The project also has a biometric fingerprint module under review. NLECTC-SE provides Project Management support for this project.

- Personal Alarm Monitor (PAM): Under an NIJ grant, the Telephonics Corporation in partnership with the Federal Bureau of Prisons, developed an officer safety device which is capable of tracking and locating an officer within a correctional facility. The system uses radio frequency (RF) tags and sensors located in each unit that read the officer's transmitter at specific locations. It also has a duress button that, when activated, can locate the officer anywhere in the facility. Phase 2 of the project will include a GPS module for tracking off-site inmates on work detail and for tracking transportation vehicles.

- South Carolina Jail Linkage System/Criminal Justice Information System: This is an internet-based information sharing database developed by the University of South Carolina (USC), Advanced Solutions Group. The system provides a jail or prison with the ability to access information from all jails and prisons in South Carolina and track inmates as they move about the criminal justice system. Currently, the database contains information from Magistrate Courts, Jails, Departments of Corrections, Superior Courts, and Probation and Parole Agencies. In addition, they have recently downloaded 4.6 million Department of Motor Vehicle records with digital photographs. This information is available to the authorized user for the cost of an Internet connection. Information in the database is all public record information with NO sensitive information provided online. However, the system provides red flags to denote VIOLENCE and MEDICAL problems. To gain access to the database, an agency agrees to download all their records each day of operation. NLECTC-SE and USC are currently working with the Social Security Administration to expand the operation across state lines.

- Mock Prison Riot: This training exercise is held once each year at the Moundsville State Penitentiary in Moundsville, West Virginia in partnership with NIJ's Office of Law Enforcement Technology Commercialization (OLETC) and the West Virginia Department of Corrections. Special Operation Forces, Corrections Emergency Response Teams, and Special Response Teams from seven states and the Federal Bureau of Prisons participate in full-scale riot scenarios. The last exercise was held in September 1998, and all fifty states were represented. Over sixty technologies were showcased. The next exercise is currently being planned for April 1999 and is expected to be twice as large as the previous one.

- Federal Surplus Property Program: Under the Department of Defense's 1033 Program, correctional agencies have access to federal surplus and excess property stored at military bases throughout the country. Correctional agencies have obtained millions of dollars worth of new equipment to support their law enforcement functions. NLECTC-SE assists correctional agencies with accessing this program.

3.2 SANDIA NATIONAL LABORATORIES

Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin company, for the United States Department of Energy under contract DE-AC04-94AL85000. In January 1997, NIJ created a Satellite

Facility at SNL to support NIJ's multidisciplinary science and technology development program. The Satellite Facility focuses primarily on:

- Test and evaluation of proposed and existing technology and equipment for state and local law enforcement and corrections,
- Research and development activities to support law enforcement "special teams" such as Special Weapons Assault Teams (SWAT) and bomb squads,
- Support to NIJ's Rocky Mountain Regional Center in Denver in explosives and drug detection, and
- Research and development activities for combating terrorism.

The Satellite Facility also provides technical assistance to the NIJ NLECTC network and their customer base of state and local criminal justice agencies.

4. VULNERABILITY ASSESSMENT METHODOLOGY

In the United States, prison systems are administered by each of the states, territories, the District of Columbia, and the federal government. Many counties and municipalities also incarcerate misdemeanants. Few of these jurisdictions have defined either threats to security or requirements for security at correctional facilities, nor have many performed vulnerability assessments. Today's physical security system at a correctional facility is an increasingly complex configuration of personnel, procedures, detection, delay, and response elements. Such complexity implies the need for increasingly complex evaluation and assessment.

Various tools and techniques can be used to analyze a physical security system in general and to evaluate its effectiveness against previously defined threats. These are used to identify system deficiencies and vulnerabilities, to evaluate possible improvements, and to help perform cost versus effectiveness comparisons. These tools and techniques can help to evaluate either an existing security system or a proposed security system design. However, such tools and techniques generally do not address the vulnerability assessment specific to a *correctional* facility. Instead, such analyses are more likely to have been done for an external threat seeking entry to steal or sabotage valuable assets.

