Right Brain Sekurity

The Journal of Physical Security

Volume 8(1), 2015

JPS

THIS ISSUE...

Editor's Comments

Welcome to volume 8 of the Journal of Physical Security (JPS). This issue has papers on a nuclear security training model, attack tree analysis for nuclear cyber security, security sensor testing, security of sealed radiological sources, adversary-based security engineering, airport and marina watch programs, and an essay on why security fails.

JPS has moved to http://jps.rbsekurity.com and is now being hosted by Right Brain Sekurity (RBS). RBS (http://rbsekurity.com) is a small company devoted to physical security consulting and R&D.

*****

Staying Focused

According to the *Chicago Tribune* (September 18, 2014, p 5), the TSA reportedly confiscating 1,813 guns at U.S. airports in 2013. A total of 1,477 of the guns were loaded. Aptly named TSA Administrator John Pistole said of the gun confiscations: "That's a distraction for us…Our singular focus is on trying to keep terrorists off planes."

*****

It Might be Bad for Morale

The *Washington Post* reports in a February 20, 2015 article by Jerry Markon, that the U.S. Department of Homeland Security (DHS) has spent $2 million in the last 3 years for 4 different studies on why DHS workers have extremely low morale. DHS has not yet released or acted on any of these studies. DHS has the lowest employee morale of any federal agency, and a serious turnover problem.

*****

Reviewing Performance Reviews

Samuel Culbert calls annual employee performance reviews, "a curse on corporate America". See the *Chicago Tribune*, February 19, 2015, page 19. Culbert point out that performance reviews are rarely objective and that most employees get completely different reviews if they are evaluated by a different boss. Moreover, the common quota system for good reviews undermines teamwork and discourages employees from speaking truth to power. He also feels that typical performance appraisals transfer all accountability to the employee, leaving supervisors and managers largely free from the responsibility of making sure that employees succeed.

According to Culbert, performance appraisals—being so biased and subjective—aren't even effective at documenting reasons for terminating employees. Performance appraisals are often useful evidence for employees claiming false termination in court.

Culbert calls for performance pre-reviewing to fix problems proactively. This should be done in a way that involves the employee, and places more accountability on the supervisor or manager, and on the employee-boss team. Effective communication and truth-telling would be encouraged.

It seems to me that the typical performance appraisals are bad for *security*. They undermine morale, increase disgruntlement and the risk from the insider threat, encourage poor supervision and management, interfere with communication, and engender groupthink.

For a similar perspective, check out this interesting book: Tom Coens and Mary Jenkins, *Abolishing Performance Appraisals: Why They Backfire and What to Do Instead*.

*****

Not Taking the Hint

In September of 2013, the U.S. Office of Personnel Management warned Anthem, the large U.S. health insurer, that its data were severely vulnerable to cyber attack. This report came 2 months after Anthem (then called WellPoint) paid a $1.7 million fine for the release of personal information on 610,000 patients, including their social security numbers. This data breach had occurred during the October 2009 to March 2010 time period.

In February of 2015, Anthem announced that it had suffered a new loss of data. This latest attack was one of the largest corporate data breaches in history. Cyber hackers obtained data on nearly 80 million current and former customers and employers, including social security numbers. Like Sony and Target, there seems to have been an inability or unwillingness to understand cyber threats and vulnerabilities, or to learn from past experience. Why is this weird organizational psychology so common?

*****

Smart People Can be Very Stupid

Richard West and Keith Stanovich have an interesting study reported in the *Journal of Personality and Social Psychology*. They maintain that smart people are actually more susceptible to reasoning errors, including preconceived notions, than people of average or lower intelligence. For more information, see http://www.newyorker.com/tech/frontal-cortex/why-smart-people-are-stupid, as well as the original study at http://www.ncbi.nlm.nih.gov/pubmed?term=west%20stanovich%20meserve.

Also check out the interesting book, *Blind Spot: Why Smart People Do Dumb Things* by Madeleine L. Van Hecke. The book discusses the 10 most common mental errors that cause serious blunders.

As a vulnerability assessor, I am sometimes asked why I think I can find security problems that very smart people missed. I usually answer it is because I am not that bright, and I have to work things out for myself. In other words, I have the right mindset to see problems. I am convinced that is the key to being a good vulnerability assessor, or even just thinking critically about your own security. It is nice to have research to back my position.

*****

Rich People Can be Very Selfish

Matthew Hutson points out that repeated studies have indicated that rich people are often more likely to behave unethically than poor people. When the poor do wrong, it is often to help others; this is because the poor tend to stick together. When a rich person does something wrong, it is often to help only himself/herself.

This suggests that the strategy for trying to prevent insider attacks might vary depending on the economic status of the insider. Rich people can be warned about the harm to themselves if they get caught. Poor people can be warned about the harm that may result to others if they engage in bad behavior.

For more information, see http://nymag.com/scienceofus/2015/02/rich-and-poor-people-cheat-for-different-reasons.html.

*****

Slow Lane

The *Financial Times* reported (February 17, 2015, p 17) that BMW was told in July of last year about a vulnerability in the carmaker's ConnectedDrive software that could allow thieves to remotely unlock the cars. According to the article, however, BMW did not begin to fix the problem—a lack of encryption for communications—until December 8. It did this by turning on a basic security protocol long used for online banking and web page authentication. The company claims there is no evidence the security flaw was exploited.

A UK government advisor warns that car security is not receiving sufficient attention. In the US, a report by Sen. Ed Markey calls into question automobile security, safety, and privacy: http://www.markey.senate.gov/news/press-releases/markey-report-reveals-automobile-security-and-privacy-vulnerabilities

*****

Really?

TheAtlantic.com reports that Vladimir Putin was the 10th most admired man in America in 2014. He came in ahead of Mitt Romney, Joe Biden, and Bono. See http://www.theatlantic.com/politics/archive/2014/12/vladimir-putin-the-10th-most-admired-man-in-america/384085/

*****

Really?

A new app was released called Invisible Boyfriend or Girlfriend. This app is available at https://invisiblegirlfriend.com. It generates text, voice mails, and pictures to give users "believable social proof" that they have a romantic partner.

What is not clear is if you need a separate "Breaking-Up" app to dump your invisible boyfriend or girlfriend when you tire of them.

*****

Really?

After a series of embarrassing problems with Secret Service agents misbehaving (involving alcohol and prostitutes), and serious security incidents (including a White House fence jumper), we now learn of yet another embarrassing incident. Two high-level Secret Service Agents allegedly were drunk when they crashed into a White House security barrier, potentially interfering with a crime scene investigation. Purportedly, a Secret Service supervisor directed police not to perform a sobriety test on the two agents and allow them to go home.

The recent White House fence jumper incident seems to be a classic example of the Waylayered Security Maxim: "Layered security will fail stupidly." The same kind of thing happened in the Y-12 nuclear security incident when an 82-year old nun and 2 fellow protestors penetrated security and were not intercepted for a considerable amount of time.

These kinds of security failures in complex, Defense-in-Depth security programs are both predictable and preventable. Too often, layered security isn't a security strategy as much as a cop out to avoid developing a real security strategy, or having to think critically about security. If we aren't careful, layered security can take away any sense of personal accountability and initiative for security professionals and regular employees.

*****

Really?

The "Think Again Turn Away" campaign and Twitter/Facebook accounts run by the U.S. Department of State have the intent of countering terrorist recruitment. They are, however, widely criticized as being incompetent.

It is remarkable that the United States—a leader in pop culture, computer applications, social media, public relations, advertising, entertainment, psychology, and education—can't put together a more effective campaign to counter terrorist recruitment. If we want to reach young people, how about getting Hollywood, the music industry, advertising firms, and young people involved?

For more information on the "Think Again Turn Away" campaign, see http://www.nydailynews.com/news/politics/state-department-embarrassing-turn-twitter-campaign-legitimizes-terrorists-expert-article-1.1941990 and http://www.motherjones.com/politics/2014/02/state-department-cscc-troll-terrorists-twitter-think-again-turn-away.

-- Roger Johnston
Right Brain Security
http://rbsekurity.com
Oswego, Illinois
March, 2015

Journal of Physical Security 8(1), 1-18 (2015)

Design of an Interactive Nuclear Security Physical Training Model

Edward Waller, Michael Adderly, Maxwell Hayward, Steven Reid, and Jillian Ruttan-Morillo
University of Ontario Institute of Technology
Faculty of Energy Systems and Nuclear Science
2000 Simcoe Street North, Oshawa, Ontario, L1H7K4 Canada

Abstract

Training personnel about physical protection systems at nuclear facilities is difficult as the security systems are in continuous operation, which makes access to these systems for training problematic. An interactive model of a nuclear facility to demonstrate physical protection systems (PPS) can provide instructive and cost-effective training to a wide range of personnel. A physical model was designed and fabricated to represent the hypothetical Lagassi Nuclear Research Institute (LNRI), which is used by the International Atomic Energy Agency (IAEA) for nuclear security training. PPS were divided into major categories, consisting of lighting, fences, cameras, motion detection, annunciation, and intrusion simulation. To allow for an interactive element, the Raspberry Pi microcomputer was used as an interface between various sensors introduced into the physical model, the alarms and the user. Interface code was written in the Python programming language to allow sensors to communicate with the computer. The model was tested for a specific fence-defeat training scenario and found to be a useful tool that allows a user both to visualize the protected area and interact with alarm panels. In addition, delays measured through the alarm sequences are interfaced through the Raspberry Pi to a spreadsheet that estimates probability of interruption, such that the user may determine whether an adversary has been interrupted prior to achieving his goal. This feature demonstrates to the user the benefit of timely alarm communications. The interactive physical model is a cost effective alternative to hands-on systems training.

Introduction

The International Atomic Energy Agency's (IAEA) Advisory Group on Nuclear Security (AdSec) defines nuclear security as "*the prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities*" (IAEA, 2005). To enable prevention, detection, and response, high security nuclear facilities use physical protection systems (PPS) and a defense-in-depth strategy. The most desirable goal of the PPS is to deter an adversary from attempting an act on a facility. When deterrence is not possible, the PPS acts to detect, delay, and provide time for security forces to respond to the adversary (Garcia, 2006). Detection is the discovery of an adversary action, including the sensing of covert or overt actions. Examples of PPS components that serve to detect include sensors, posted guards, and entry control systems. Delay is the slowing down of an adversary's progress and can be accomplished with, for example, personnel, barriers, or locks. Response is the activation of either on- or off-site personnel to interrupt and/or neutralize the adversary.

Methods used in nuclear security, such as PPS, allow for the protection of facilities which develop, use, or store nuclear/radiological materials, by detecting, delaying, and responding to adversaries. However, available data and models depicting real PPS are often difficult to obtain for security reasons, hindering training outside of the facility. The model developed here of a hypothetical nuclear facility is intended to be used in a training environment, allowing operators, security personnel, nuclear security students, and future security professionals to examine specific aspects of a PPS, and analyze their requirements and interactions. The complexities of these interactions can be seen in the model, but it is not intended to be a representation of a licensable nuclear facility.

Design Basis: Lagassi Nuclear Research Institute (LNRI)

The facility was modeled after the hypothetical Lagassi Nuclear Research Institute (LNRI) which is utilized by the IAEA for nuclear security training (IAEA, 2014). From the description of the hypothetical facility, the hypothetical Republic of Lagassi operates a

light-water moderated, HEU-fueled, pool-type reactor (PTR). The reactor is used for research on advanced reactor components, special fuel assemblies, and the production of radionuclides (details important for threat assessment). A CAD plan view of the LRNI is depicted in figure 1, and an isometric view is depicted in figure 2.

The Lagassi complex has a single fence outer perimeter, demarking the off-site to limited area, and both the reactor building and waste storage facility protected areas are enclosed by double fences. Vital areas (not shown) are located within the protected areas and contain the reactor core, control and safety systems, fuel and radioisotopes. A single security entrance is provided as well as a number of administrative buildings and small internal roadway structure. The CAD model was used as a basis for the physical model, described below.

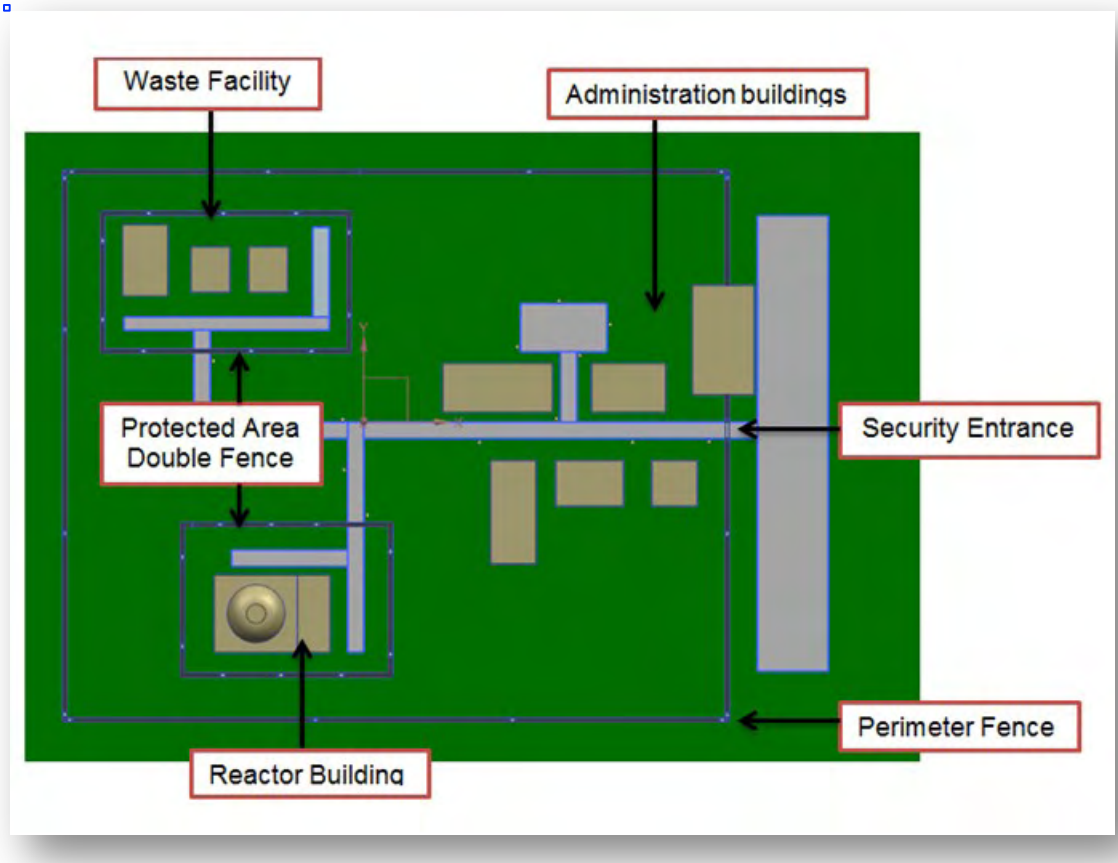


Figure 1 - Plan View Layout of Lagassi Nuclear Research Institute (LNRI).

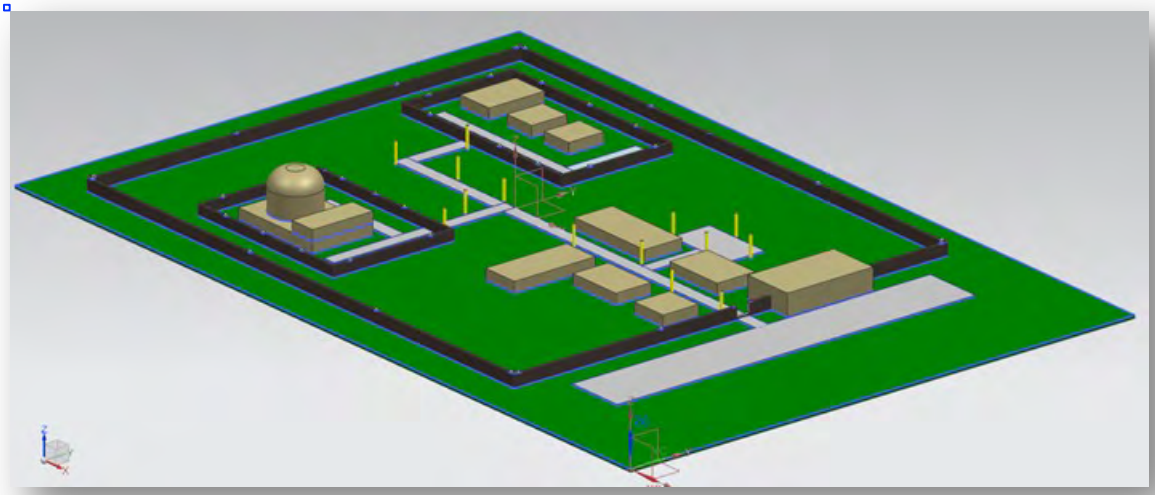


Figure 2 - Isometric View of LNRI.

Physical Design and Fabrication of Model

To convert the hypothetical LNRI CAD model into a physical model, a number of design requirements were established, as listed below.

- The design of the nuclear facility physical model must be modular—t*o allow for the addition of new components based on more technically advanced components or changes in industry standards.*
- The components of the physical model related to PPS must be interactive—t*o allow for the representation of PPS functionality and provide an improved training environment.*
- A computer interface system will be used to control the input received from PPS sensors—t*o interact with other PPS and provide data to be used in simulations and calculations.*
- The platform that the model is constructed on must be portable and have the ability to maneuver through standard double doors—t*o allow for the portability of the model to various training locations.*
- The physical model must be cost effective—*ideally, the model should cost less than $1000 (US dollars) for materials.*

We determined early in the design that the waste facility would not be replicated in the physical model, primarily due to space issues. The LNRI physical model design consists of a main base, which was constructed as a large flat rectangle fabricated from plywood with

total external dimensions of 40" x 60" x 11 ¾" (101.6 cm x 152.4 cm x 29.85 cm), the forward face having a 45° angle, and the top board being hinged to access the wiring underneath. The control panel portion of the model is located behind the angled face, and consists of two LCD monitors, a small panel center panel with control buttons for the lighting and intrusion scenario, one large alarm button centered between the monitors, and a video multiplexer for the Closed Circuit Television (CCTV) system. A protective angled spruce wood face opens to be parallel with the bottom of the model base (approximately 135°) and the sides of the model are also fabricated from spruce wood. The top of the base is essentially a large spruce wood lid, which is fastened to the base of the body via a piano hinge. All electrical components (wires, electric motors, computer systems, etc.) are located beneath the lid in the box. The box is large enough so that additional components may be added in the future. All of the model details, observable by the users, are located on the top of this lid. In order to fasten model buildings, fences, and various wiring, the model was separated from the lid using polystyrene foam with a thickness of approximately 1" (2.54 cm).

The model is designed to represent the main areas of the LNRI, with the exception of the waste facility. There is an outer perimeter (limited area) fence of approximately 3.3 meter scale height. Toward the front of the model (the direction of the control panel) there is a road which connects to the reactor facility, a small parking lot, a main guard house, and an intrusion gap in the fence (the location of the intrusion scenario, discussed below). Several general purpose buildings are located within the limited area, but outside of the protected area security fences. The protected area security fences consist of two parallel sets of fences, the outermost security fence is separated by approximately a 5.8 meter scale distance from the inner fence, and is approximately 6 meter scale height. The essential systems of the model, the lighting and annunciation system, the camera systems (and fences), the motion sensor, and the intrusion scenario are all located within the boundaries of the model.

Construction of the model base involved the preparation of engineering drawings for delivery to a wood-cutter, after which the surfaces were sanded and stained (American

Chestnut). At the assembly stage, wood screws were used to attach fixed components to each other. Two hinges were attached to the model (at the lip of the base to be attached to the control panel front cover; and at the top edge lip of the right-side wall). The top lid and control panel cover were then mounted to their respective hinges.

We decided that polystyrene foam sheets were to be used as an attachment surface for various N-scale buildings, automobiles and other features. The polystyrene foam sheets were cut such that an approximately 1" (2.54 cm) gap existed between the edge of the polystyrene foam and the edge of the wooden base, to allow for the future inclusion of a protective Plexiglas cover (to prevent against accidental damage and to reduce dust buildup). The polystyrene foam sheet was then fixed to the lid surface using wood glue. The groove for the intrusion scenario track was cut using a combination drill and jigsaw. Model grass sheets were placed on the surface of the secured polystyrene foam and the locations of the buildings were planned to best use the available grass sheets. The footprints of the buildings and roads were cut out and reused to fill gaps on the polystyrene foam surface. For minor adjustments, grass powder was used to fill in the space between adjacent grass sheets. To allow for a uniform and realistic physical model, N-scale components were assembled and used for facility buildings and representation of the reactor building. To enhance realism, shrubbery, staff and vehicles were incorporated. A front photograph view of the completed model is provided in figure 3. The physical model is seen on the top of the box, and the LCD monitors and switches may be seen in the front.

Physical Protection System Elements

A number of physical protection system elements were incorporated into the LNRI model. Some of the elements are static (for example, fences), and some are interactive (for example, security and interior lighting, passive infrared detector, video cameras and alarms). In addition, an intrusion scenario was generated and the components needed for the scenario were incorporated into the physical model. A CAD representation of the

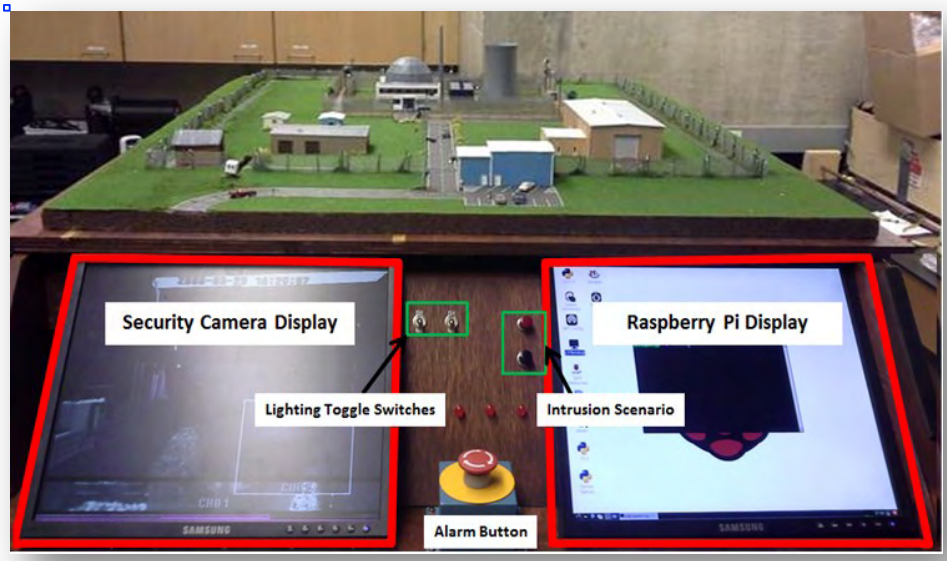


Figure 3 - Front view of LNRI physical model.

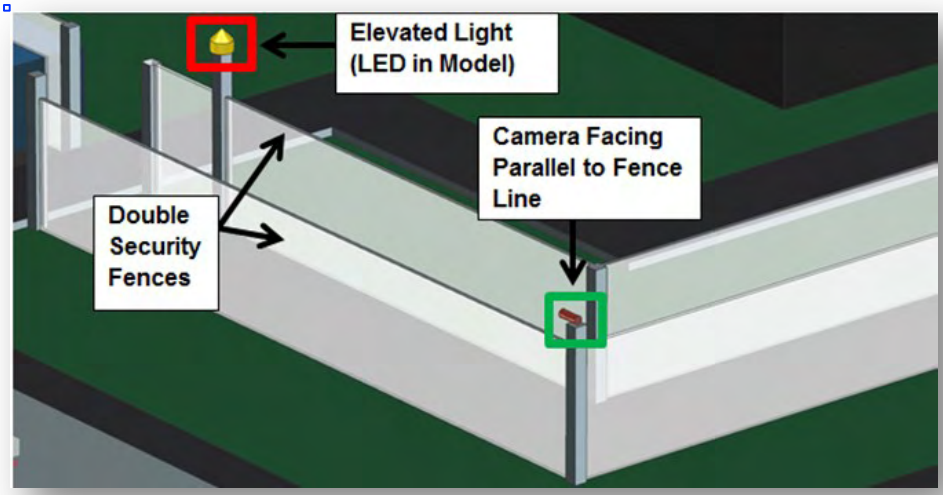


Figure 4 - Example of physical protection elements around the protected area.

location of physical protection elements in provided in figure 4. It may be seen that security lighting is located at various fence points, and cameras are used to view down fence lines.

The various physical protection elements used in the LNTRI model are discussed below.

Fencing - In a security setting, fencing is used to create a physical and psychological deterrent to adversaries, and also delay intrusion into the area. The delay of intrusion provides the response personnel with time to interrupt these adversaries. Fences also aid

in controlling access to the facility and assist in directing persons to designated entrances. Fences interact with other physical protection systems to ensure optimal facility security. For the LNRI model, the goal was to design a perimeter (limited area) fence and inner (protected area) security fence system representative of a typical nuclear facility. The perimeter fence surrounds the limited area of the model and is a barrier that prevents accidental alarms by animals or individuals. The perimeter fence has the additional function of delaying adversaries, allowing the CCTV system an early opportunity to assess alarms. The inner security fence, which is taller than the perimeter and consists of additional security features, surrounds the vital area and the asset. The perimeter fence, which surrounds the entire facility, is made of commercially available aluminum mesh wire and standard finishing nails. The finishing nails are attached to the fence using hot glue with spacing approximately 4 cm apart. This distance was chosen to keep the perimeter fence consistent with the security fence spacing. The finishing nails, used as the fence posts, secure the fence into the underlying foam. The inner protected area security fence system surrounding the research reactor is a double fence with gravel separation. The security fences are HO-scale (1:87) purchased from a hobby store (compared to N-scale which is approximately 1:148; the differences in scale were inconsequential visually to the model). HO-scale fences were used due to their appropriate features and their cost. The fence sizes were compatible with the N-scale model and differences in scale were insignificant in the model. The protected area fencing may be seen in figure 5.

Figure 5 - Protected area fences in LNRI physical model.

There is a single entrance through the perimeter fence at the front of the model. Two entrances are within the security fence, one at the front and the other at the side, towards the rear of the facility. All fence entrances have guard houses placed at the entrance, used to monitor the incoming personnel and vehicles. The perimeter fence also has a small opening for the intrusion scenario to pass through. For simplicity, this opening is a permanent cut in the fence, and does not open and close with the movement of the vehicle.

Lighting - Of the four objectives of a PPS (deter, detect, delay, respond), the lighting system's primary purpose is to aid in the detection of adversaries, although deterrence is a desirable side effect. Artificial lighting provides illumination to allow nuclear security officers (NSOs) to visually locate and identify targets. Specific lighting is designed to illuminate the area of observation for cameras and areas where NSOs patrol. In combination with cameras, lighting allows for both video surveillance and video assessment. A secondary purpose of station lighting is to deter low-level threats away from the facility. In the LNRI model, the standby lighting was installed along the perimeter fence line with one LED located every 7.6 cm. The placement of the luminaires in relation to their desired areas of illumination was determined based on best practices from the Illuminating Engineering Society of North America (IESNA, 2003) including positioning away from the fence line to prevent its use as a climbing aid by an adversary. A total of 46 LEDs were installed along the limited area perimeter fence. To reduce the amount of wiring necessary to connect 46 LEDs in parallel, the negative leg of each LED was electrically connected to the aluminum mesh fence. To hold the LEDs in place, they were weaved through the fence and solder was applied to ensure they did not slip out. Then the negative side of the circuit was connected at four points along the entire fence, and the metal fence acted to complete the circuit. As the LEDs were flush against the fence, the positive leg needed to be insulated with heat shrink tubing, which also helped to hold the resistor that was soldered to the positive leg of each LED. In addition to the fence lighting, a variety of realistic N-scale lights were utilized in the model. Two 10 mm floodlights were installed on buildings and directed to illuminate the facility's gates. One 78-mm tall, pole mounted spotlight was placed near each camera to illuminate the assessment area in the inner protected area. Finally, two 70-mm tall streetlights were placed along the protected area roadway and one

was placed at the facility's exterior intersection. All of the N-scale buildings in the model have penetrations for windows or other openings, and interior lighting was installed for realism. A simulated night view of the illuminated model is shown in figure 6.

Cameras – A closed circuit television (CCTV) system in a security setting allows personnel to effectively monitor a facility or area from a distance, at a central location. Personnel are able to observe and react promptly to suspicious activity or security breaches. The CCTV system is monitored at all times to ensure the safety of critical areas within the facility and works in conjunction with other physical protection systems to limit the threat of adversaries. For the LNRI model, the goal was to design a CCTV system that is able to continuously monitor the nuclear facility, verify sensor alarms and detect an adversary.

Figure 6 - Illumination of LNRI model.

