The Journal of Physical Security

Volume 9(1), 2016

(ISSN 2157-8443)

IN THIS ISSUE...

Table of Contents

Journal of Physical Security, Volume 9(1), 2016

Editor's Comments

Welcome to volume 9, issue 1 of the *Journal of Physical Security* (JPS). In addition to my usual editor's rants and news about security that appear immediately below, this issue has papers about modeling the optimum number of security guards; mitigating workplace violence; the problem of missing vulnerability assessments; modeling, designing, and evaluating a physical security system for protecting radioactive material; and nuclear licensing and regulatory requirements in Egypt.

All papers are peer reviewed unless otherwise noted. We are very grateful indeed to the anonymous reviewers who contribute their time and expertise to advance our understanding of security without receiving recognition or compensation. This is the true sign of a professional!

Past issues of JPS are available at http://jps.rbsekurity.com, and you can also sign up there to be notified by email when a new issue becomes available.

JPS is hosted by Right Brain Sekurity (RBS) as a free public service. RBS (http://rbsekurity.com) is a small company devoted to physical security consulting, vulnerability assessments, and R&D.

As usual, the views expressed in these papers and the editor's comments are those of the author(s) and should not necessarily be ascribed to their home institution(s) or to Right Brain Sekurity.

*****

Welcome to Wal-Mart (Again)

Wal-Mart announced May 4th that the company will hire additional employees so that greeters will return to most stores. The greeters, often senior citizens, will welcome customers to the store as they come in the entrance. (At stores with security problems, "greeters" will also check receipts and provide other security functions.)

Wall-Mart greeters were introduced in 1983 by company founder Sam Walton after he had a pleasant experience being greeted by an older man in a store in Louisiana. Wal-Mart greeters have been used less frequently in recent years but this is scheduled to change.

Greeting customers at the entrance to retail stores is known to substantially reduce shoplifting. This is often called the "Wal-Mart Effect". It may work because customers feel they are being watched, and are thus less willing to risk being caught at shoplifting. It is also possible that being greeted warmly by a human being puts more of a human face on the company, making potential shoplifters feel guiltier about stealing.

It is entirely possible that the Wal-Mart Effect might work to reduce security risks from employees or visitors in any kind of business or facility, not just retail stores. Having a manager personally welcome people at the entrance might improve security and reduce the insider threat.

*****

Making Bystanders More Activist

The March 4, 2016 edition of the *Chronicle of Higher Education* had a thoughtful article (page B17) about the University of New Hampshire's campaign to prevent sexual assault. The program materials, which are available for purchase by other colleges and universities, "teaches people to safely intervene when a situation looks as if it could become dangerous, and it is aimed at increasing their willingness to do so." The program is based on research and evidence-based prevention. If, for example, a student observes that another student has become intoxicated at a party, the observer is encouraged to take concrete actions that might reduce the danger of sexual assault or other injury.

There is also an accompanying article (pages B14-B16) entitled, "Culture of Consent: Colleges Focus on Preventing Sex Assaults Before They Happen"; this is very much worth reading as well.

*****

Adam Bashes the Garden of Eden!

Check out the amusing, educational, and contrarian TV Series, "Adam Ruins Everything" at http://www.trutv.com/shows/adam-ruins-everything/videos/index.html. Adam takes on a lot of myths and misconceptions, many of them about security. For example, you can find video clips about how polygraphs are pseudo-scientific nonsense and why finger-printing is flawed, as well as discussions of the lack of security with credit cards and problems with the TSA.

*****

We Don't Need No Stinking Badges

Two reports in April by the Inspector General's Office of the General Services Administration (GSA) found serious problems and vulnerabilities with the use of government security badges (including the HSPD-12 badges) at numerous federal facilities. The reports can be found at:

https://www.gsaig.gov/sites/default/files/ipa-reports/OIG%20EVALUATION%20REPORT_Facility%20Specific%20Building%20Badges.pdf

https://www.gsaig.gov/sites/default/files/ipa-reports/OIG%20EVALUATION%20REPORT_GSA%20Management%20of%20Contractor%20HSPD-12%20PIV%20Cards.pdf

*****

Election Security

The April 26 issue of the *Financial Times* (page 4) includes an article by Hannah Kuchler about the security and privacy risks associated with voter apps. Candidates running for office in the United States often have smart phone apps so that their supporters can track news about them. The apps often send personally identifiable information (PII) unencrypted about the app user such as current location, political preferences, phone numbers, and the apps on their phone. This can be a serious security/privacy risk for the user, especially when they use public WiFi networks.

*****

Election Selfies

Snapchat has filed an amicus brief with the Federal appeals court hearing a case about New Hampshire's ban on taking photographs inside the voting booth. Snapshot would like voters to be able to record selfies of their voting. Traditionally, states ban photographing of voting because the photos could be used to prove how a citizen voted, theoretically making bribing of voters easier.

Snapchat argues that the freedom to document your voting is a First Amendment right. Moreover, there is evidence that photos might increase voter turnout. Facebook users who saw photos of their friends voting were more likely to go and vote themselves.

For more information, see http://www.dailydot.com/technology/snapchat-voting-booth-selfie-ban-court-filing/.

*****

Boring is Good

Creativity is important for having good security. Identifying security vulnerabilities requires thinking like the bad guys; devising improved security approaches often requires novel thinking.

Somewhat counter-intuitively, boredom turns out to be good for creativity. Researchers have shown that subjects who are given boring tasks, then immediately asked to do creative problem-solving are more creative than subjects not asked to perform the mundane tasks. See http://medicalxpress.com/news/2013-01-creative.html. Being bored

from time-to-time seems to be useful in permitting daydreaming that can help engender creativity.

Critical thinking is also important for good security, especially in making the difficult value judgments inherent in security and risk management. There is some kind of connection between creativity and critical thinking—what enhances one has a tendency to enhance the other. On the other hand, creativity and critical thinking have differences. For an excellent discussion of the issue, see an interesting paper by Matt Baked entitled, "Relationships Between Critical and Creative Thinking": http://pubs.aged.tamu.edu/conferences/SRAERC2001/pdf/e2.pdf.

*****

Agree or Disagree?

So you want to be a security guard? See http://advice.careerbuilder.com/posts/so-you-want-to-be-a-security-guard for a description of the job. I don't fully agree with everything in the description, and it is certainly incomplete, but it is nevertheless an interesting perspective.

There has been a shortage of serious studies of security guards (who sometimes prefer to be called "security officers") and the jobs that they do. This is particularly remarkable given the high turnover rate for guards (often 40-400% per year for contract guards) which has serious economic and security implications.

Here are a few studies of security guards and their work that I have been involved in that might be of interest:

EG Bitzer, PY Chen, and RG Johnston, "Security in Organizations: Expanding the Frontiers of Industrial-Organizational Psychology", *International Review of Industrial and Organizational Psychology* **24**, 131-150 (2009).

E Bitzer, "Strategies for Cutting Turnover", *Security* Management **50**(5**)**, 88-94 (2006).

EG Bitzer and RG Johnston, "A Taxonomy for Security Assignments", *Journal of Security Administration* **26**(2), 1-11 (2003/2006).

*****

NNSA Follies (Con't)

1. The National Nuclear Security Administration (NNSA) is about to issue its final requests for proposals to run Sandia National Laboratories in Albuquerque. NNSA, however, has been slow to release the 2015 evaluation of Sandia performance under

Lockheed Martin, the current operator, as well as report the 2015 fees to be awarded to Lockheed Martin for running Sandia. This is probably due to the controversy surrounding the 2014 report by the Department of Energy (DOE) Inspector General that concluded Sandia illegally used federal funds for lobbying, and improperly paid "consulting" fees to former U.S. Rep. Heather Wilson (R-NM). Lockheed Martin wants to continue to operate Sandia despite the wrongdoing.

2. The General Accounting Office (GAO) reported in May that the NNSA has not completed an Infrastructure Security Plan, as required by law: http://www.gao.gov/products/GAO-16-447R.

3. NNSA has decided not to fine Babcock & Wilcox Technical Services, the contractor that once ran the Y-12 nuclear facility, for 20-years of discarding sensitive and classified documents in regular trash. Y-12 has had multiple security problems, including a 2012 incident where an 82-year old nun and two other peace activists penetrated Y-12 security without a proper security response for an extended period of time.

4. The history of anti-nuclear activity and U.S. nuclear security problems is nicely summarized in a 2015 article in The New Yorker: http://www.newyorker.com/magazine/2015/03/09/break-in-at-y-12.

5. The Project on Government Oversight has an updated "Federal Contractor Misconduct Database" that includes fines related to operating the U.S. nuclear weapons complex from 1995 to the present. See http://www.pogo.org/blog/2015/12/nuclear-weapons-complex-misconduct-by-the-numbers.html. This is sobering reading.

*****

What a Flop

The U.S. Department of Defense still relies on 8-inch floppy disks for control systems that direct nuclear bombers and intercontinental ballistic missiles. For more information, see: https://www.washingtonpost.com/news/the-switch/wp/2016/05/26/the-real-reason-america-controls-its-nukes-with-ancient-floppy-disks/

*****

Homeland Security 1 - Is That a Gun in Your Pocket, or Are You Just Happy to Avoid Checked Bag Fees?

Last year, the Transportation Security Administration (TSA) seized 2,653 guns from airline passengers at airports—a 20% increase over 2014. More than 80% of the seized guns were loaded.

*****

Homeland Security 2 – Neutralizing 6 Year Old Terrorists

A 6-year-old first grade student in Ohio was suspended for pretending to be a Power Ranger and firing an imaginary bow and arrow during recess. The school has a zero tolerance policy for "any real, pretend, or imitated violence". See http://www.nydailynews.com/news/national/schoolboy-6-suspended-shooting-imaginary-bow-arrow-article-1.2424301.

*****

Homeland Security 3 – See Something, Say Something (Stupid)

A passenger on a flight from Philadelphia to Syracuse was responsible for creating a 2-hour delay after accusing a curly-haired fellow passenger of being a terrorist and writing in Arabic. The "suspect" was interrogated by officials and eventually allowed to re-board the plane.

Turns out the suspected terrorist was University of Pennsylvania economist Guido Menzio, an Italian with an accent, who was writing out mathematical equations while sitting in his seat and waiting for the plane to take off.

For details, see:
https://www.washingtonpost.com/news/rampage/wp/2016/05/07/ivy-league-economist-interrogated-for-doing-math-on-american-airlines-flight/.

*****

Highway Robbery

A Russian government official was arrested for masterminding a scheme to steal a 31-mile stretch of road. It was dismantled and sold in pieces over the course of a year. For details, see https://www.theguardian.com/world/2016/jan/13/russian-prison-official-accused-stealing-30-mile-road-alexander-protopopov.

*****

It Still Beats Any Adam Sandler Movie

Movie censors in the UK were required to watch a 10-hour film of white paint drying on a wall. The movie was made to protest England's movie rating laws. The censors rated the film "suitable for viewers age 4 and over". Apparently the movie is too racy for kids 0 to 3

years old. See http://qz.com/604112/heres-how-uk-film-censors-rated-a-10-hour-film-of-paint-drying/.

*****

Mechanical Doping

Pro cyclists now have a new way to cheat: using a small motor to power a bicycle's back wheel. For more information, see http://gizmodo.com/how-pro-cyclists-cheat-using-motorized-bikes-1756414521.

*****

Staying Hydrated

A man in Canada purchased a bottle of vodka from a liquor store. When he opened it at home, it discovered that the bottle was 100% water. He called the liquor store to report the tampering but was told, "it happens all the time".

*****

Bully Pulpit

The Anti-Defamation League (ADL) has identified warning signs or traits that may indicate that a child is a bully. These include the need to be in control, being easily frustrated or angered, a history of depression or anxiety, a lack of compassion or empathy, and having been the target of bullying himself or herself. The ADL also offers extensive advice for how to help such a child. See http://www.adl.org/assets/pdf/education-outreach/What-to-Do-if-Your-Child-Exhibits-Bullying-Behavior.pdf.