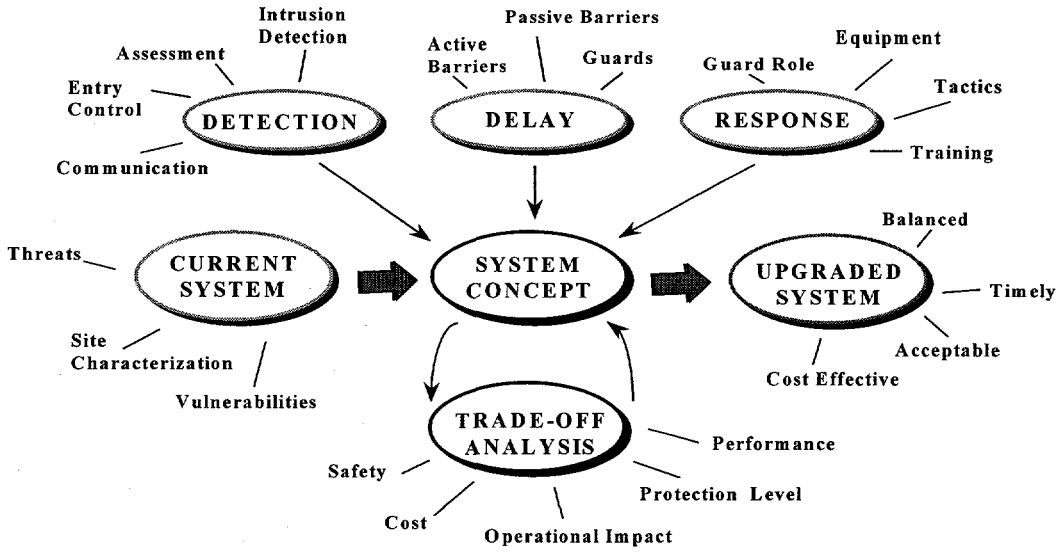
To ensure effectiveness of a system, security threats must be defined systematically, security targets must be identified, and facility operations must be carefully understood. Physical security systems must then be designed to protect against these threats while maintaining efficient operations. Failure to perform this assessment function means that the facility may have vulnerabilities that are not fully understood and accepted. Examples also exist where some sort of vulnerability analysis was performed but not heeded; an identified weak point at one facility pointed to an escape path utilized years later.

4.1 Design of a Physical Security System for a Correctional Facility

The design of an effective security system for a correctional facility requires a methodical approach in which the designer weighs the objectives against available resources, and then evaluates the proposed design. Otherwise, the security system might waste valuable resources on unnecessary security or, worse yet, fail to provide adequate security at critical points of the facility. For example, maximum-security measures at a facility's main vehicle sally port might be wasted if entry or exit were also possible through an unguarded gate at the prison industries building.

The first step in the development of a security system design is to determine the objectives of the security system. To formulate these objectives, the designer must first:

- Characterize (understand) the facility operations and conditions,
- Define the security threat at that facility, and
- Identify escape scenarios and other potential targets of adversaries to the security system.



Security System Design
Figure 1

In characterizing facility operations, one develops a thorough, systematic understanding of everything that goes on within the correctional facility walls, as well as all constraints. Policy requirements must be understood, as well as manpower utilization. In addition, everyday operational procedures, procedures to be employed during abnormal conditions, extraordinary events that might occur, area threat assessments from law enforcement agencies, inspection and maintenance requirements and procedures, misconduct information, future facility expansion or contraction plans, key system control, weapon availability, and so forth are considered. A thorough understanding must be developed of facility floor plans, including location, capabilities, and function of all security related equipment and resources.

To define the security threat, one must understand the types of adversaries to the security of the facility, their tools, their capabilities, their motivation, and their probability of attack. Adversaries to the security system at a correctional facility can generally be separated into four classes:

- Inmates who wish to escape, to wreak violence against facility personnel or other inmates, to possess contraband, or to pose various other security threats to the system;
- Facility insiders (excluding inmates) who may be a threat to security, for instance a compromised employee smuggling in drugs;
- Outsiders, such as families and friends of incarcerated offenders who might aid in an escape attempt or smuggle in contraband, as well as others with various agendas such as members of organized crime or political activists; and
- Outsiders acting in collusion with inmates or insiders.