The CCTV system for the LNRI physical model consists of a total of four cameras, each placed in a corner of the outer protected area security fence. The cameras used in the model produce a black and white video image and are night-vision capable. Each camera faces down a fence line so the system is able to monitor the entire perimeter of the security fence. The cameras are placed on wooden dowels to achieve the desired height for the

camera. The cameras' height was selected based on the height of the fences and the effects of lighting. The lighting, both natural and the facility lighting, can affect the video quality produced by the cameras. The height of the cameras had to be adjusted accordingly, and the cameras were placed on the wooden dowels using hot melt glue. The camera width and height is 16 mm, while the depth is 10.5 mm. These cameras are not N-scale, as N- or HO-scale cameras were prohibitively expensive for this project. Therefore, the design of the CCTV system had to be modified in order to allow for the larger components. The cameras have both an RCA output and require an AC power adapter. An RCA male-to-male extension was attached to the cameras to allow for the camera wire to extend across the length of the box. All wires from the cameras are concealed in the foam underneath the grass covering and lead into the box through holes drilled into the wood. The multiplexer used for the CCTV system has a BNC input and therefore, connectors were required to connect the cameras to the multiplexer. RCA-to-BNC connectors allowed for the connection of the cameras to the multiplexer. A VGA cable is used to connect the multiplexer to the monitor on the control panel where the 4 fence lines may be simultaneously observed. The camera installation in the model and the multiplexed display is seen in figure 7.

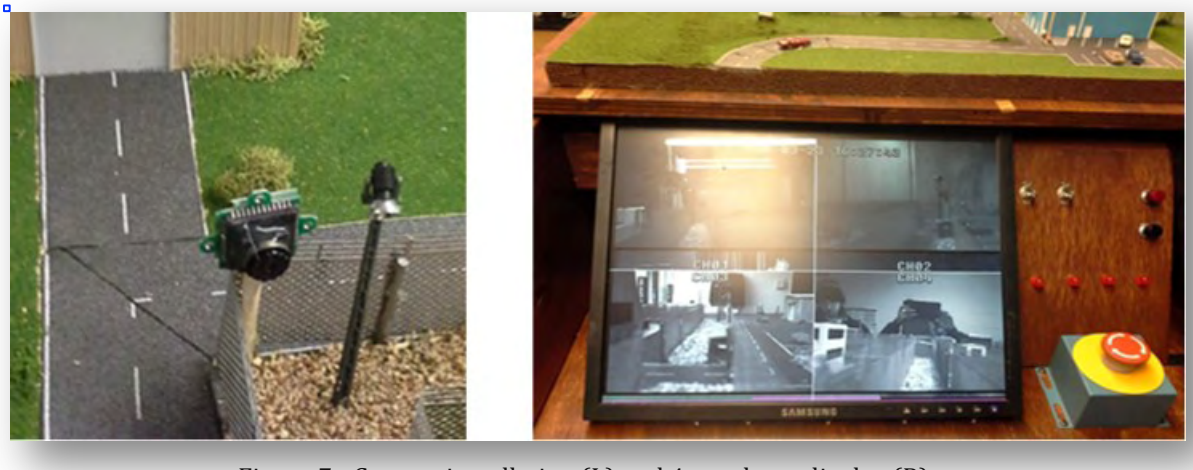


Figure 7 - Camera installation (L) and 4-quadrant display (R).

Motion detection – Passive detection is a useful strategy in security systems, with nuclear facility security being no exception. In the construction of the LNRI physical model, we

agreed that such a method of detection would be incorporated. A passive infra-red (PIR) module was selected and controlled through the use of the Python programming language on the Raspberry Pi computer. Although most IR detectors are incorporated into the area of assessment or vital area, it was decided that the motion detector would be located at the perimeter security fence to provide early detection of the intrusion (see section on Intrusion Scenario). A diagram of the PIR sensor interface to the Raspberry Pi is depicted in figure 8.

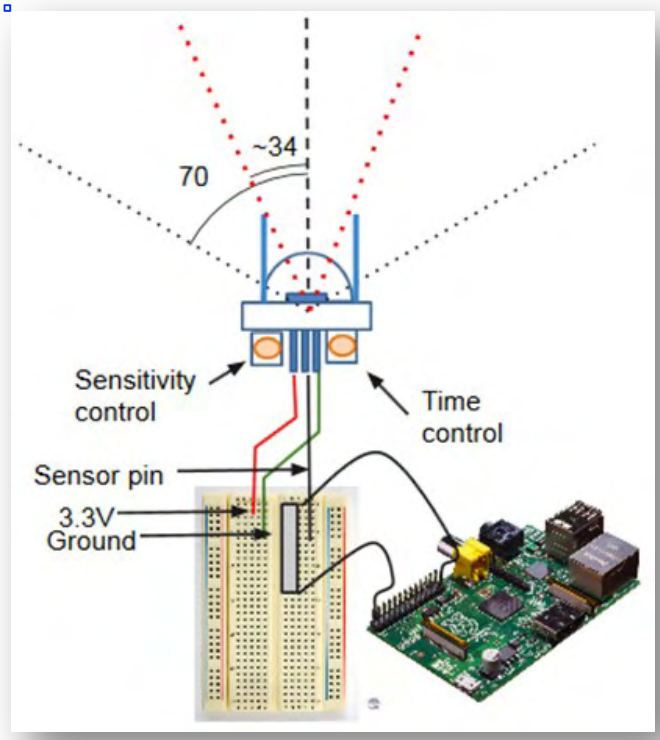


Figure 8 - PIR sensor connection to Raspberry Pi.

As most PIR detectors have a range of 15 to 18 feet, and the model width was 40 inches, the location of the PIR sensor was such that it would detect the intrusion scenario. This decision was made for model training purposes; a real physical protection system would have multiple sensors (and indeed, a variety of strategies) to detect intruders at various locations around the facility.

Alarm - The function of the alarm and annunciation system is to indicate that an event is taking place and response is required. The sounding of the alarm alerts site staff and NSOs

to a suspected or actual event. In the LNRI physical model, the lighting system is interconnected with an alarm system, which is activated by an alarm button. A typical event initiation is as follows:

1. Vehicle breaches the fence line (intrusion scenario, described in the next section).
2. Vehicle is detected by PIR sensor
3. Sensor-specific alarm is generated on the Raspberry Pi interface indicating that something has triggered the PIR detector. At this point, the alarm has not been assessed.
4. Console operator (nuclear security operator), in response to the PIR alarm, uses cameras to assess the alarm as a true attack against the facility, and the facility alarm button is depressed.
5. The facility alarm initiates signals from the Raspberry Pi to the facility lighting system which lights all areas, activates a red flashing alarm strobe, and sounds an audible alarm.
6. The time delays from first detection of the intruder to the initiation of the facility alarm are sent to a spreadsheet which calculated probability of interruption.

Intrusion Scenario

Intrusion scenarios, specifically those that represent a design basis threat (DBT) of a facility, are essential for conducting an overall vulnerability assessment of a facility. DBTs are constructs which are established by the regulator and driven by threat assessment and operating experience from the several industries around the world. Many factors from DBTs must be analyzed depending on the type and nature of the threat, the number of adversaries, the tactical competency of the response team, the weapons used by the adversaries and the characteristics of the tools and vehicles used. The basic intrusion scenario model we decided upon for the LNRI physical model was a track system which would move a representation of an adversary (in this case, a model truck) across one of the essential boundaries (limited area perimeter fence). Buttons on the control panel (depicted in figure 3) activate a 3-volt motor controlling a chain track system, which moves

the model vehicle forwards or backwards through a breach in the limited area perimeter fence line. The motor and track system, which is located under the lid of the model, may be seen in figure 9. The PIR sensor is located such that when the vehicle passes by the sensor, it initiates a sensor alarm. The top surface of the LNRI physical model, depicting the pathway of the adversary and the location of the PIR sensor, is depicted in figure 10.

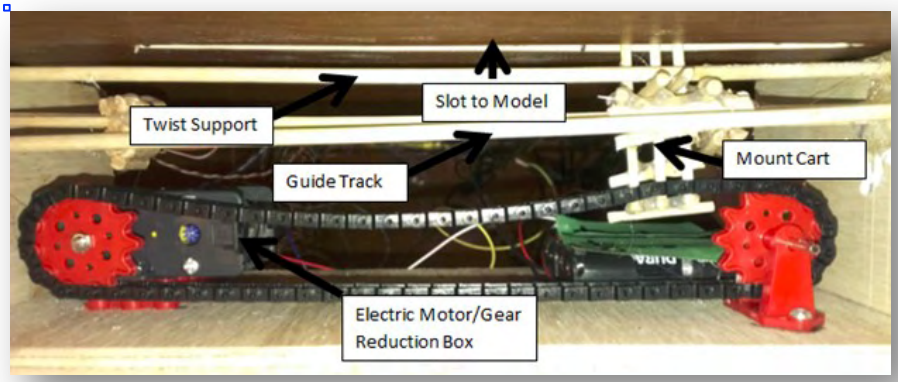


Figure 9 - Motor and track system for intrusion scenario.

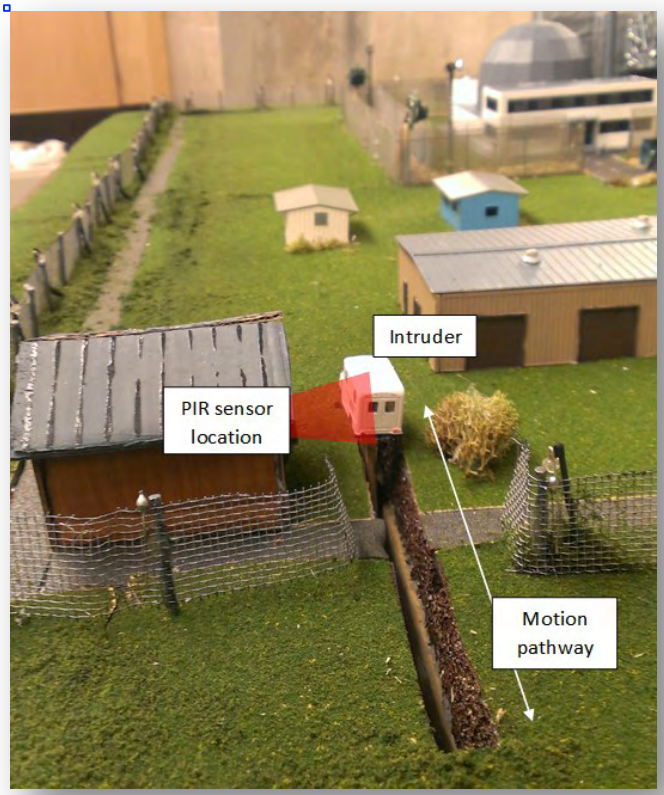


Figure 10 - Intrusion scenario in LNRI model.

Integrated EASI Analysis

We designed and fabricated the LNRI physical model to be used as a robust training tool for nuclear security physical protection scenarios. The Estimate of Adversary Sequence Interruption (EASI) program is a convenient method of calculating the probability of interrupting adversaries over specific paths (Garcia, 2008). The EASI program for use in the LNRI model was designed to analyze four path types, the first analyzes the path with the least total delay, the second analyzes the path with the smallest probability of detection at each stage, the third path is a random path (this would represent an adversary with a loose plan), and finally the user can input specific values representing a path of their choice. With the activation of the intrusion scenario in the LNRI physical model, times are logged by the Raspberry Pi for the moment of detection by the motion sensor and the moment that the alarm is addressed. These values are delay factors that can affect whether or not an adversary can be interrupted by the response force. In order to visualize the effects of delays between an attack initiation, detection, and addressing of an alarm, an adversary sequence graph is generated. The final design for the EASI program and adversary sequence graph (for simulation results) uses the LibreOffice (2014) spreadsheet program (which is an Openware alternative to Microsoft Excel) with BASIC programming language macros that are used to calculate the probabilities of interruption of various paths or determine if an adversary was interrupted before reaching their target. The workbook consists of 6 separate worksheets, namely

(i) UserInput - The user input sheet has a pre-set list of six physical barriers, with potential methods to breach the barriers. There are 2 user-defined barriers, which can be altered by the user to identify the effects of adding physical barriers to the probability of interruption. Each barrier has 2 user-defined path ways, which are additional barriers that can be added to the system. The probability of detection and the delay for each barrier are user-defined variables. Several buttons are located on the right side of the spreadsheet, which activate specific macros. The fastest path, least probable, and random path buttons generate a column of data which is referenced by the EASI spreadsheets.

(ii) EASI1, EASI2, EASI3 and EASI4 – EASI(1-4) spreadsheets reference values from the UserInput sheet in order to generate the appropriate path. Each EASI spreadsheet references a specific path type: EASI1 generates a path with the shortest delay, EASI2 generates a path with the least probability of detection at each stage, EASI3 generates a random path, and EASI4 is a user freeform spreadsheet where a user can add any values that they choose. The probability of interruption cell calculates the probability using information from columns that are hidden from the user. The EASI spreadsheets are essentially ported and modified version of the EASI spreadsheet in Microsoft Excel, described by Garcia (2008).

(iii) Simulation - The results from the intrusion scenario are fed into the Simulation spreadsheet on the EASI workbook. The data communicated to the program is the amount of time between the adversary start and button pressed. The response time is referenced from the UserInput spreadsheet. When the user requests results, a graph is generated to show the adversary interruption sequence, as depicted in figure 11. It may be seen that the point of adversary interruption occurs when the response force timeline crosses the adversary timeline, which is stepped due to delays at various stages in progress from off-site towards the target.

The interactivity between the LNRI physical model and the EASI calculations in LibreOffice demonstrate to the user the importance of timely relay of alarm condition. It is also possible to introduce errors (either discrete or random) into the system that might mimic realistic scenarios, such as malfunctioning sensors or breakdown in communications.

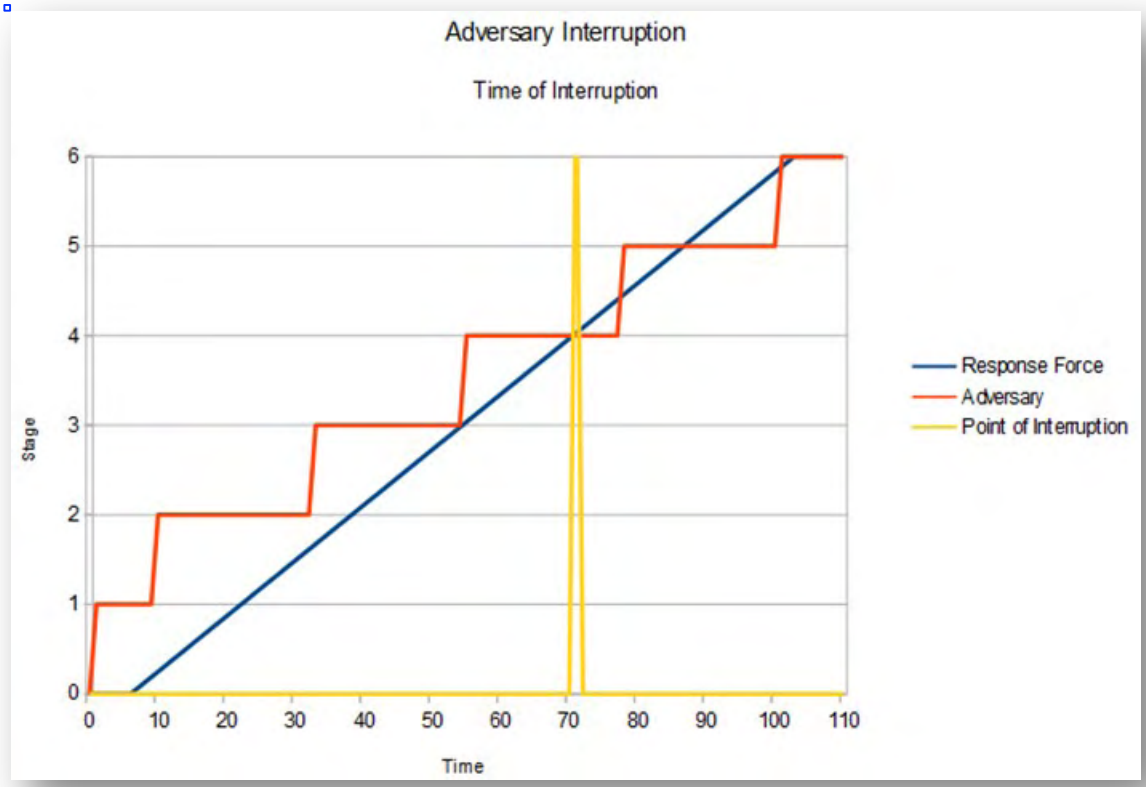


Figure 11 - Adversary sequence interruption.

Conclusions

Training of persons responsible for security at nuclear facilities is resource intensive. The physical model we have developed here is unique insofar as it integrates a physical model of a nuclear facility with interactive elements such as cameras and alarms, and also provides rudimentary analysis using the EASI approach. The total cost of the components used in the model was under $1000 (US dollars), excluding labor. The most expensive components were the model HO- and N-scale buildings, fences, and features which add to the realism of the model. As one of the design goals for the model was modularity, it is relatively straightforward to add additional sensors and intrusion scenarios. We feel that this approach of integrating a physical (visual) model with user interactivity and simple analysis combined through a low-cost computing platform provides an intuitive and cost-

effective alternative for training nuclear security professionals on physical protection systems.

References

Garcia (2008). The Design and Evaluation of Physical Protection Systems, 2nd Ed. By M.L. Garcia. Elsevier Butterworth-Heinemann. New York, NY.

Garcia (2006). Vulnerability Assessment of Physical Protection Systems. By M.L. Garcia. Elsevier Butterworth-Heinemann. New York, NY.

IAEA (2014) Exercise Data for the General Hypothetical Facility and PTR Data. IAEA nuclear Security Training Material NS6.2. International Atomic Energy Agency. Vienna, Austria.

IAEA (2005). *Nuclear Security - Measures to Protect Against Nuclear Terrorism GC(49)/1*. obtained from IAEA.org: http://www.iaea.org/About/Policy/GC/GC49/Documents/gc49-17.pdf

IESNA (2003) Guideline for Security Lighting for People, Property, and Public Spaces. Illuminating Engineering Society of North America. New York, NY.

LibreOffice (2014) LibreOffice – The Document Foundation. Available at http://www.libreoffice.org/

Cyber-Security Evaluation for a Hypothetical Nuclear Power Plant Using the Attack Tree Method

Akinjide A. Akinola
University of Lagos, Lagos, Nigeria
and
Ayoade Kuye and Abiodun Ayodeji
University of Port Harcourt, Port Harcourt, Nigeria

Abstract

The widespread introduction of digital network systems in nuclear power plants has increased the vulnerability to cyber-attacks. We present an attack tree approach to evaluating and analyzing cyber attacks quantitatively in a nuclear power plant network. Information on a hypothetical nuclear power plant network was used to build attack trees that show different attack paths that external adversaries can use to compromise the network. To characterize the ease or difficulty of compromising each attack tree, numerical values were assigned to the leaf nodes. The Return on Attack (ROA) for each intermediate node and the root node were then calculated. This calculation was done by randomly varying the vulnerability values of the leaf nodes within the designated range. On observing high ROA values with the two attack trees, countermeasures were then implemented, a modified network systems constructed, and the ROA re-calculated. The ROA values for the nodes were observed to decrease after implementing the countermeasures on the networks.

Keywords: Attack Tree, Cyber-Attacks, Cyber-Security; Return on Attack, Vulnerability Assessment; Nuclear Power Plant, Return on Attack, ROA, Nuclear Security, Nuclear Safeguards

Introduction

The frequency and impact of cyber attacks on computer/control systems in nuclear power plants (NPPs) have shifted attention to cyber-security. These attacks have also prompted states to establish new regulations to strengthen cyber defense. These regulations established computer security requirements which affect nuclear and related facilities at the various stages of operation. Increasingly, real physical security requires better cyber-security, and also requires physical security practitioners to work with software programs and with hardware devices interfaced to complex cyber networks that have substantial embedded computing or microprocessor power. Cyber vulnerabilities can become quickly physical security vulnerabilities and vice versa (Johnston, 2010a, 2010b). Hence, achieving nuclear security objectives depends largely on the efficiency of computer security controls.

The difficulty involved in protecting cyber-space was highlighted by the recent attempt by the North Atlantic Treaty Organization (NATO) to establish international laws against cyber-attacking of critical infrastructures, including NPPs. A draft copy of the bill is similar to the international rule of engagement during war (Klimburg, 2012). Some suggested solutions for cyber-security are not properly analyzed, or are expensive, time and resources consuming, ineffective, or some combination of these things.

Some of the approaches also fail to recognize the uniqueness of the cyber-threat. For example, cyber- threat actors use no bombs, cars loaded with IEDs, or hijacked planes. One of the unique attributes of cyber-criminals, which could have a high return on attack (ROA), is that they can carry out the most devastating attack just by pressing a computer keyboard, without being physically present at or near the facility where the theft or sabotage is intended. As a result, measures to be adopted must factor in these issues for effective cyber defense.

There are few detailed attempts at quantifying vulnerabilities in networks. Since system security cannot be absolute, quantifiable security metrics are needed. Many studies (Dacier, 1994; Dacier, Deswarte and Kaaniche, 1996; Balzarotti, Monga and Sicari, 2005; Edge, Raines, Baldwin and Grimaila, 2007; LeMay, Ford, Keefe, Sanders and Muehrcke, 2011; Akinola, Kuye and Ayodeji, 2014) have used attack trees, attack graphs, or privilege graphs for both the qualitative and quantitative analysis of network system security. Attack graphs present various interdependencies between attack paths; however, they contain redundant and unnecessary nodes, making it complicated and difficult to analyze quantitatively. The attack tree model provides insight into the attack methodology. The model displays step-by-step methodology involved in carrying out an attack successfully (Amenaza, 2003). Commercial software for constructing attack trees (Amenaza, 2012; Kordy and Schweitzer 2013) for easy and scalable modeling of complex systems is available, but user-defined metrics cannot be added to the model design.

To evaluate information security, Cremonini and Martini (2005), proposed using the ROA and the return on investment (ROI) to measure how the attackers' preferences change with the selected security measure. Their work compares the capital invested on the security apparatus and the gains from such investments. It reveals the cost implication and possible profit from security investments. However, these models were not tested on any practical system.

The Common Vulnerability Scoring System (CVSS) presented by Mell, Scarfone and Romanosky (2006) provides a framework for presenting the characteristics and impacts of system vulnerabilities. CVSS-based metrics apply directly to the

exploitability of the vulnerability and are updated as knowledge about attacks becomes available.

Edge et al. (2007) analyzed security measures for mobile *ad hoc* networks using attack and protection trees. Defense-trees were used to depict how vulnerabilities could be eliminated. This approach, however, did not consider the fact that some security measures can eliminate several vulnerabilities in cyber-space. Hence, their defense trees have overpopulated and redundant nodes. The commitment of an attacker was also not considered in these models. Commitment refers to the willpower an attacker exhibits and time committed in pursuit of a goal. This metric will determine the level of risk the attacker is willing to take.

Akinola et al. (2014) quantitatively evaluated the effect of cyber attacks on a school network. They established that by implementing countermeasures, the risk of cyber attacks could be reduced. The current work applies a similar methodology to a hypothetical nuclear power plant network. However, unlike the work of Akinola et al. (2014), which uses single values for the leaf nodes, the current work generates these values randomly.

The Hypothetical Nuclear Power Plant Network System

The computer network for a hypothetical nuclear power plant is shown in figure 1. The network topology is divided into 4 units comprising the Safety Control Unit (Zone A), the Business Processing Unit (Zone B), the Data Acquisition Unit (Zone C), and the Process Control Unit (Zone D). The control room is at the center of the units, connected with the other units via data cables. The remote shutdown (control room B) is also connected with the safety unit via a wired network.

The Business Processing unit houses the Business and Information local area network (LAN) and its systems are connected to the Internet via a hardware firewall (Firewall B) and an edge router. The hosts on the Business Processing unit network are the Database Server (Cent OS), Windows 7 workstations, and a Linux 14.1 Operating System Application Server. The four zones are linked with a wired network. There are three hardware firewalls; each provides access controls to Zone A (Firewall A), Zone B (Firewall B), and the control room (Firewall D). The control room is connected to a acquisition network via Firewall D, and the safety network gateway is connected to the business LAN via Firewall A.

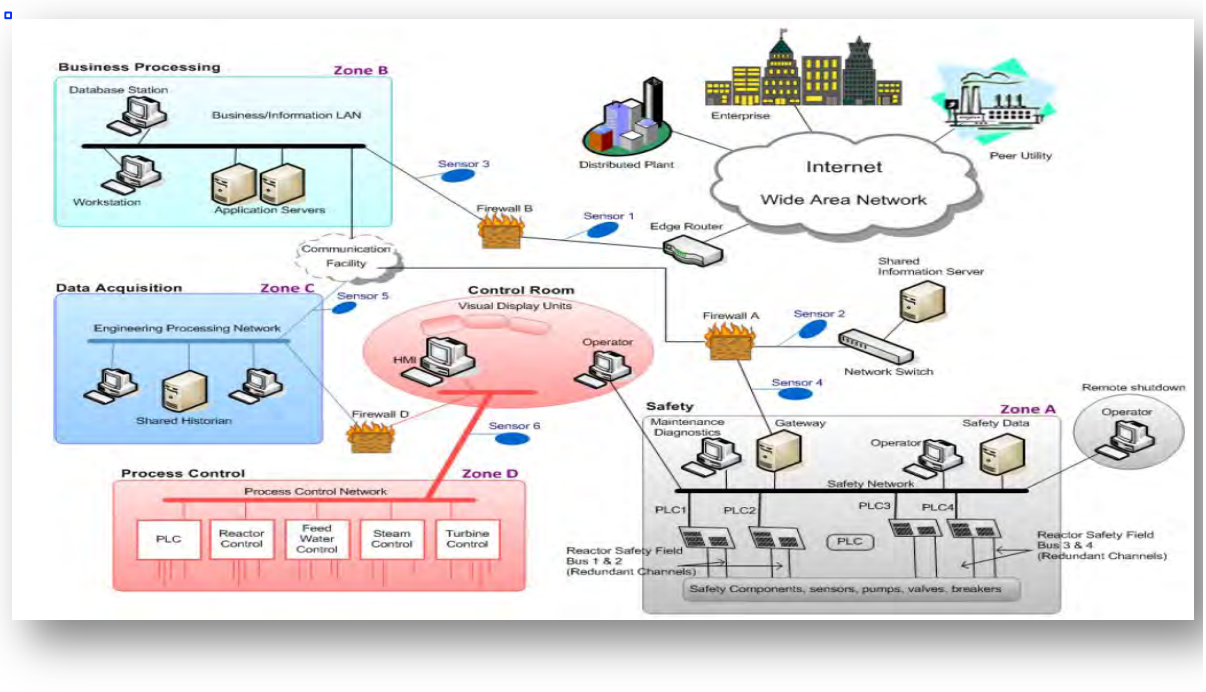


Figure 1 - A Network Diagram of Hypothetical Nuclear Power Plant (USNRC, 2012).

The Safety network system topology and the associated instrumentation and control system are represented by Zone A. The device of interest for the analysis is the operator workstation (OW), Maintenance and Diagnostic system (M&D), and the Gateway, housing firewall A. A gateway is positioned at a network point to control the entrance or exit of data flows between networks. The safety network system is connected to the business processing unit (Zone B) through firewall A. The operator workstation (OW) and Maintenance system (MD) are Siemens Process Control System (Siemens PCS step 7) running on a Windows operating system.

In the data acquisition network system (Zone C), there are two hosts and a server. The two hosts are host 1 (H1, running on Linux 14.2 OS), and host 2 (H2, running on Windows 2000) respectively. The Zone C network is connected via firewall D to the control room by a data cable.

The Attack Tree Model

Two Attack Tree scenarios by which the Control Room (root node) could be compromised were identified. The tasks needed to achieve the success of the attack are presented in figures 2 and 3. The Attack Trees were constructed in consultation with knowledgeable persons in the field. On the Attack Trees, the task that must be performed simultaneously in order to compromise a node are joined be an arc, while those that are not, requires one or the other of the tasks to achieve success.

Mathematically, this can be represented using the Boolean notation "AND" or "OR" respectively.

The Return On Attack (ROA) in this work is given by (Akinola et al., 2014):

$$R = P_o C P_s \quad (1)$$

where P_o = payoff; C = commitment; P_s = probability of success.

P_s is assumed to have a unit value (100% chance of success) since credible attackers have the capability and the intention to exploit a node. The payoff values range from 1 to 10 and are classified as shown in table 1 (Edge et al., 2007). L, M, H and VH represent Low, Medium, High, and Very High, respectively.

Table 1: Quantifying Attack Payoff (Edge et al., 2007)

Numerical Range	Payoff definition
1-3 L	Minor impact to the system. Attack could be easily detected and/or repaired.
4-6 M	Moderate impact to the system. There is reduced performance or interruptions in resource availability. Integrity, confidentiality and availability of the system are affected. Requires special effort to detect and/or repair.
7-9 H	Severe impact to system. Significant damage results. There are considerable informational disclosure and access to some system files. Considerable effort required to detect and/or repair damage.
10 VH	System completely compromised, inoperable, or destroyed. The attacker can render the resource completely unavailable.

The probability of success is calculated using the equation:

$$P_s = A_{cv} * C_A * A_u \quad (2)$$

where A_{cv}=Access Vector, C_A= Access Complexity, and A_u=Authentication.