*****

Killing the $100 Bill

Former Treasury Secretary Lawrence Summers has called for the United States to phase out the $100 bill. The European Central Bank is similarly considering getting rid of the 500 Euro bill. High denomination bills are favored by criminals and terrorists because they take up less space than smaller denominations and attract less attention. For example, a standard briefcase can hold about $1 million of $100 bills, weighing around 27 pounds. If the same $1 million is in the form of $20 bills, however, it requires 5 briefcases and weighs 135 pounds.

For more information, see http://time.com/money/4226174/kill-100-dollar-bill-500-euro-phase-out/.

*****

Counterfeit Coins

Recent jumps in the prices of gold and silver have led to a substantial increase in the appearance of counterfeit bullion coins. The fakes are made of a combination of cheaper metals, and often have the wrong thickness and diameter in order to mimic the heavier weight of gold and silver. For more information, see http://universalcoinandbullion.dallasobserver.com/counterfeit-gold-silver-coin-fraud/.

*****

DNA: Do Not Always Believe

DNA is often considered the gold standard for criminal forensics and biometrics. In fact, DNA analysis has many serious problems—so much so that it often cannot be fully trusted. The June 2016 issue of *Playboy* magazine has an easy to understand article about this issue: https://www.playboy.com/articles/the-unraveling-of-dna-forensics.

*****

The Bedrock of Our Marriage

A Spanish company has developed a high-tech mattress that can tell if your partner is cheating on you while you are away. Sensors in the bed—part of a "Lover Detection System"—identify "suspicious" movements in the bed, and a warning notification is sent to your smart phone. For more information, see: http://www.telegraph.co.uk/news/2016/04/15/smart-mattress-lets-you-know-if-your-partner-is-cheating/.

*****

AI: Artificial Inanity

Microsoft Corporation recently unleashed a new AI chatbot on Twitter. The artificial intelligence program was meant to go forth and learn how to converse on Twitter in a more human manner.

After 24 hours of interacting with Twitter users, "...Tay 'learned' to be a genocidal racist, calling for the extermination of Jews and Mexicans, insulting women, and denying the existence of the Holocaust". Tay also called for the use of illegal drugs.

Microsoft apologized, quickly shut Tay down for a time, and deleted some of its more disturbing tweets. See http://www.nytimes.com/2016/03/25/technology/microsoft-created-a-twitter-bot-to-learn-from-users-it-quickly-became-a-racist-jerk.html?_r=0.

Seems to me that Tay learned what it is to be human just fine.

*****

Casey Jones, Jihadi Terrorist

Engineers of Jihad, a new book by Diego Gambetta and Steffen Hertog, examines the long-recognized fact that radical Islamists seeking power in Muslim-majority countries tend to be dominated by engineering or applied science students rather than graduates in law, the social sciences, or pure science. They found that engineers are over-represented among Islamist activists by a factor of 17 times their occurrence in the relevant society as a whole. Medical doctors are over-represented by a factor of 10.

The authors believe thwarted aspirations are the cause. The combination of high social status for engineers after many years of study, but low employment opportunities in many Muslim-majority countries contributes to their disgruntlement. This makes sense to me because disgruntlement by employees in corporations or the government (a major insider threat risk factor) is all about unmet expectations, not about objective reality.

The authors believe that engineering students tend to have a narrower, more rigidly defined worldview than students in the humanities or the pure sciences. Scientists and social scientists ask a lot of questions and seek out ambiguities, but engineers tend to focus on finding the "right answer". This may make engineers more susceptible to radical movements, and less likely to critically question them.

*****

Oh, Good! Your Boss is Consistently a Jerk!

New research is also supportive of the idea that disgruntlement isn't about how an employee is treated, but rather about how he/she is treated relative to expectations. A new study out of Michigan State University suggests that employees are less disgruntled when they have a boss who is consistently a jerk, compared to having a boss who is unpredictably a jerk. If you *expect* to be treated badly because your boss is always a jerk, you aren't necessarily disgruntled.

In thinking about the insider threat, security managers need to focus on the employees and contractors who have unmet expectations, not just on those who are consistently treated badly. Indeed, technical personnel and middle-level managers in many large

organizations—especially when their responsibility is not commensurate with their authority—tend to be disgruntled despite having good salaries and respected positions. The guys who work in the mailroom may be treated badly, but they are not necessarily disgruntled if they *expect* to be treated badly.

For more information on the study, see https://www.washingtonpost.com/news/on-leadership/wp/2016/03/02/the-worst-kind-of-boss-is-not-the-one-whos-always-a-jerk/.

*****

There's Still Room for Super Heroes

Antonio Cortes in Gloucester in the UK wrestled a mugger to the ground while dressed in a Superman costume, and held him there until police arrived. Cortes was taking a break at a local pub, after dressing up like the super hero as part of a local charity fundraiser, when he saw a woman at an ATM being accosted by the would-be mugger. Police were reportedly pleased and amused by "Superman's" assistance. See http://www.bbc.com/news/uk-england-gloucestershire-35422123.

*****

Don't Touch That Thing, You Don't Know Where It's Been!

Researchers at the University of Illinois report that nearly one-half of people who find an abandoned thumb drive in the parking lot will plug it into their computer and open the files to see who it belongs to (or just to be nosy). This, of course, can severely compromise computer and network security. Most of the people who undertook such dangerous actions were fairly computer literate.

Organizations should test their employees with periodic thumb drives in the parking lot as an educational exercise to alert employees to the risk.

The researchers propose another countermeasure as well: if the thumb drive was labeled, "If lost, please return to xxxxx" with an email address, people who discovered the "lost" thumb drive were much less likely to open any files.

For more information on the study, see http://www.news-gazette.com/news/local/2016-04-12/oh-hey-look-someone-dropped-usb-drive.html.

*****

Risky Business

An interesting article in the *Financial Times* by Oliver Ralph cites statistics from the consulting firm Ocean Tomo: 84% of the S&P 500's market value was held in intangible assets last year, versus 17% 40 years ago. Intangible assets include intellectual property, trade secrets, and organizational reputation/goodwill. Physical assets are no longer the major assets needing protection.

The article also maintains that most business insurance policyholders believe that the insurance industry is not offering enough coverage of business risk, nor offering sufficiently innovative insurance products.

See http://www.ft.com/cms/s/0/b480829e-297f-11e6-8b18-91555f2f4fde.html#axzz4BrQKYqex.

*****

You Smell Like a Dog

Field and Stream magazine has conducted a serious of informal experiments on masking human odors from wild game and dogs, including drug-sniffing dogs. The results are quite interesting. See:

http://www.fieldandstream.com/articles/2014/07/sniff-test-scent-control-products-and-practices-vs-a-drug-dog

http://www.fieldandstream.com/articles/2014/07/sniff-test-do-scent-control-measures-really-make-a-difference

http://www.fieldandstream.com/articles/hunting/2014/07/does-it-work-ozone-scent-control-vs-drug-sniffing-dog

http://www.fieldandstream.com/articles/hunting/2011/07/sniff-test

http://www.fieldandstream.com/articles/hunting/2015/10/can-scent-elimination-sprays-beat-the-nose-of-a-drug-sniffing-dog

*****

Everybody Must Get Stoned

A total of 4 states have legalized the recreational use of marijuana, and 24 states plus Washington D.C. now allow medical use. More states are expected to decriminalize marijuana at some point in the future.

Previous research has suggested that marijuana does not represent a major crash risk for motor vehicle drivers under its influence. A new study, however, reports that the rate of fatal crashes involving drivers who had recently used marijuana doubled after Washington

state legalized marijuana in 2012. Such drivers, however, also often had alcohol or other drugs in their blood as well, complicating the issue.

Part of the problem is that it is a difficult to determine when somebody is "too high" to drive safely. Unlike alcohol, THC, the active ingredient in marijuana, affects people quite differently. THC blood levels that significantly affect one person may have little effect on another. Moreover, regular users of marijuana can have high levels of THC in the blood for a long time after use, while levels may drop too quickly in occasional users to be detected by a blood test. Field "sobriety" tests that measure drivers' physiological and behavior factors may make more sense than blood tests for marijuana.

For more information, see a new study by the AAA Foundation for Traffic Safety: https://www.aaafoundation.org/impaired-driving-and-cannabis.

-- Roger Johnston
Oswego, Illinois
June, 2016

Journal of Physical Security 9(1), 1-22 (2016)

Probabilistic Estimates of Incident Response Times for Security Personnel

David Rogers, Christopher Briscoe, Ph.D., Jean Gobin, and Carl Young

Stroz Friedberg, LLC
32 Avenue of the Americas, 4th Floor
New York, NY 10013

ABSTRACT

We use a probabilistic model to determine the minimum number of security guards within a facility based on a maximum incident response time. We obtain a distribution of response times, where the speed of the guard and the population density of the space to be monitored are taken to be normally-distributed random variables. We present the analysis for cases where the space can be approximated by both one- and two-dimensional models. Our analysis finds the probability of achieving response times of T = 300 seconds for various guard densities (e.g., 1 guard per 200 meters, 1 guard per 500 meters, and 1 guard per 1000 meters) to be 99.95%, 81.61%, and 0.31% respectively. We identify the guard density required to achieve a response time of 60 seconds in 75% of one-dimensional scenarios to be approximately 1 guard per 106 meters. Additionally, this investigation analyzes the form of the response time distribution in two-dimensions and compares the calculated guard densities to those resulting from a simplistic extension of the one-dimensional solution. In both models, we present an exemplary cost-benefit analysis.

1 INTRODUCTION

Determining the required number of guards in a facility is a longstanding problem in security risk management. It has been observed that the cost of security personnel can comprise up to 85% of an organization's security budget [1]. To date, there have been few quantitative models that provide guidance in assessing the requirement for this costly yet important security resource. A critical function of security guards is to respond to incidents in a timely fashion, especially when a life-threatening situation is occurring. Further, this is also a responsibility in which staffing is often based on an inadequate number of drivers [2]. This is arguably the most important function of security guards, and is therefore the driving feature of the model used in this analysis.

This paper details an application of the "Probability of Protection" method [3]. In this method, we assume that the value of a factor affecting the vulnerability to a given threat is normally distributed since its *a priori* value is unknown. The limits on this distribution are based on scenario-specific conditions. We substitute this distribution into a physical security model for a key vulnerability parameter, which yields a distribution of values for that parameter. The minimum parameter value required to achieve effective mitigation can then be compared to the resulting distribution, which yields the probability that a given value will be effective based on the spectrum of possible vulnerability scenarios. Importantly, this method facilitates quantitative decisions on a particular security control implementation because it can be used to compare effectiveness and cost-effectiveness of specific defensive strategies.

In this analysis, we determine the distribution of times for guards to respond to an incident, accounting for uncertainties in both guard mobility and the density of obstacles in their path. We then compare this distribution against proposed response times a given organization may request, allowing an analytic determination of the appropriate number of guard personnel to ensure protection against an agreed percentage of possible scenarios. We further provide an indicative cost analysis as defined by these constraints and realistic

physical values. Our approach considers both one- and two-dimensional models of guard response times, applicable to a variety of real world scenarios.