For each class of adversary to the security system, we must understand possible tactics (such as deceit, force, and stealth), capabilities and skills, level of motivation, speed with which the plan might be carried out, and ability to obtain, hide, and carry tools and weapons. The threat of *inmate escape* can be considered in terms of the likelihood of it happening by means of deceit, stealth, or force. The frequency, type, and time of inmate "headcounts" can be analyzed. The availability of

equipment that might aid in the escape should be considered. The threat of *inmate violence* should be considered in such terms as areas where violence is likely to occur; physical layouts of the most likely locations; the expected number of people involved; whether the focus is on the individual, a rival gang, or towards staff; the most likely time of day; the degree of the violence; the past history of violence and expectations for the future; possible "weapons" that could be employed; and available intelligence information about possible violence. The threat of *contraband* could involve weapons, drugs, money, electronic devices, or other objects, which could be delivered by staff, visitors, or incoming inmates. The path of introduction and the necessary packaging need to be considered. *Outsiders* could enter through the perimeter or by routes such as the delivery routes for goods.

Finally, all credible escape scenarios and other security targets should be considered. These considerations might include the defeat or by-passing of security system components or barriers by force or stealth, breaching of structural features, use of facility features as climbing or bridging aids, or the defeat of procedures by deceitful means such as forged identification.

As potential escape routes are identified, decisions are made about the extent of vulnerability to escape. The natural focus of security system design is to harden those features that are most obvious and likely to be used in an escape. Each improvement moves the attention of the potential adversary to the next easiest path of opportunity. The cost of a proposed improvement can be measured against the reduction in vulnerability to determine its worthiness for consideration. As the level of vulnerability decreases, we eventually reach the point of "acceptable risk" below which we are willing to accept the vulnerability because additional security is not worth the cost.

In addition to the primary responsibility of correctional institutions to protect the public by preventing escape of convicted criminals, the correctional officials are also responsible for the safety of inmates in their custody. The design objectives for the security system must therefore include measures to detect and counteract criminal activity by inmates that threaten the safety and well being of other inmates and staff. These activities could include drug trafficking, trade in other types of contraband, prostitution, and violence directed against other inmates or correctional officers.

Given the information obtained through facility characterization, threat definition, and target identification, the designer can determine the security objectives of the security system. An example of a security objective might be to "interrupt a knowledgeable and motivated inmate before he can escape the confines of the facility."

The next step in the process is to determine how best to combine such elements as sensors, cameras, lighting, fences, barrier systems, contraband detection, entry control, personnel and inmate identification, control of interior movement, procedures, communication devices, and response force personnel and weaponry into a security system that can achieve the security objectives. The resulting security system design should meet these objectives within the operational, safety, and economic constraints of the facility. The primary functions of a security system are detection and assessment of any adversary, delay of that adversary, and response by the correctional officers, while continuing to maintain an efficiently operating institution.

Certain general guidelines should be observed during the security system design. A security system generally is more effective if detection is accomplished early such as at the beginning of a breakout attempt, and if delay mechanisms are in place after the point of detection to interrupt the escapee's progress and expose him to a prompt response. In addition, there is close association between detection and assessment. Detection includes both some indication of an undesired act plus an assessment of what caused the indication or alarm. Another close association is the relationship between response and communications. A response force cannot respond unless it receives a reliable communication request for a response.

These and many other particular features of security system components help to ensure that the designer takes advantage of the strengths of each piece of equipment and uses equipment in combinations that complement each other and protect against weaknesses.

4.2 Vulnerability Assessment of a Correctional Facility

A correctional facility vulnerability assessment typically begins with an on-site, thorough examination of site operations and other pertinent information. Such an activity is likely to take a team of a few people a week or more to accomplish. During the visit, thorough documentation is begun for all pertinent information. Such information should be treated as sensitive and protected from exposure to those people without a need to know the information, in order not to compromise site security. After the on-site visit, time is required to use evaluation tools and to develop a detailed report with recommendations.

We do not recommend a checklist approach to the design and evaluation of a security system. More sophisticated analysis and evaluation techniques can be used to better estimate the minimum performance levels achieved by a security system. Such techniques are most effective when they utilize test and evaluation.

An existing security system at an operational correctional facility cannot normally be fully tested as a system. Drawing the attention of the inmate population to the various features of the security system, and demonstrating their strengths and weaknesses, can only provide inmates with information that they have no need to know. Since full system tests are not practical, evaluation techniques are based on performance tests of component subsystems. Component performance estimates are combined into system performance estimates by the application of system modeling techniques.