The access vector (A_{cv}) shows how a vulnerability might be exploited. The access complexity (C_A) metric describes how easy or difficult it is to exploit the discovered vulnerability. The authentication (A_u) metric describes the number of times that an attacker must authenticate to a target node in order to exploit it. It does not include (for example) authentication to a network to gain access. For locally exploitable vulnerabilities, this value should only be set to Single or Multiple if further authentication is required after initial access. Numerical values for the access vector,

access complexity, and authentication are derived from the Common Vulnerability Scoring System guide (Mell et al., 2006).

The intermediate and root nodes, P_o and P_s, are calculated using equations (3), (4), (5) and (6) (Edge et al, 2007):

For AND nodes:

$$P_s = \prod_{i=1}^{k} prob_i \quad (3)$$

$$P_o = \frac{10^k - \prod_{i=1}^{k}(10 - payoff)}{10^{k-1}} \quad (4)$$

For OR nodes:

$$P_s = 1 - \prod_{i=1}^{k}(1 - prob_i) \quad (5)$$

$$P_o = Max_{i=1}^{k} payoff_i \quad (6)$$

where $Prob \in (0,1)$; $Payoff \in [1,10]$; k= number of leaf nodes.

Results and Discussion

For the two Attack Trees in figures 2 and 3, the Payoff, Access Vector, Access Complexity, and Authentication values are obtained from experts in the field; these are presented in tables 2 and 3. These values are used to calculate the ROA values for the leaf and intermediate nodes. These values are used to calculate the ROA values required to compromise the Control Room for Attack Trees A and B (figures 2 and 3). The ROA values are 7.98 and 9.40 at the root node for Attack Trees A and B, respectively. Clearly the ROA values at the root nodes indicate that the vulnerability of the control room can be exploited easily since they values fall in the High range as defined in table 1—the attack tree B being easier because the ROA value exceed 9.

The expert opinion values in tables 2 and 3 may not represent the real situation. We therefore varied the access vectors, access complexities, and authentication values randomly within a 1%, 5%, 10%, 20%, 30%, 40% and 50% range of the expert opinion values in Tables 2 and 3. The calculations for ROA were performed 10,000 times to simulate probably situations. The results obtained are shown in figures 4 and 5 for Attack Trees A and B, respectively.

Figure 4 shows that for Attack Tree A, the maximum and minimum ROA values are 9.76 and 2.61 when the access vectors, access complexities, and authentication values are varied randomly within $\pm$50% of expert opinion. The implications is that if an error in the expert opinion values are high (50%), the calculated ROA value to compromise the root node may be very high or very low. However, the average for the 10,000

computed values is almost the same as 7.98 that shown in figure 2, confirming that the vulnerability of the control room is still high

Table 2: Data Used to Calculate the Return on Attack for Attack Tree A

Node	Task Name	P_o Payoff	A_u Authentication	C_A Access Complexity	A_{cv} Access Vector
LN1	Install Keylogger	4	1	0.6	1
LN2	Intercept Password	8	1	0.6	1
LN3	Port Scanning	5	1	0.9	1
LN4	Xss attack	6	1	0.6	1
LN5	Client side attack	7	1	0.9	1
LN6	Network Eavesdropping	3	1	0.6	1
LN7	SQL Injection	8	1	0.6	1
LN8	Password Cracking	6	1	0.6	1
LN9	MAC spoofing	5	1	0.6	1
LN10	Packet Sniffing	4	1	0.6	1
LN11	Social Engineering	7	1	0.4	1
LN12	Encrypt Malicious Packet	8	1	0.6	0.4

Table 3: Data Used to Calculate the Return on Attack for Attack Tree B

Node	Task Name	Payoff	A_{cv} Access Vector	C_A Access Complexity	A_u Authentication
LN1	Social Engineering	7	1	0.4	1
LN2	Packet Sniffing	4	1	0.6	1
LN3	Brute force attack	6	1	0.6	1
LN4	Obtain Root Password	7	1	0.9	1
LN5	Cross Site Scripting	8	1	0.9	1
LN6	Inject SQL	8	1	0.9	1
LN7	SSH Attack	5	1	0.6	1
LN8	Winback Callback Elevation Attack	8	0.4	0.6	1
LN9	Ping Sweep	6	1	0.9	1

The maximum and minimum ROA values are 9.40 and 9.19 for the Attack Tree B (figure 5) when the Access Vectors, Access Complexities, and Authentication values are varied randomly within $\pm$50% of expert opinion values. In this case, however, the

difference between the maximum and minimum ROA values are smaller. The error is within 2% of the ROA value for the root node in figure 3, even when the error in expert judgment values is 50%. The maximum ROA values are approach the average values regardless of the magnitude of the error in expert judgment values.

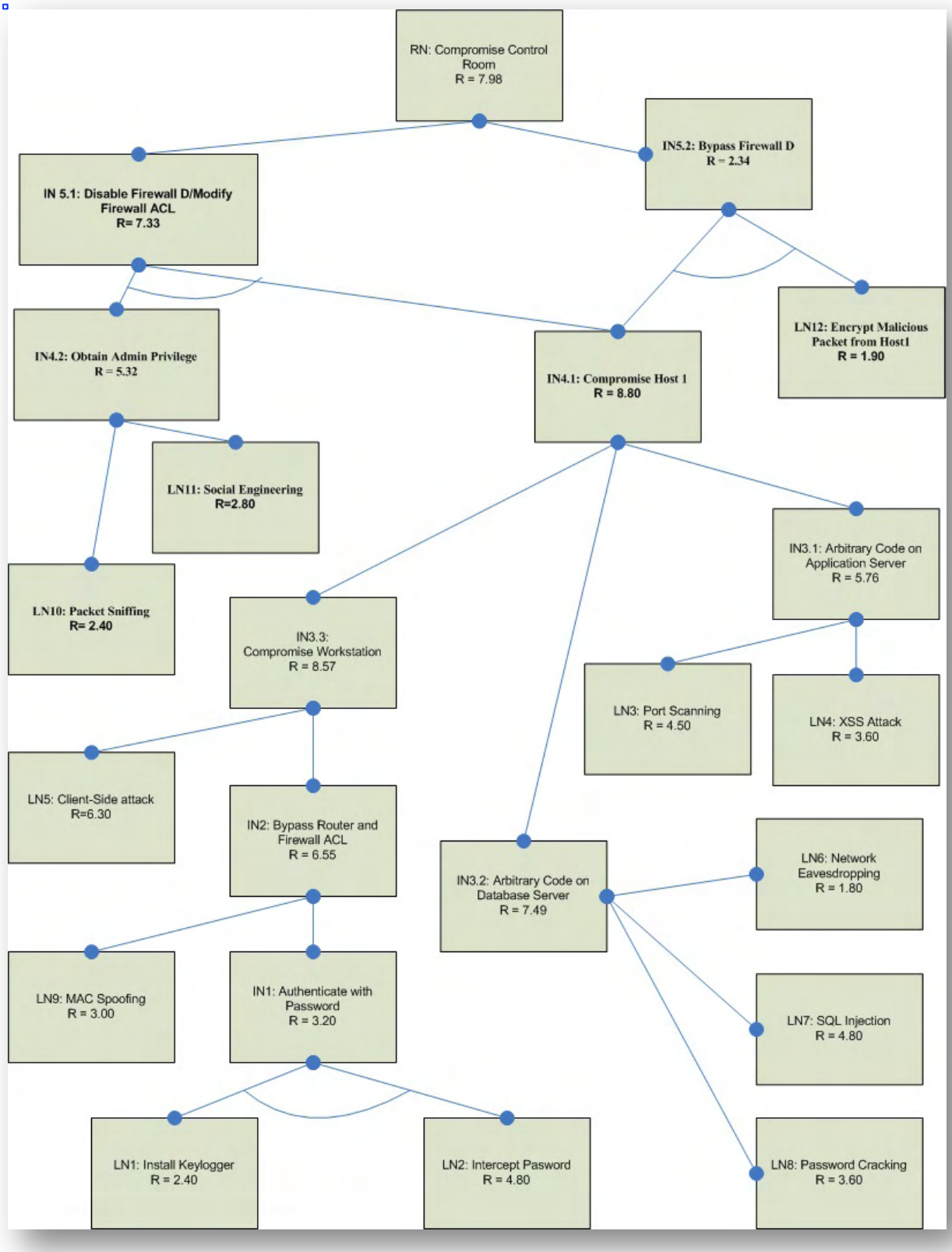


Figure 2 - Attack Tree A.

Clearly, the ROA values in both the Attack Tree A and B are high. The implication is that an upgrade of the two trees is needed to reduce their vulnerability. The suggested upgrades are:

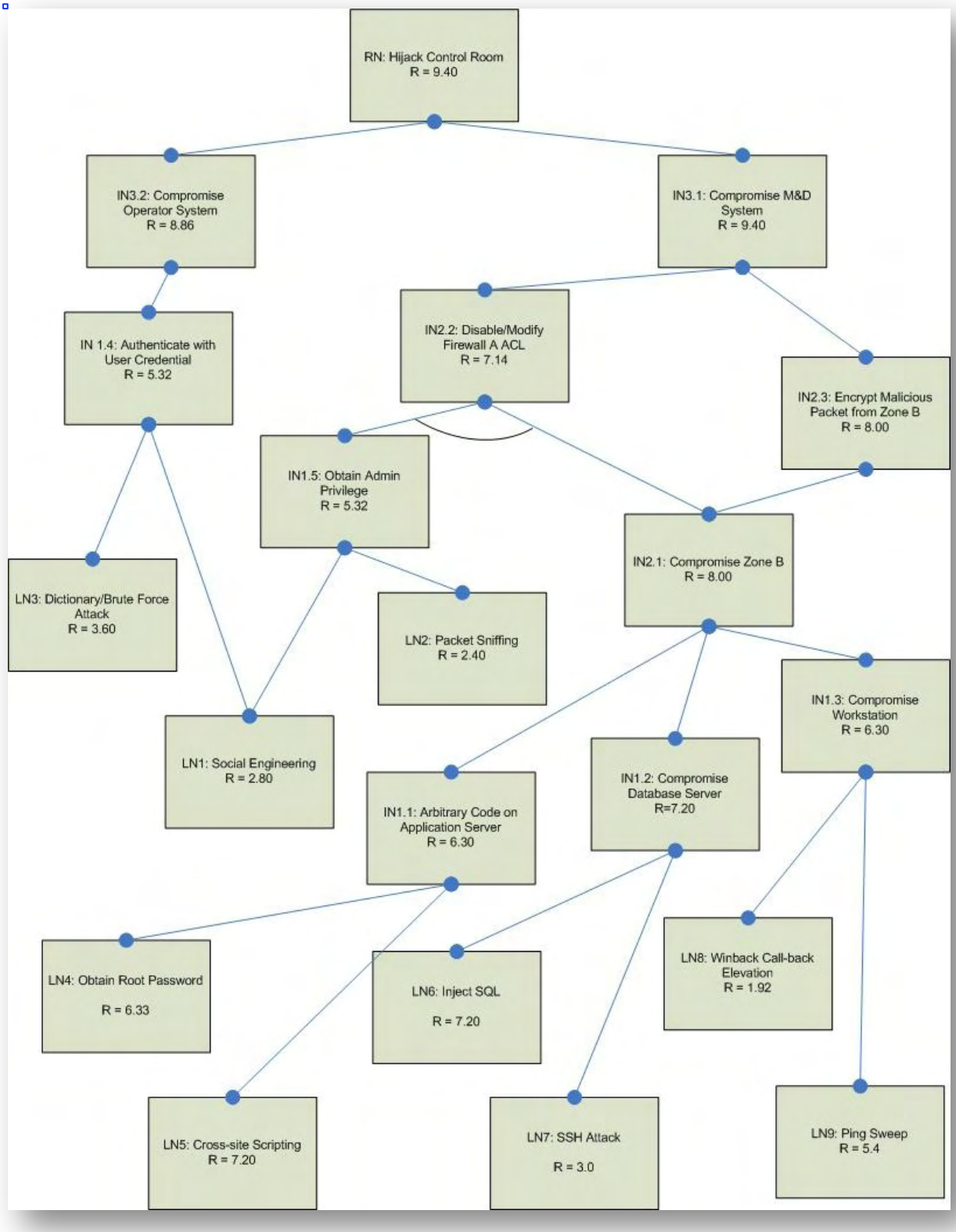


Figure 3 - Attack Tree B.

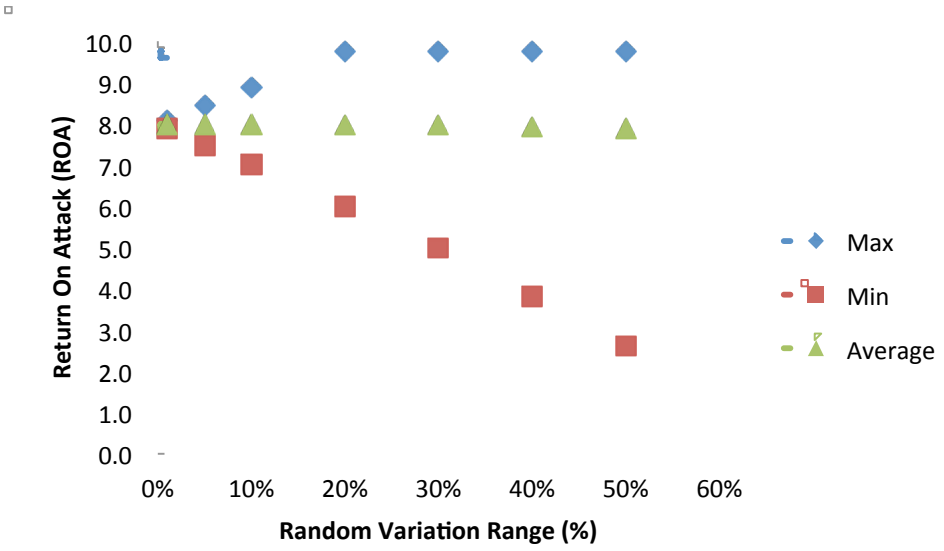


Figure 4 - ROA values with random variation in A_{cv}, C_A, and A_u values For Attack Tree A.

Figure 5 - ROA values with random variation in A_{cv}, C_A, and A_u values For Attack Tree B.

The required upgrades for the component tasks on the Attack trees are:

1. Adding Intrusion Detection and Prevention Systems (IDPS) at "sensors" on the network diagram
2. Replacing Windows Operating System machines with Linux Operating System computers, as the latter have more security features than the former.
3. Adding Remote Access Servers (RAS) before the business processing unit of the NPP digital Network, as all inbound and outbound traffic is routed through this unit.

These security upgrades are implemented at the Leaf Nodes. Again, using expert judgment, new Access Vectors, Access Complexities, and Authentication values are obtained for the Attack Trees A and B. These values are shown in tables 4 and 5 for the Attack Trees A and B, respectively. The ROA values for the nodes are recalculated and the results are presented in figures 6 and 7 for the upgraded Attack Trees A and B respectively. The nodes where upgrades were implemented are marked with a star in the diagrams.

The ROA at the root nodes are 4.32 and 6.63, respectively for Attack Tree A and Attack Tree B. These values are lower than what they were before the upgrades, and the values fall in the medium score range for ROA values. Thus, the suggested upgrades would reduce the vulnerability of the control room.

Table 4: A Data Used to Calculate the Return on Attack for Attack Tree A After Upgrade

Node	Task Name	Payoff	A_u Authentication	C_A Access Complexity	A_{cv} Access Vector
LN1	Install Keylogger	4	0.7	0.6	0.4
LN2	Intercept Password	8	0.7	0.4	0.6
LN3	Port Scanning	5	1	0.4	1.0
LN4	Xss attack	6	0.7	0.6	0.4
LN5	Client side attack	7	0.7	0.6	0.4
LN6	Network Eavesdropping	3	0.7	0.4	0.6
LN7	SQL Injection	8	0.7	0.6	0.4
LN8	Password Cracking	6	0.7	0.6	0.6
LN9	MAC spoofing	5	0.4	0.9	0.4
LN10	Packet Sniffing	4	0.7	0.4	0.6
LN11	Social Engineering	7	1.0	0.4	1.0
LN12	Encrypt Malicious Packet	8	0.4	0.4	0.4

Again, to obtain a better estimate of the ROA values at the Root nodes for each Attack Trees, repeated calculations were performed by randomly varying the Access Vector, Access Complexity, and Authentication values up to the $\pm$50% range. The calculations were performed 10,000 times with randomly generated values of Access Vectors, Access Complexities, and Authentication. A summary of the results is shown graphically in figures 8 and 9 for Attacks Trees A and B, respectively. Again the results show that the error in ROA vale increase proportional with the errors in Access Vector, Access

Complexity, and Authentication values; however, the ROA values average out to the values obtained in figures 6 and 7 for the Attack Tree A and B, respectively.

Conclusion

This work considered two attack scenarios on the control room of a hypothetical NPP network and quantitatively evaluated the network security using an attack tree model. Using the developed models, the calculated ROA for each attack scenario were high (> 7.9). This means that the control room can be easily compromised. When suggested upgrades were implemented, the ROA values reduced to 4.32 and 6.63 for Attack Tree A and Attach Tree B, respectively. Even when errors in the Access Vector, Access Complexity, and Authentication values were used to calculate the ROA values, the values fell within the 4 – 7 range, which is an acceptable range. The model can, therefore, be used to quantify the vulnerability of computer network.

Table 5: A Data Used to Calculate the Return on Attack for Attack Tree B After Upgrade

Node	Task Name	Payoff	A_{cv} Access Vector	C_A Access Complexity	A_u Authentication
LN1	Social Engineering	7	0.6	0.4	0.4
LN2	Packet Sniffing	4	0.6	0.4	0.7
LN3	Dictionary/Brute force	6	0.4	0.6	0.4
LN4	Obtain Root Password	7	0.4	0.6	0.4
LN5	Cross site scripting	8	0.6	0.4	0.7
LN6	Inject SQL	8	0.6	0.4	0.4
LN7	SSH attack	5	0.6	0.4	0.4
LN8	Winback callback elevation attack	8	0.6	0.4	0.4
LN9	Ping sweep	6	0.6	0.6	0.4

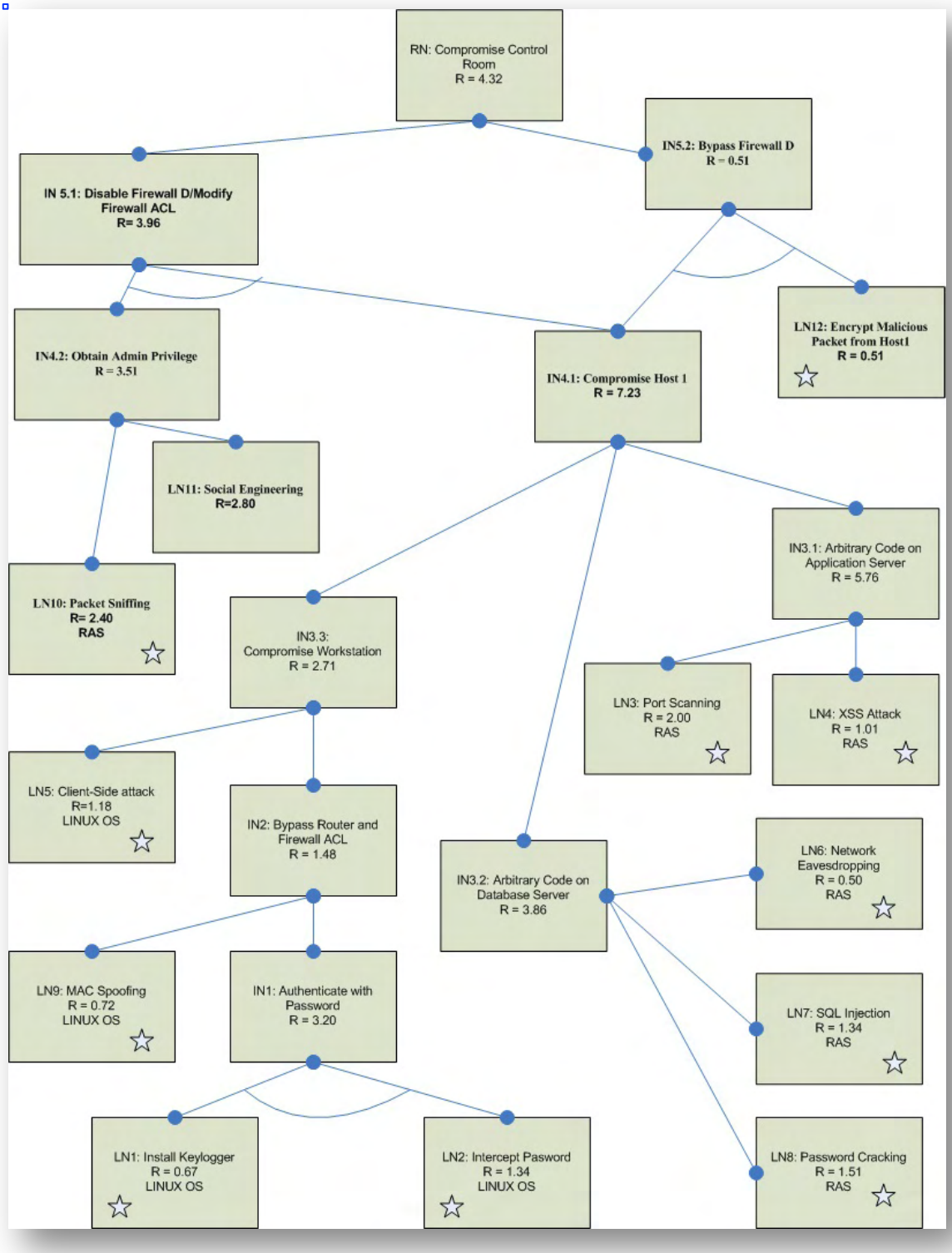


Figure 6 - Attack Tree A After Implementing Upgrades.

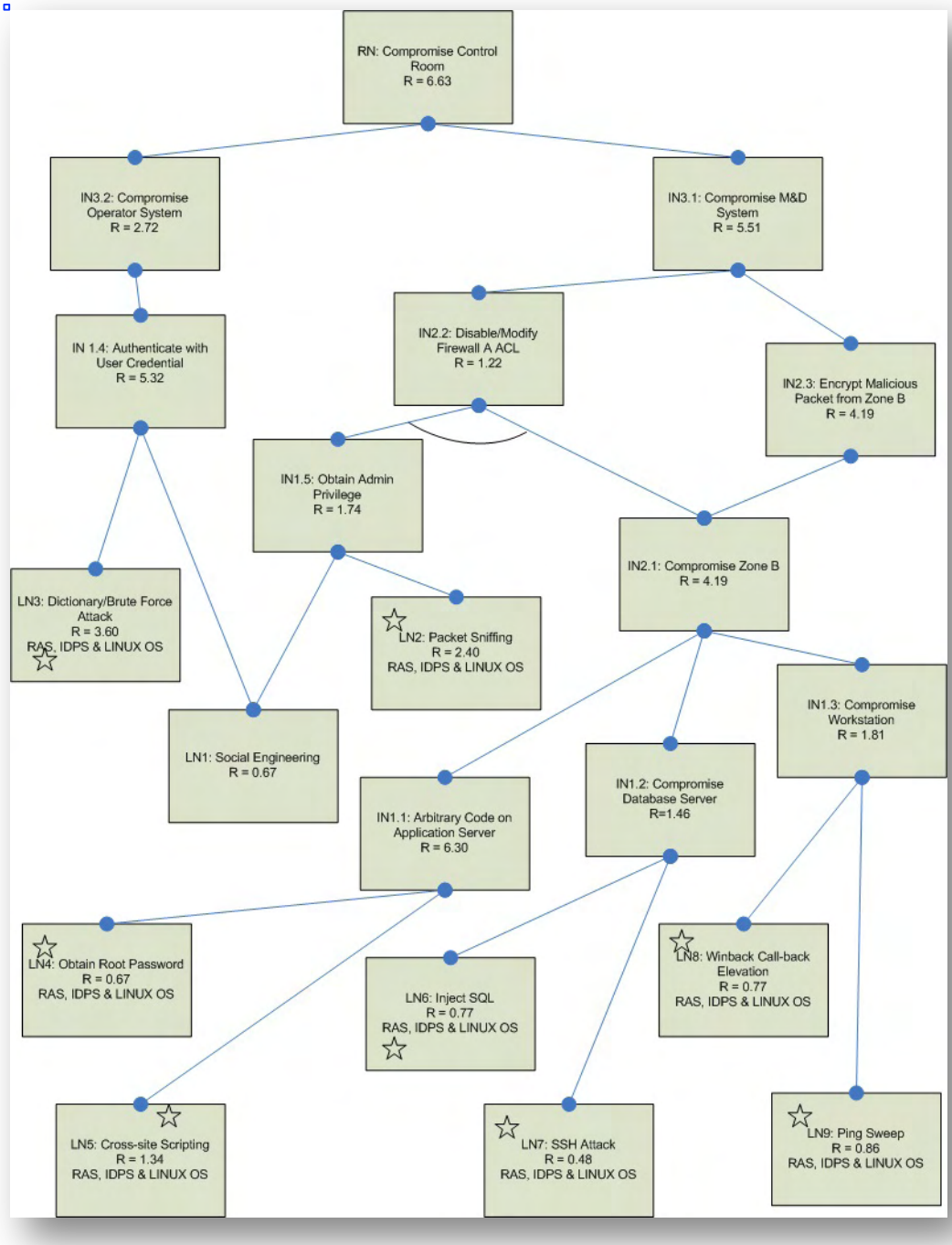


Figure 7 - Attack Tree B After Implementing Upgrades.

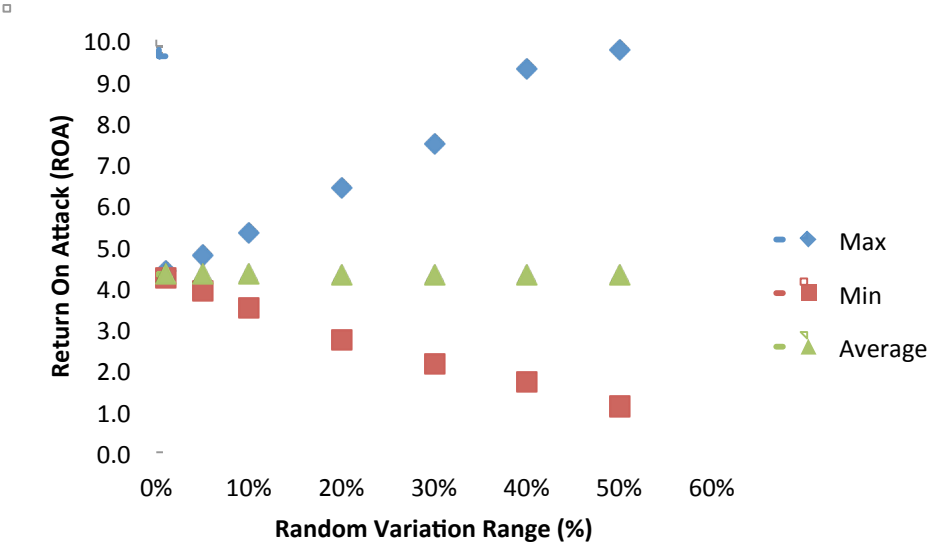


Figure 8 - ROA values with random variation in A_{cv}, C_A $and A_u$ values For Attack Tree A after upgrade.

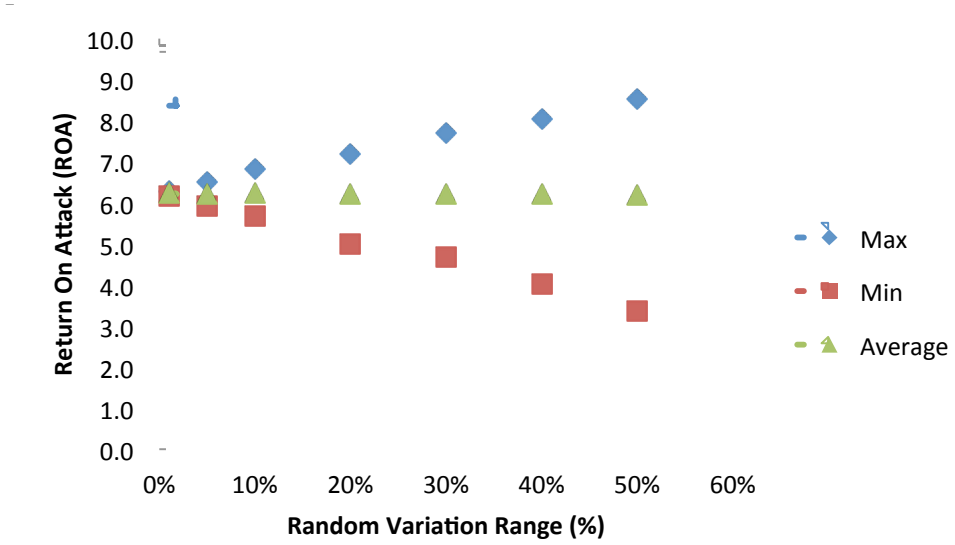


Figure 9 - ROA values with random variation in A_{cv}, C_A $and A_u$ values For Attack Tree B After Upgrade.

Acknowledgement

The authors are grateful for the financial support provided by the Nigeria Atomic Energy Commission (NAEC), Abuja, Nigeria for this research.