2 Analytic Expression for Response Time

We first examine the case where a security guard is free to move in one dimension. This approximation is justified in scenarios where motion in the remaining two spatial dimensions is comparatively negligible (e.g., a corridor spanning one floor of a commercial building with its length much greater than its width, an airport security line). Starting from basic principles, we can determine a formula for the time it would take a security guard to reach an event, while incorporating some density of obstacles the guard may have to circumvent. In a given time *t* without any added delays, the distance *r* covered by a single guard is:

$$r = vt \tag{1}$$

where *v* is the guard's (average) velocity. If the area to be monitored contains a density λ of obstacles, each adding a fixed amount of distance α per obstacle to the path traveled by the guard, the distance traveled becomes:

$$\begin{aligned} r' &= vt + \alpha\lambda vt \\ &= vt(1 + \alpha\lambda) \end{aligned} \tag{2}$$

Note that the model includes obstacles that add distance to a guard's response path. Equation 1 demonstrates that distance is proportional to time, as parameterized by the guard velocity, *v*, so the added obstacles therefore increase a guard's response time. This results in a dilated time required for a guard to traverse a given distance:

$$t' = \frac{r'}{v} = t(1 + \alpha\lambda) \tag{3}$$

We use this to determine the reduced velocity:

$$v' = \frac{r}{t'} = \frac{vr}{r'} = \frac{v}{1 + \alpha\lambda} \tag{4}$$

The above relation (4) demonstrates a reduced velocity due to a number of obstacles preventing a guard from taking the shortest possible path to the scene. This allows the expression for the distance $\bar{r}$ that this single guard can cover to be written as:

$$\bar{r} = 2v't = \frac{2vt}{1 + \alpha\lambda} \tag{5}$$

The initial problem statement assumes that the guard is aware of the incident location prior to initiating their response. The multiplicative factor of 2 in equation 5 follows from a guard's knowledge of the incident location, and corresponds to their ability to follow a path within a one-dimensional space, or a line, in both the positive and negative directions to circumvent the obstacles described by the parameter α. In this example, the obstacles are represented by a population density and we assume that the increased distance a guard must travel around an individual is constant. More complex analysis might include different types of obstacles (e.g., columns, desks) and differing interference distances. As the distance per obstacle and/or density of obstacles are reduced, this expression correctly simplifies to the familiar one-dimensional Newtonian kinematic relation for distance traveled. As α and λ grow very large, the solution for the distance approaches the static case.

Equation 5 represents the distance covered by a single guard. Then for a given number of guards, G, the total distance they can maximally cover—assuming even spacing between the guards and no overlap in coverage area—is $G\bar{r}$. These assumptions are valid as we seek solutions that minimize the number of guards required to protect against a certain percentage of possible scenarios, or equivalently that each guard's coverage area is maximized. For a space defined by a length, L, we define the intrinsic guard density g of the space as:

$$g = \frac{G}{L} \tag{6}$$

Then the fraction, M, of the space the guards can cover is:

$$\begin{aligned} M &= \frac{G\bar{r}}{L} \\ &= \frac{G}{L} \cdot \frac{2vt}{1+\alpha\lambda} \\ &= \frac{2vtg}{1+\alpha\lambda} \end{aligned} \tag{7}$$

It should be noted that the guard density itself is not included in the hallway population density, and this analysis most accurately applies to the cases where the hallway density is significantly larger than the guard density (i.e., $\lambda \gg g$). In other words, this requires that guards are not interfering with each other's paths. If $\lambda = \lambda(g)$, manipulations of the statistical quantities associated with λ and outlined in section 3 are difficult to express in a closed form. Further, an analysis based on worst-case scenarios requires that the number of guards in a given space to be monitored to be less than the hallway population itself. We look to determine a solution for the case where any single guard is able to respond to an incident in any location within a certain time. Therefore, we require the entire area to be covered by security personnel, or $M = 1$. The response time in this worst-case scenario is then given by:

$$t = \frac{1+\alpha\lambda}{2vg} \tag{8}$$

where, recalling that the parameters g and α are fixed for a given scenario, we define two new quantities:

$$X = \frac{1+\alpha\lambda}{2g} \tag{9}$$

and

$$Y = \frac{1}{v} \tag{10}$$

Equation 8 can then be written as:

$$t = X \times Y \tag{11}$$

where the above substitution simplifies the expression for t into the product of two independent terms which each depend on a single random variable (λ and v). [Random variables are quantities whose possible values are subject to variation, taking on multiple different values each with an associated probability.] In the following sections, we determine a probability density for t, where the distributions for λ and v are known, and g (and possibly α) are adjustable parameters that impact the shape of the respective curve, and ultimately the cumulative density function.

3 Distribution of Response Times

Due to variability in both the population density of an area (λ) and the speed of the guards themselves (v), we assume that these quantities can be modeled as normally distributed random variables, i.e., symmetrically distributed about the mean with a width defined by the variance.

Mathematically, this means the possible values allowed for each random variable are defined by the following probability density functions:

$$f_\lambda(\lambda \mid \lambda_0, \sigma_\lambda^2) = \frac{1}{\sqrt{2\pi\sigma_\lambda^2}} e^{-\frac{(\lambda-\lambda_0)^2}{2\sigma_\lambda^2}}$$

$$f_v(v \mid v_0, \sigma_v^2) = \frac{1}{\sqrt{2\pi\sigma_v^2}} e^{-\frac{(v-v_0)^2}{2\sigma_v^2}} \tag{12}$$

We adopt a normal distribution of densities λ as it models the set of "worst-case" scenarios, where the obstacles' impact on a guard's responsiveness is greatest. That is, the density of obstacles during off-peak hours may not be accurately modeled by a normal distribution, but achieving an organization's desired "Probability of Protection" as calculated against these worst-case distributions will ensure protection against the entire set of possible scenarios. The distribution of velocities describes the range of average foot speeds that a guard may take on when responding. The variability in this quantity could account for uncertainties in both human reaction times, as well as in the (constant) distance added to the guard's path α. We use the cumulative distribution functions F_λ and

F_v (obtained via standard integration from each corresponding normal probability density function), along with equations 9 and 10 to obtain the cumulative distributions F_x and F_y:

$$F_x(X \leq x, g) = F_\lambda\left(\lambda \leq \frac{2gx-1}{\alpha}\right)$$
$$F_y(Y \leq y) = F_v\left(v \leq \frac{1}{y}\right) \tag{13}$$

The derived probability density functions f_x and f_y are found to be:

$$f_x(x, g) = \frac{2g}{\alpha} f_\lambda\left(\frac{2gx-1}{\alpha}\right)$$
$$f_y(y) = \frac{1}{y^2} f_v\left(\frac{1}{y}\right) \tag{14}$$

Then, due to the independence of *X* and *Y*, we express the cumulative distribution function for *t* as the product of two independent distributions, or:

$$F_t\Big(T \leq t, g\Big) = \int_0^\infty \int_0^{\frac{t}{x}} f_x(x, g) f_y(y)\ \mathrm{d}y\mathrm{d}x \tag{15}$$

The corresponding probability density function, which will describe the set of possible guard response times, is then:

$$f_t(t, g) = \int_0^\infty \frac{1}{x} f_x(x, g) f_y\left(\frac{t}{x}\right)\ \mathrm{d}x \tag{16}$$

We define the following constant quantities:

$$\mathcal{C}_1 = \frac{1}{2\sigma_\lambda^2}$$
$$\mathcal{C}_2 = \frac{1}{2\sigma_v^2} \tag{17}$$

Equations 17 are used to express the functions:

$$a = a(t,g) = \mathcal{C}_1 \cdot \left(\frac{2g}{\alpha}\right)^2 + \mathcal{C}_2 \cdot \left(\frac{1}{t^2}\right)$$
$$b = b(t,g) = \mathcal{C}_1 \cdot \left(\frac{4g(1+\alpha\lambda_0)}{\alpha^2}\right) + \mathcal{C}_2 \cdot \left(\frac{2v_0}{t}\right)$$
$$c = \mathcal{C}_1 \cdot \left(\frac{(1+\alpha\lambda_0)^2}{\alpha^2}\right) + \mathcal{C}_2 \cdot \left(v_0^2\right) \tag{18}$$

which then allow the solution of equation 16 to be written as:

$$f_t(t,g) = \frac{ge^{-c}}{2\sqrt{\pi}\alpha\sigma_v\sigma_\lambda} \cdot \frac{b}{a^{\frac{3}{2}}} \cdot \frac{e^{\frac{b^2}{4a}}}{t^2} \tag{19}$$

Equation 19 diverges as $t \to 0$, however, the contribution to the total probability at this point is somewhat minimized by small constants in the exponential (i.e., $\frac{b^2}{4a} - c = Cons., c \gg 0$) and further, the situation becomes unphysical (i.e., near instantaneous response times are limited by human reaction speed). The function is maximized at the expected value of $t = \frac{1+\alpha\lambda_0}{2v_0 g}$. In the neighborhood of this value, the distribution $f_t(t,g)$ can be estimated to be approximately Gaussian in form. As t grows larger, $f_t(t,g)$ exhibits behavior akin to that of an exponential decay. This demonstrates that, despite beginning with normally-distributed random variables for guard speed and obstacle density, the combined distribution $f_t(t,g)$ is not Gaussian, as more of the probability density is located further from the maximum value of t. This intuitively makes sense and comports with our hypothesized result (i.e., that a physically realizable response time on the order of minutes should be more likely than one on the order of seconds).

3.1 Calculating Probability of Protection

Figure 1 plots equation 19 for three distinct values of g, considering realistic parameters for population density, average guard speed, distance per obstacle, and uncertainty in density and speed. As each plot represents a normalized probability density of response times, integrating a given curve up to a desired response time T will provide the probability

of a guard reaching an incident within the period defined by T. We observed the behavior of equation 19 near the origin and found that the value of the distribution is seen to be small ($f_t(t, g) \to 0$) and remain nearly constant.

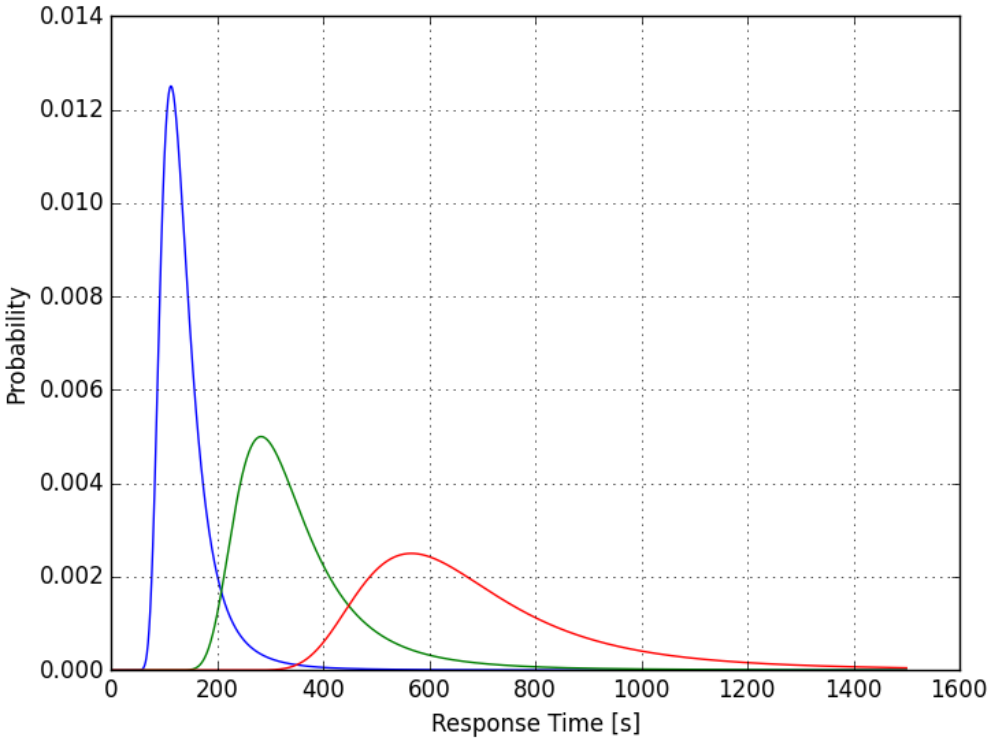

Figure 1: Distribution of response times (equation 19) for several values of the guard density g. From left to right, g = 5 × 10^{-3} (1 guard per 200 meters), 2 × 10^{-3} (1 guard per 500 meters), 1 × 10^{-3} (1 guard per 1000 meters). In all cases, the values of the associated constant parameters are as follows: $\alpha = 2.37\,[\mathrm{m}], \lambda_0 = 0.55\,\left[\frac{1}{m}\right], \sigma_\lambda = 0.05\,\left[\frac{1}{m}\right], v_0 = 2.39\,\left[\frac{m}{s}\right], \sigma_v = 0.5\,\left[\frac{m}{s}\right]$.