The end result of this phase of the design and analysis process is a system vulnerability assessment. Analysis of the security system design will either find that the design effectively achieved the security objectives or it will identify weaknesses or both. If the security objectives are achieved, then the design and analysis process is completed. However, the security system should be analyzed periodically to ensure that the original security objectives remain valid, that the threat definition remains current, and that the security system continues to meet them.

An adversary path is an ordered series of actions against a target which, if completed, results in successful accomplishment of adversary objectives. Protection elements along the path detect and delay the adversary. Detection includes not only sensor activation but also alarm communication and assessment. Both the delay times associated with various security elements and the cumulative probability of detection along a specific path are needed for evaluating the effectiveness of the physical security system along that path. The identification and evaluation of adversary paths is usually a complex process.

One measure of system effectiveness is timely detection. A timely detection is an acceptable cumulative probability of detecting the adversary while there is enough time remaining for the response force to interrupt the adversary. Timely detection considers detection, delay, and correctional officer response time only. It does not consider engagement between the response force and adversaries; that is, it does not model neutralization of the adversary.

To truly deduce the effectiveness of a total physical security system, one must consider the most critical path. That is the path with the lowest probability of interruption of the adversary. The protection system is really only as effective as its protection of this path. The critical path characterizes the effectiveness of the protection system in detecting, delaying, and interrupting the adversary.

4.3 Vulnerability Assessment Tools

Various tools are available for assessing vulnerabilities of a facility in general, although none that we are aware of has been created specifically for analyzing the vulnerabilities of a correctional facility. Sandia National Laboratories uses tools and techniques such as EASI, ASD, SAVI, and ASSESS to measure the effectiveness and timeliness of protective systems. These tools were developed under sponsorship from the Department of Energy for the analysis of security at nuclear-related facilities. These tools are described below. Other tools are available from various organizations and commercial companies.

EASI (Estimate of Adversary Sequence Interruption) was developed in the 1970's and models one path at a time, as selected by the user. EASI runs on a personal computer and is a simple-to-use model. It uses specific detection, delay, response, and communication performance values to compute the probability of interrupting the adversary before he accomplishes his objective. It can be used to perform sensitivity analyses and to analyze physical protection system interactions and time trade-offs along specified paths.

ASD (Adversary Sequence Diagram) is a manual method of graphically modeling the security system at a facility. Once completed, it identifies paths which adversaries can follow to accomplish their objective. The most vulnerable path can be determined and used to measure the effectiveness of the entire security system. There are three steps in developing an adversary sequence diagram for a specific site. The first step is to model the facility by separating it into adjacent physical areas. Next, protection layers are defined between the adjacent areas. Each protection layer includes one or more protection elements, which are the basic building blocks of a security system. Examples of protection elements are doors, fences, surfaces, and portals. Finally, path segments can be drawn between the areas through the protection elements. Both entry and exit paths can be modeled.

SAVI (Systematic Analysis of Vulnerability to Intrusion) was developed in the 1980's and runs on a personal computer. SAVI contains an extensive database of representative detection probabilities and delay times, developed through years of testing at Sandia National Laboratories. However, the analyst can change default times and probabilities to more accurately reflect the specific facility being modeled. SAVI performs an ASD type of analysis and presents the results in an easy to understand format. SAVI models all paths using ASD methodology, graphically represents the paths, and identifies the most critical path. An analysis using SAVI begins with constructing a site-specific ASD for the given target. Input to the SAVI code includes the characteristics of the threat, response force deployment time, and delay and detection values for each protection element on the ASD. The code calculates the probability of interruption for each path. It lists the ten most vulnerable paths and ranks them in order of their vulnerability. The analysis results are given in the form of graphs and path displays. A distribution graph shows the distribution of the probability of interruption for all paths, given a specific response force time. A sensitivity graph provides information on the sensitivity of response force time. A vulnerability graph describes the probability of interruption and the time remaining after interruption for the ten most vulnerable paths, given a specific response force time. The interpretation of these results can suggest the need for sensitivity analysis of data that has been input to the code, as well as possible physical protection system upgrades to the most vulnerable paths.