References

Akinola A. A, Kuye A. O. and Ayodeji A. (2014), Cyber-Attacks Analysis of a School Network , 55th Annual Meeting of the Institute of Nuclear Materials Management (INMM) to be held at the Atlanta Marriott Marquis in Atlanta, Georgia, USA, July 20-24, 2014.

Amenaza (2005), Fundamentals of Capabilities-based Attack Tree Analysis, Amenaza Technologies Limited, Suite 550, 1000 8th Ave SW, Calgary, Alberta, Canada T2P 3M7.

Amenaza (2012), Creating Secure System through Attack Tree modeling, Amenaza Technologies Limited, Suite 550, 1000 8th Ave SW, Calgary, Alberta, Canada T2P 3M7.

Balzarotti D., Monga, M. and Sicari, S., (2005), Assessing the risk of using vulnerable components ; In Proceedings of the 1st Workshop on Quality of Protection. New York, NY, USA.

Cremonini, M., and Martini, P., (2005), Evaluating Information Security Investments from Attackers Perspective: the Return-on-Attack (ROA), 4th Workshop on the Economics on Information Security, Kennedy School of Government, Harvard University, Cambridge, MA, USA,

Dacier, M., (1994), Towards Quantitative Evaluation of Computer Security, Ph.D. Thesis, Institute National Polytechnique de Toulouse

Dacier, M., Deswarte, Y. and Kaaniche M., (1996), Quantitative assessment of operational security: Models and tools. Published in:Information systems security, Pages 177-186 Chapman & Hall, Ltd. London, UK, UK ©1996 ISBN:0-412-78120-4

Edge, K., Raines, R., Baldwin, R., and Grimaila, M., (2007), Analyzing security measures for Mobile Ad hoc Networks Using attack and Protection Trees, Proceedings of 2nd international conference on i-warfare and security, Naval Postgraduate School, Monterey, California, USA. Ppg 50-51. http://wwwpub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

Johnston, R. G., (2010a), Being vulnerable to the threat of confusing threats with vulnerabilities, Journal of Physical Security, 4(2), 30-34(2010).

Johnston, R. G., (2010b), Changing Security Paradigms, Journal of Physical Security 4(2), 35-47 (2010).

Kilmburg, A., (Ed), (2012), National Cyber Security Framework Manual, NATO CCD COE Publications, Filtri tee 12, 10132 Tallinn, Estonia, ISBN 978-9949-9211-1-9

Kordy, B. and Schweitzer, P., (2013).The ADTool Manual., Retrieved October 2, 2013 from www.satoss.uni.lu/projects/atrees/adtool.

LeMay, E., Ford, M.D., Keefe, K., Sanders W.H. and Muehrcke, C., (2011), Model-based Security Metrics using ADversary VIew Security Evaluation (ADVISE), Proceedings of the 8th International Conference on Quantitative Evaluation of SysTems (QEST 2011), Aachen, Germany, Sept. 5-8, 2011, pp. 191-200.

Mell, P., Scarfone, K. and Romanosky, S. (2007),. A Complete Guide to the Common Vulnerability Scoring System Version 2.0., IEEE Security& Privacy Magazine, 4(6):85–89.

United State Nuclear Regulatory Commission (USNRC), (2012), Secure Network Design. Prepared by, Michalski, J. T. and Wyant, F. J., Division of Engineering, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001,NRC Job Code N6116.

About the Authors

Dr. Akinjide A. Akinola graduated from the University of Ife, Nigeria in 1979 with a degree in Chemical engineering. He later went to the University of Strathclyde, Glasgow, UK where he obtained a Master's of Science degree in Plant and Process Design in 1981 and a Ph.D. in Chemical and Process Engineering in 1985. Dr. Akinola also holds a Masters of Business Administration degree with emphasis on Technology Management from the University of Phoenix, Arizona, USA. He has worked as a consultant, both in the Information Technology and Engineering industries for various companies in Europe, the United States of America, and Nigeria. Professionally, Dr. Akinola is a Registered Engineer (COREN) in Nigeria, a Member of the American Institute of Chemical Engineers, a Member of the Nigerian Society of Engineers, and a Member of the Nigerian Society of Chemical Engineers. In his present appointment, he lectures at the University of Lagos, and has adjunct positions in Cyber Security at the University of Maryland, University College, USA and the Centre for Nuclear Energy Studies at the University of Port Harcourt, Nigeria.

Dr. Ayoade O. Kuye graduated from the University of Lagos, Nigeria in 1978 and later received a doctorate degree in Chemical Engineering from the University of Strathclyde, Glasgow in 1984. Dr. Kuye started his academic career at the Department of Chemical Engineering, University of Port Harcourt, Port Harcourt in 1985 and rose to the rank of Professor by 1996 in the same department. His research work falls within the computer-aided mathematical modeling area of Chemical Engineering with an emphasis on process simulation, synthesis and optimization, and alternative energy sources. To date, he has numerous journal publications and books and numerous technical reports/monographs to his credit. He is an external examiner and external assessor to many Universities in Nigeria. Professionally, Dr. Kuye is a Registered Engineer (COREN), a Fellow of the Nigerian Society of Chemical Engineers, and a Member of the Institute of Nuclear Materials Management. In his present appointment, he is the Director of the Centre for Nuclear Energy Studies at the University of Port Harcourt, Nigeria.

Mr. Abiodun Ayodeji obtained his Bachelor of Engineering degree in Electrical Engineering from the University of Ilorin, Nigeria, in 2007. He obtained his Masters

degree in Nuclear Engineering in 2014 from the Centre for Nuclear Energy Studies, University of Port Harcourt, Nigeria. He has worked as a Research Engineer at the Centre for Energy Research and Development, Obafemi Awolowo University, Ile-Ife, Nigeria. In his present appointment, he works at the Nuclear Power Plant Development Division, a Directorate in Nigeria Atomic Energy Commission, Abuja, Nigeria. Mr Ayodeji is a member of World Institute for Nuclear Security (WINS), and a member of International Network of Emerging Nuclear Specialists (INENS).

Journal of Physical Security 8(1), 37-39 (2015)

Viewpoint Paper

Why Security Fails*

Roger G. Johnston, Ph.D., CPP
Right Brain Sekurity

In thinking about how nuclear security and safeguards can fail, it is useful to keep in mind why security usually fails in general. Most security managers and organizations have a good understanding of the assets they are trying to protect, the resources available to them to protect those assets, and the consequences should security fail (though this is sometimes greatly underestimated). They often have a reasonably accurate understanding of the threats they face—who might attack, why, how, when, and with what goals and resources. What is often lacking is a good understanding of the vulnerabilities—the weaknesses in the security that can be exploited by the threats—and how those vulnerabilities can be mitigated or eliminated.

Some recent major security failures serve as good examples. The intrusion deep into the Y-12 nuclear facility by an 82-year old nun and her fellow protesters wasn't because nuclear protesters weren't understood as a threat for trespassing. Similarly, the recent incident at the White House where an individual jumped the fence and entered the unlocked front door of the White House is another example where the threat was well understood—people have been jumping the fence at the White House for a long time—but the security vulnerabilities were either unrecognized or not properly neutralized. The damaging cyber attacks at Target and Sony were similar in that the threat was not new, but the vulnerabilities were poorly recognized and dealt with.

Much of the problem in my view is that the vulnerability assessment (VA) component of risk management—especially for nuclear security/safeguards and especially for layered security—is largely missing in action. Nuclear facilities and organizations will frequently claim to analyze their security, but these assessments are often highly inadequate for understanding vulnerabilities, including those that can be exploited by insiders

A number of different security analysis techniques—while still potentially useful—frequently get confused with VAs. These include security surveys (walking around with a checklist), security audits (checking if the rules are being followed), comparing security practices with general "standards" or "guidelines" or "best practices" (which may themselves be flawed or too simplistic or too generalized for the local culture). Other techniques not very effective at finding vulnerabilities include threat assessments, feature

---

* *This viewpoint paper was not peer-reviewed. A version of this paper appeared in Nuclear Security Matters, February 11, 2015.*

analyses, fault or event tree analyses (from safety engineering; often very problematic for security analysis), the Delphi Method (a technique for getting a decision from a panel of experts), software assessment tools, the CARVER Method (often used by the U.S. Department of Defense and law enforcement), and Modern Risk Management.

The widely used Design Basis Threat (DBT)—the common sense idea that security should be designed to counter real threats—is particularly bad at identifying vulnerabilities because it is a threat analysis technique. The common practice of using DBT to "test" nuclear security and safeguards is potentially disastrous because the logic is circular; DBT is used to define the security problem in the first place, so it cannot be used to reliably determine the efficacy of the security that was deployed as directed by the DBT model itself

"Red Teaming" is often held up as a kind of VA, but in the nuclear realm, the term has frequently come to mean a narrowly defined, binary, unrealistic or rigged occasional "test" of a small subset of possible attack scenarios and vulnerabilities. This "test" is often undertaken by unimaginative personnel burdened by a significant conflict-of-interest in regards to the results.

What is sorely lacking is frequent, independent, imaginative, and comprehensive VAs by personnel who are skilled at finding vulnerabilities and countermeasures, and who aren't subject to "shooting the messenger". Their findings and recommendations must be objectively evaluated free from organizational wishful thinking and cognitive dissonance. Good security is proactive, and that requires understanding and managing vulnerabilities in an honest way. Few nuclear facilities or organizations seem to be able to do this, despite frequent assertions to the contrary.

There is another aspect of VAs that is also underutilized, especially in the nuclear arena. With something as important as nuclear security and safeguards, there is a natural tendency to want to provide "" that the security and safeguards are adequate. But this is a difficult and value-judgment kind of problem.

There is a more effective way to judge security efficacy, which I call the Marginal Analysis or (Differential Analysis). The idea is to find the set of security parameters that best minimizes the risk. This is a complex problem because there are a myriad of possible security parameters, each with a lot of possible values or settings. Analyzing all possible parameters and settings is not practical. What makes more sense is to consider our current security parameters and settings, then consider changes to them. If these changes make the risk go lower, we may want to try more changes of this type. If the changes make the risk worse, we may want to try other possibilities.

This is where vulnerability assessors come in. They can tell you how much security would improve if you make any given set of changes. The goal then is not to seek absolute, binary assurance, but rather to experiment, at least in principle, with security changes to help find ways to reduce vulnerabilities, complicate things for adversaries, and lower

overall risk. We know that we have "pretty good security" (at least for the moment) when we can't find any practical changes that significantly decrease our risk.

[For those mathematically inclined (and skip this paragraph if you're not), this process is analogous to plotting the security risk in N-dimensional space against the values of a large number, N-1, of security parameters. The goal is to find a deep local minimum in this complicated surface in N-dimensional space in order to minimize the risk. In theory, we would like to find the absolute minimum because this would tell us how to *best* configure our security. In practice, however, it is mathematically challenging to find the absolute minimum in a space of many dimensions for such a complex surface. We should settle instead for a good *local* minimum and not let the best become the enemy of the good. In applied mathematics, local minima are often found by taking trial steps in various directions in N-dimensional space in order to determine where the gradient points downward the steepest. As with any minimization problem in N-dimensional space, it is often wise to consider large changes in order to check whether there are better minimums "over the hill". Thus, not all considered changes should be minor tweaks. Note also that finding the mathematical minimum in N-dimensional space is only an analogy. Optimizing security is not really a mathematical problem, at least at this stage of our understanding of security. It is, course, important to bear in mind as well that the risk surface in N-dimensional space is not static, but is always morphing over time with changes in threats, technology, assets we need to protect, resources available to us to provide security, etc. Thus, we can't sit permanently at one point in N-dimensional space and think we are good for all time.]

The Marginal Technique can do more than just help us judge our security while avoiding absolutist, binary, wishful-thinking about "assurance". With this technique, we are constantly thinking about security and about security *changes*. This can help a security program remain flexible, adaptable, and proactive, and avoid the problem of inertia commonly found in large bureaucratic organizations.

About the Author: Roger G. Johnston, Ph.D., CPP was the head of the Vulnerability Assessment Teams at Los Alamos National Laboratory (1992-2007) and at Argonne National Laboratory (2007-2015). Currently he is the CEO of Right Brain Sekurity (rbsekurity@gmail.com), a company devoted to creative security solutions.

Estimation of Cluster Sensors' Probability of Detection for Physical Protection Systems Evaluation

W. I. Zidan

Nuclear and Radiological Regulatory Authority, Nuclear Safeguards and Physical Protection Department, P.O. Box 11762, Cairo, Egypt, najzidan@yahoo.com

Abstract

Cluster sensors are vital components of physical protection systems, and are used extensively to detect intrusion. It is essential to insure that a particular sensor will meet the design criteria of the physical protection system. In this paper, performance evaluation and operational procedures of Glass Breakage (GB) and Open Door (OD) sensors are presented and discussed. Several intrusion tests were carried out inside the detection areas of the sensors in order to evaluate their performance during a particular intrusion process. Experimental results are presented here. The probabilities of detection for both GB and OD sensors were estimated.

Keywords: *Physical Protection Systems, Intrusion Detection, Cluster Sensors, Security Sensors, Intrusion Detection.*

1. Introduction

Nuclear security focuses on prevention and detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities. It aims to protect persons, property, society, and the environment from harmful consequences of a nuclear security event.[1] One of the main pillars of nuclear security is physical protection which is an integral part of nuclear security. Physical protection systems (PPSs) for nuclear facilities are necessary to achieve the desired protection, and they

are based on a combination of personnel, hardware, procedures, and facility design.[2] All PPSs must be subjected to vulnerability assessments or tests, to judge how effective they will be in warding off attacks from adversaries.

This paper is concerned with protection of nuclear facilities using hardware, specifically electronic hardware. Because the evaluation of the performance of equipment used in PPS is an important element in designing and maintaining PPS, we applied a method for evaluating the performance of intrusion detection systems (IDSs). The IDSs used in this study were Glass Breakage (GB) and Open Door (OD) sensors. This evaluation can be used to compare the performance of intrusion detectors, and to evaluate performance goals for them. The operational procedures and probability of detection (PD) for the tested sensors were investigated and are discussed in this paper.

2. Physical Protection Systems

A PPS is an integrated set of physical protection measures intended to prevent the completion of a malicious act.[3] The purpose of a PPS is to prevent an adversary from successful completion of a malevolent action against a facility or its personnel. The primary PPS functions are detection, delay, and response. For a system to be effective, there must be awareness that there is an attack underway (detection), and slowing of adversary progress to the targets (delay), thus allowing the response force enough time to interrupt or stop the adversary (response).[4] PPSs at different sites are seldom identical because of the differences in facilities, targets, and threats. The basic design for PPSs is quite well established, though considerable engineering and design fine-tuning is usually required for each site.[5]

The physical protection sub-system first encountered by adversaries in any facility should serve as a substantive deterrent by presenting a difficult obstacle to penetrate. The obstacle usually involves non-electronic systems such as steel gates, but in recent times, there has been an increased use of electrified fences and armored floodlights as the first line of defense.[6] In designing PPSs, several criteria have to be taken into

consideration; this includes such things as the characteristics of PPSs, functional conformity, vulnerability assessments, and the nature of adversaries.[7]

Detection—which is the discovery of an intrusive action at any point in the protection system—is usually reported by an intrusion sensor and announced through the alarm communication sub-system. The intrusion alarm must then be followed by an assessment; if appropriate, the response force will then be notified. The detection of an intrusion or an attempted intrusion into a protected area is one of the basic functions of a PPS. It is important to make this detection as early as possible after the start of the intrusive action in order to provide the maximum time for assessment and response. Maximum delay usually requires detection as far from the target as possible.[5]

3. Intrusion Detection Systems

Attempts to breach a protected area have to be detected by a PPS, and this is mostly achieved by the use of electronic sensors. These are typically devices that detect changes in a physical quantity (heat, motion, vibration) and convert them to electrical signals. These signals are then made readily available for indication and/or annunciation at the central alarm station (CAS) via transmission sub-systems. Providing a supplementary means of indication at the point of detection may also serve as a deterrent.

IDSs are usually considered as the second line of defense; they can protect with high accuracy against internal attacks. This mechanism allows detecting abnormal or suspicious activities on the relevant target, and triggers an alarm when intrusion occurs. Many studies in the application of the IDS technology in *ad hoc* networks have been done, in contrast to wireless sensor networks where few studies have been undertaken. The reason is probably the limited energy and computing storage capacity for wireless sensor networks.[8] In practice, IDSs are needed to detect both known security exploits and novel attacks that have yet to be experienced.[9] Reliable intrusion sensors are used extensively as single units and in multiple-unit networks in detection systems of all sizes. Intrusion detectors are often used in overlapping arrays for mutual protection

and reliability.[9] IDSs consist of exterior and interior intrusion sensors, video alarm systems, entry control, and alarm communication system all working together. Interior sensors are those used inside buildings and usually involving the use of a different set of sensors from exterior sensors, which are used in an outdoor environment and are usually mounted on the walls, windows, or doors of a building.[10]

Interior intrusion sensors, when integrated into a system using administrative procedures, access control, and material monitoring, can be highly effective against insider threats. Using interior intrusion sensors that can be correctly placed, installed, maintained, and tested, an alarm can be generated with the occurrence of unauthorized acts or the unauthorized presence of insiders as well as outsiders. There are three main applications for interior sensors [4]:

1- Boundary penetration sensors for detecting penetration of the boundary of an interior area.
2- Interior motion sensors for detecting the motion of an intruder within a confined interior area.
3- Proximity sensors for detecting an intruder in the area immediately adjacent to an object in an interior area, or when the intruder touches the object.

Boundary penetration sensors include vibration, electromechanical, infrasonic, capacitance, proximity, and passive sonic sensors. "Cluster sensors"—distributed arrays of networked sensors—are widely used in PPSs and installed in huge numbers inside nuclear facilities to detect intrusion. They may include Glass Breakage sensors (GBs), Balanced Magnetic Switches (BMSs), or Open Door Sensors (ODs).

A GB sensor is any device intended to detect the breakage of protected glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range. GB sensors use microphone transducers to detect the glass breakage and listen for frequencies associated with breaking glass. A processor filters out all unwanted frequencies and only allows the frequencies at certain ranges to be analyzed. The processor compares the frequency received to those registered as being associated with glass breakage. If the received signal matches frequencies characteristic of breaking glass, then an alarm will be generated. The sensor element is often equipped with a

light emitting diode (LED) activation indicator. The LED should be kept lit until it is turned off.[11]

OD sensors are typically used to detect the opening of a door. These sensors can also be used on windows, hatches, gates, or other structural devices that can be opened to gain entry. When using a BMS, a magnetic unit is mounted on the movable part on the door or window adjacent to switch unit. Typically, the BMS has a three-position reed switch and an additional magnet (called the bias magnet) located adjacent to the switch. When the door is closed, the reed switch is held in the balanced or center position by interacting magnetic fields. If the door is opened or an external magnet is brought near the sensor in an attempt to defeat it, the switch becomes unbalanced and generates an alarm. See Figure 1. A BMS must be mounted so that the magnet receives maximum movement when the door or window is opened. BMSs provide higher level of protection for doors and windows than either magnetically or mechanically activated contacts or tilt switches.[4]

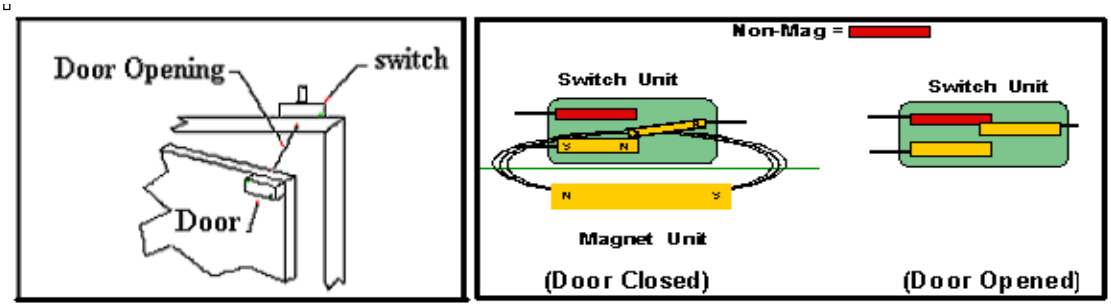


Figure 1 - Schematic diagram of the Balanced Magnetic Switch (BMS).

The intrusion detection evaluation problem and its solution usually affect the choice of the suitable intrusion detection system for a particular environment, depending on several factors. The most basic of these factors are the false alarm rate and the detection rate.[12] IDS accuracy involves evaluating the performance of the IDS and determining the best configuration.[13] Sensor performance testing is usually performed to determine whether a particular sensor will be acceptable for a particular design. These tests permit the user to evaluate the current status of the overall PPSs. It helps to identify shadowed areas from uneven terrain that result in weak (low

detection) spots. Performing a few tests near the sensor head is usually done to determine the optimum offset.[14-15]

Intrusion sensor performance is described by three fundamental characteristics: probability of detection (PD), nuisance alarm rate, and defeat vulnerabilities.[16] An understanding of these characteristics is essential for designing and operating an effective intrusion sensor system. Thus, the present study focuses on determining the probability of detection for certain intrusion detectors in order to evaluate their performance and the appropriateness of their use in the current PPS for a nuclear facility.

4. Experimental Work

4.1. GB sensor performance measuring procedures

I determined the PD by undertaking 10 intrusion trials.[17,18] The sound created by knocking metal keys on the glass windows from outside the building was used to test the GB alarm to see if it generated an alarm or not. All trials were performed on different areas and many fields of sensors.

4.2. GB sensor technical specifications and hardware description

The following are the sensor spectificaitons. Type: VISONIC GFD-20 GLASS BREAK audio discriminator and detector; Detection range: 15 m radius adjustable; Coverage Area: up to 500 m^2; Cut out frequency: 4 kHz; Detection Current: 20 mA; Alarm period: 2-3 Sec; Power supply voltage: 9 to 16 VDC; Working ambient temperature: -20C to 60^oC.

The GB detector board was tested using the MSP430F2274 board, which is a 16-bit microcontroller (MCU). The supply voltage required for the microcontroller spans a broad range from 1.8 V to 3.6 V. The MCU is capable of operating at frequencies up to 16 MHz. The CPU has a 16-bit RISC architecture with a total of 51 instructions (27 core

and 24 emulated). It supports a single-cycle shift and single-cycle add/subtract instructions. This enables efficient multiplication in the absence of a hardware multiplier.[18] The MCU also has an internal very-low-power, low-frequency oscillator (VLO) that operates at 12 kHz at room temperature. This oscillator eliminates the need for an external onboard crystal for the operation of the device. However, an option has been provided on the board to use external crystal/resonators of up to 16 MHz. The MCU has two 16-bit timers (Timer A and Timer B), each with three capture/compare registers. An integrated 10-bit analog-to-digital converter (ADC10) supports conversion rates of up to 200 kilo samples per second (ksps). The ADC10 can be configured to work with to on-chip operational amplifiers (OA0 and OA1) for analog input signal conditioning. The memory model supports up to 32 kB of flash memory and 1 kB of RAM in addition to 256 bytes of information memory. This device comes with four 8-bit I/O ports that can be used to control external devices. The current consumption of 0.7 mA during standby mode and active mode current of just 250 mA at 1 MHz make this device an excellent choice for battery-powered applications. Figure 2 shows the setup for the Glass Breakage detector using this device. The microphone captures the analog input, and a buzzer or LED indicates detection of glass breakage. The op amps internal to the MSP430 are connected to a few external passive components as part of the design of active analog filters.

4.3. GB sensor's on-site experimental steps and evaluation procedures

1. Turn off the GB sensor power.
2. Open the front cover.
3. Use a screwdriver to short the operation mode pads on the PC board.
4. Connect an oscilloscope device to the output terminal of GB sensor.
5. Connect two digital voltmeters to the output terminal of amplifier 1 (QA1) and the output terminal of amplifier 2 (QA2).
6. Close the front cover.
7. Turn on the GB power and wait until the detector’s green LED blinks approximately once per second to indicate that it has entered operation mode.
8. Stand within 4.6 m (15 feet) of the detector.

9. Generate a flex signal by carefully striking the glass with a cushioned tool (or by vibrate a collection of metal keys. For high amplitude excitation a loud sound above 2 kHz is used. The GFD-20 responds with a burst of glass break audio or from the audio generated by the metal keys. If the detector receives both the flex and audio signals properly, its red alarm LED lights.
10. Measure the output currents at the output connection port, and record the alarms which generated as the intruder breaks the glass and high frequency sound is generated.
11. Repeat the intrusion process several times (10 trails). After each test, ensure that the GB sensor is ready, and then generate the sound. Adjust all setting after each test.
12. Record the output signals and alarms generated by AQ1, AQ2, output terminals of GB sensors and LED flashing, and then determine PD.

4.4. OD sensor performance measuring procedures

The PD was measured using at least 10 intrusion trials.[19] The intrusion process included multiple opening and closing of one selected door inside a certain nuclear facility. The OD sensor was installed at the top of the door and it depended on an open circuit during the opening process of the door, and closed circuits in case of closing of the door.

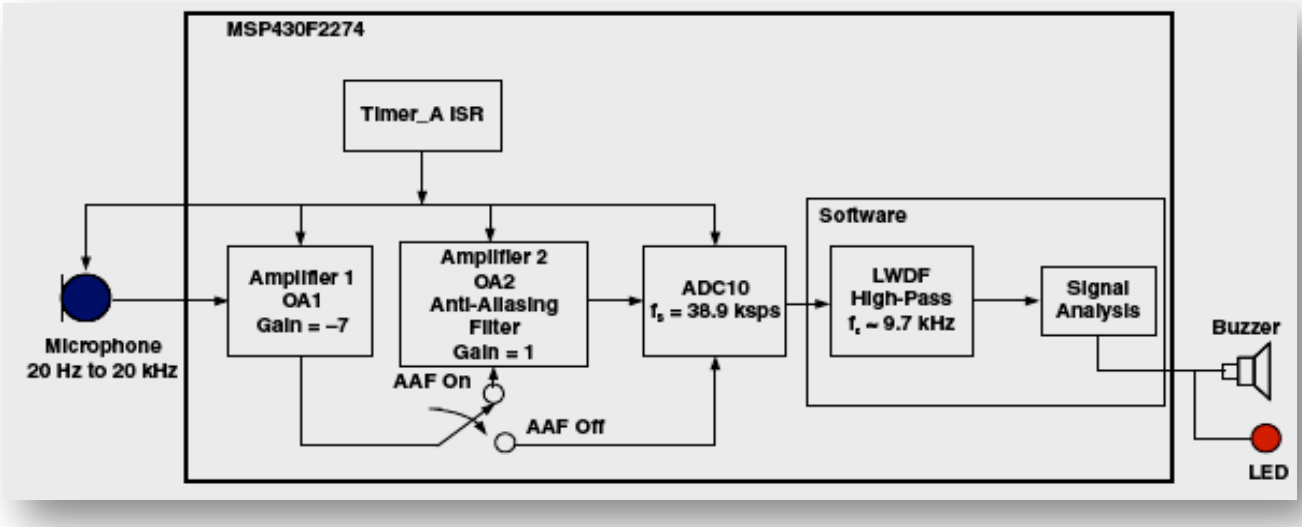


Figure 2 - Glass Breakage detector setup.

4.5. OD sensor technical specifications and hardware description

The sensor used for the OD measurements consisted of an actuating magnetic assembly and switch assembly that detects 6 mm (0.25”) of relative movement between the magnet and the switch housing. Upon detecting such movement, it transmits an alarm signal to the alarm annunciation system. The switch mechanism is of the balanced magnetic type. Each switch is provided with an overcurrent protective device, rated to limit current to 80 percent of the switch capacity. The housings of the surface mounted switches and magnets were made of nonferrous metal and are weatherproof. The housings for the recess-mounted switches and magnets need to be made of nonferrous metal.

4.6. OD sensor's on-site experimental steps and evaluation procedures

1. Ensure that the card reader, open door sensor, TL unit and electrical lock are working.
2. Turn off power to all electronic units of the door (card reader, comparator TL unit, main PAU unit). See Figure 3.
3. Open the front cover of the OD sensor.
4. Connect a digital voltmeter to the output terminal of the OD sensor
5. Adjust the voltmeter to measure the output signal.
6. Close the front cover.
7. Turn on power to the TL device and the OD, and wait.
8. Stand at the front of the door and open it rapidly
9. Measures the output volts using the digital voltmeter at the output terminals of OD sensor (at input terminals of TL unit), and record the generated alarms when the intruder opens the door.
10. Close the door again.
11. Repeat the intrusion process several times (10 trial). After each trial, ensure that the OD sensor is working properly.
12. Record the results and then determine the PD.