The values of g are also chosen to represent realistic estimates for the guard density as compared to λ (*N.B.* this method requires $\lambda \gg g$ to provide accurate results, here $\lambda \propto 100 \times g$). We choose T = 300 s (5 minutes) as one possible response time that an organization may set as a requirement or benchmark. Each curve is then integrated numerically from T'= *0* to T to provide the following Probabilities of Protection:

g $[\frac{1}{m}]$	Probability of Protection [%]
5×10^{-3}	99.93
2×10^{-3}	81.61
1×10^{-3}	0.3093

Table 1: Probability that a security guard will be able to respond to an incident in at least *T = 300* s for three values of the guard density *g*. In all cases, the values of the associated constant parameters are as follows: $\alpha = 2.37\ [\mathrm{m}], \lambda_0 = 0.55\ \left[\frac{1}{m}\right], \sigma_\lambda = 0.05\ \left[\frac{1}{m}\right], v_0 = 2.39\ \left[\frac{m}{s}\right], \sigma_v = 0.5\ \left[\frac{m}{s}\right]$.

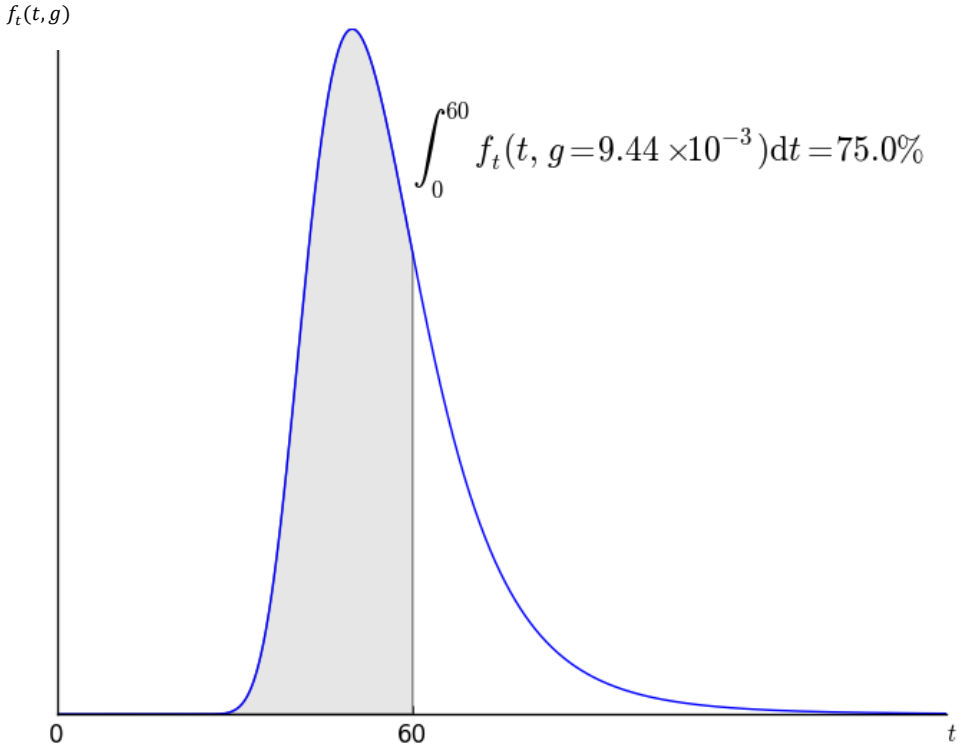

Figure 2: Area under curve $f_t(t, g)$, where as an example the desired response time is taken to be t = 60.0 s and the desired probability of protection is 75.0%. The value of g that satisfies these conditions is found to be 9.44×10^{-3} (about 1 guard per 106 meters). If the length of corridor to be monitored *L = 200* m, the number of guards required is G = $g \times L$ = 1.88. As above, the values of the associated constant parameters are: $\alpha = 2.37\ [\mathrm{m}], \lambda_0 = 0.55\ \left[\frac{1}{m}\right], \sigma_\lambda = 0.05\ \left[\frac{1}{m}\right], v_0 = 2.39\ \left[\frac{m}{s}\right], \sigma_v = 0.5\ \left[\frac{m}{s}\right]$

The total number of guards required to achieve the desired Probability of Protection is simply g multiplied by the length to be guarded. Different real world scenarios may require different response times and operate in environments where λ is significantly larger, or smaller, in certain (or all) circumstances. Equation 19 is well equipped to provide valuable metrics in guiding the correct number of guards to deploy in a given environment, assuming one-dimensional conditions, that is, where motion in a particular direction is relatively unbounded with respect to the other. Assuming 1-D conditions, however, is not always valid when operating in environments where movement is relatively unbounded in both the X and Y directions. A naive approach may be to simply square the values of the densities g and λ to arrive at an estimate of the distribution of response times in two-dimensions. In section 4, we show that a two-dimensional analysis is more appropriate than extending the one-dimensional result in order to accurately determine the Probability of Protection in certain scenarios.

4 The Two-Dimensional Case

Many circumstances exist where motion is not restricted from a 2-D perspective (e.g., stadiums, auditoriums, large lobbies), warranting an investigation of 2-D response time and guard density. Analogous to the 1-D case, we look to determine the "Probability of Protection" for desired response times based on geometric considerations and realistic parameters. We follow the same approach, namely we assume that the two-dimensional obstacle density ρ and average guard speed v are normally distributed random variables, or:

$$f_\rho(\rho \mid \rho_0, \sigma_\rho^2) = \frac{1}{\sqrt{2\pi\sigma_\rho^2}} e^{-\frac{(\rho-\rho_0)^2}{2\sigma_\rho^2}}$$

$$f_v(v \mid v_0, \sigma_v^2) = \frac{1}{\sqrt{2\pi\sigma_v^2}} e^{-\frac{(v-v_0)^2}{2\sigma_v^2}} \tag{20}$$

Here, ρ describes the density of obstacles in the space to be monitored in guards per meter squared (i.e., $\rho \propto \lambda^2$). Further, we assume that the obstacles described by ρ are distributed uniformly across the Cartesian plane, as shown in figure 3.

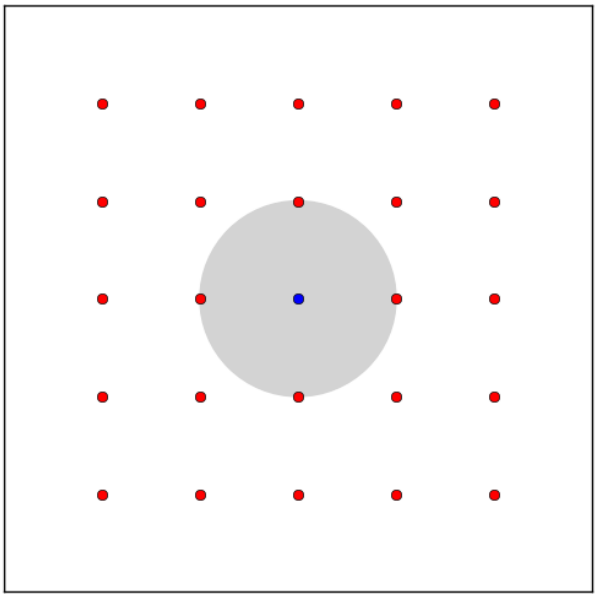

Figure 3: Obstacles (solid red dots) distributed uniformly across the two-dimensional Cartesian plane. The shaded region represents the area covered by a single guard (solid blue dot). The shaded region depicts the area accessible in a fixed time *T*.

The above demonstrates that the maximum area a guard could possibly cover in a fixed time is characterized by a circle centered at the guard's current location. Using equation 5 to now represent the radius of this circle, the area covered by a single guard in two-dimensions is given by:

$$\bar{A} = \pi \left(\frac{vt}{1 + \alpha\lambda} \right)^2 \tag{21}$$

For a space defined by an area *S*, the ratio of space the *G* guards can cover is:

$$N = \frac{G\bar{A}}{S} \tag{22}$$

where we again seek solutions where the entire space is covered by guard personnel (i.e., *N* = 1). We define the 2-D guard density as:

$$g_2 = \frac{G}{S} \tag{23}$$

Then the analytic expression for a guard's response time in two dimensions is:

$$t = \frac{1 + \alpha\lambda}{v(g_2\pi)^{\frac{1}{2}}} = X \times Y \tag{24}$$

Where

$$X = \frac{1 + \alpha\lambda}{(g_2\pi)^{\frac{1}{2}}} \tag{25}$$

and

$$Y = \frac{1}{v} \tag{26}$$

Note that, when expressed in polar coordinates, a uniform distribution of obstacle density, (i.e., $\rho(x, y) = \rho$), becomes a function of the angle θ, which parametrizes the route a guard chooses to move along to reach the scene of an incident. When responding, a guard will intuitively "pick out" the shortest route to the scene (i.e., they will seek the straightest path) which reduces the problem to one dimension. A notable difference between the one- and two-dimensional cases is in two-dimensions the path chosen determines a particular linear density of obstacles λ that add to the guard's path. Equivalently, for a two-dimensional space parameterized by a radius *R* and angle θ, $\lambda \neq \rho^{\frac{1}{2}}$ for all values of the angle θ. The two-dimensional problem is thus to determine the distribution of linear densities, given a Gaussian distribution of ρ. Due to the symmetries of the described configuration, we found the average value of λ(θ) over the range $0 < \theta < \frac{\pi}{4}$ by examining its value at the extrema.

$$\theta = 0 \rightarrow \lambda = \rho^{\frac{1}{2}}, \quad \theta = \frac{\pi}{4} \rightarrow \lambda = \frac{\rho^{\frac{1}{2}}}{\sqrt{2}} \tag{27}$$

This behavior is described by the function:

$$\lambda(\theta) = \rho^{\frac{1}{2}}\beta(\theta) = \rho^{\frac{1}{2}}\cos\theta \tag{28}$$

which has an expected value of:

$$\begin{aligned}\langle\lambda\rangle &= \rho^{\frac{1}{2}}\langle\beta\rangle \\ &= \sqrt{\frac{8\rho}{\pi^2}}\end{aligned} \tag{29}$$

This also yields an expression for ρ as a function of λ:

$$\rho = \left(\frac{\lambda}{\beta}\right)^2 \tag{30}$$

We found the probability density function for λ by first examining the cumulative distribution:

$$F_\rho(\rho^{\frac{1}{2}} < \frac{\lambda}{\beta}) = \int_0^{(\frac{\lambda}{\beta})^2} f_\rho(\rho)\mathrm{d}\rho \tag{31}$$

Since we assume $f_\rho(\rho)$ describes a normal probability density function, the function $f_\lambda(\lambda)$ follows as:

$$\begin{aligned}f_\lambda(\lambda) = \frac{\mathrm{d}F_\rho}{\mathrm{d}\lambda} &= \frac{\mathrm{d}F_\rho}{\mathrm{d}\rho}\frac{\mathrm{d}\rho}{\mathrm{d}\lambda} \\ &= f_\rho(\rho)\frac{\mathrm{d}\rho}{\mathrm{d}\lambda}\end{aligned} \tag{32}$$