ASSESS (Analytic System and Software for Evaluating Safeguards and Security) was developed in the early 1990's in coordination with Lawrence Livermore National Laboratories (LLNL). ASSESS is a comprehensive approach for evaluating security effectiveness, but was developed primarily for theft or sabotage of nuclear materials. The code consists of six modules: MANAGER, FACILITY DESCRIPTION, INSIDER EVALUATION, OUTSIDER EVALUATION, NEUTRALIZATION, and HAND-OFF. MANAGER keeps track of analyses completed and in progress for the analyst. FACILITY DESCRIPTION allows the analyst to describe the facility targets and security components. The three evaluation modules use information gathered by FACILITY DESCRIPTION. INSIDER includes extensive databases for insider adversary attributes and strategies and contains a reference detection database. OUTSIDER is an enhanced version of SAVI. NEUTRALIZATION is based on the BATLE (Brief Adversary Threat Loss Estimator) program from LLNL. HAND-OFF considers collusion between an insider and an outsider.

5. NIJ CORRECTIONAL FACLITY VULNERABILITY ASSESSMENT PROJECT

The need exists for developing an analysis and modeling tool for use by correctional agencies to help them better construct/modify their facilities and deploy security equipment to keep inmates from escaping and contraband from entering the facility, and to minimize violent attacks on correctional officers and inmates. In addition, classes need to be developed to teach these techniques.

We are currently attempting to define, analyze, and assess the security vulnerabilities of selected correctional facilities across the United States. We expect the findings to generally be applicable to all correctional facilities. Reports of the effort will assess the vulnerabilities of at least two of the correctional facilities we visit: (a) a new facility in the "blueprint" stage and (b) a facility about to undergo security modification or improvements. These reports will be treated as sensitive and not publicly released. Sandia National Laboratories, collaborating with NLECTC-SE, will use its expertise in vulnerability assessment and will use the Department-of-Energy-developed software, ASSESS, in a modified mode by a knowledgeable user, for vulnerability assessment at these two facilities.

The second part of this project will be an assessment, based upon knowledge gained in the first part of the task, of what is required in such a facility vulnerability analysis, as well as the requirements for a software modeling and analysis tool to meet the needs of corrections. This will result in a document drawing a roadmap for correctional vulnerability analysis and for developing such a tool. The project is closely coordinated with the corrections community to ensure a beneficial product.

6. CONCLUSIONS

A design and analysis procedure, together with appropriate physical security technology, provides the basis for good security for correctional facilities. It is important to provide classes and workshops to teach these techniques. The design and analysis procedure consists of three phases: determine, design, and evaluate. The first phase includes the determination of the system objectives which involve correctional facility characterization, threat definition, and security target identification. A good security system design provides detection, delay, and response. Analysis of the security system design begins with a review and understanding of the objectives the design must meet. Evaluation of the design normally requires the application of modeling techniques and software tools. If the evaluation reveals unacceptable system weaknesses, the system is generally upgraded and an analysis on the redesigned system is performed.

7. REFERENCES

1. B. Gardner, and W. Paulus, and M. Snell, "Determining System Effectiveness Against Outsiders Using ASSESS", *Proceedings of the Institute of Nuclear Materials Management*, Vol. 20, 605-610, New Orleans, LA, 28-31 July 1991.
2. D. Crist, and D. Spencer, "Perimeter Security for Minnesota Correctional Facilities", *Proceedings of SPIE's First Annual Symposium on Enabling Technologies for Law Enforcement and Corrections*, Volume 2934, Pages 116-124, Boston, MA, 19-21 November 1996.
3. Sandia National Laboratories, *Physical Protection of Nuclear Facilities and Material,* Class notebooks for International Training Course, supported by the International Atomic Energy Agency, the US Department of Energy, the US Department of State, and the US Nuclear Regulatory Commission, latest class held April 27 – May 15, 1998.
4. Sandia National Laboratories and Science and Engineering Associates, *SAVI: Systematic Analysis of Vulnerability to Intrusion,* Unlimited Release Sandia National Laboratories Report SAND89-0926, December 1989.
5. M. Snell, and C. Jaegar, "Using Vulnerability Assessments to Design Facility Safeguard and Security Systems", *Proceedings of the Institute of Nuclear Materials Management*, Vol. 23, Pages 943-948, Naples, FL, 17-20 July1994.
6. D. Spencer, "Vulnerability Assessment, Correctional Facilities Are Only As Secure As Their Weakest Point", *Corrections Today Magazine,* Page 88-92, July 1998.