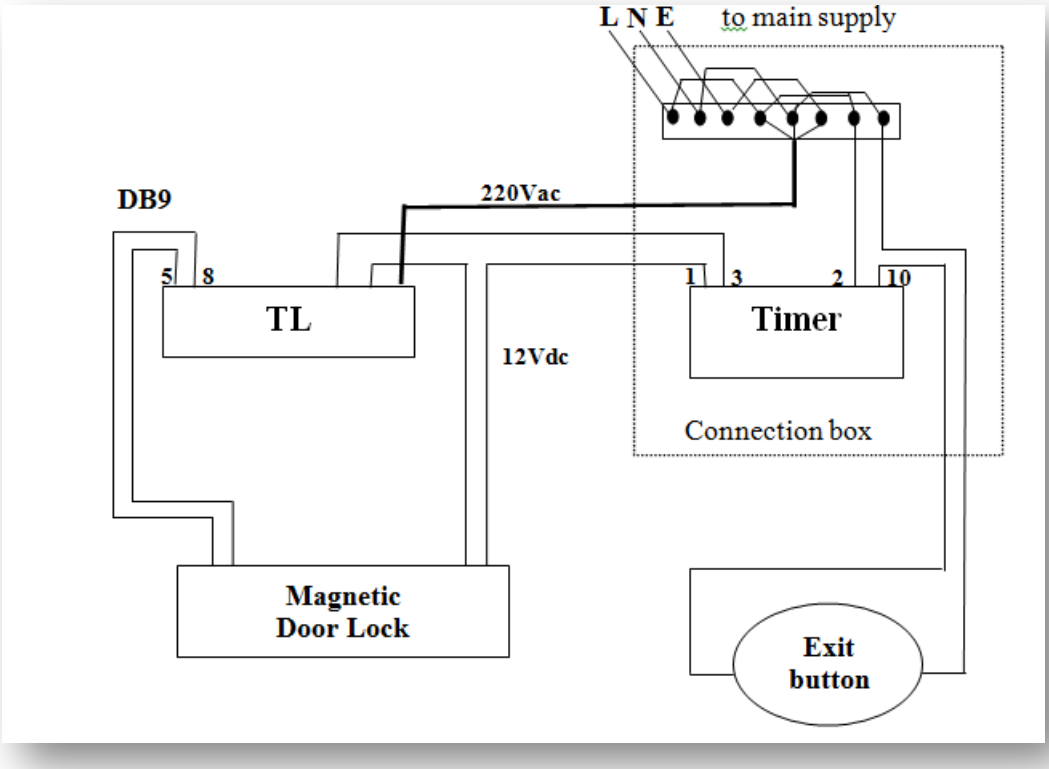


Figure 3 - Magnetic door sensor circuit diagram.

5. Results and Discussion

While designing a PPS, there a number of kinds of attacks which should be considered. These include [20]: ***False Alarming***: which refers to the situation where the adversary induces random, multiple false alarms in a system in order to undermine its usefulness and the confidence placed in it. ***Fault analysis:*** which refers to the situation where an adversary, typically exploiting technical savvy, makes a system function in an abnormal manner by altering its operational parameters, in order to obtain useful information that can be exploited, e.g., changing the ambient temperature around a sensor. ***Poke the System:*** which refers to the situation where an adversary probes the system without tampering with it and observes its responses, in order to obtain useful information, e.g., taking note of how near one can get to a motion sensor before it detects a presence.

5.1. GB sensor evaluation results

The GB detector was equipped with two LEDs **indicators**, a green event LED and a red alarm LED. When the LEDs are enabled, they light in a variety of patterns to convey the detector's operational status. Table (1) summarizes the LED messages obtained during the intrusion process.

Table 1 - GB LED output messages.

Condition	Green LED	Red LED
Normal	OFF	OFF
Normal, event detected	Flicker	OFF
Normal, break detected	OFF	ON 5 seconds
Normal, alarm latched	OFF	ON
Power up	ON (1 second)	ON (1 second)
Low voltage	Flash ON/OFF	Flash ON/OFF
Operation mode	Flash once per second	OFF
Test mode, event detected	Flicker	OFF
Test mode, alarm	Flash once per seconds	ON 5 seconds

The output results and the GB timing diagram obtained from an oscilloscope are illustrated in figure 4. It was noted that in three trials (trials 3, 4, 9), the GB sensor failed to detect the glass breakage, and the output current was 0 mA, 3 mA, 8 mA; these values were not considered as alarm values. One trial (trial 6) recorded 13 mA, which was considered as a fraction of the alarm value (20 mA). In the remaining six trials, the GB sensor succeeded in recording alarms and the output current was 20 mA. See figure 5. The tests and recorded data and all results obtained during intrusion process are shown in table 2.

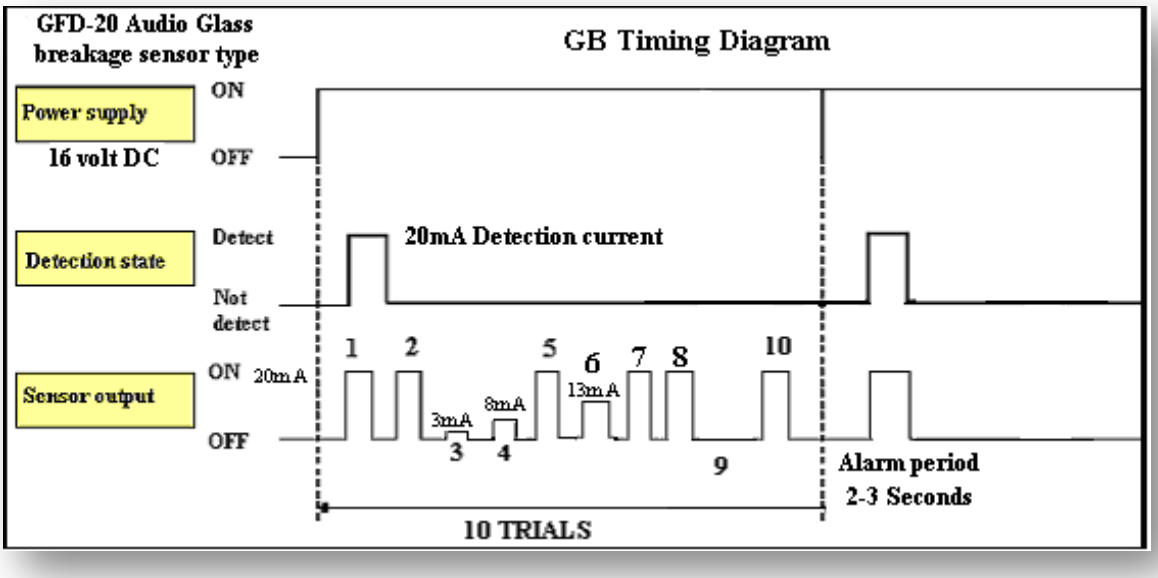


Figure 4 - GB Timing Diagram.

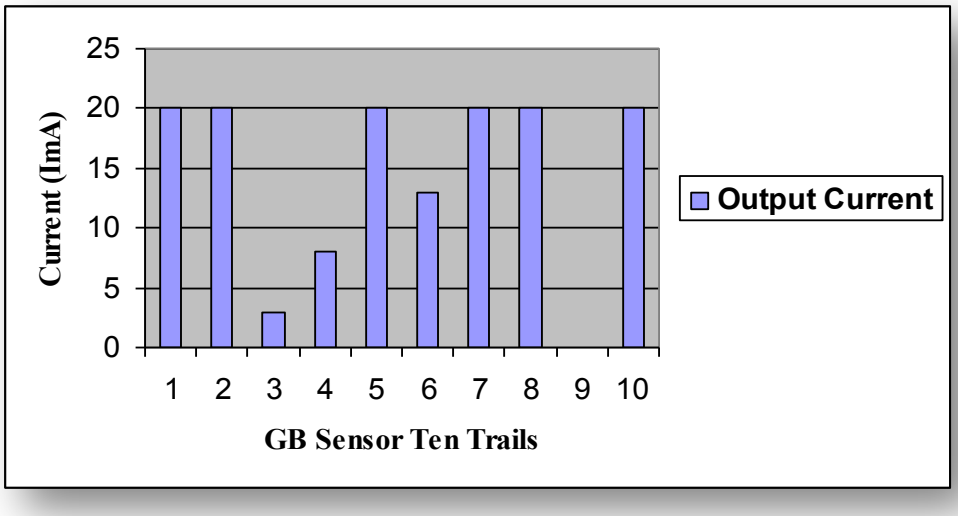


Figure 5 - GB sensor's test output current results.

5.2. OD evaluation results

Good access control systems should be capable of controlling the physical barrier at the entrance/exit point automatically by preventing access until authorization is

granted, thus contributing to the delay function. This is mostly achieved by electromechanical sub-systems such as door strikes and rotating doors.[7] The access control/anti-intruder system described in this paper uses a microcontroller chip to achieve the coordination function.

After finishing the intrusion process for the OD sensor and recording the alarms which had been generated from the OD sensor during the intrusion process, the OD sensor's test output voltage results are listed in table 2. As previously stated, 10 trials had been undertaken. In two trials (trials 4 and 8), the OD sensor failed to detect the intrusion process while it succeeded in recording alarms in the remaining 8 trials and the output voltage across the two output terminals was the nominal value.

Table 2 - Glass Breakage and Open Door sensor results.

Test Type	Sensor Type	No of Trials	Success (Alarm)	Failed (No-Alarm) & Current	Small Current "Alarm"	Probability of Detection (PD)
Intrusion Sound	Glass Breakage	10	six IO/P=20mA	three ; I1O/P=8mA I2O/P=3mA I3O/P=0mA	One trial IO/P=13mA	**65%**
Intrusion	Open Door	10	8	2	--	**80%**

6. Conclusion

The probability of detection for intrusion detection sensors is an important factor for evaluating physical protection systems. This work determined the probability of detection (PD) for Glass Breakage (GB) and Open Door (OD) cluster sensors. These are widely used in nuclear facilities. The GB and OD sensors were found to have a PD of 65%, and 80% respectively.

7. References

1. IAEA-Nuclear Security Series no. 20, *Objective and Essential Elements of a State's Nuclear Security Regime*, Vienna, Austria (2009).

2. IAEA- INFCIRC/225/ Rev.3, *The Physical Protection of Nuclear Materials and Facilities*, Vienna, Austria (1993).

3. IAEA- INFCIRC/225/ Rev.5, *Nuclear Security Recommendation on Physical Protection of Nuclear Materials and Facilities*, Vienna, Austria (2011).

4. Mary Lynn Garcia, *Design and Evaluation of Physical Protection Systems*, Butterworth-Heinemann (2008).

5. Lionel S. Johns, *Technology Against Terrorism: Structuring Security*, OTA-ISC-511, Washington (1992).

6. *Enhanced Physical Protection Measures and the Agency's Plan of Action for Protection Against Nuclear Terrorism*; T. Rauf, presented at the 2003 NPT PrepCom, 6th May (2003).

7. B. Nkom, I.I. Funtua, and L.A. Dim, "Design of an Access Control System: A Paradigm for Small Nuclear Facilities", *Journal of Physical Security* 7 (2) (2014).

8. Hichem Sedjelmaci, and Mohamed Feham, "Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network", *International Journal of Network Security & Its Applications* 3(4) (2011).

9. Chong Eik Loo, Mun Yong Ng, Christopher Leckie, and Marimuthu Palaniswami, "Intrusion Detection for Routing Attacks in Sensor Networks", *International Journal of Distributed Sensor Networks* 2 (4) (2006).

10. Robert L Barnard, *Intrusion Detection Systems*, Butterworth-Heinemann, (1988).

11. James D. Williams, *Physical Protection System Design and Evaluation*, IAEA-CN-68/29, Vienna, 10-12 November (1997).

12. M.E. Elhamahmy, Hesham N. Elmahdy and Imane A. Saroit, **"**A New Approach for Evaluating Intrusion Detection systems**"**, *CiiT International Journal of Artificial Intelligent Systems and Machine Learning*, Vol 2, No 11, November (2010).

13. Alvaro A. Cardenas, John S. Baras, and Karl Seamon, "A Framework for the Evaluation of Intrusion Detection Systems", *Proceedings of the 2006 IEEE Symposium on Security and Privacy* (2006).

14. Headquarters, Department of the Army, *Physical Security Field Manual no.3-19-30*, Washington, DC, 8 January, USA, (2001).

15. KUBE Electronics Ltd, Garstligweg 2, *SF389 PIR Circuit IC Passive Infra-Red Alarm Preliminary Datasheet*, 8634 Hombre-chtikon, Switzerland, Revision 1.1, January (2003).

16. John J. Fay, *Encyclopedia of Security Management*, 2nd edition, Butterworth-Heinemann (2007).

17. Safety Analysis Report (SAR) of Safari Reactor of South Africa, *SECURITY SYSTEM BASIC DESIGN*, (1999).

18. 18th International Training Course, *Physical Protection of Nuclear Facilities and Materials*, Sandia National Laboratories, Albuquerque, New-Mexico, USA, (2004).

19. J.C. Beef, J. Josiak, S.F. Mahmoud, and V. Rawat, "Continuous access guided communication (CAGC) for ground-transportation systems; *Proc. IEEE*, vol. 61, pp. 562–568, May (1973).

20. R.G. Johnston, et al., "Effective Vulnerability Assessments for Physical Security Devices, Systems, and Programs"; *NUMAT Conference Proceedings*, Salzburg, Austria, 08–13 September (2002).

Journal of Physical Security 8(1), 55-68 (2015)

Threats of Radiological Terrorism and the Securing of Radioactive Sources

Raphaël Duguay, M.Sc., PSP
Nuclear Security Division, Canadian Nuclear Safety Commission (CNSC), Canada

Abstract

This paper presents a high-level overview of the threats that high-risk radioactive sources represent, and their potential use as radiological weapons. The objective is to provide a discussion on existing threat assessment methodologies and security practices to protect high-risk radioactive sources, including physical protection systems and security management. I explore the particular challenges associated with protecting high-risk radioactive sources against potential insider threats, and some of the gaps related to transportation of such sources. Following the theory of Situational Crime Prevention, I propose different security approaches for mitigating the risk, and explore different options and offer recommendations.

The Canadian Nuclear Safety Commission (CNSC) plays an important role ensuring that Safety and Security are harmonized. In 2013, CNSC published regulatory document *REGDOC2.12.3 to* enhance the security of radioactive sealed sources in Canada. In doing so, CNSC's role in securing radioactive sources made sure that safety and security can work together without impeding one another. Radioactive sources are used worldwide and provide many benefits to the population. In this perspective, the Canadian approach emphasizes the importance of safety and security interfaces, not forgetting the fact of the benefits arising from the use of sealed sources.

Terminology

In this paper, the term "radioactive sources" refers to radioactive nuclear substances that are contained in a sealed capsule or in a cover to which the substance is bonded, where the capsule or cover is strong enough to prevent the release of the nuclear substance under ordinary conditions.

What is the Threat Related to Radioactive Sources?

Radioactive sources can be used as weapons of terror, such as "dirty bombs" or as radioactive dispersal devices (RDD). Consequently, the International Atomic Energy Agency (IAEA) and the international community revised the Code *of Conduct on the Safety*

and Security of Radioactive Sources in 2003 to place more emphasis on radioactive source security. Since then, the IAEA and the international community has worked to establish recommendations and guidance to provide answers to the following questions:

- What must be protected?
- What must it be protected against?
- What level of protection is adequate?

From 1993 to 2012, the IAEA Incident Trafficking Database (ITDB) report[i] documented 419 incidents involving unauthorized possession and related criminal activities, 615 incidents of theft or loss, and 1,244 other unauthorized activities and reported events involving nuclear substances and radioactive sources. According to a 2014 report by the Center for International Trade and Security (CITS), the majority of these reported incidents involved radioactive sources used in industrial and medical applications. In the industrial sector, most of them involved radioactive sources used in construction, mining and oil exploration. In the medical sector, most of them were related to the loss of a radioactive source used in diagnostic and radiotherapy applications[ii].

In addition to the ITDB, INTERPOL's Project Geiger[iii] focuses on collating and analysing information on illicit trafficking and other unauthorized activities involving nuclear substances or other radioactive material. It combines data from the IAEA with additional publicly available information and data from classified reports from law enforcement collected through INTERPOL's channels and provided to INTERPOL member country officials. This group produces reports related to radioactive source trafficking and nuclear terror plots and threats. There has been evidence that terrorist groups have expressed interest in gaining access to radiological sources through illicit trafficking and using these sources to conduct radiological terrorism.

In general terms, radiological terrorism is a potential act involving the use of radioactive sources for malicious purposes. The threats can be from terrorist organisations or militant groups such as the event reported in 1995 in Moscow[iv] or from a lone wolf such as the José Padilla arrested in 2003 for plotting an RDD attack in the US. The threat can also be of a criminal nature or threats by an insider. Most of the incidents reported to the IAEA are the result of "criminal opportunities" where the source(s) are left unattended, under poor security control, or not under surveillance. In some cases, criminals steal sources for financial gain, ransom, extortion, or for malicious purposes such as exposing individuals to ionising radiation (i.e., radiation poisoning), or for revenge against an organization. There have been incidents where thieves stole transport vehicles without knowing radioactive sources were onboard. There have, however, also been cases where the targeted radioactive source was stored inside vehicles and the security measures were defeated.

Some recent incidents received significant media attention such as the theft and recovery of a Category 1 Cobalt-60 source during transport in Mexico in December 2013. This event raised public concern due to the potential impacts of an RDD and the motivation of the perpetrators. There is much misinformation and disinformation that continues to circulate on the Internet and in the media about dirty bombs; this contributes to public confusion. According to Stewart (2010), the misinformation stems from long-held misconceptions and

scaremongers hyping the threat for financial and political reasons to gain more interest in radioactive source security and associated projects.

As mentioned by Fergusson et al.(2005), malevolent actors could also use different pathways to acquire radioactive sources through assistance from an insider, licensing fraud, unauthorized or illegal transfer, exploitation of weaknesses during transport, sources that are no longer under regulatory control (a.k.a. "orphan" sources), the involvement of organized crime, or access to radioactive sources from the black market. It is also possible to acquire radioactive sources through a legal purchase from a legitimate supplier, or from a country where laws and regulations are less prescriptive or poorly enforced. For example, in 2006, undercover investigators from the United States Government Accountability Office (GAO) were able to purchase a small number of radioactive sources from a commercial supplier by posing as employee of a fictitious company without being challenged. According to the GAO report, GAO's investigators entered the US borders using counterfeit documents with enough radioactive material in their vehicle trunks to make two dirty bombs. In another case, a US citizen posed as a visiting professor at the University of Rochester, and illicitly used university resources to obtain the radioactive sources from suppliers. That same individual had been previously arrested in Toronto on a US fugitive warrant and was found to have illegally obtained a radioactive source and stashed it in a public storage locker[v].

A study by Kupatadze (2010) on nuclear smuggling trends in the Soviet Republic of Georgia found that nuclear smuggling typically involves opportunist smugglers and amateurs, as opposed to professional criminal and terrorist networks. Based on unique empirical data and interviews with smugglers of radioactive sources and police investigators, the author suggests that professional criminals are rarely involved in this type of smuggling. This is due to the unreliable nature of the market for radioactive sources and the professional risks that radiological smuggling could pose to their ability to wield political power and operate legal commercial business. The black market remains an attractive pathway for adversaries to minimise risks and gain access to radioactive sources. However, most documented cases reveal that these transactions are mostly scams or special sting operations pre-arranged by law enforcement to lure potential adversaries.

According to Ferguson et al. (2009), the IAEA ITDB has reported many cases of opportunist thieves trying to sell radioactive sources. This data, however, must be treated with caution because countries are not required to report all incidents. In many of these cases, the traffickers who were caught were caught because they were not able to find a buyer (many were caught in sting operations) and it is uncertain if the radioactive sources had enough radioactivity or sufficient characteristics to be considered a risk.

Since 2001, Argonne National Laboratory[vi] has collected and compiled data on events, including the malicious use of radioactive sources worldwide. The Theft and Diversion Incident Analysis System (THADIAS) database interfaces with a Geographical Information System to map incidents. According to a THADIAS report[vii], most incidents of lost/stolen items involved exposure devices used in industrial radiography. Exposure devices typically

contain Category 2 radioactive sources and are more prone to theft because they are used and transported worldwide and they are mobile.

As mentioned by Ferguson[viii]: "National or local political turmoil such as the overthrow of a government could create opportunities for looting facilities containing radioactive sources". This is true and has been witnessed in Syria (2013) where there were cases of Category 2 radioactive sources, i.e., exposure devices, being stolen from facilities during political instability. During the conflicts in Libya (2013) and Iraq (2014), there were multiple news articles related to jihadist groups having access to low-level radioactive and nuclear materials that could be smuggled out of the country or used as a weapon.

There are several studies on the effects and potential impacts of an RDD published and available worldwide. There are, however, few studies and limited research available on potential threat scenarios and risk analysis for radioactive sources. A report from the US Congressional Research Service (2011) argues that the threat is plausible but the frequency of events and the sample size of publicly available information is not large enough to support predictions of the likelihood of such attacks. According to Dood (2005), quantifying risk is almost impossible because it requires knowing the probability of a person wanting to develop and use a radiological device, and the probability of them being able to get access to the device. According to this research, it is hard to identify the likelihood or probability of an event. However in some studies, experts assessed the use of probabilistic risk analysis to measure the potential terrorism risk in order to assist decision makers.

A study by Ezell et al. (2010) reviewed the applicability of probabilistic and decision analysis approach to bioterrorism risk and the bioterrorism risk assessment methodology used by the Department of Homeland Security. This study, however, was criticized by the National Research Council Committee (NRCC) because of the adaptive nature of terrorists and concluded that probability of terrorist events and event trees are not suitable for bioterrorism risk analysis. An event tree is a graphical representation that examines chronological events and can be used to explore different responses or outcomes. In 2004, the Canadian Department of Research and Development (DRDC)[ix] developed a probabilistic risk assessment tool for RDDs to assess which radioactive sources used in medical application would be of highest appeal to radiological terrorism. According to Larsson (2004), lower-activity radioactive sources with less severe security requirements still pose a threat because multiple radioactive sources could be combined together into a single device. This study was integrated into a risk assessment database as part of a radiological terrorism risk assessment.

A recent paper from the Foreign Policy Research Institute[x] raises concerns about the availability of high-risk radioactive sources in countries exposed to high or extreme risk of terrorism. The researcher compared the *Terrorism Risk Index* developed by Maplecroft and two IAEA databases with information on type and locations of high-risk radioactive sources used for agriculture and medical applications. The result of his analysis showed that there are 758 Cobalt-60 teletherapy units located in *extreme risk* states and another 69 located in *high risk* sates. Due to the lack of security and controls, these sources could be smuggled or

moved transnationally without being detected, and used for a malicious act. According to the author, the threat of an "effective" RDD is serious and should not be underestimated because of the potential impact on the population, in particular the mass psychological and economic effects.

Radiological weapons

Radiological sealed sources are used every day in medical, industrial, academic and research, as well as in commercial applications. They are produced in nuclear facilities and accelerators. They are assets that are *inter alia* very important and beneficial to society for a variety of uses such as radiation therapy, nuclear medicine, monitoring of industrial processes, analysis of environmental samples. Radioactive sources are used worldwide and their abundant availability makes them attractive to individuals with malicious intent. Some radioactive sources are easy to conceal and to transport. Like explosives, if they are used as a weapon, they could create panic, economic disruption, death and injuries but they would also pose unique challenges to the public due to radiation and possible contamination. Radioactive sources could be used in a weapon of terror, a "weapon of mass disruption". An attack would be unlikely to cause mass casualties from radiation exposure; the event would more likely cause disruption, fear and panic. This could result in massive damage to the economy[xi], and negatively impact the environment. According to Stewart, dirty bomb attacks would likely be directed against highly symbolic targets—such as one representing the economy or government.

Some radioactive sources have a greater potential for dispersion and may have higher penetrating radiation because of their isotopic composition. Some forms of isotopes can be dissolved in solvents and sprayed widely, burned, or vaporised[xii]. Radiological weapons can take a variety of forms such as a radiological dispersal device (RDD), a radiological emitting device (RED), or a radiological incendiary device (RID) [xiii]. There are multiple scenarios including inhalation, ingestion, and immersion attacks. According to Zimmerman et al. (2004), the potential impact and radiation exposure may vary depending on various factors, including the size and radioactivity of the device (e.g., small RDD 1-100 curies, large RDD 1,000-10,000 Ci, super RDDs >10,000 ci). According to Stewart (2010), the effectiveness of a dirty bomb may produce a wide range of effects depending on the size of the explosive or explosive device, the amount, the form and type of radioactive sources and environmental factors such as terrain, weather conditions, and the density of the population. However, there are many factors that could make it difficult for an attacker to administer a deadly dose of radiation through a dirty bomb because of the dispersion and spread of the radioactive substances over a large area and the evacuation and decontamination of intended victims after the explosion (Stewart, 2014). A radioactive source could also be used as a low-tech weapon depending on the motivations of the attackers. Other scenarios include the use of a radioactive source to surreptitiously expose people to radiation over a long period of time, such as placing the device on public transport or deploying it during an important event in order to cause fear and panic, such as the Olympic Games or other high-profile international/national event.

From a regulatory perspective, it is important to base the legal framework and regulations on risk. To prevent radioactive sources from being lost, stolen, or used in a malicious act, the regulatory body must focus on the radioactive sources that are the most dangerous. It must apply a graded approach based on principles of risk management. It is important to focus on the high-risk radioactive sources but the regulatory body should also provide requirements, recommendations, and guidance for licensees with medium and low-risk radioactive sources to prevent the "displacement effect". A displacement effect is the relocation of a crime (or criminal act) as a result of crime prevention effort at the original site, such as hardening the target or increasing the risk for the adversary. One may argue that it is impossible to protect all radioactive sources and protect all potential targets. Nevertheless, it is the responsibility of the licensee to ensure that radioactive sources remain under control at all times to prevent loss due to negligence. It is also possible to deter potential perpetrators by implementing crime prevention measures to increase the risk of getting caught, increase the required effort of the adversary, and reduce criminal opportunities. The use of medium and low radioactive sources could still cause significant contamination and be attractive if multiple sources were mixed and/or aggregated together to create an RDD.

According to Dood (2005), efforts to counter radiological terrorism should have several objectives, such as:

1. Prevent acquisition of the target radioactive sources, or access to the target facilities.
2. Detect attempts to acquire, or actual acquisition of, radioactive sources and,
3. Effectively detect and respond to the use (or threat of use) of these sources, or sabotage of the facilities.

International standards and recommendations

The *Code of Conduct on the Safety and Security of Radioactive Sources* (hereafter referred to as "the Code") provides recommendations for the safety and security of radioactive sources based on relevant international standards. As of late 2013, a total of 119 member states have made a political commitment to follow the Code. The Code, however, is not a legally binding document such as a treaty or the Convention on Physical Protection of Nuclear Materials. The Code does not have the same legal basis and there are limited enforcement tools to ensure a country fully implements the recommendations. The responsibility of radioactive source security falls on the State. As part of these responsibilities, the State should identify national threats, vulnerabilities, and consequences in order to implement strategies, policies, and countermeasures to reduce the risks. This also includes transnational threats and the possibility for an adversary to acquire radiological sources illegally and export it for use as a weapon in another country. It is important to note that there is a wide difference in regulatory oversight of radioactive sources between countries with a nuclear power infrastructure and those with no such infrastructure.

In some cases, the state does not have laws or regulations and/or has not completed a national inventory, and there is no formal regulatory body. Such states struggle to meet the Code and to implement solutions to ensure that radioactive sources are under control and

used in a safe and secure manner. In 2011, the IAEA published the Nuclear Security Recommendations on Radioactive Material and Associated Facilities, as well as two implementing guides for storage and transport of radioactive sources. Currently, there is limited international guidance on planning, implementing, and maintaining a national threat assessment for radioactive sources. Some States use a Design Basis Threat (DBT) for radioactive sources but this approach may be difficult for countries that have limited resources or that have a wide variety of licensees and operators. There are also limitations in sharing sensitive information contained in the DBT with stakeholders and the lack of resources to continuously assess the threat (i.e., DBT cycle). Every country is unique and the approach taken should be tailored to their needs and national environment. Unfortunately, it may take a RDD attack before the international community and the political decision makers implement a stronger, binding international framework on radioactive source security commensurate with the risk in each country.

National threat assessment for radioactive sources: risk-based threat assessment

As noted in the previous section, the threat level is not the same for every country and may even be different between regions within a country. Conducting a threat assessment may present a number of challenges as there are different methodologies that can be used, the availability of targets and assets may change over time, and there can be a lack of political will or of resources to conduct these studies. In some countries, people in charge of safety are also responsible for security and they may not have the expertise, knowledge, or the capacity to properly understand the threats to adequately tackle radioactive source security requirements.

Conducting a National Threat Assessment (NTA) is an important undertaking that can be used to justify the need for law, regulations, regulatory oversight, and security requirements for high-risk radioactive sources. It is also a valuable tool that can be used to educate and inform industry stakeholders, first responders, and licensees about the credible threats, and to identify specific threat profiles and scenarios that are more likely to occur. There is also a responsibility to continuously assess the threat environment to prepare appropriate countermeasures if the threat level changes.

An NTA should also consider transportation. In order to do so, there should be joint efforts or partnerships between government entities, law enforcement agencies, industry associations, and licensees. The regulatory focus should be on identifying risk reduction countermeasures to prevent, detect, interdict, and mitigate these threats. In addition, while the State may be responsible for conducting an NTA, licensees should also conduct their own facility-specific threat assessment to be able to identify the risks associated with their source(s) and implement safety and security measures specific to their sites and/or activities. An NTA may also consider transnational threats, such as the possibility of smuggling radioactive sources inside or outside the country, and their use as a weapon against another country.