From equation 30, we find the required derivative with respect to λ:

$$\frac{\mathrm{d}\rho}{\mathrm{d}\lambda} = \frac{2\lambda}{\beta^2} \tag{33}$$

then the distribution of the linear density λ is given by:

$$f_\lambda(\lambda) = \frac{2}{\sqrt{2\pi}\beta^2\sigma_\rho}\lambda e^{\left[-\frac{\left(\left(\frac{\lambda}{\beta}\right)^2-\rho_0\right)^2}{2\sigma_\rho^2}\right]} \tag{34}$$

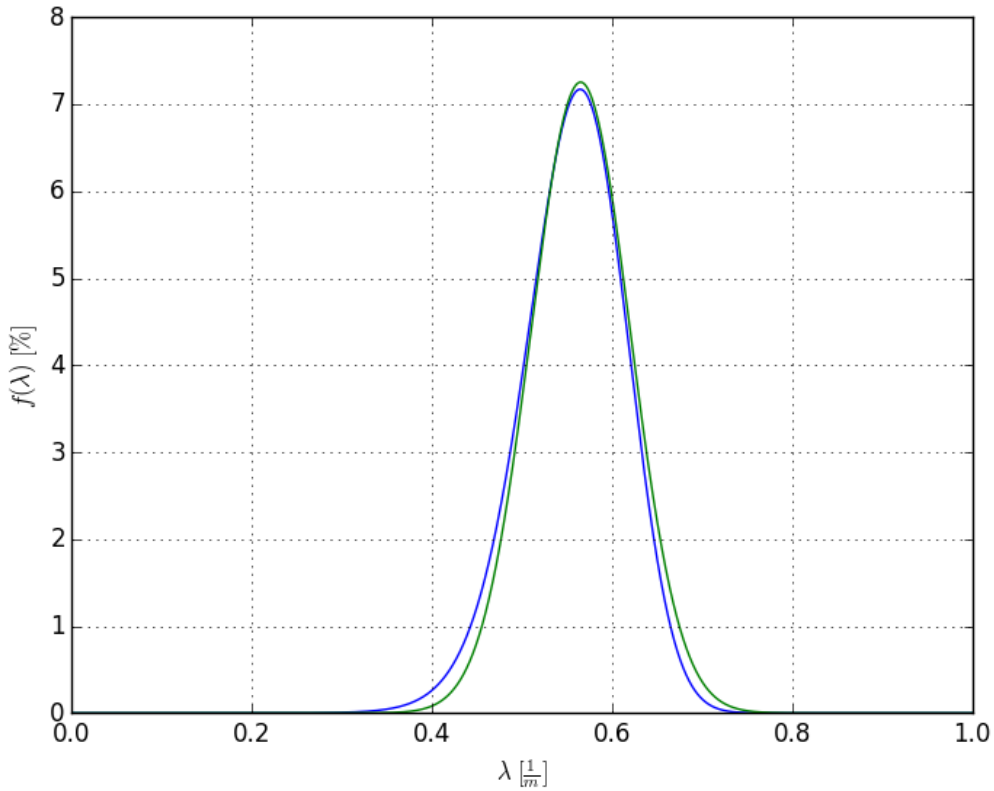

Figure 4: Distribution of linear obstacle densities (λ); the blue curve represents equation 34, the green curve shows the corresponding Gaussian distribution.

The above function can be used as input to an expression for the response time of a guard in two dimensions. We follow Laplace's method to estimate equation 34 as demonstrated in Figure 4 [4]. The expected value of the linear density λ_0 can be approximated (to first order) as:

$$\lambda_0 \approx \beta \rho_0^{\frac{1}{2}} \left[1 + \frac{1}{4} \left(\frac{\sigma_\rho}{\rho_0} \right)^2 \right] \tag{35}$$

Equation 35 imposes a restriction on the parameters that define the distribution $f(\rho)$, namely that the ratio $\frac{\sigma_\rho}{\rho_0} << 1$. This restriction assures that the distribution will not take on negative values for the velocity (an unphysical result) and will approach the expected value. Note that, in the limit where $\sigma_\rho \to 0$ the expression for λ_0 reduces to that which was derived analytically in equation 27. We arrive at an expression for the variance σ_λ as a function of σ_ρ from the coefficient of equation 34:

$$\frac{1}{\sigma_\lambda} \approx \frac{2\rho_0^{\frac{1}{2}}}{\beta\sigma_\rho}\left(1+\frac{1}{8}\left(\frac{\sigma_\rho}{\rho_0}\right)^2\right) \tag{36}$$

The coefficient of the argument of the exponential (34) also provides an expression for σ_λ, which when simplified reduces to:

$$\frac{1}{\sigma_\lambda} \approx \frac{2\rho_0^{\frac{1}{2}}}{\beta\sigma_\rho}\left(1+\frac{3}{8}\left(\frac{\sigma_\rho}{\rho_0}\right)^2\right) \tag{37}$$

This means that our calculated approximation of equation 32 is not perfectly Gaussian in form, but is offset by a fraction of the ratio $\frac{\sigma_\rho}{\rho_0}$. A comparison of these curves (and their associated integrals) demonstrates that the value of σ_λ derived from the coefficient (equation 37) most closely matches the behavior of equation 34. Then, we can take the one-dimensional density as a normally-distributed random variable with λ_0 equal to the average value found in equation 29, and σ_λ given by equation 37 above. Following the same method as outlined in section 3, we arrive at an expression for the distribution of response times in two dimensions. The distribution of a guard's response time in two dimensions is given by:

$$f_2(t,g_2) = \frac{g_2^{\frac{1}{2}}e^{-c_2}}{4\alpha\sigma_v\sigma_\lambda}\cdot\frac{b_2}{a_2^{\frac{3}{2}}}\frac{e^{\frac{b_2^2}{4a_2}}}{t^2} \tag{38}$$

with the coefficients expressed as functions of t and g_2 as:

$$\begin{aligned} a_2 = a_2(t,g_2) &= \mathcal{C}_1\cdot\frac{g_2\pi}{\alpha^2}+\mathcal{C}_2\cdot\left(\frac{1}{t^2}\right) \\ b_2 = b_2(t,g_2) &= \mathcal{C}_1\cdot\frac{2(g_2\pi)^{\frac{1}{2}}(1+\alpha\lambda_0)}{\alpha^2}+\mathcal{C}_2\cdot\left(\frac{2v_0}{t}\right) \\ c_2 &= \mathcal{C}_1\cdot\frac{(1+\alpha\lambda_0)^2}{\alpha^2}+\mathcal{C}_2\cdot v_0^2 \end{aligned} \tag{39}$$

Where in two dimensions the coefficients are defined as:

$$\mathcal{C}_1 = \frac{1}{2\sigma_\rho^2}$$

$$\mathcal{C}_2 = \frac{1}{2\sigma_v^2} \tag{40}$$

Comparing equation 38 with equation 19 and noting the preceding analysis demonstrates that the form of the solution is consistent in both one- and two- dimensions, with the differences comprised of the values of the various constants.

4.1 Calculating Probability of Protection

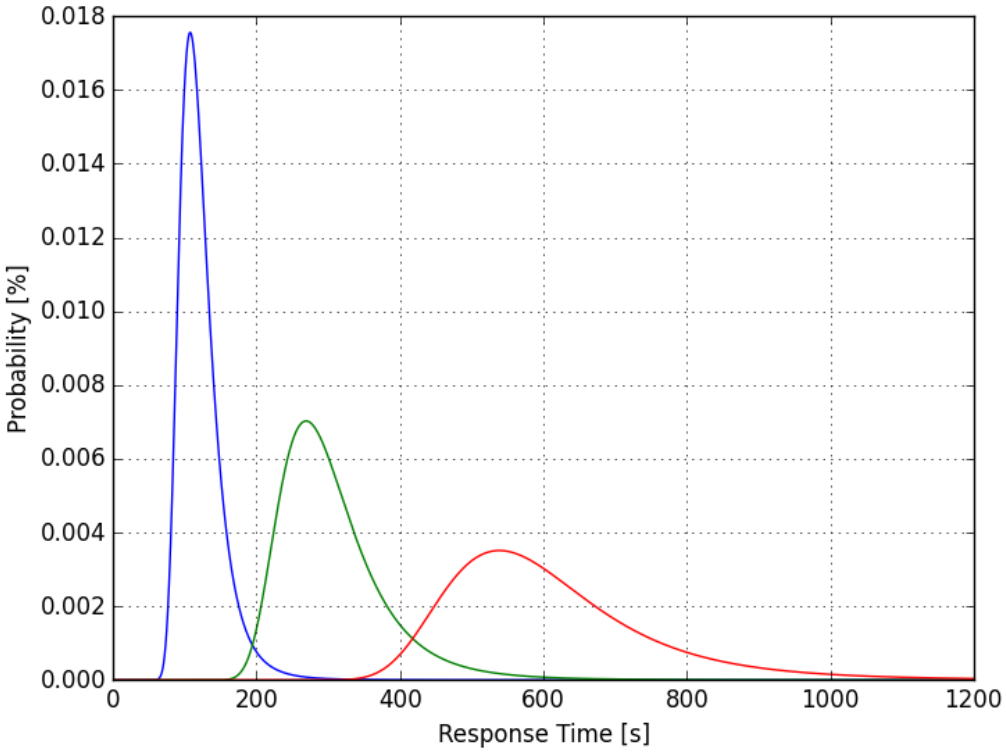

Figure 5: Distribution of response times in two dimensions (equation 38) for several values of the guard density. From left to right, g = 25 × 10^{-6} (1 guard per 40,000 sq. meters), 4 × 10^{-6} (1 guard per 250,000 sq. meters), 1 × 10^{-6} (1 guard per 1,000,000 sq. meters). In all cases, the values of the associated constant parameters are as follows: $\alpha = 2.37$ [m], $\lambda_0 = 0.618 \left[\frac{1}{m}\right]$, $\sigma_\lambda = 0.0299 \left[\frac{1}{m}\right]$, $v_0 = 2.39 \left[\frac{m}{s}\right]$, $\sigma_v = 0.5 \left[\frac{m}{s}\right]$.

Figure 5 plots equation 38 for three distinct values of g_2, which are the squares of values for g used in table 1. Calculations are performed to obtain the cumulative probability analogous to the processes undertaken in Section 3.1 and considering realistic two-dimensional parameters. Results are presented in table 2. The parameters describing the distribution of guard speed should not be adjusted, as motion remains one-dimensional in both cases.

g_2 $[\frac{1}{m^2}]$	Probability of Protection [%]
25×10^{-6}	99.8
4×10^{-6}	55.5
1×10^{-6}	0.000698

Table 2: Probability that a security guard will be able to respond to an incident in at least $T = 300$ s for three values of the guard density g_2. In all cases, the values of the associated constant parameters are as follows: $\alpha = 2.37$ [m], $\lambda_0 = 0.618 \left[\frac{1}{m}\right]$, $\sigma_\lambda = 0.0299 \left[\frac{1}{m}\right]$, $v_0 = 2.39 \left[\frac{m}{s}\right]$, $\sigma_v = 0.5 \left[\frac{m}{s}\right]$.

Comparison of the results presented in table 2 with those calculated in table 1 indicates that naively extending the results of section 3.1 into two-dimensions by "squaring the answers" results in dimensionally-correct solutions with significant differences in computed probability. The two-dimensional analysis suggests that a greater quantity of guards is required to meet a given protection requirement than the one-dimensional extension.

Starting from the guard density value derived in figure 2 and performing the naive extension into two dimensions suggests that $\rho_0 = \lambda_0^2$ over an area L^2 and therefore that $g_2 = g^2 = 8.91 \times10^{-5} [\frac{1}{sq.\ m}]$. In this case $\int_0^{60} f_2(g_2, t)dt = 44.7\%$, significantly lower than the 75.0% probability of protection determined with the corresponding values in the 1-D analysis. This therefore demonstrates the need to analyze the 2-D case separately. Alternatively, this demonstrates that the two dimensional model requires a different

quantity of guards (found by multiplying the calculated guard density by the area to be monitored) to achieve an organization's desired probability of protection. Extending to three dimensions, while mathematically possible, becomes unphysical as guards can no longer move continuously through space in any direction, and rather must use discontinuous methods such as stairs or elevators. It may be of interest to investigate this problem using Monte-Carlo techniques with random initial conditions and carefully calculated guard motion in response to an incident.