The specific challenge of preventing or mitigating the insider threat

The risk of theft by an insider is difficult to predict. In particular, an employee may be coerced to provide security information or access to attackers. To mitigate against this potential threat scenario, the licensee should use a combination of people, procedures, and security systems/devices. There should be clear requirements from the regulator to ensure that individuals with a legitimate requirement for unescorted access to radioactive source are trustworthy and reliable, and this should be reassessed on a continuous basis. The licensee should also implement multiple levels of security measures to prevent and/or detect this pathway and ensure that employees are well trained. Employee training should include knowledge of their role and responsibilities in regards to security, and they should be able to recognize and report suspicious behaviors and activities and promote a robust security culture.

In some cases, conducting trustworthiness and reliability verification is a challenge because it is done by radiation safety officers (RSOs), managers, or individuals responsible for the licence who are not security experts. These individuals may lack the proper training and may not have access to the proper tools to make the best decisions when trying to mitigate against the potential of an insider threat.

In some locations, security awareness must be developed and efforts must be made to maintain a strong security culture. It is particularly more challenging for licensees in public facilities or hospitals that have students or foreign workers because the background information is not always available or verifiable. In these cases, the licensee needs to interface with their Human Resources Department and/or contracting authorities and implement a risk decision process to ensure they have the proper information to make the correct decision.

Security of radioactive sources during transport

From a security perspective, there are heightened security risks during transportation of radioactive sources. This is particularly a concern with third-party companies and carriers that are not bound or required to implement security measures by any government entity. During transport, radioactive sources are more vulnerable to hijacking, interdiction, diversion, or to attacks designed to breach and scatter the radioactive substance. As mentioned by the CITS (2014) report, a potential adversary—especially an insider—could choose a point along the route where the shipment would be most vulnerable and security measures least effective to conduct an attack.

The main international regulations governing the transport of radioactive sources are the IAEA *Regulations for the Safe Transport of Radioactive Materials* and the *IAEA Recommendations for Radioactive Material and Assorted Facilities*. There are other international instruments that incorporate the IAEA Regulations, such as the *Technical Instructions for the Safe Transport of Dangerous Goods by Air* published by the International Civil Aviation Organization (ICAO) and the *International Maritime Dangerous Goods Code* (IMDG Code). Others provide guidance and recommendations for States and governments (for example,

the UN *Recommendations on the Transport of Dangerous Goods - Model Regulations*, the Code and recommendations documents). These regulations and instruments focus on the

safety aspects of transportation, not so much the security aspects. As such, transportation is considered to be the weak link during the lifecycle of a radioactive source, i.e., from production to disposal. In some cases, there is an absence of specific national security requirements for transportation of dangerous goods and these requirements are not harmonized with other regulations. In addition, transport of dangerous goods may cross multiple government jurisdictions and the responsibility of applying and enforcing security requirements during transport is not clear and consistent. There are also specific security challenges for licensees using sources in the industrial radiography and well-logging sectors because they may store sources overnight inside the vehicles, sometimes in remote locations where the response time for law enforcement agencies is longer and where satellite or cellular network coverage is limited. In all cases, the licensees must maintain continuous control and/or surveillance and implement measures to prevent the vehicle containing the device from being stolen. Finally, in some cases, there is an absence or a lack of harmonisation related to security clearance and background verification for individuals responsible of handling and/or transporting theses hazardous materials.

The regulator should consult other government agencies responsible for regulating the transportation of dangerous goods, industry associations, and licensees to find adequate solutions to mitigate these risks. Also, medium and low-risk sources that are transported should be subject to a set of minimum security measures based on prudent management practices and on a graded approach to security. For example, prudent measures can include restricting access to radioactive source by an authorized and trained individuals, using security barriers to prevent easy removal, monitoring shipments/receipts, conducting regular inventory verification along the route, etc. There are also promising tracking technologies that can be integrated into a security system to enhance recovery efforts in case a source is stolen, lost or misplaced. However, more research needs to be conducted in this area and there needs to be a risk analysis to justify active tracking systems.

Using crime prevention strategies to mitigate the threat to radioactive source

According to Clarke and Newman (2006)[xiv], terrorism is not much different from traditional types of crime, and there are similarities in the opportunity structure. For example, perpetrators of traditional crime look for targets that are concealable, removable, available, enjoyable, and disposable (CRAVED). Some of these characteristics are similar for terrorist groups or individuals. There are differences with respect to motives and aim, but the Situational Crime Prevention theory is focused on dealing with the opportunity structure to convert vulnerable places into a defensible space. Table A uses Clark's model of situational crime prevention techniques to explore potential solutions to reduce the risks of radioactive sources falling into the wrong hands. There are different modus operandi across incidents reported that describe different methods and tactics to prevent these events. Using the lessons from the Center for Problem Oriented Policing and the research from Clarke and Newman (2006), the table identifies different solutions such as (1)

increasing the perceived efforts, (2) increasing the perceived risks, (3)reducing the anticipated rewards and provocations and (4) removing excuses.

Discussion

It is important to know the threats and to prepare against them. There is a need to share threat information with stakeholders because it is important to educate the public and increase the awareness of competent authorities about the threats and potential consequences. The objective is to include them in the efforts to prevent, detect/interdict, and mitigate against an event involving a radiological dispersal device or a radiological emitting device. Everyone has a role in security and there is a need to ensure that adequate security measures are implemented and maintained. As mentioned by the CITS (2014) report, "the entire secure regime stands or falls based on the people involved. Without a strong substructure of beliefs and attitudes about threats, an effective nuclear security regime culture cannot exist". Table A presents situational prevention techniques related to physical security and security management that could reduce the potential risks. However, additional effort is needed to address remaining gaps. This can include implementing national threat assessment and/or transnational threat assessment, increasing awareness of competent authorities on the threats and consequences, establishing effective oversight of companies transporting radioactive sources to ensure adequate safety /security, and ensuring that individuals dealing with high risk radioactive sources provide and maintain background verification and security clearance.

The development and implementation of an effective security culture for radioactive sources is needed, and States should be encouraged to develop their own National Threat Assessment to understand the nature of the threat and the risks associated (CITS, 2014). This may create opportunities for stakeholders to establish relations with licensee representatives from industry and appropriate experts to develop and implement Threat Assessment instruments in order to assess ongoing threats to radioactive sources and to exchange information on suspicious incidents. These efforts would be aligned with the IAEA Code of Conduct and encourage regulators to share information with law enforcement agencies, customs, and other competent authorities and licensees to increase their awareness and promote a strong security culture.

It may be prudent to provide more international guidance for the security of medium and low-risk radioactive sources (Category 3, 4 and 5), and place more emphasis on security during transportation in order to provide clear and comprehensive requirements on security. At the international level, there are multiple stakeholders that need to be involved in the security of radioactive sources and they need to be integrated in the solutions (e.g., licensees, industry associations, and third-party carriers). There are also areas for improvement related to trustworthiness verification (e.g., background check and security clearance) to mitigate against the insider threat, tracking of Category 2 and 3 radioactive sources in particular for industrial radiography and well logging applications, and the international challenges presented by the voluntary adherence to the Code of Conduct and its supplementary guide.

It is pertinent to conduct an international study and compare the implementation of National Threat Assessment for Radioactive Sources in several countries to understand its implication, its benefits, and the impacts on the overall security regime. Countries with an NTA are probably better equipped to deter potential adversaries, detect incidents, and counter the threats compared to countries that do not have this tool. In this optic, it would be relevant to assess the impact before and after the implementation of the NTA and measure its consequences on the nuclear security infrastructure.

Table A: Techniques of Situational Crime Prevention for Protecting Radioactive Sources

1.Increase Perceived Effort	2.Increase Perceived Risks	3.Reduce the anticipated Rewards and Provocations	4.Remove Excuses
Target hardening • physical barriers, secure containers • force adversary to use different tools • Secure windows and access to facilities or vehicle • vehicle disabling device (steering locks), locks, immobilizer • tamper-proof packaging • In-delay devices • defence in depth approach • security by design • utilise existing safety measures (ex: source shielding)	**Detect unauthorized access** • intrusion detection system or human surveillance • assessment cameras activated upon motion • alarm response protocol • technology to locate cars, trucks, cell phones • GPS tracking, geofencing • communication devices and regular radio checks during transport • concealed duress alarms • Security patrols • Radiation detectors • utilise existing safety measures (ex: inventory control*) • using special seals	**Conceal targets** • May not be applicable because of safety considerations • Avoid excessive or false advertisement (i.e. radiation signs/posters) • Using camouflage or protective enclosure during transport to cover package	**Set rules** • Criminalizing terrorist attack using nuclear or radioactive sources • Punishing perpetrators • Regulations and security requirements • Licence process, procedures and policies • Site Security Plan/Transport Security Plan
Control access to facilities and RM during transport • access control devices • individual pin codes and electronic card access • Escort visitors and contractors • Two-person rule during transport • Radiation portal monitors/devices	**Extend guardianship** • Personnel training • Security awareness program • Security policy • Familiarization with security response force (in-house and off-site) • strengthen formal and informal surveillance, • reward vigilance	**Remove targets** • Return sources to home base after use • Remove radioactive source from vehicle • Using alternative technologies (non-radioactive)	**Post Instructions** • use signage • clear security procedure • site security plan/transport security plan
Screen for RM removal • radiation detection devices • tracking documents and inventory control • Use electronics merchandises tags • Anti-tamper devices	**Assist natural surveillance** • Improve lighting around facility and storage location (including when storing source at overnight temporary locations) • Community approach, neighborhood watch, industry peers • Promote ties with local police and communities	**Reduce frustration and stress or internal disputes** • Personnel trustworthiness and reliability for employees with unescorted access • Continuous behavioral observation program	**Alert conscience** • Security awareness program • Outreach with key stakeholders • Communicate threat information • Performance testing • Practices and exercise

1.Increase the Effort	2.Increase the Risks	3.Reduce the Rewards and Provocations	4.Reduce Excuses
Deflect offenders • Close other pathways to facility • Use Crime Prevention Through Environmental Design (CPTED) concepts	**Reduce anonymity** • Use identification • Use uniform • Register visitors and contractors • Visitor escort policy • Use surveillance cameras	**Identify property** • Property marking • Vehicle licensing and parts marking • Branding on source containers • Protect sensitive information	**Assist compliance** • Site security plan and contingency procedures • Target folder for response force • Familiarisation visit with first responders
Control tools • Vehicle Disabling devices • Restrict access/remove tools that could be used to breach security barriers	**Strengthen formal surveillance** • Assessment cameras link to intrusion detection systems • Patrols • Security officers, surveillance by employees	**Disrupt markets** • Monitors Internet/social media • Controls on classified ads • License vendors, service providers and manufacturer	**Regulatory oversight** • Regulatory requirements and guidance • Regulatory inspection and compliance verification activities • Outreach activities with stakeholders and licensee

*These techniques must be effective and should not be easily forged, tampered or bypassed without detection

Endnotes

[i] International Atomic Energy Agency (2013). IAEA Incident and Tracking database (ITDB) 2013 fact sheet.
[ii] CITS (2014). The Human Dimension of Security For Radioactive Sources: From awareness to culture. *Center for International Trade and Security*. University of Georgia.
[iii] Interpol website, Project Geiger - specialized reports, *www.interpol.int/en/Crime-areas/.../Project-Geiger-specialized-reports/*
[iv] Kolesnikova, L. (2010). Case study: A Radioactive IED. *Homeland Newsletter.* Counter Terrorist magazine.
[v] Fergusson, C. and Lubeneau, J. O.(2004). Securing U.S Radioactive Sources. *Issues in Science and Technology.*
[vi] Lindley R.A. et al. (2006). Perspective on International Radiological Trafficking. Prevention, Detection and Response to Nuclear and Radiological Threats. Springer 2006.
[vii] Adduci, J. (2012). Argonne National Laboratory THADIAS: Theft and Diversion incident Analysis System. US Department of Energy.
[viii] Fergusson,C. (2009). Radiological Weapons and Jihadist Terrorism. Assessing Radiological Weapons: Attacks Methods and Estimated Effects. *Defence against Terrorism review*.
[ix] Larsson, C. (2004). Availability and Use of Medical isotopes in Canada. Performed as part of a Radiological Terrorism Risk Assessment. DRDC.
[x] Haines. J.R.(2014). Dirty Bombs: reason to Worry ? Analysis. *Foreign Policy Research Institute*. July 2014.
[xi] Cousins, T. and Reichmutch,B. (2007). Preliminary Analysis of the Economic Impact of Selected RDD events in Canada, Defence Research and Development Canada and Battelle, PNWD-SA-7845.
[xii] Zimmerman, P. and Cheryl L. (2004). Dirty Bombs: the Threat Revisited. *Defense Horizons.* No. 38.
[xiii] Joseph W. Pfeifer (2006)., Improvised Incendiary Devices. Risk Assessment, Threats, Vulnerabilities and Consequences, master's thesis, Monterey: Naval Postgraduate School, September 2006.

References

1. Clarke R.V, Newman G.R (2006). Outsmarting the Terrorists, *Global Crime and Justice*, Prager Security International.
2. Dood, B. (2005). International efforts in Countering Radiological Terrorism. *Health Physics Society Journal*, November 2005, Volume 89, Number 5
3. Ezell et al. (2010). Probabilistic Risk Analysis and Terrorism Risk. *Risk Analysis*, Vol. 30, No. 4.
4. Fergusson, D. C. and William C.P. (2005). Four Faces of Nuclear terrorism. Monterey Institute- *Center for Non Proliferation Studies*- Nuclear Threat Initiative.
5. Ferguson, C. et al. (2003). Commercial Radioactive Sources: Surveying the Security Risks, *Center for Non-proliferation Studies.*
6. Hanson, Joel,T. (2008). Radiological Dispersal Device Primer From A Terrorist Perspective. Air War College, Air University.
7. International Atomic Energy Agency (2008). Nuclear Security Series No. 9. Implementing guide, Security in the Transport of Radioactive Source.
8. International Atomic Energy Agency (2003). Code of Conduct on the Safety and Security of Radioactive Sources. Vienna, 2003. Available online at: www-pub.iaea.org/books/IAEABooks/8616
9. International Atomic Energy Agency (2009). Nuclear Security Series No. 11, Security of Radioactive Sources.

10. International Atomic Energy Agency (2011). Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Source and Associated Facilities.
11. International Atomic Energy Agency (2005). Safety Guide RS-G-1.9, *Categorization of Radioactive Sources*, Vienna, 2005.Available online at www-pub.iaea.org/MTCD/Publications/PDF/Pub1227_web
12. Kupatadze, A. (2010). Organized Crime and the Trafficking of Radiological Materials: the Case of Georgia. Monterey Institute of International Studies, July 2010 issue.
13. Medalia, J. (2011). Dirty Bomb: Technical Background, Attack Prevention and Response. *Congressional Research Service.*
14. Morris, F., Reed, B., Murray, A. (2013). The Distinctive Challenges of Protecting Radioactive Sources, Proc. International Conference on Nuclear Security: Enhancing Global Efforts, IAEA, Vienna, July 2013.
15. Stewart, S. (2014). The Biggest Threat Dirty Bombs Pose is Panic. *Forbes newsletter*. September 11, 2014.
16. Stewart, S. (2010). Dirty Bombs Revisited: Combating the Hype. *Stratfor.* Dated April 22, 2010.
17. United States Government Accountability Office (2006). Border Security-Investigators Transported Radioactive Sources Across Our Nation's Borders at two locations. March 26, 2006.
18. Visger, B.F. (2004). Dirty Bombs: The Technical Aspects of Radiological Dispersion Devices. Thesis. Naval Postgraduate School, Monterey, California.
19. Wood, D.W., Robinson, D.M. (2009). International Approaches to Securing Radioactive Sources Against Terrorism. Springer. *NATO Science for Peace and Security Series*.

Journal of Physical Security 8(1), 69-92 (2015)

Operative Deterrence: Adversary-Based Security Systems Engineering

Col Raymund M. Tembreull, USAF
and
David T. Young, Analytic Services Inc., Lt Col (USAF Ret.)

During the Cold War, the goal of nuclear deterrence strategy was to deter an attack by the Soviet Union through the certainty of unacceptable consequences. The consequences—the threat of nuclear punishment—extended a type of reciprocal protection to lower operational levels that included tactical weapon generation areas, launch sites, and storage points.[1] The two-plus decades since the dissolution of the Soviet Union have witnessed the primacy of conventional precision weapons (from the JDAM to special operators) in conflict along with significant reductions in the size and diminished efficacy of the strategic deterrent. Despite the potential implications, no definitive efforts have analyzed the corresponding impact of the decline of the U.S. nuclear arsenal on the U.S. ability to deter threat actors from attacking our nuclear sites. By developing a high-end threat model and unique analytical tools to quantify tactical-level deterrence, the adversary's perspective and intentions can be understood and harnessed to prevent attacks on nuclear sites and inform physical security improvements at those locations.

A relic of the Cold War, nuclear units take credit for strategic deterrence at the tactical level within their overall protection strategy. During the Cold War, an attack on a launch delivery platform by a state actor (i.e., the Soviets) could provoke a strategic nuclear attack on the part of the United States. Since the nuclear deterrent is no longer the centerpiece of our national security strategy, we cannot continue to take deterrence for granted. Oblivious to the changing strategic environment, and in spite of improvements to small arms and security technologies, the approach to nuclear weapon security has remained relatively unchanged. Traditionally, the security community has largely relied on the convention of *guards, gates, and guns* as a basis for security and tactical deterrence.

These are primarily visual deterrents that form the basis of features-based security criteria; i.e., it looks impressive and is easy to inspect, but the effects on adversary perception remain undetermined. Our faith in the current system seems to be another artifact of the Cold War.

Failing to acknowledge the dramatic changes in the strategic landscape over the last 20 years, security professionals continue to look at tactical deterrence as a constant in calculating the ability to defeat attacks while the threat profile grows more complex and diffused by the day. A radical divergence from the Cold War threat archetype breaks down the concept of tactical deterrence as a subset of strategic deterrence. Further, in the case of violent extremists, the only thing standing between the *non-event* and an attack could be the adversary's perceived probability of achieving success.[2]

Security experts often dismiss such radical elements as a viable threat against our nuclear sites, claiming an inability among these groups to mount sophisticated attacks, but recent history suggests otherwise (Benghazi and the Westgate shopping mall in Nairobi, Kenya being two recent examples)[3]. Radical Islamic elements have demonstrated the will, aptitude, and capabilities necessary to mount successful attacks against our nuclear sites. Compounding the security problem is that just repelling the attack is not enough, as the act itself (particularly an attack approaching access) would have huge strategic implications, which could completely undermine the foundations of our national security strategy. A deliberate process for preventing an attack altogether is the only acceptable alternative. In other words, the nuclear security enterprise has an obligation to deter.

As distinguished from other threat actors, radicalized Islamists often do not fall neatly into the Western definition of that which is rational. However, such violent extremists all have one thing in common regardless of their cause or their target—*they do not want to fail*. Elaine Bunn establishes that even Islamist extremists are vulnerable to tailored deterrence because, "even terrorists with suicidal inclinations want to die to accomplish something and that defensive deterrence—that is, denying them the accomplishment, or the 'benefits' of their actions—may, over time, be the more effective

way to think about deterring terrorists."[4] Thus, the adversary decision calculus is susceptible to being targeted, shaped, and affected because regardless of the objective, the desire to succeed is a basic human trait and an operational imperative.

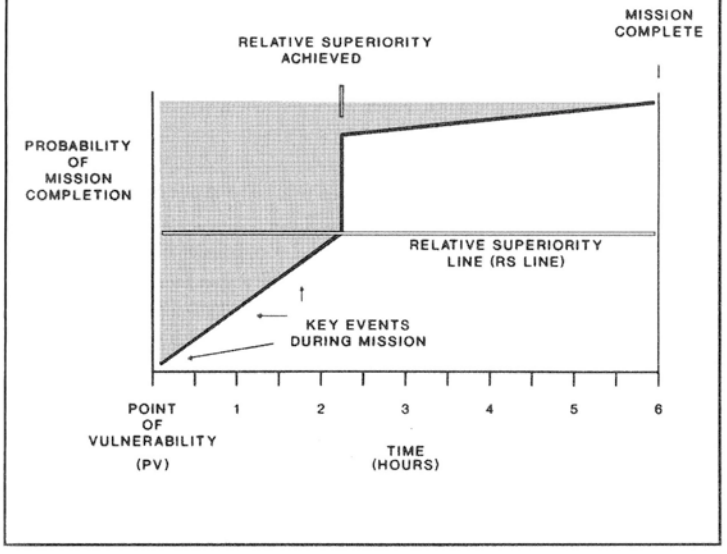
Acknowledging this essential element—*the human desire to succeed*—is the crux of a new security methodology for engineering tactical deterrence. The approach involves taking an outsider's view of the security enterprise. Employing a process called *counter-analysis*, a conceptual threat model and qualitative force analysis tools can be used to understand the task-dependent variables affecting the adversary's mission planning. This understanding is the basis for effectual security system improvements designed to *change the adversary's perception*, and failing that, disrupting or defeating the threat in overt action—the intent of preemption and erosion operations, respectively. "Since deterrence is about influencing the perceptions—and ultimately, the actions—of another party, deterrence is really the ultimate mind game."[5] Thus, deterrence is the nuclear security system's operational imperative and the *operative deterrence* construct provides a deliberate analytical process for incorporating attack prevention and defender superiority into security system design.

A Framework for Counter-Analysis

As a starting point for counter-analysis, a working model of the postulated threat must be developed. An appropriate threat profile can be derived from William H. McRaven's theories on conducting successful special operations forces (SOF) missions. According to McRaven in *SPEC OPS*, a SOF mission is best defined as a *direct action mission*, which is "designed to achieve specific, well defined, and often time-sensitive results of strategic, operational, or critical tactical significance."[6] Our nuclear weapon sites meet this target criterion, representing strategic assets vital to our national security. For the most complex adversary tasks, such as access and theft, the assumption is that our current physical security systems, though not optimized, are robust enough to drive the attacker to this higher level of effort to guarantee a reasonable chance for success.[7]

Identifying a near SOF-capable unit as the threat baseline implies a physical security system must be capable of defeating well-conceived and effectively executed direct-action missions. Security systems built to defeat high-end threats inherently provide sufficient countermeasures to deal with lesser adversaries (with the exception of active insiders). Thus, for the purpose of our analysis, the adversary will strive to gain *relative superiority* over the guard force within the requisite amount of time. McRaven defines this as, "a condition that exists when an attacking force, generally smaller, gains a decisive advantage over a larger or well-defended enemy."[8] McRaven's *Relative Superiority Graph* is illustrated in figure 1.[9]

Figure 1: McRaven's Relative Superiority Graph



In order to leverage the relative advantages of both surprise and speed, SOF are designed to operate as small, lightly armed yet highly capable force packages. These attributes also constitute their inherent weakness in that they are unsuited for sustained action against a large defensive force. Thus, as depicted in figure 1, the adversary must

achieve relative superiority early in the engagement and retain it while minimizing the corresponding time on the objective. The choice of timing and location belong to the threat so the early advantage belongs to the adversary by virtue of speed, surprise, and initiative.[10]

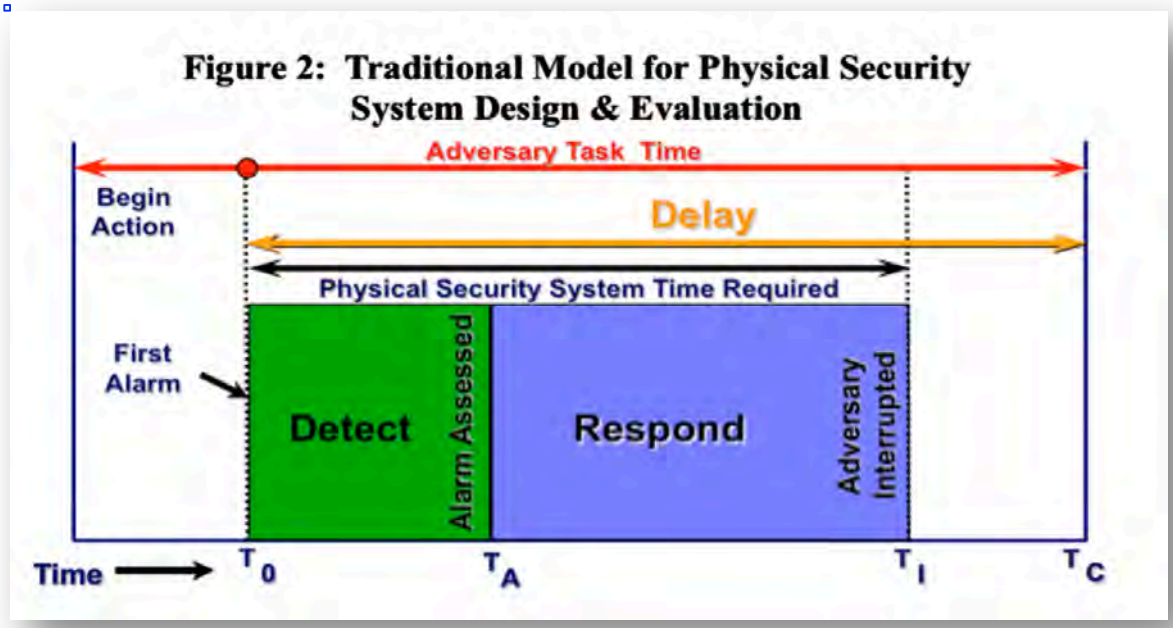
Friendly security objectives, then, must become the converse of the threat with nuclear site security measures designed to deny the adversary relative superiority. To achieve this, system designs must include early warning and detection; deception, delay and denial penalties; and a robust response subsystem. All site countermeasures work in concert to present a hard target, likely never to be selected as the adversary's final objective. Subverting and expanding McRaven's model is the basis of a conceptual framework for building security systems that achieve these core functions.

At the tactical level, deterrence doctrine and site protection strategy have a shared objective: *attack prevention*. The decision to attack occurs early in engagement sequencing and the process of assessment and evaluation to arrive at that decision occurs even earlier. Although McRaven's relative superiority graph provides the springboard for our counter-analysis, the model only provides the context for analyzing the force-on-force engagement from attack commencement. The decision to attack has already been made and the process behind the *why* of that decision has already been completed. This downstream starting point is consistent with the traditional analytical tools and modeling and simulation applications security experts currently employ to assess protection system performance. In order to assess a site security system's ability to deter attacks, our counter-analysis must begin much earlier in the adversary task sequence—when pre-attack preparations are underway and the probability of failing is being assessed.

Counter-Analysis Phase I: The Relative Strength Model

In our analysis, McRaven's graph (figure 1) depicts adversary actions. To generate an overlay representative of friendly actions and countermeasures, a departure must occur

from the traditional paradigm of physical security assessment. Customarily, physical protection systems (PPS) have been built around three primary subsystems: (1) the detection subsystem; (2) the delay subsystem; and (3) the response subsystem.[11] See figure 2. Typically, security experts assess how these three subsystems interact in a post-detection mode with effectiveness judged by the system's *reaction* to an incursion or attack. A recognized truth of system design is that a "PPS system performs better if detection is as far from the target as possible and delays are near the target."[12] The reality of most legacy systems is that detection and assessment occur simultaneously, typically tied to PPS alarm annunciation at the nuclear site. Unfortunately, the adversary's attack is already underway.



To affect the adversary's decision calculus and create these additional detection and disruption opportunities, the PPS must expand the defended space and produce effects much earlier in the adversary task sequence. To do this, the PPS must generate both direct and indirect effects to impact the adversary operations prior to the start of direct action. The security system must generate greater situational understanding for the guard force

while simultaneously confusing, intimidating, and producing misconceptions in an enemy who is still planning, watching, and unprepared to act overtly.

To leverage the full range of disruption opportunities, the PPS must target the broad spectrum of preparatory actions that must occur prior to direct action. During this period, enemy activities include planning, reconnaissance, surveillance, recruiting, training, and resource procurement, which occur over an extended timeline running from weeks to years. The enemy is dispersed and weak during these passive precursor events. By pushing security operations off-site and off-base, the guard force is afforded an expanded detection envelope and engagement area to shape an environment of friendly relative advantage. More specifically, the PPS must optimize capabilities in those areas of the task sequence where friendly forces retain a relative force advantage and improve performance in those critical junctures of the continuum of struggle where relative superiority is in doubt. The ideal end-state is a formidable security system that drives the adversary's to abandon the attack in favor of a softer target or be defeated in the process of planning the attack.

By overlaying the expanded adversarial task sequence with revised security system objectives, and by charting the relative advantage of both friendly and adversary forces throughout the entire task time, the continuum of struggle is depicted in a manner that enables a more definitive investigation of deterrence-centric site protection capabilities. See figure 3.[13] The *y-axis* delineates the relative strength advantage between opposing forces—friendly guard forces and protection system elements versus a capable adversary—with respect to time (*x-axis*). Along the x-axis, three distinct engagement zones—*Find*, *Fix*, and *Finish*—manifest themselves, culminating with the *Assess and Recovery* phase. Thus, the relative strength (RS) model documents the continuum of struggle, representing the contest of two opposing forces striving to gain relative superiority over one another. Each of the designated engagement zones call for their own brand of combined effects to counter anticipated enemy activities.