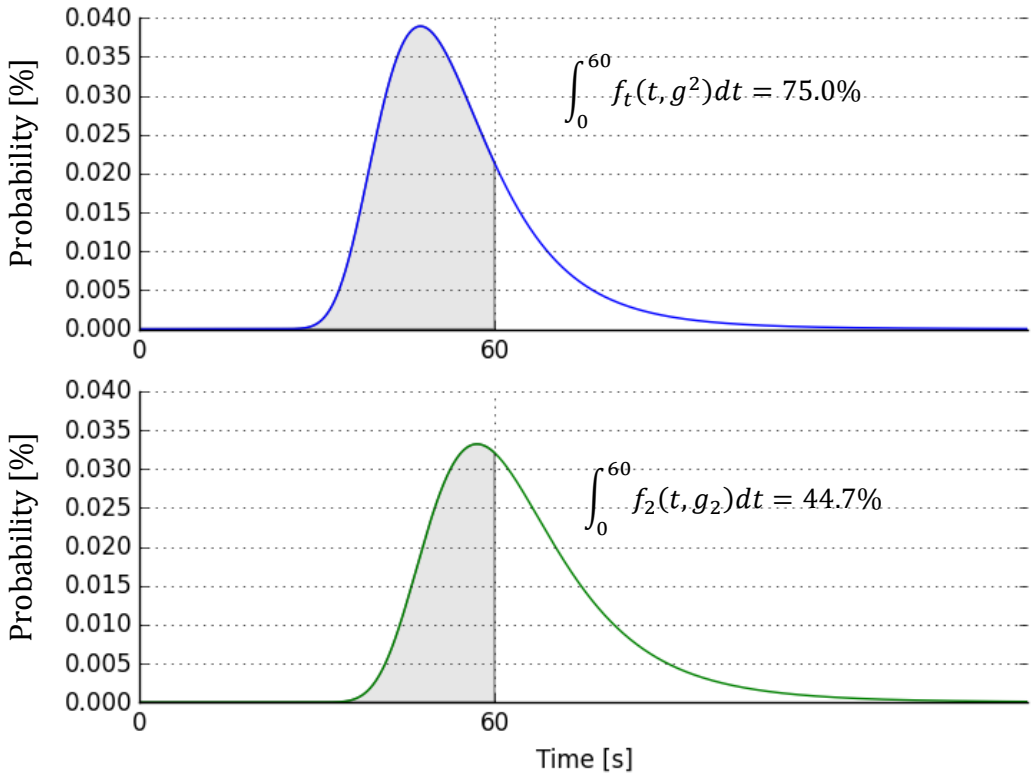

Figure 6: Comparison of two dimensional response time distribution (green) with one dimensional distribution (blue) where it is seen that the "Probability of Protection" (shaded area) is larger for the one-dimensional curve; here we take the uninformed approach where $\rho_0 = \lambda_0^2$, the guard density $g_2 = g^2$ where $g = 9.44$ $g = 9.44\times10^{-3}$ found in section 3.1 required to achieve a 75% "Probability of Protection". The ratio of the means linear density to its variance is preserved in extending to two dimensions.

5 Conclusions and Next Steps

In the world of physical security one of the most important controls, and at times the most expensive, are individuals hired to perform safety and security roles. The individuals

require salary, benefits, training, and other expenses to an institution, and cost-based decisions alone can often render these roles ineffective. For example, hiring security guards increases an organization's legal liability; the individuals have the potential to harm visitors intentionally or otherwise, and maintain an increased risk of personal injury (e.g., medical, firearms, etc.). The addition of security personnel also increases the risks associated with insider threats, as guards are often granted privileged, physical access to sensitive areas. This demonstrates that a quantitative analysis of the amount of guards required for a given location tells only a part of the story, and while the above results do not address every possible scenario where an institution may require a staff to deliver physical security services, they do address a common problem that rarely, if ever, is addressed by the application of quantitative metrics to help determine an appropriate number of guards in a given environment.

This paper provides metrics that may expand on existing cost-benefit analysis by focusing on the threshold for response time against the expenses incurred by the institution to achieve that threshold. As seen in the plots above, a successful guard density results in a probability of protection, as defined by the institution, that is weighed against the cost of hiring those guards, as defined by the market or vendor of guard services. The institution, if unable or unwilling to accept that cost, may either adjust the physical layout, compare prices with another vendor (if possible) or adjust their acceptable probability of protection if allowed. However, the decisions can now be made based on a deeper understanding of the control provided by the guards and not budget concerns alone.

Our one dimensional analysis shows the plots of $f_t(t, g)$ as continuous functions (figure 1). Despite this, we know that guards are of course not a fractional expense (e.g., one cannot hire 5.5 guards) and therefore must round the calculated number of guards required to meet a particular density requirement to integer values. This is demonstrated in figure 2, where the desired probability of protection is 75.0%, requiring $g = 9.44\times10^{-3}$ guards per meter. But determining the actual number of guards (by multiplying the calculated guard density by a length of corridor (e.g. L = 2000 m), requires 18.8 guards to achieve the protection requirement and must therefore round up to 19 guards to cover the

entire space. Employing 19 guards will effectively increase the functional probability of protection to 75.8%, above the organizational required 75.0% and over-covering the space (i.e. $g \rightarrow 9.50\times 10^{-3}$). However, rounding down to 18 guards will decrease the functional probability of protection to 68.3% and under-cover the space (i.e., $g \rightarrow 9.00\times 10^{-3}$).

Of course, the calculations in one and two dimensions presented above represent certain idealized variables and conditions. Population density may not fit a normal distribution at all times in a given environment, and the study may only apply to worst-case scenarios (e.g., rush-hour foot traffic in a busy office building). As the probability of protection calculation is designed to consider the cumulative distribution, successfully applying guards to the worst-case scenario implies success for all scenarios with a uniform population density at a given time. As the probability density of λ is not a function of position, this analysis does not account for any clustering of obstacles that may occur near, say, an elevator or turnstile. As suggested in examining the possible three-dimensional probability of protection, Monte-Carlo techniques may be helpful in examining scenarios where the population density is initially uniform in an environment with sources and sinks that allow $\lambda \rightarrow \lambda(x, y)$ and $g \rightarrow g(x, y)$. Other assumptions include a nearly constant distance per obstacle (α), which may only be reasonable if all obstacles are uniform (i.e., not a mixture of desks, columns, or other construction), and a normal distribution for guard velocity. While adding distance per obstacle as another random variable is an interesting study, it adds to the complexity of the analysis substantially. Considering guard velocity to be nearly constant and considering a normal distribution for the distance per obstacle is a more realistic follow-up to this study.

Other scenarios may benefit from an analogous study, such as the number of guards required to inspect individuals/packages arriving at a random rate. The generalized stochastic approach can also be repeated for other kinds of physical security problems commonly encountered by an organization's Chief Security Officer or equivalent, such as impact to windows [3], doors, bollards and other obstacles where the relative success of the protective control is measured by a threshold below (above) which is success and above (below) which is failure, that is, an application of cumulative probability. While the

approach is suitable to any statistically modeled physical problem looking to examine such conditions, complex analytical equations as compared to Equation 19 may result in more difficulty in achieving a probability density function without multiple numerical integration steps and/or less accurate estimation techniques. However, normal distributions are not a requirement of the approach, and others (e.g., exponential, gamma, power-law) may both be more physically reasonable for a given variable and easier to manipulate in the above framework even with a complex set-up equation.

References

[1] Broder, J. F., and Tucker, E., Risk Analysis and the Security Survey. 4th ed. Amsterdam: Butterworth-Heinemann (2012).

[2] Vellani, K.H., Emery, R.J., Parker, N., Staffing benchmarks: a model for determining how many security officers are enough, Journal of Healthcare Protection Management 28(2), (2012).

[3] Chang, D.B., and Young, C.S., Probabilistic Estimates of Vulnerability to Explosive Overpressures and Impulses, Journal of Physical Security 4(2), 10-29 (2010).

[4] Laplace, P. S. Memoir on the Probability of the Causes of Events. Statistical Science Statist. Sci., 1(3), 364-378. (1986).

Viewpoint Paper

Mitigating Workplace Violence

Bill Martin, PPS
Advanced Security Protection

People do not just suddenly snap; there is usually an emotional build-up or a stressor/ trigger that precipitates the outburst or violent incident.

Consider a once social employee who has previously enjoyed the lunchroom atmosphere and was known to be cordial and interactive with his co-workers. Recently he has started to withdraw and isolate himself. He has begun to talk about how he is really down on life. Does this recent behavior bring any concerns? Well maybe?

What else is going on with so and so; what else is happening?

The ability to distinguish the differences between everyday stress and someone who may be on a pathway to violence is sometimes very challenging and difficult. Threat assessment professionals tend to look for a cluster of red flags and concerning behaviors, but you do not have to be a security professional to know something is amiss.

Those who tend to nurse grudges and fantasize of revenge are known as "Injustice Collectors".

An employee who is just momentarily upset and angry may vent their frustration and give reason for concern; but those who keep score of all the wrongs that were done to them (real or imagined) and purposely pull away from their co-workers should send up some red flags. Suffering some type of traumatic loss such as love or status are igniters for an already volatile individual. Understanding the role of fantasy and the impact it has on the psyche of such an individual is a key to shaping our interventions and strategies.

The more you think about something, the closer you come to doing it.

If a person believes in something so strongly and intensely, it will begin to leak out

Fantasy exists before the action; you can see fantasy before the action through leakage.

Therefore understanding behavior through the concepts of leakage is a huge benefit and a proactive step in workplace violence prevention.

A co-worker who is talking about how they were wronged and that somebody is going to have to pay should send up a red flag. What if they are also sympathizing with those who have resorted to violence in past incidents and statements are heard like, "I can understand why they did what they did". Someone is going to have to make meaningful contact before the individual of concern decides to act out with violence. Sometimes there are internal or external restraints that prevent such an action from coming into fruition and fantasizing is at the continuum's end.

We must pay attention to the words, behaviors, and actions of our employees and co-workers. If they feel there is no one to help them with their concerns and sometimes grievances, then making a dramatic statement is not out of the equation. We cannot afford to ignore these warning signs and behaviors. Sometimes the help someone needs is just beyond the scope of our expertise. We must be willing to acknowledge our limitations and abilities and enlist the assistance of someone with the experience for handling such cases. Just take a volatile person, add some powerful stressors into the mix, and we may be sitting on a huge powder keg.

Key Mitigating Factors

1. Be Observant and Pay Attention

We have to train ourselves to observe behavior. What is this person's normal everyday behavior? Has there been a noticeable change? We all know that adversity and personal difficulties do exist, and the ability to handle stress and cope varies from person to person. The two most common stressors that impact men in particular are the loss of relationship and the loss of job or status. Suffering wrongdoing is something most people will experience during their lifetime. Most of us will choose a higher pathway and channel our energies into constructive alternatives. Some individuals, however, will nurse and fuel the fire of injustices until it reaches a boiling point; they will keep score of the wrongs they have endured until the moment they decide to lash out in anger and aggression.

2. Show Support, Care and Understanding

Listening and caring is probably the single most essential and important mitigating tool we have to prevent a workplace violent incident. I cannot begin to tell you how many stories could have been re-written if someone in upper management had taken the time to simply listen (not talk), but really listen and care. This simple supportive intervention is oftentimes overlooked and, sadly, not considered as a mitigating tool.