The clock starts ticking with the adversary's passive preparatory activities, such as planning and surveillance, and culminates in task completion, task disruption, or defeat by the guard force. Considering the readiness timeline required to launch an effective attack

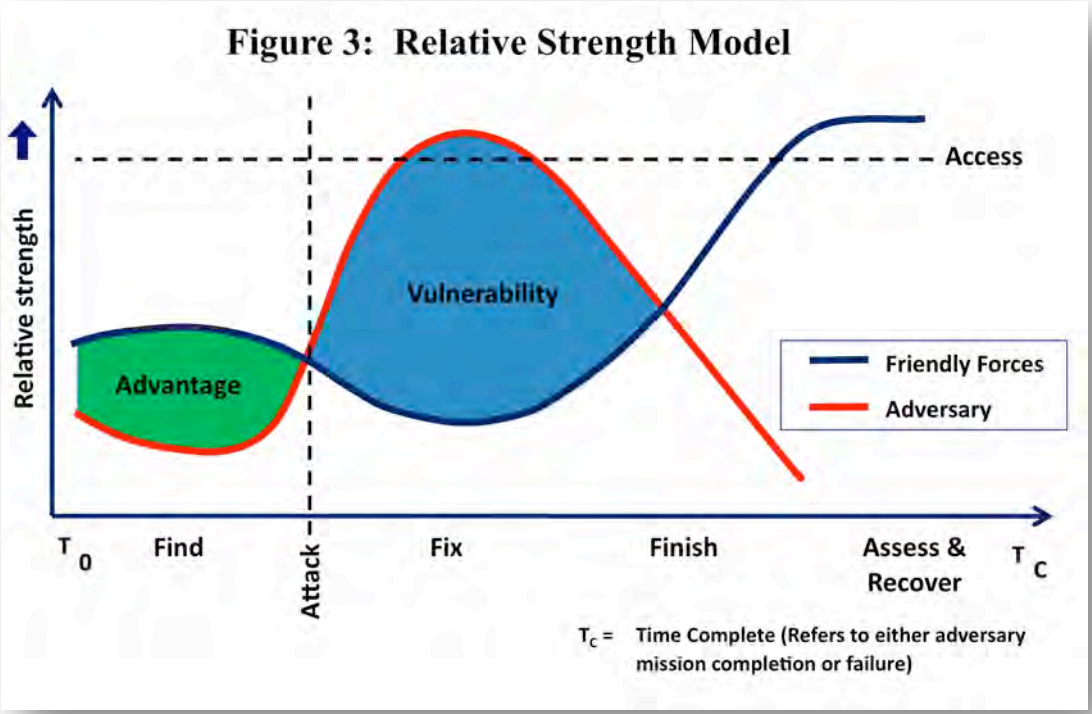


Figure 3: Relative Strength Model

on a nuclear site, the graph's "Find" engagement phase is the longest (sizing in the model is representative only). The adversary is capable of being deterred anytime from T_0 until the initiation of the attack (i.e., the Find phase). With respect to the vertical axis, both friendly and enemy forces operate from a position of relative strength at different points in the continuum. Relative strength lines demarcate areas of vulnerability that equate to exploitation opportunities for the stronger of the two opposing forces at any given point in the engagement. The goal of both friendly and adversarial forces is achieving and maintaining a relative force advantage in pursuit of divergent objectives. The defender's first order objective is *tactical deterrence* while that of the adversary is *access*.

Counter-Analysis Phase II: The Relative Strength Equation

The RS model is only one of two analytical components. The second is a balanced expression composed of the most influential factors in the attacker-defender engagement.

In McRaven's *Relative Superiority Graph*, T_0 (referred to as the "Point of Vulnerability" in figure 1) is the point at which attack commences, carrying through all active attack phases. In this case, McRaven's graph depicts the relative strength of adversary actions. The expanded continuum of struggle depicted by the RS Model (figure 3) is necessary to find areas of friendly force advantage. Note the RS model pushes T_0 to the left to cover all of the adversary's passive activities. This added time domain becomes an entirely new engagement phase covering the period for pre-attack preparations (mission planning, objective reconnaissance, surveillance, logistics support, etc.). During this period, the adversary is dispersed, weak and at greatest risk of exposure. Because of the early comparative advantage for the defense force in this domain, it is also the window of opportunity for deterring the adversary.

By looking at the activities required for success of either party in both the passive and active phases in figure 3, the primary elements shared by opposing forces that determine the outcome of the engagement can be identified and expressed in terms of the following balanced equation, referred to as the relative strength (RS) equation[14]:

$$[I_t^2(t) \times R_t(t)]SOS_t = [I_{SF}^2(t) \times R_{SF}(t)]SOS_{SF}$$

Where the variables are defined as follows,

- I = *Intelligence* refers to the entire apparatus in place to provide situational awareness and understanding, including early warning and detection systems. "I" represents the information needs of both sides. The adversary's task is to determine vulnerabilities. Since nuclear operations are highly visible in many environments, the adversary must determine the fine details to identify the

exploitable gaps and seams. Government force information needs are associated with threat characterization and pre-attack detection. If the adversary is discovered prior to initiation of the attack (T_{attack}), the net result is mission failure, and likely, the complete destruction of the threat organization. Thus, the variable "I" is squared due to the relative importance of intelligence in influencing the final outcome of the engagement.

- R = *Resources Available* to friendly forces to counter adversary operations and to the adversary for actioning a target (e.g., nuclear weapons storage, generation, and delivery sites).
- SOS = *Security Operating Structure* encompasses those elements of the security architecture external to both the defender's and attacker's organizations, including intangible contributions that can tip the scale in favor of one force or the other. To the defense, SOS really represents the interagency and civil-military effort. For the adversary, the support architecture includes the facilitation networks that smuggle in or locally procure weapons and equipment. Thus, SOS entails those essentials that both directly and indirectly enhance each force's "I" and "R".

NOTE: The superscripts, "t" and "SF", represent *threat* and *security force*, respectively.

The RS equation depicts a precarious balance where equilibrium correlates to the *non-event*. Because the attacking force is striving for relative superiority over the guard force while the guard force is simultaneously determined to deter an attack or maintain relative strength in the face of attack, equilibrium is in a constant state of tension involving unstable elements. Both sides can be envisioned as always competing for conditions beyond equilibrium.

I and *R*, as time dependent variables, require significant investments of resources, man-hours, and support infrastructure to realize incremental improvements in capability. *SOS*, however, is not time dependent; it is an ordinal variable with a total value of 1. For

example, if $SOS_t = 2$, then $SOS_{SF} = {}^1/_2$. Thus, *SOS* is a *capability multiplier* depicting the preparedness of opposing forces in relation to each other. Through its influence over those activities that occur prior to direct action, *SOS* may ultimately prove to be the decisive factor in attack prevention.

Creating Operative Deterrence

The term, tactical deterrence, is not sufficient to describe the desired end state since the intended effects are far more precise then the term implies. *Operative* is the key word in this perception-oriented defensive scheme, meaning "producing a desired effect." In his celebrated interwar work, *DEFENSE*, Field Marshal General Ritter Wilhelm von Leeb introduced the concept of establishing an "operative defense,"[15] in which he promoted the idea of opening a campaign with an active defense in preparation of a later offensive. Key among von Leeb's military precepts was that "defense is dependent upon attack. It must be adapted to the measures of the aggressor. Its state is that of operative and tactical dependence upon the attacker."[16]

To move from von Leeb's operative defense to *operative deterrence*, the defense must be so masterfully adapted to the measures of the aggressor as to render the prospects of victory highly improbable; so improbable that offensive operations are never undertaken. Thus, the concept of operative deterrence for nuclear weapon security is predicated on two assumptions: (1) the task complexity presumes some level of rationality in the adversary; and (2) the adversary does not want to fail.

Applying these assumptions to the tools derived from counter-analysis provides the means for identifying the elements to achieve both operative deterrence and a relatively superior defense posture. Creating this dual phenomenology within the physical protection system requires targeting the *Find* and *Fix* engagement phases within the continuum of struggle. For this discussion, protection system measures designed to counteract adversary actions in the Find phase will be designated *preemption operations*

while friendly countermeasures in the Fix phase will be referred to *erosion operations*. The physical security system mandate then becomes: achieve operative deterrence through *preemption operations*, and failing that, disrupt and defeat adversary attempts to achieve relative superiority through *erosion operations*.

Preemption Operations

Having established the case for "why," determining the "what" and "how" of preemption operations requires a much deeper examination of the *Find* phase of the engagement sequence. The implication of these actions are obvious—*attack prevention*. Thus, corresponding objectives are designed to frustrate the adversary's decision cycle, complicate his planning processes, distort his perception of the protection system, reduce resource availability, deny insider assistance, and make target observation and definition a difficult and hazardous venture.

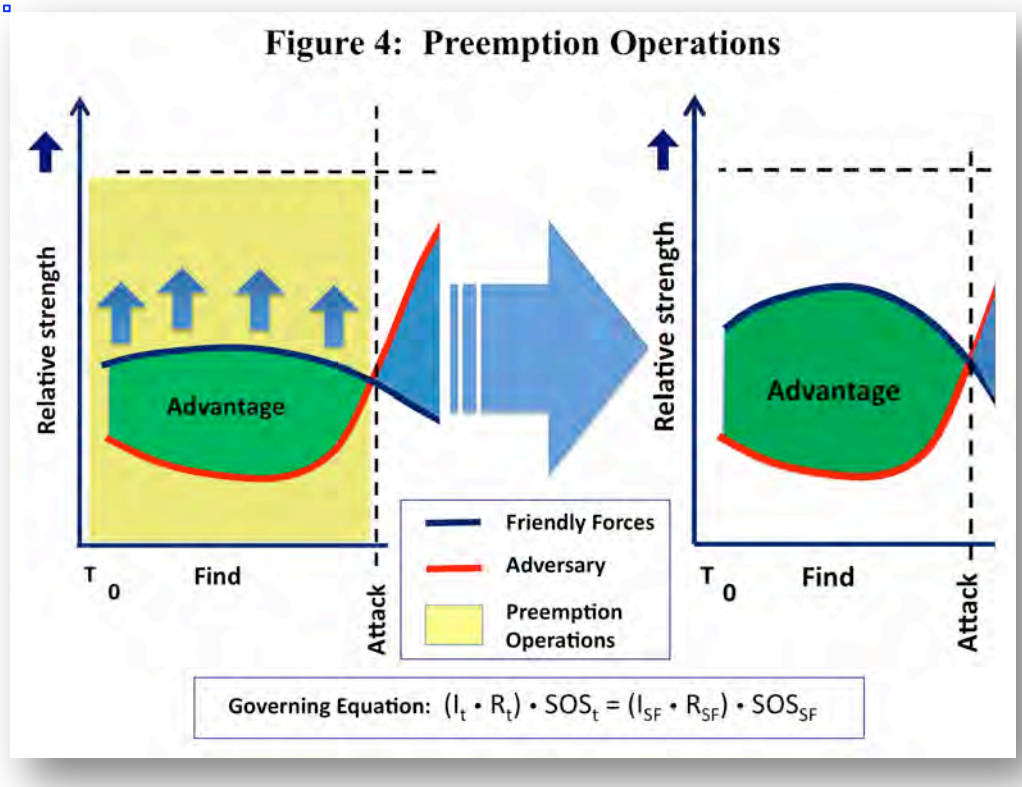


Figure 4: Preemption Operations

As figure 3 illustrated, friendly forces maintain a relative advantage throughout the *Find* phase, equating to an area of vulnerability for the adversary. Hence, the intent of preemption operations is to employ a combination of measures to expand the adversary's vulnerability while simultaneously providing greater opportunity to deter or disrupt the threat. See figure 4. All three RS equation variables—intelligence (*I*), resources available (*R*), and security operating structure (*SOS*)—are all in play prior to the attack, and thus, capable of influencing the outcome.

The variable *I* dominates the RS equation, manifesting itself in a counteractive relationship between I_{SF} and I_t. Guard force measures to attack I_t often indirectly improve I_{SF} with the converse frequently proving true as well. Hybrid security force approaches combining tactical deception with randomized defense routines are a prime example. *I* is inextricably linked to security force detection ability and the threat planning cycle. The mathematics of surveillance suggests the adversary must account for the random presentation of security measures as planning constants. In this way, the security force can artificially enlarge its force signature from the outside observer's perspective, i.e., that observed at least once, must be planned for as always present. If forces engaged in randomized measures and tactical deception are further charged with counter surveillance responsibilities, the protection system is simultaneously attacking I_t while enhancing I_{SF}. Because of the inordinate influence of *I* in the RS equation, I_{SF} improvements coupled with degradations to I_t are the single greatest factor in expanding the adversary's area of vulnerability in the *Find* engagement phase.

Building a refined understanding of the objective using covert surveillance and intelligence gathering requires substantial time observing the target and security force operations. If such methods are the only means available to the adversary, a detailed and accurate intelligence picture entails greater risk of exposure, equating to more opportunities for PPS detection. This information-related Achilles' heel can be exploited by tailored security forces actions. In the *Find* phase, adversary options are much more restricted. Post-infiltration, one of the few options left to an adversary for improving I_t beyond conventional means is through insider assistance from either sleeper agents or co-

opted support. Passive insiders from the right functional areas can provide key insights on unobservable target information to enhance adversary planning. However, reliance on insider assistance represents another source of operational risk since current PPS countermeasures make co-opting insider support extremely difficult. PPS susceptibility to insider threat exploitation can be further reduced by additional measures, e.g., continuous vetting, split knowledge/handling, random duty assignments, etc.

In the absence of early warning, resources available to the security force (R_{SF}) are finite while operating in standard posting configurations. However, intentional actions to conceal or obscure on-site resources can frustrate adversary planning while tactical deception can complicate the endeavor. Resources available to the adversary (R_t) pose a more difficult logistical problem. The attacker must either infiltrate with required equipment or stockpile the necessary gear and resources within the area of operations (or pursue a combination of both actions). Since task complexity drives *R*, most required resources would likely be procured and gathered post-infiltration. Thus, R_t is both a function of time, and the time required is a function of task complexity. Adversary path analysis is a tool that can provide additional insight to security forces about likely adversary courses of action. These results can inform the security force on the critical equipment needs, providing a starting point to secure the supply chain and make the most vital items difficult to obtain. Deliberately increasing R_t (both actual and perceived) and complicating critical equipment resourcing can produce potent effects that expand the adversary's area of vulnerability, driving the outcome toward a "no attack" decision.

Security Operating Structure, *SOS*, is a different animal altogether. Its strength, the ability to enable, is not exclusively dependent on time. On the friendly side of the equation, the biggest enemy of SOS_{SF} is apathy. If leadership emphasis and attention to the nuclear mission falters, defense force leadership looks inward as they tend to morale issues and seek to maintain existing capability. When the efficacy of a mission declines, it no longer attracts the most talented leadership or garners favored resourcing status. Conversely, units in high priority nuclear missions are well led, sharply focused, and better equipped. During these times, engaged leaders look outward, building relationships with civilian law

enforcement units and counterintelligence agencies and increasing public and private awareness networks within the local community. An enhanced security architecture expands detection capabilities well beyond nuclear site boundaries and degrades SOS_t by restricting adversary activities and suppressing covert support networks. *SOS* is a fickle beast, seesawing back and forth over time in favor of each side. However, the defender on home turf has the advantage in maximizing *SOS*.

The analysis of preemption operations, using both counter-analysis tools, is simplified by the choice of scenario in this case. All nuclear sites are situated in the continental United States or on highly secure military installations in allied countries. The absence of war, or of targetable installations located in contested territories, removes many dynamic factors from the assessment. With the exception of what the adversary infiltrates in with, the environment can be treated as a closed system. This is a huge advantage for the defender who has a tremendous amount of control over many aspects of the expanded defense area, and by default, the *Find* phase of the continuum of struggle.

By attacking the adversary *I*, *R* and *SOS*, while simultaneously enhancing his own position in those three areas, the defender can unbalance the RS equation in his favor. If the adversary's area of vulnerability is large enough, the nuclear site will never make the target list. Lesser effort or success may result in initial target selection, but by driving up perceived risk to unacceptable levels, adversary plans for direct action will likely be abandoned. Simply driving up the operational costs and complexity to the point where enhanced friendly networks (a combination of I_{SF} and SOS_{SF}) can detect or capture the adversary prior to the attack is another potential outcome.[17] *Preemption operations* have achieved their desired effects when the RS equation favors the defender and the adversary's area of vulnerability has grown insurmountably large—the greater the relative imbalance in *I*, *R* and *SOS*, the greater the preemptive effects.

Erosion Operations

Consider this situation: Attack prevention has failed and adversary direct action has commenced. This triggers a defensive transition from preemption operations to active defense—the domain of *erosion operations*. Erosion operations seek to affect the front end of the *Fix* phase of the engagement. See figure 3. They are designed to absorb and turn the adversary's primary thrust in the critical first minutes of direct action. Success in this domain of action does not require the security force to win outright, but only to extend the engagement. Like a SOF raid, the adversary is operating in hostile territory and bringing everything to the fight—no reinforcements, no resupply. The attacker is a slave to task time, and the guard force imperative is to exploit that weakness: *because the adversary's resources are limited, his combat power will attenuate over time*.

This is no easy assignment for the defender. The attacking adversary has a great deal of confidence, engaging the security force at the time and place of his choosing. The attacker is buoyed by speed, surprise, and violence of action. His success will largely be determined by the gains achieved in the critical first minutes and, the nuclear security force does not have the option of falling back to regroup. Presidential directives call for denying access at all costs, which mean the defender will more than likely be fighting from positions of disadvantage early in the fight in order to deny access and extend the engagement until reserve forces can respond en masse.

In the absence of resupply, effects achieved by adversary firepower will likely peak relatively early. The attacker must gain access as quickly as possible, ideally with minimal lose of resources and personnel. At access, the threat's threshold objective is achieved, opening up multiple follow-on options depending on remaining R_t and time available (e.g., weapon theft, destruction, deliberate unauthorized use, etc.).

By referring back to the *Fix* engagement phase in figure 3, the adversary's relative strength advantage and the defender's area of vulnerability are immediately obvious. Thus, the objective of erosion operations is to "squeeze" the friendly area of vulnerability by forcing an early, rapid attenuation in adversary combat power and task-essential resources. See figure 5.

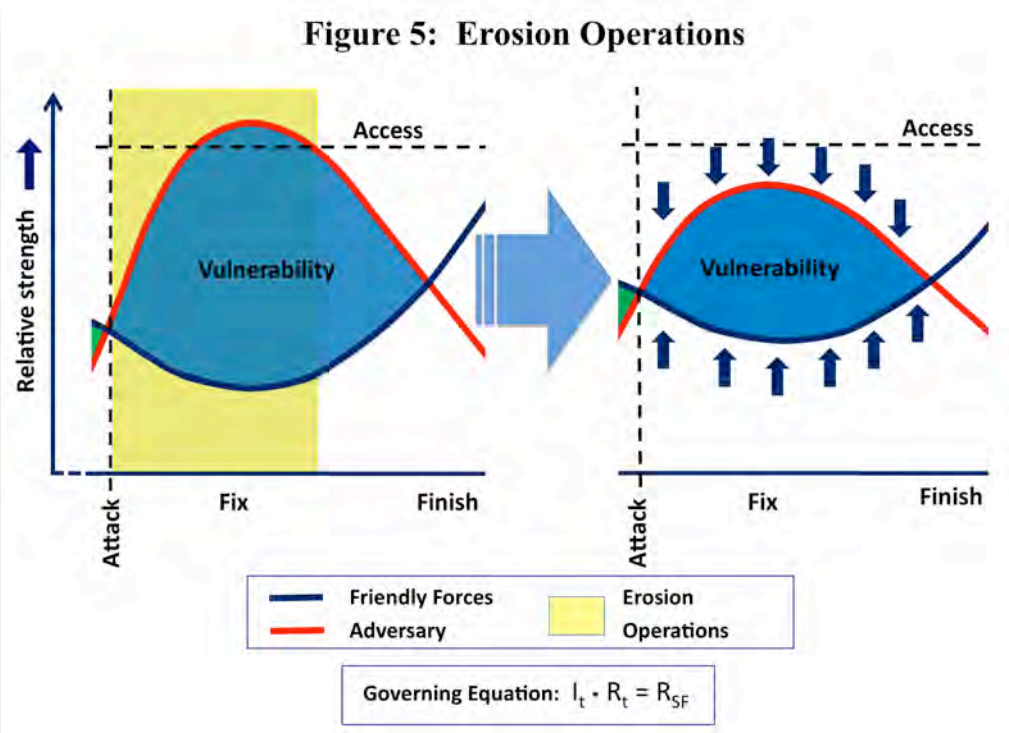
For this engagement phase, isolating the causal variables from the relative strength equation can identify erosion-enabling concepts. Prior to the onset of direct action,

$$(I^2_t \cdot R_t) \cdot SOS_t = (I^2_{SF} \cdot R_{SF}) \cdot SOS_{SF}$$

The capability multiplying effects of *SOS* no longer directly influence the outcome of the engagement after direct action has commenced. Thus,

$$(I^2_t \cdot R_t) \cdot \cancel{SOS_t} = (I^2_{SF} \cdot R_{SF}) \cdot \cancel{SOS_{SF}}$$

$$(I^2_t \cdot R_t) = (I^2_{SF} \cdot R_{SF})$$



Once the adversary has progressed to attack, the friendly intelligence apparatus is no longer relevant with the exception of close-in detection (e.g., electronic sensors or posted sentries). Friendly forces gain nothing more from I_{SF} than a small reactionary gap. For I_t, the adversary gleans significant advantage from the element of surprise, starting the

fight with specific targeting information on defense force dispositions and weapon(s) locations. Hence, the RS equation is reduced to the following for direct action:

$$(I^2_t \cdot R_t) = (I^2_{SF} \cdot R_{SF})$$

$$I_t \cdot R_t = R_{SF}$$

All remaining variables are time dependent. The threat's advantage in *I* diminishes rapidly and can only be prolonged by retaining the initiative. Well-trained and superbly led defenders can quickly negate and reverse the adverse effects of I_t within a properly designed PPS. R_t diminishes over time as the adversary experiences casualties, expends ammunition and suffers equipment losses. For R_{SF}, the opposite is true. The defender will certainly suffer casualties early in the engagement, but if the engagement is maintained and access is denied, incremental reinforcement by backup forces enables the defender to achieve localized parity first followed eventually by relative superiority. Thus, the key for the defender is to extend adversary task time by denying access and extending the engagement. Consequently, erosion operations help the security force withstand the adversary's early I_t advantage and attack R_t through task complexity and protection system delay/denial countermeasures.

Understanding the nexus upon which the outcome of the battle hinges is integral to identifying defense options. Since the threat seeks to locally overmatch in-place security forces, enhanced guard force survivability is about force protection, maneuver, and dispersion. Diffused posting schemes complicate adversary targeting when combined with the requisite command and control and mobility to rapidly mass at the point of attack and jam a blunt wedge into the threat's initial thrust at the target.

To take advantage of inherent limitations in threat force size, the PPS must be designed to dilute adversary combat power at the onset of the engagement through task complexity. A layered protection system with a host of active and passive delay/denial features pushes up adversary resource requirements, indirectly stressing the adversary logistics network and forcing the adversary to divide up his forces to deal with new

targeting problems. Additionally, required actions on target and weapon access should drive overwhelming task specialization (e.g., explosive breachers, weapon techs, and task-specific equipment operators), removing pure shooters from the fight. Every added problem, every additional feature, and every posted sentry that survives the initial attack in fighting condition adds to the defender's competitive advantage: *the delay necessary to mass overpowering force*.

Conclusions

Like McRaven's relative superiority graph, both elements of counter-analysis—the RS model (figure 3) and its companion equation—are not quantitative mission analysis tools. Both the model and the equation illustrate the relationships and interactions between the key factors involved in tactical deterrence and successfully defending a nuclear site or any fortified target from a SOF-capable raid. These crucial factors are essential to understanding the adversary's requirements for success and establishing corresponding linkages to actionable principles and objectives to achieve *operative deterrence*.

Operative deterrence is specifically designed to influence adversary perception, achieving attack prevention by driving up the probability of failure to unacceptable levels. Thus, the concept is not dependent on any reciprocal contributions from the strategic nuclear deterrent. Failing attack prevention, the operative deterrence construct goes a step further by informing physical security system design features that will deny an attacking force the ability to achieve relative superiority, ultimately contributing to adversary mission failure.

To expose the inherent fragility in raids and direct action missions conducted by small units operating in hostile territory, the adversary task sequence was expanded well beyond the bounds framed by McRaven's mission analysis graph and the traditional models and means for assessing PPS performance. In order to identify the crucial factors in

deterring adversary actions at the tactical level, as well the exploitable vulnerabilities in the attacking force, the RS model encompasses the preparatory activities that must be accomplished prior to direct action. The expanded threat scope, referred to as the *continuum of struggle*, is further broken down in engagement phases *Find, Fix*, and *Finish*. Employing the second element of counter-analysis, the constituent elements of the RS equation were used to analyze the *Find* and *Fix* phases and develop threat countermeasures—defined as *preemption* and *erosion* operations. Both types of operations are specifically tailored to attack adversary perceptions and intentions within their respective phase.

The post-Cold War world has witnessed the rise of the dispersed threats disassociated from the nation state and the information age has multiplied their abilities to influence global politics and world powers. Now, the outcome of single engagements can shape the collective will of nations and multinational coalitions. Recent history is replete with examples of both victories and defeats based on the planning and execution of opposing forces within the *Find* and *Fix* phases of the continuum of struggle.[18] The choices and investments of authoritative powers to fashion the operational environment within the domains of preemption and erosion operations largely determine the outcome before the first shot is fired—or even if it is fired at all. Any potential contest can be analyzed with counter-analysis tools as long as the battlespace can be localized to the point where an attacker, an environment and target can be effectively isolated and defined.

Although preemption and erosion operations are oriented around two separate phases of the continuum of struggle, it is important to note they are complementary concepts that both contribute to operative deterrence. As long as measures implemented for erosion operations are integral parts of the steady-state protection system, they affect the adversary's decision calculus. Every added countermeasure that increases the probability of failure contributes to attack prevention, and thus, to preemption operations and operative deterrence as a whole. RS analysis tools provide the means for achieving operative deterrence through implementation of a site protection system that subverts adversary perceptions to reduce options and decrease of probability of achieving sought-

after objectives. Thus, operative deterrence quantifies and harnesses tactical-level deterrence to both prevent attacks on our nuclear sites and improve the physical security at those locations.

References and Notes

1. The assumption is the perpetrator could only be someone preparing to engage in nuclear war. During the Cold War, attacking a nuclear weapon and nuclear deterrent forces carried the possibility of provoking nuclear conflict and invoking a nuclear exchange.

2. This decision process is well documented with respect to suicide bombers.

3. Attribution for September 2012 attack on the U.S. diplomatic mission in Benghazi, Libya is still in dispute with many sources giving Al Qaeda credit for the terrorist attack.

4. Elaine Bunn, "Can Deterrence be Tailored?" Institute for National Security Studies, *Strategic Forum* 225 (January 2007): 3, http://www.hsdl.org/?view&did=481759 (accessed November 27, 2013).

5. Ibid.

6. William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (New York: Ballantine Books, 1996), 2-3.

7. The assumption is any adversary worth planning for will understand the capabilities necessary to achieve an acceptable chance of success.

8. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice*, 4.

9. Ibid., Fig. 1-1. "Sample Relative Superiority Graph," 7.

10. The result of adhering to the SOF operational principle of simplicity and conducting rehearsals; both of which often dependent on effective reconnaissance.

11. Mary Lynn Garcia, *The Design and Evaluation of Physical Protection Systems* (U.S.A.: Elsevier Science, 2001), 55-58.

12. Ibid., 5.

13. The *Relative Strength Model* is the joint intellectual property of Young and Tembreull. The concept was developed and refined over from 2007 – 2012 where the authors were serving as nuclear security squadron commanders and eventually served together on the Air Staff with the responsibility for writing USAF nuclear security guidance.

14. The *Relative Strength Equation* is the intellectual property of Young with minor contributions from Tembreull in refining the concept. The equation was developed while the authors were serving an Air Staff tour, AF/A7S, tasked with revising USAF nuclear security guidance (2011) and is based on instruction from Naval Postgraduate School's Special Operations/Low-Intensity Conflict program.

15. von Leeb, Field Marshal General Ritter, *Defense*, first translation, 1943, by Dr. Stefan T. Possony and Daniel Vilfroy, Book 3, *Roots of Strategy* (Harrisburg, PA: Stackpole Books, 1991), 6.

16. Ibid.

17. Among nuclear weapon and nuclear energy facilities, deter or post-incursion capture have been the only outcomes to date.

18. Three post-Cold War examples that illustrate the application of operative deterrence principles include the 1995 Battle for Grozny, the 2007 "Fort Dix Six" conspiracy, and the U.S. Navy SEALs failed October 2013 raid against al Shabaab in Somalia. Inferior Chechen forces employed deception operations extensively to bolster *I* resulting in many wins on the battlefield where final Russian victory was only achieved at tremendous

cost. A robust U.S. domestic *SOS* following 9/11 and successful FBI infiltration of a terrorist group averted a planned attack against a military target. Early detection by a single al Shabaab sentry in final movement to the objective exposed the SEALs during the fragile stage of a direct action mission, providing enough early warning for a larger, yet lesser-trained and equipped defending force to deny the SEALs relative superiority.

Journal of Physical Security 8(1), 93-110 (2015)

The Impact of the Aircraft Owners and Pilots Association "Airport Watch Program" on Crime at Pennsylvania General Aviation Airports

Daniel J. Benny, Ph.D., CPP, PCI, CFE, CCO, CASP, CIPM

Bachelor of Science in Aviation Security Program Chair
Embry Riddle Aeronautical University Worldwide

Abstract

This study examined the Aircraft Owners and Pilots Association (AOPA) Airport Watch Program (AWP) at 118 general aviation airports throughout the Commonwealth of Pennsylvania. The quantitative research was conducted to establish if the AWP had an impact on the airport crime rate.

Introduction

In March 2003, the Aircraft Owners and Pilots Association (AOPA) announced the Airport Watch Program (AWP). The goals were to enhance security at general aviation airports, to aid in the prevention and reduction of crime in the general aviation community, and to potentially avoid mandated security regulations from the Transportation Security Administration (AOPA, 2003).

The AOPA's AWP is not a new concept. It is based on existing crime watch programs. The modern concept of the community crime watch program was conceived and implementted in the United Stated during the 1970s.

In 2005, a qualitative study was conducted within the United States airline industry. The goal was to evaluate the concerns of pilots, aircrews, and passengers in light of the recent implementation of the new Department of Homeland Security (DHS) commercial airport and airline crime prevention measures. The research found that pilots, aircrews, and passengers had reduced fears about terrorism and aviation crime with the implementtation of the new DHS measures.

Since the events of September 11, 2001 and the revelations that terrorists have used the general aviation community to train for airborne terrorism, there has been no new research on the impact of the Airport Watch Program (AWP).

The AOPA's AWP encompasses two concepts: physical security and security awareness. As it relates to physical security, the program recommends and encourages general aviation airport managers, aircraft owners, and pilots to utilize good physical security practices to prevent and reduce crime (AOPA, 2003).

The security awareness aspect of the program focuses on making general aviation airport owners and employees, as well as aircraft owners and pilots, aware of their surroundings. This includes being alert to what is normal activity at the general aviation airports and what is not (AOPA, 2003).

The crimes that can occur at a general aviation airport include crimes against persons, the airport property, the fixed base operation (FBO), and aircraft located at the airport. Crimes against a person can include any crime that has an impact on a person present at the airport. This includes the crimes of murder, rape, robbery, assault, stalking, kidnapping, and harassment (Sweet, 2009).

Crimes against airport property or the FBO only affect the physical structures. Such crimes can include burglary, theft, arson, and vandalism. The crimes that could be perpetrated against the aircraft situated in a hanger or tie-down area at the airports include

theft of the aircraft, theft of aircraft avionics, sabotage of the aircraft, hijacking, and vandalism (Sweet, 2009).

Statement of the Problem

The impact of crime prevention efforts such as the AOPA's AWP is unknown because of the lack of research in this area. This has created a gap in the knowledge related to general aviation, and leaves the general aviation community without a baseline of knowledge and information regarding the impact of crime prevention programs (Bisignani, 2006).

This work attempts to bridge the gap between community crime watch research and commercial aviation crime prevention research. This is accomplished by providing new knowledge with regard to the impact of general aviation security and the AOPA's AWP. The purpose of the study is to determine the effects of the program on crime at the airports that adopted the AWP during the period from 2002 to 2004.

This research examined and answered the following question:

Q1: Is there a difference in the number of crimes between general aviation airports that have adopted the AWP and those that have not?

The hypothesis and null hypothesis examined in this study are the following:

H1: There is a difference in the number of crimes between general aviation airports that have adopted the AOPA's AWP and those that have not.

H01. There is no difference in the number of crimes between general aviation airports that have adopted the AOPA's AWP those that have not.

A quantitative research method was selected for this study because it is the most effective research method for the collection and evaluation of factual data relating to crime statistics. The philosophical foundation for quantitative research originates from the logical positivist, post-positivist, post-modernism, or pragmatism traditions (Champion, 2006). To make a

determination of the impact of the AOPA's AWP on crime at general aviation airports, the collection of data based on observable facts conforms to the logical positivist approach.

Research Design and Methodology

A quantitative statistical methodology was utilized to examine the intervention and the control groups. The intervention group consisted of those airports that have adopted the watch program, while the control group consists of those airports that did not adopt the watch program. I examined two existing groups that have not been manipulated or changed during the study. This is because the manipulation has already occurred at the general aviation airports in the Commonwealth of Pennsylvania who have adopted the AOPA's AWP and general aviation airports in the Commonwealth of Pennsylvania that have not adopted the program (Creswell, 2003).

The data were derived from a survey of the general aviation airports located in the Commonwealth of Pennsylvania. An Ex-post-facto design was selected because this research explores the impact of the Aircraft Owners and Pilots Association Airport Watch Program on the crime at the general aviation airports after the fact. What was researched has already occurred and there is no treatment applied. The Ex –post- facto design can be utilized to examine the possible independent variables that may be apparent in the research and where experimentation is impossible because the events have already taken place. Ex – post- facto design can also be utilized as a possible causal model that may be tested via additional research (Champion, 2006).

The study's sample data were collected using a survey that was emailed to the 122 general aviation airports in the Commonwealth of Pennsylvania, along with a consent form, and a letter of introduction with instructions. The airports chosen for study were obtained from a list of the licensed general aviation airports in the Commonwealth of Pennsylvania that is compiled by the Pennsylvania Department of Transportation Bureau of Aviation (Pennsylvania Bureau of Aviation, 2008).

Of the 122 general aviation airports that were sent the survey, 4 had closed, leaving a total of 118 general aviation airports. Of these 118 airports, 67 responded to the survey. A total of 37 (55%) of these had adopted the AWP, and 30 (45%) had not. To establish the sample size necessary for the statistical analysis, one should consider the power, effect size, and level of significance. Thus, I considered the sample size (N), significance criterion (ft), population effect size (ES), and the statistical power (Cohen 1992). Given a large effect size of 0.50, a generally accepted power of 0.80, and a 0.05 level of significance, the necessary sample size to achieve empirical validity for this study is 26 for each group (52 observations in total). For 52 observations (26 adopters and 26 non-adopters), the desired sample size would require a be a response rate of at least 42.5% for each group (Cohen 1992).

Data were entered into SPSS 16.0 for Windows. Descriptive statistics were applied to the demographic data. SPSS, the *Statistical Package for the Social Sciences*, was developed in 1968 by Norman Nie, C. Hadlai Hull, and Dale H. Bent. The SPSS software system was based on the idea of using statistics to turn raw data into useful information or intelligence that could be used in business and the intelligence community for decision-making (Cronk, 2006). SPSS was used in this research to convert the raw data collected from the general aviation airports to useful information to determine the impact of the airport watch program on crime.

To examine research question Q1, level 3 of the Maryland Scale of Scientific Methods was used to make a comparison between comparable units, one adopting the program and one not adopting the program. I compared the general aviation airports located in the suburbs that had local police protection with the general aviation airports located in rural areas that lacked local police protection. A one-way ANOVA (analysis of variance) on the number of crimes (i.e., people, property, and aircraft) for AWP adopters vs. non-adopters was undertaken. The assumptions of ANOVA—normality and homogeneity of variance—were assessed, i.e., whether the appropriate analysis based on the dependent variable and the independent variable is categorical (Cronk, 2006). The independent variable is the adoption of the AWP.

Discussion

The methodology being Ex –post- facto in design has a limitation in that it is examining events that have already taken place. Based on this fact, there is no ability to control the research parameters. The issues of internal validity and external validity were also addressed.

Internal validity can be described as the approximate truth with regard to cause-effect and casual relationship associated with the research (Champion, 2006). The primary concern was to observed changes in the number of crimes at the general aviation airports in the Commonwealth of Pennsylvania that can be attributed to the AOPA's AWP, and the role of the AWP or security personnel. Other possible causes or alternative explanations included a decrease in crime in the area of the airports due to changes in community demographics, and possible variations in the type of police forces near the airports.

External validity can be described as a generalization based on research and the study of a specialized area. The research of the general aviation airports in the Commonwealth of Pennsylvania and the results of the impact on crime with the adoption of the AWP can be generalized to state that the results in Pennsylvania is relevant to other comparable general aviation airports in other states. The sampling model can improve the external validity and the proximal similarity theory. This was accomplished because the sample represents the general aviation community (Champion, 2006).

In order to conduct the research of the general aviation airports that are operated independently of each other, no permission was required from any aggregate body. The research followed ethical guidelines in areas of protection from harm, informed consent, assurance of volunteerism, right to privacy, anonymity, confidentiality, and honesty with professional colleagues. An informed consent document was used, as required and approved by Capella University, as this research was part of my dissertation. Based on the nature of the research, there was no risk or potential for harm to the airport managers who

completed the surveys or to the general aviation airports. The completion of the surveys took place with the full knowledge and consent of the general aviation airport managers.

Regarding the issues of privacy, anonymity, and confidentiality, only I knew the identity of the airports that responded. The report of the results of the amount of crime against persons, property, or aircraft or the level of security that has or has not been adopted by the general aviation airports did not identify any of the individual general aviation airports that responded. The data that were collected during the research were not associated or identified with any specific airport that responded to the survey. The original copies of the survey are secured in a locked security container in my office, and protected by an intrusion detection system.

The survey was the main instrument that was be used for the research. The research survey is the most common method of measurement in criminal justice research (Champion, 2006). This method of research encompasses a measurement procedure that involves asking questions of the general aviation airports in the Commonwealth of Pennsylvania (the target group) in written form.

Results

This study showed there was a reduction in crimes against, people, property, and aircraft that it can be contributed to the AWP. Thus, hypothesis H1 is verified. Some of the possible variables such as the size of the police forces near the airports, police budgets, and precise accounting of changes in demographics and population were explored as to their impact on the crime rate at the airports.

Tables 1, 2 and 3, show that between 2002—the year before the AWP was introduced—and 2004—the year after the program was implemented—there was a reduction in crime at

the airports that adopted the program. There was also an increase in crime at the airports that did not adopt the program.

According to Table 1, crime against people at adopter airports went down from a total of 5 to 0, while the number of crimes against people went up at non-adopter airports from 3 to 6. The number of property crimes when down for adapter airports from 80 to 3, but went up at non-adapter airports from 45 to 88. Crime against aircraft at adopter airports similarly decreased (from 29 to 2), while it went up at non-adapter airports (from 4 to 13). The changes are summarized in figure 1.

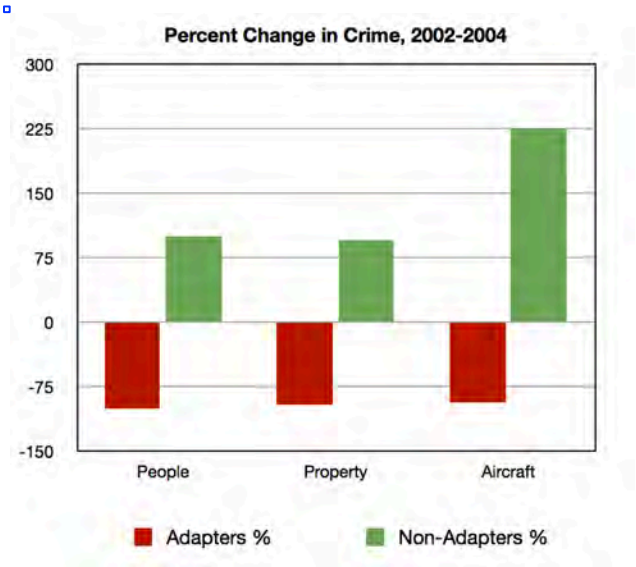


Figure 1 - Percent change in 3 types of crime at Pennsylvania general aviation airports for Adapters and Non-Adapters of the Airport Watch Program between 2002 and 2004.

This study confirms what previous research on various watch programs has shown. The utilization of a crime prevention program in a housing community, at a university, or even at a general aviation airport, has a positive impact in the reduction of crime.

While few incidents have been related to general aviation aircraft or airports, it does create a sense of fear in the mind of the public and airport security is of concern to the Department of Homeland Security Transportation Security Administration. Continued terrorist incidents involving general aviation aircraft could lead to new security mandates

for general aviation airports. One of goals of the AOPA's Airport Watch Program was to avoid such mandates (AOPA, 2003).

Table 1 - Chi-square values for crime against people, property, and aircraft for 2002 and 2004.

Year Crime Reported	**AOPA Adopters (37)**	**AOPA Non-Adopters (30)**	**Total**	x^2	**p**
Crimes Against People 2002	62.5% (5)	37.5% (3)	8	0.50	0.480
Crimes Against People 2004	0% (0)	100% (6)	6	-	-
Crimes Against Property 2002	64% (80)	36% (45)	125	9.80	0.002
Crimes Against Property 2004	3% (3)	97% (88)	91	79.40	0.001
Crimes Against Aircraft 2002	88% (29)	12% (4)	33	18.9	
Crimes Against Aircraft 2004	13% (2)	87% (13)	15	8.07	0.005

Table 2 - *ANOVAs for crimes against people, property, and aircraft for adapters vs. non-adapters of the AWP for 2002 and 2004.*

Variables	F	Sig.	Eta	Power	Adopters		Non-Adopters	
					M	SD	M	SD
People 2002	0.15 (0.14)	.702	.002	.067	0.14	0.42	0.10	0.31
People 2004	6.34 (0.11)	.014	.089	.698	0.00	0.00	0.20	0.48
Property 2002	3.62 (2.01)	.062	.053	.466	2.16	1.66	1.50	1.04
Property 2004	63.20 (2.13)	.001	.493	1.00	0.08	0.28	2.93	2.16
Aircraft 2002	9.96 (0.70)	.002	.133	.875	0.78	1.08	0.13	0.35
Aircraft 2004	13.76 (0.17)	.001	.175	.955	0.05	0.23	0.43	0.57

Table 3 - Analysis of Variance (ANOVAs) for crimes against people, property, and aircrafts by year (2002 vs. 2004)

Variables	F	Sig.	Eta	Power	2002		2004	
					M	SD	M	SD
People	0.33 (0.09)	.568	0.01	0.09	0.12	0.37	0.09	0.34
Property	2.94 (2.93)	.091	0.04	0.39	1.87	1.44	1.36	2.04
Aircraft	4.75 (0.51)	.033	0.07	0.56	0.49	0.89	0.22	0.45

Conclusions

The original hypothesis for this study was that the AOPA's Airport Watch Program (AWP) would have an impact on crime against people, property, and aircraft at general aviation airports in the Commonwealth of Pennsylvania. This hypothesis proved to be correct: general aviation airports in the Commonwealth of Pennsylvania that adopted the AWP experienced a reduction in crime against people, property and aircraft. In contrast, crime against people, property, and aircraft *increased* for airports that did not adopt the AWP

This work shows that crime prevention programs, specifically the Aircraft Owners and Pilots Association Airport Watch Program, can be a useful tool in general aviation security in the Commonwealth of Pennsylvania, and potentially across the United States. In light of the fears and concerns after 9/11, as well as the evolving homeland security initiatives to counter new aviation security threats, this work suggest that the AOPA's

Aviation Watch Program (AWP) is an effective tool for reducing crime and improving the security of the aviation infrastructure. It also allows the general aviation community to be proactive in aviation security by developing and implementing a volunteer security program.

Acknowledgements

The author is grateful to the Editor and anonymous reviewers for suggested improvements to the text. The Editor generated figure 1.

References

Aircraft Owners and Pilots Association (2003). *AOPA Airport Watch*. Frederick, MD: AOPA

Barkan, S. E. (2006). *Criminology: A social understanding* (3rd ed.). Upper Saddle River, NY: Pearson.

Bartol, C. R,. & Bartol, A. M. (2005). *Criminal behavior: A psychosocial approach* (7th ed.). Upper Saddle River, NJ: Pearson/Prentice Hall.

Bennett, T (1989). An assessment of the design, implementation, and effectiveness of neighborhood watch in London. *The Howard Journal of Criminal Justice*, 274(4), 241-256.

Beeler, K. J., Bellandes, S. D. & Wiggins, C. A. (1991) *Campus safety: A survey of administrative perceptions and strategies.* Washington, DC: National Association of Student Personal Administrators, Inc.

Bisignani, G. (2006). Airlines. [Electronic version]. *Foreign Policy*, 22-28.

Boetig, B. (2006.) The routine activity theory: A model for addressing specific crime issues. *The FBI Law Enforcement Bulletin*. June , 2006, 32-46.

Bohm, R.M., Reynolds, K.M. & Holmes, S.T. (2000). Perceptions of neighborhood problems and their solutions: Implications for community policing. *Policing: An International Journal of Police Strategies and Management,* 23(4), 439-465.

Brevard, R. (1995). Crime prevention at Tuffs University. Hartford, CT: International Association for Campus Law Enforcement Administrators.

Bullock, J. A., Haddow, G. D., Coppola, D., Ergin, E., Westerman, L. & Yeletaysi, S (2006). *Introduction to homeland security* (2nd ed.). Burlington, MA: Elsevier Butterworth-Heinemann.

Burling, P. (2003). *Acquaintance rape on campus*. Washington, DC: National Association of College and University Attorneys.

Carter, D. (2002). *The Police and the Community*, Upper Saddle River, NJ: Prentice Hall.

Champion, D. J. (2006) *Research methods for criminal justice and criminology*, (3rd Ed.). Upper saddle River, NY: Pearson/Prentice Hall.

Clarke, R.V. (1992) Situational crime prevention: Successful case studies. Albany, NY: Harrow and Heston.

Clarke, R.V., & Cornish, D.B. (1983). *Crime control in Britain: A review of policy and research*. Albany, NY: State University of New York Press.

Cohen, L.E. & Felson, M. (1979) Social change and crime rate trends: A routine activity approach. *American Sociological Review.* Volume 44 588-608.

Cohen, J. "Quantitative Methods in Psychology: A Power Primer." *Psychological Bulletin.* 112, no. 1 (1992): 155-159.

Commonwealth of Pennsylvania Bureau of Aviation (2007). *Regulations for general aviation airport operation*. Harrisburg, PA; Commonwealth of Pennsylvania.

Cornish, D.B., & Clarke, R.V. (1986). *The reasoning criminal*. New York, NY: Springer-Verlag.

Cronk, B. C. (2006). *How to use SPSS*. Glendale, CA: Pyrczak Publishing.

Culp, R. F., & Bracco, E. (2005). Examining Prison escapes and the Routine Activities Theory. *Corrections Compendium.* (2005, May-June) 1-5, 25-27.

Currran, D. J., & Renzetti, C. M. (2001). *Theories of crime* (2nd ed.). Boston, MA: Allyn and Bacon.

Criswell, J. W. (2003). *Research design qualitative, quantitative and mixed method approaches.* (2nd ed.).Thousand Oaks, CA: SAGE Publications.

Emerson, S. (2006). *Jihad incorporated.* Amherst, NY: Prometheus Books.

Farrington, D. P., & Welsh, B.C. (2007). *Saving Children form a life of Crime: Early Risk Factors and Early Intervention Studies on Crime and Public Policy*. New York, NY: Oxford Press

Fischer, R. J.& Green, G. (2004). *Introduction to security* (7th ed). Burlington, MA: Elsevier.

Groff, E. (2007). *Simulation for theory testing and experimentation: An example using routine activity theory and street robbery*. Journal of Quantitative Criminology Volume 23 (pp 75-103).

Hope, T (2005). The Anti-Social Bias and the Maryland Method Scientific Methods Scale*. European Journal on Criminal Police and Research*. (pp 275-296).

International Association of Campus Law Enforcement Administrators (2004). *University Crime Prevention Survey*. Hartford, CT: International Association of Campus Law Enforcement Administrators.

Jackson, A, Gilliland, K, & Veneziano, L. (2006). Routine activity theory and sexual deviance among male college students*. Journal of Family Violence*. (pp449-640).

Lindsay, B., & McGillis, D. (1986). Citywide community crime prevention: An assessment of the Seattle program. In D.P. Rosenbaum (Ed.), *Community crime prevention: Does it work? (*pp. 46-67. Beverly Hills, CA: Sage.

Meadows, R. J. (2007). *Understanding violence and victimization* (4th ed.). Upper Saddle River, NY: Pearson/Prentice Hall.

Martin, G. (2006). *Understanding terrorism: Challenges, perspectives and issues* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Mac Kenzie, D. L., & Hickman, L. J. (1998) *An Examination of the Effectiveness of the Type of Rehabilitation Programs Offered by Washington State Department o Corrections.* College Park, MD, University of Maryland.

Moore, K.C. (2000). *Airport, aircraft & airline security*. Burlington, MA: Elsevier

Butterworth-Heinemann.

Morgan, D. (2006). Femicide: *The impact of victim/offender relationships on crime.* New York, NY: University of New York Press.

Neuman, W.L.(2006). *Social Research Methods Qualitative and Quantitative Approaches.* New York, NY: Pearson.

Nyatepe-Coo, A. A., & Zeisler-Vralsted (2004). *Understanding terrorism: Threats in an uncertain world.* Upper Saddle River, NJ: Pearson/Prentice Hall.

Pizarro, J., Corsaro, N., & Violet, S. (2007). Journey to crime and victimization: An application of routine activity theory and environmental criminology to homicide. *Victims & Offenders* (pp. 374-394).

Pennsylvania Bureau of Aviation (2008). *Directory of Pennsylvania General Aviation Airports.* Harrisburg, PA: Commonwealth of Pennsylvania.

Savage, M. (2003). *The enemy within*. Nashville, TN: WND Books

San Miguel, C. (2005). An analysis of neighborhood watch programs in Texas Huntsviille, TX: Sam Huston state University.

Schmalleger, F. (2007). *Criminal justice today* (9th ed.). Upper Saddle River, NJ: Prentice Hall

Sherman, L.W., Farrington, D. P., Gottfredson, D. C., & Welsh, B. C. (2002). *Evidence-Based Crime Prevention*. New York, NY, Routledge

Simonse, C. E., & Spindlove, J. R. (2007). *Terrorism today: The past the players the future* (3rd ed.). Upper Saddle River, NJ: Pearson/Prentice Hall.

Smith, B.W., Novack, K.H., & Hurley, D.C. (1097) Neighborhood crime prevention: The influence of community-based crime prevention and neighborhood watch. *Journal of Crime and Justice, 20(20), 69-86.*

Sperry, P. (2005). *Infiltration: How muslin spies and subversives have penetrated Washington.* Nashville, TN: Nelson Current.

Straw, J. (2010). The Evolving Terrorist Threat. *Security Management*. 4-10, pp.46-49.

Swanson, C, Territo, L., & Taylor, R. (2005). *Police Administration,* Upper Saddle River, NJ: Prentice Hall.

Sweet, K.M., (2009). *Aviation and airport security*. Upper Saddle River, NJ: Pearson/Prentice Hall

Sperry, P. (2005). *Infiltration,* Nashville, TN: Nelson Current.

Turney, A. M., Bishop, J. C. & Fitzgerald, P. C. (2004). Measuring the importance of recent airport security interventions. [Electronic version]. *Journal of Air Transportation*, 9, 3.

Turvey, B. (2001).*Criminal Profiling an Introduction to Behavioral Evidence Analysis*, San Diego, CA: Elsevier Academic Press.

Vold, G. B., Bernard, T., & Snipes, J. B. (2002). *Theoretical criminology* (5th ed.). New York, NY: Oxford University Press.

Wiencek, D. (2005). Open skies? *The Journal of Counterterrorism and Homeland Security International* 11, 12-24.

Zhao, J., He., & Lovrich, N.P. (2003). Community policing: Did it change the basic function of policing in the 1990s? A national follow-up study. *Justice Quarterly*, 20(3), 697-724.

Journal of Physical Security 8(1), 111-116 (2015)

The Impact of the United States Coast Guard "America's Waterways Watch Program" on Crime at Pennsylvania Marinas

Daniel J. Benny, Ph.D., CPP, PCI, CFE, CCO, CASP, CIPM
Bachelor of Science in Aviation Security Program Chair
Embry Riddle Aeronautical University Worldwide

Abstract

This study examined the America's Waterway Watch Program (AWWP) to determine if it has been implemented at marinas throughout the Commonwealth of Pennsylvania in an attempt to prevent and reduce crime in the maritime community. The quantitative research using the Ex-Post-Facto design, meaning that the security procedures have or have not already been put in place at the time of the study, was conducted to establish if the AWWP when implemented at marinas had an impact on the crime rate. The study's sample included 33 marinas located in the Commonwealth of Pennsylvania. Data were collected by examining the uniformed crime reports in the location that the marinas were located during the period from 2010 to 2013. Data were also collected by visiting each marina to observe if the AWWP was being used

Introduction

This study is an attempt to determine if the United States Coast Guard's *America's Waterway Watch Program* (AWWP) has an effect on crime. The AWWP is a public outreach program encouraging participants to simply report suspicious activity to the Coast Guard and or other law enforcement agencies. Unlike some other neighborhood watch programs, there is no formal organization; there are no meetings, membership cards, or membership requirements. By participating in the program, citizens do not become agents of the Coast Guard or any other law enforcement agency.

The goal of the program is to seek the participation of all members of the maritime community such as towboat operators, recreational boaters, marina operators, and individuals who live, work, or engage in recreational activity around America's waterways. Participating in the AWWP is similar to participating in successful neighborhood residential watch programs (United States Coast Guard, 2014).

Individuals who spend time on or near the water already know what is normal and what is not. They are well suited to notice suspicious activities possibly indicative of threats to the United States homeland security. Participants in AWWP should theoretically adopt a heightened sense of awareness toward unusual events or individuals they may encounter in or around ports, docks, marinas, riversides, beaches, or waterfront communities (United States Coast Guard, 2014).

America's Waterways Watch Program Security Recommendations

The following security procedures recommended by the United States Coast Guard are keys to the success of the program. Boats should be secured and locked when not attended. AWWP decals should be prominently displayed on the window of boats, or at maritime facilities. Marinas and other waterfront businesses should display an AWWP poster, and

have informational brochures and decals readily available for customers who want to participate in the program. A key deterrent to terrorism is publicizing the fact that people are watching for suspicious activity.

The crimes that may occur at a marina could be crimes against persons, the marina facility, or watercraft located at the marina. Crimes against a person would include any crime that has an impact on the person who is at the marina. This includes crimes such as murder, rape, robbery, assault, stalking, kidnapping, and harassment. Crimes against marina property only affect the physical structures at the marina. Such crimes can include burglary, theft, arson, and vandalism. The crimes that could be perpetrated against the watercraft located at the marina would include theft of the watercraft, theft of marine avionics, vandalism, or even hijacking (United States Coast Guard, 2014).

Purpose of the Study

This work involved a review of the AWWP at marinas in the Commonwealth of Pennsylvania during the period from 2010 to 2013. The relationship between the program and the crime at the marinas was examined to determine effects of the AWWP crime at the marinas.

Research Question and Hypothesis

The research examined the following question:

Is there a difference in the number of crimes between marinas that have adopted the AWWP and those that have not?

The hypothesis and null hypothesis were the following:

H1: There is a difference in the number of crimes between marinas that adopted the AWWP and those that have not.

Ho1: There is no difference in the number of crimes between marinas that adopted the AWWP and those that have not.

Research Design

I used a quantitative statistical methodology to examine the intervention and the control groups. The intervention group consisted of those marinas that have adopted the watch program. The control group consisted of those marinas that did not adopt the AWWP.

The completed research examined two existing groups that have not been manipulated or changed during the study (Criswell, 2003). This is because the manipulation or change has already occurred at the marinas in the study.

Data were collected by examining the uniformed crime reports in the marina locations. I visited the marines studied to observe if they had implemented the AWWP or not. This Ex-post-facto design was selected because the security procedures have already been made (Criswell, 2003).

Data Analysis Procedures

Data was entered into SPSS 16.0 for Windows (Cronk, 2006). Descriptive statistical analyses were conducted on the demographic data. These were used to convert the raw data collected from the marinas to information more useful for directly determining the impact of the AWWP on crime. The dependent variable in the study was whether or not

there was a change in crime (against people, property, and watercraft) at the marinas that adopted the AWWP.

Findings and Conclusion

I found that between 2010 and 2013, there was a reduction in crime at the marinas that adopted the AWWP ("adopters"), and an increase in crime at the marinas that did not adopt the program ("non-adopters"). Crime against people at adopter marinas went down from a total of 5 to 0, and the number of crimes went up at non-adopter marinas from 3 to 6.

For adapter marinas, the number of crimes against property went down from 80 to 3, while the number of crimes went up at non-adopter marinas from a total of 45 to 88. Crimes against watercraft at adopter marinas went down from 29 to 2, while the number of watercraft crimes went up at non-adopter marinas from to 4 to 13.

This research shows that the AWWP can be a useful tool for maritime security in the Commonwealth of Pennsylvania, and potentially across the United States.

Acknowledgements

The author is grateful to the Editor and anonymous reviewers for suggested improvements to the text.

References

Cronk, B. C. (2006). *How to use SPSS*. Glendale, CA: Pyrczak Publishing.

Criswell, J. W. (2003). *Research design qualitative, quantitative and mixed method approaches.* (2nd ed.).Thousand Oaks, CA: SAGE Publications.

United States Department of Justice Uniformed Crime Report (2010, 2011,2012) Washington, DC: United States Government Printing Office.

United States Coast Guard (2014) America's Waterways Watch Program. Washington, DC: U.S. Government Printing Office.

.