Sitting with a co-worker or employee and sincerely listening and caring can alleviate a lot of stress and pay great dividends for any organization. We must show that we care and are offering to help in any way we can. A management team that cares enough to listen to the needs and concerns of their employees is taking a prudent step in the right direction. We may not be able to solve all of their problems, but there is something to be said of a caring leadership team.

3. Establish Policies, Procedures and Protocols

Workplace prevention policies should be outlined and simplified. Procedures on handling and addressing violations in policy and those who appear to be exhibiting threatening and/or concerning behaviors should be simplified and outlined for the staff and employees. Employees must know where to go and who to report their concerns to and how to report their concerns. There must be a sense that things will be followed through and our management team really does care for our safety and security.

Protocols and training programs should be made available for all staff and employees on an ongoing basis. We should develop a leadership team who maintains accountability for staff training programs. There could be a structured team in place that handles threatening/concerning behaviors. Each organization could have its own threat management team which could be comprised of several disciplines experienced in handling the case load of threats and/or concerning behaviors. There is too much at stake to not take a proactive step in the right direction to ensure the safety and security of our workplaces.

The emphasis in this paper is about mitigating factors for workplace violence. The same mitigating factors, however, may well be useful in mitigating non-violent retaliation or sabotage by disgruntled employees, former employees, or contractors.

About the Author

Bill Martin is from the greater New York City Area and is an expert in threat management, executive protection, and behavioral analysis. He is a trainer and expert in security for houses of worship. He can be reached at Twitter @bmartin683.

Viewpoint Paper

Avoiding Shock and Awe*

Roger G. Johnston, Ph.D., CPP
Right Brain Sekurity
http://rbsekurity.com

I find two recent security incidents to be particularly disturbing because they highlight the frequent lack of vulnerability assessments (VAs), or even a mindset that allows for the contemplation of security vulnerabilities. This almost always leads to serious security failures.

The first incident involves allegations of Russian tampering with urine samples used for testing athletes for banned performance-enhancing drugs. The *New York Times* reported that there has been extensive state-sponsored doping of Russian international athletes, hidden via tampering with urine testing samples.[1] The tampering was reportedly implemented by tampering with so-called "tamper-proof" urine sample bottles. In a follow-up story on the front page of the New York Times[2], Don Catlin, the former head of the UCLA Olympic Analytical Laboratory is quoted as saying, "I tried to break into those [urine sample] bottles years ago and couldn't do it. *It's shocking*." [Italics added for emphasis.]

In the same story, Catlin further states that when the manufacturer first showcased the urine sample bottles used for athlete drug testing to a roomful of doctors, "All of us were particularly pleased and excited by this bottle because it *looked* pretty bulletproof." The manufacturer is quoted as saying about the allegations of Russian spoofing of the "tamper-proof" sample bottles that, "We're all a bit speechless, to be honest...*No one can believe it*." [Italics added for emphasis.]

Shocked? No one can believe it? Really?!? The fact is that reliable tamper-detection is a largely unsolved problem.[3,4] Moreover, 7 years ago, my colleagues and I demonstrated that 23 widely-used urine collection kits could be easily tampered with using only low-tech methods.[3] (Unfortunately, we did not evaluate the Berlinger bottle that is at the center of the current accusations of Russian tampering.) We also found that the drug testing protocols typically used, including for international athletes, have serious security problems.[3]

The shock and disbelief at the idea that the so-called "tamper-proof" bottles can be defeated is very consistent with a number of general security maxims. In particular:

---

* This Viewpoint paper was not peer reviewed.

Backwards Maxim: Most people will assume everything is secure until provided strong evidence to the contrary—exactly backwards from a reasonable approach.

Narcissist Maxim: Security managers, bureaucrats, manufacturers, vendors, and end-users will automatically assume that, if they cannot readily conceive of a way to defeat a security product (or a security program), then nobody else can. Remarkably, this will be true even for people with little or no experience, resources, or aptitude for defeating security, and even if they are spectacularly unimaginative.

Mermaid Maxim: The most common excuse for not fixing security vulnerabilities is the belief that they simply can't exist. Comment: Often, the evidence offered that no security vulnerabilities exist is that the security manager who expresses this view can't personally imagine how to defeat the security.

You Could've Knocked Me Over with a Feather Maxim 1: Security managers, bureaucrats, manufacturers, vendors, and end users will always be amazed at how easily their security products or programs can be defeated.

[Unfortunately, in my experience as a vulnerability assessor, the following associated maxim equally proves to be true:
You Could've Knocked Me Over with a Feather Maxim 2: Having been amazed once, security managers, bureaucrats, manufacturers, vendors, and end users will be equally amazed the next time around.]

And finally:
Tamper-Proof Maxim: Any claim by a salesperson about the performance of a physical security product (including the claim of absolute security) will be believed by default by the customer, while warnings about vulnerabilities or limitations by vulnerability assessors or others with first-hand experience will be met with incredulity. Comment: A classic example of this can be found in the all-to-common seal customers who maintain that their seals cannot not be spoofed because the manufacturer calls them "tamper-proof".

(My complete set of Security Maxims can found in the Appendix of this paper.)

The second recent, highly disturbing "security" incident that suggests the absence of effective VAs was the horrific killing of a 2-year old child by an alligator at a Walt Disney resort in Orlando, Florida. Now alligators might be more conventionally considered a safety issue rather than a security issue, but security is fundamentally about trying to counter malicious actions by a nefarious adversary. Alligators would seem to fall into that category, in contrast to other forces of nature such as hurricanes, tornados, and earthquakes—usually thought of as safety threats—that do not.

Risk Management has to include not just an understanding of the threats, but also an understanding of the vulnerabilities. In the case of the Orlando incident, the alligator

threat must certainly have been hard to overlook, even before the attack. According to the Associated Press, Florida has about 1 million alligators and officials receive 16,000 complaints about alligators each year. Last year, more than 7,500 nuisance alligators were relocated. Since 1973, 23 people have been killed by wild alligators.

Shortly after the attack, 5 alligators were removed from the lake where the attack took place, though none of them were involved in the incident.

The Walt Disney resort reportedly had no fences and no signs warning visitors about the alligators and how to behave safely around them. This is surely a serious vulnerability. Orlando is visited by large numbers of children and adults from all 50 states and many different countries where people may not be familiar with alligators and the risk they represent.

Hindsight is always 20-20 after a security incident, but it seems likely that even a rudimentary vulnerability assessment prior to the attack would have easily identified the lack of warning signs as a serious problem.

There are a number of reasons why people and organizations may overlook vulnerabilities and effective vulnerability assessments (VAs). Sometimes, threats are confused with vulnerabilities.[5] Often, various activities get confused with VAs. Examples include threat assessments, security surveys, compliance auditing, fault or event tree analysis, Design Basis Threat, the CARVER Method, penetration testing, performance or reliability testing, and "Red Teaming".[6,7] While these things can certainly be useful, they are not vulnerability assessments, and they are usually not very effective at finding security vulnerabilities. Another problem may be that, for many organizations, threats are much easier and more comfortable to contemplate and deal with than vulnerabilities.[6,7]

Many organizations have these kinds of problems. In my view, however, the most troubling examples of such organizations are the National Nuclear Security Administration (NNSA) and the International Atomic Energy Agency (IAEA). Both of these organizations are responsible for nuclear security and safeguards, and both are at significant risk for serious security incidents largely because of a fundamental failure to accept that vulnerabilities exist, and to properly address them. I believe they also suffer from many of the other security problems covered in the Security Maxims given in the Appendix.

So what exactly is a good vulnerability assessment? It is a holistic, creative exercise in thinking like the bad guys. It involves discovering and perhaps demonstrating vulnerabilities (weaknesses in the security) that might be exploited by the bad guys. It often also includes suggesting possible countermeasures to mitigate the vulnerabilities.

An effective VA is not constrained by wishful thinking, conflicts of interest, departmental politics, bureaucracy, lack of imagination, "shooting the messenger", political correctness, cognitive dissonance, phony constraints, excessive formalism, or arbitrary boundaries between disciplines or hardware/software modules. It does not ignore the insider threat, focus only on frontal force-on-force attacks by outsiders, or consider only previous attacks.

It recognizes that all security is local, and that compliance and security are not the same thing. And it avoids confusing vulnerabilities with threats or with features of the security or the facility in question.

The purpose of a VA is to realistically improve your security. A VA is not a test you "pass" or a way of reassuring yourself everything is fine. It is not a software program you run, a model you "crank", an audit you conduct, or an exercise in finding "gaps" (though these things may be helpful).

The ideal outcome of a VA is not finding zero vulnerabilities—indicating the VA is worthless—but rather findings lots of vulnerabilities, which are always present in large numbers. This is true even after a good VA is completed and new countermeasures have been implemented.

A VA must be undertaken by imaginative, resourceful, independent people who genuinely want to find problems and suggest solutions. There must be no risk of retaliation for what they find and recommend. An effective VA is not undertaken by safety experts using safety models (though having the vulnerability assessors confer with safety people is a good idea). It is not a one-time thing, but rather an exercise that is done early, iteratively, and often.

References

1. RR Ruiz and M Schwirtz, "Russian Insider Says State-Run Doping Fueled Olympic Gold", May 12, 2016, http://www.nytimes.com/2016/05/13/sports/russia-doping-sochi-olympics-2014.html?_r=0.

2. RR Ruiz, "Mystery in Sochi Doping Case Lies with Tamper-Proof Bottle", May 13, 2016, http://www.nytimes.com/2016/05/14/sports/russia-doping-bottles-olympics-2014.html?_r=0.

3. RG Johnston and JS Warner, "How to Choose and Use Seals", *Army Sustainment* ***44****(4), 54-58 (2012),* http://www.almc.army.mil/alog/issues/JulAug12/browse.html

4. RG Johnston, "Tamper-Indicating Seals", *American Scientist* **94**(6), 515-523 (2005), http://www.americanscientist.org/issues/feature/2006/6/tamper-indicating-seals.

5. RG Johnston, EC Michaud, and JS Warner, "The Security of Urine Drug Testing", *Journal of Drug Issues*, **39**(4) 1015-1028 (2009), http://jod.sagepub.com/content/39/4/1015.full.pdf+html.

6. RG Johnston, "Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities", *Journal of Physical Security* **4**(2), 30-34 2010.

7. RG Johnston, "Focusing on the Threats to the Detriment of the Vulnerabilities: A Vulnerability Assessor's Perspective", Chapter 14, S Apikyan and D Diamond (Editors), *Nuclear Terrorism and National Preparedness*, NATO Science for Peace and Security Series B, Springer (2015).

Appendix: Security Maxims

While these security maxims are not theorems or absolute truths, they are in my experience essentially valid 80-90% of the time in physical security and nuclear safeguards. They probably also have considerable applicability to cyber security.

Note that some of these maxims are obviously hyperbole and/or tongue-in-cheek, but that does not necessarily make them untrue. You ignore these maxims at your own (and others') peril, especially the ones in red!

Arrogance Maxim: The ease of defeating a security device or system is proportional to how confident/arrogant the designer, manufacturer, or user is about it, and to how often they use words like "impossible" or "tamper-proof".

Warner's (Chinese Proverb) Maxim: There is only one beautiful baby in the world, and every mother has it. Comment: Everybody's security or security product is beautiful (to them).

Be Afraid, Be Very Afraid Maxim: If you're not running scared, you have bad security or a bad security product. Comment: Fear is a good vaccine against both arrogance and ignorance.

So We're In Agreement Maxim: If you're happy with your security, so are the bad guys.

Ignorance is Bliss Maxim: The confidence that people have in security is inversely proportional to how much they know about it. Comment: Security looks easy if you've never taken the time to think carefully about it.

Infinity Maxim: There are an unlimited number of security vulnerabilities for a given security device, system, or program, most of which will never be discovered (by the good guys or bad guys). Comment: We think this is true because we always find new vulnerabilities when we look at the same security device, system, or program a second or third time, and because we always find vulnerabilities that others miss, and vice versa.

Thanks for Nothin' Maxim: A vulnerability assessment that finds no vulnerabilities or only a few is worthless and wrong.

Weakest Link Maxim: The efficacy of security is determined more by what is done wrong than by what is done right. Comment: Because the bad guys typically attack deliberately and intelligently, not randomly.

Safety Maxim: Applying the methods of safety to security doesn't work well, but the reverse may have some merit. Comment: Safety is typically analyzed as a stochastic or fault tree kind of problem, whereas the bad guys typically attack deliberately and

intelligently, not randomly. For a discussion about using security methods to improve safety, see RG Johnston, *Journal of Safety Research* **35**, 245-248 (2004).

High-Tech Maxim: The amount of careful thinking that has gone into a given security device, system, or program is inversely proportional to the amount of high-technology it uses. Comment: In security, high-technology is often taken as a license to stop thinking critically.

Doctor Who Maxim: "The more sophisticated the technology, the more vulnerable it is to primitive attack. People often overlook the obvious." Comment: This quote is from Tom Baker as Doctor Who in *The Pirate Planet* (1978).

Low-Tech Maxim: Low-tech attacks work (even against high-tech devices and systems). Comment: So don't get too worked up about high-tech attacks.

Schneier's Maxim #1 (Don't Wet Your Pants Maxim): The more excited people are about a given security technology, the less they understand (1) that technology and (2) their own security problems. Comment: From security guru Bruce Schneier.

What a Deal Maxim: The introduction of high-tech security products into your security program will: (1) probably not improve your security, (2) almost certainly increase your overall security costs (though perhaps it will decrease inventory, shipping, or other business costs), and (3) probably increase security labor costs (with the sometimes exception of CCTV).

Too Good Maxim: If a given security product, technology, vendor, or techniques sounds too good to be true, it is. And it probably sucks big time.

You Must Be High Maxim 1: Any security product that is labeled "high security" isn't.

You Must Be High Maxim 2: "High Security" is a context- and application-dependent value judgment, not a product attribute.

That's Extra Maxim: Any given security product is unlikely to have significant security built in, and will thus be relatively easy to defeat.

I Just Work Here Maxim: No salesperson, engineer, or executive of a company that sells or designs security products or services is prepared to answer a significant question about vulnerabilities, and few potential customers will ever ask them one.

Bob Knows a Guy Maxim: Most security products and services will be chosen by the end-user based on purchase price plus hype, rumor, innuendo, hearsay, and gossip.

He Just Seems So Knowledgeable Maxim: Most organizations get the majority of their physical security advice from salespeople (who somehow seem to recommend their own products).

Tamper-Proof Maxim: Any claim by a salesperson about the performance of a physical security product (including the claim of absolute security) will be believed by default by the customer, while warnings about vulnerabilities or limitations by vulnerability assessors or others with first-hand experience will be met with incredulity. Comment: A classic example of this can be found in the all-to-common seal customers who maintain that their seals cannot not be spoofed because the manufacturer calls them "tamper-proof".

Magic Light Inside the Refrigerator Maxim: Deploying a simple mechanical tamper switch or light sensor to detect tampering with a device or container is approximately the same thing as having no tamper detection at all.

Key Maxim (Tobias's Maxim #1): The key does not unlock the lock. Comment: From Marc Weber Tobias. The point is that the key activates a mechanism that unlocks the lock. The bad guys can go directly to that central unlocking mechanism to attack the lock (or do other things) and entirely bypass the key or pins. This maxim is related to the "I am Spartacus Maxim" below and to a corollary (also from Marc Weber Tobias) that "electrons don't open doors, mechanical mechanisms do".

Tobias's Maxim #2: Things are rarely what they appear to be. Comment: From Marc Weber Tobias. Or as Yogi Berra said, "Nothing is like it seems, but everything is exactly like it is."

There's The Opening Maxim (Tobias's Maxim #3): Any opening in a security product creates a vulnerability. Comment: From Marc Weber Tobias.

Tobias's Maxim #4: You must carefully examine both critical and non-critical components to understand security. Comment: From Marc Weber Tobias.

Contrived Duelism/Dualism Maxim: The promoters of any security product meant to deal with any sufficiently challenging security problem will invoke a logical fallacy (called "Contrived Dualism") where only 2 alternatives are presented and we are pressured into making a choice, even though there are actually other possibilities. Comment: For example: "We found a convicted felon, gave him a crowbar, and he couldn't make the lock open after whaling on it for 10 minutes. Therefore, the lock is secure." Another example, "Nobody in the company that manufacturers this product can figure out how to defeat it, and I bet you, Mr./Ms. Potential Customer [never having seen this product before in your life] can't think up a viable attack on the spot. Therefore, this product is secure."

Familiarity Maxim: Any security technology becomes more vulnerable to attacks when it becomes more widely used, and when it has been used for a longer period of time.

Antique Maxim: A security device, system, or program is most vulnerable near the end of its life.

Schneier's Maxim #2 (Control Freaks Maxim): Control will usually get confused with Security. Comment: From security guru Bruce Schneier. Even when Control doesn't get confused with Security, lots of people and organizations will use Security as an excuse to grab Control, e.g., the Patriot Act.

Father Knows Best Maxim: The amount that (non-security) senior managers in any organization know about security is inversely proportional to (1) how easy they think security is, and (2) how much they will micro-manage security and invent arbitrary rules.

Big Heads Maxim: The farther up the chain of command a (non-security) manager can be found, the more likely he or she thinks that (1) they understand security and (2) security is easy.

Huh Maxim: When a (non-security) senior manager, bureaucrat, or government official talks publicly about security, he or she will usually say something stupid, unrealistic, inaccurate, and/or naïve.

Voltaire's Maxim: The problem with common sense is that it is not all that common. Comment: Real world security blunders are often stunningly dumb.

Yippee Maxim: There are effective, simple, & low-cost counter-measures (at least partial countermeasures) to most vulnerabilities.

Arg Maxim: But users, manufacturers, managers, & bureaucrats will be reluctant to implement them for reasons of inertia, pride, bureaucracy, fear, wishful thinking, and/or cognitive dissonance.

Show Me Maxim: No serious security vulnerability, including blatantly obvious ones, will be dealt with until there is overwhelming evidence and widespread recognition that adversaries have already catastrophically exploited it. In other words, "significant psychological (or literal) damage is required before any significant security changes will be made".

Could've, Would've, Should've Maxim: Security Managers will dismiss a serious vulnerability as of no consequence if there exists a simple countermeasure—even if they haven't bothered to actually implement that countermeasure.

Payoff Maxim: The more money that can be made from defeating a technology, the more attacks, attackers, and hackers will appear.

I Hate You Maxim 1: The more a given technology is despised or distrusted, the more attacks, attackers, and hackers will appear.

I Hate You Maxim 2: The more a given technology causes hassles or annoys security personnel, the less effective it will be.

Colsch's (KISS or Kitchen Sink) Maxim: Security won't work if there are too many different security measures to manage, and/or they are too complicated or hard to use.

That's Cold Maxim: An adversary who attacks cold (without advance knowledge or preparation) is stupid and amateurish, often too much so to be a real threat. Moreover, he almost never has to attack cold. Comment: Thus don't overly focus on this kind of attack, or use it as an excuse not to fix vulnerabilities.

Shannon's (Kerckhoffs') Maxim: The adversaries know and understand the security hardware, software, algorithms, and strategies being employed. Comment: This is one of the reasons why open source security (e.g., open source cryptography) makes sense.

Corollary to Shannon's Maxim: Thus, "Security by Obscurity", i.e., security based on keeping long-term secrets, is not a good idea. Comment: Short-term secrets can create useful uncertainty for an adversary, such as temporary passwords and unpredictable schedules for guard rounds. But relying on long term secrets is not smart. Ironically—and somewhat counter-intuitively—security is usually more effective when it is transparent. This allows for more discussion, analysis, outside review, criticism, accountability, buy-in, and improvement.

Gossip Maxim: People and organizations can't keep secrets. Comment: See Manning and Snowden.

How Inconvenient! Maxim: Convenience is typically not compatible with good security, yet, paradoxically, security that isn't convenient usually doesn't work well.

Plug into the Formula Maxim: Engineers don't understand security. They tend to work in solution space, not problem space. They rely on conventional designs and focus on a good experience for the user and manufacturer, rather than a bad experience for the bad guy. They view nature or economics as the adversary, not people, and instinctively think about systems failing stochastically, rather than due to deliberate, intelligent, malicious intent. Being intelligent does not automatically make you think like a bad guy. (Magicians and con artists know that technical people are often the easiest people to scam because they think logically!)

Rohrbach's Maxim: No security device, system, or program will ever be used properly (the way it was designed) all the time.

Rohrbach Was An Optimist Maxim: No security device, system, or program will ever be used properly.

Ox Votes for the Moron Maxim: "Election Security" is an oxymoron.

Insider Risk Maxim: Most organizations will ignore or seriously underestimate the threat from insiders. Comment: Maybe from a combination of denial that we've hired bad people, and a (justifiable) fear of how hard it is to deal with the insider threat?

We Have Met the Enemy and He is Us Maxim: The insider threat from careless or complacent employees and contractors exceeds the threat from malicious insiders (though the latter is not negligible.) Comment: This is partially, though not totally, due to the fact that careless or complacent insiders often unintentionally help nefarious outsiders. Also, see Schryver's Law below.

Fair Thee Well Maxim: Employers who talk a lot about treating employees fairly typically treat employees neither fairly nor (more importantly) well, thus aggravating the insider threat and employee turnover (which is also bad for security).

The Inmates are Happy Maxim: Large organizations and senior managers will go to great lengths to deny employee disgruntlement, see it as an insider threat, or do anything about it. Comment: There are a wide range of well-established tools for mitigating disgruntlement. Most are quite inexpensive.

Two Kinds Maxim 1: Disengaged employees fall into 2 categories, those who quit and leave, and those who quit and stay.

Two Kinds Maxim 2: Disgruntled employees fall into 2 categories, those who engage in retaliation & sabotage, and those who are currently contemplating it.

Beef Jerky Maxim: Employees don't leave jobs, they leave jerks.

Troublemaker Maxim: The probability that a security professional has been marginalized by his or her organization is proportional to his/her skill, creativity, knowledge, competence, and eagerness to provide effective security.

Feynman's Maxim: An organization will fear and despise loyal vulnerability assessors and others who point out vulnerabilities or suggest security changes more than malicious adversaries. Comment: An entertaining example of this common phenomenon can be found in "Surely You are Joking, Mr. Feynman!", published by W.W. Norton, 1997. During the Manhattan Project, when physicist Richard Feynman pointed out physical security vulnerabilities, he was banned from the facility, rather than having the vulnerability dealt with (which would have been easy).

Irresponsibility Maxim: It'll often be considered "irresponsible" to point out security vulnerabilities (including the theoretical possibility that they might exist), but you'll rarely be called irresponsible for ignoring or covering them up.

Backwards Maxim: Most people will assume everything is secure until provided strong evidence to the contrary—exactly backwards from a reasonable approach.

Narcissist Maxim: Security managers, bureaucrats, manufacturers, vendors, and end-users will automatically assume that, if they cannot readily conceive of a way to defeat a security product (or a security program), then nobody else can. Remarkably, this will be

true even for people with little or no experience, resources, or aptitude for defeating security, and even if they are spectacularly unimaginative.

You Could've Knocked Me Over with a Feather Maxim 1: Security managers, bureaucrats, manufacturers, vendors, and end users will always be amazed at how easily their security products or programs can be defeated.

You Could've Knocked Me Over with a Feather Maxim 2: Having been amazed once, security managers, bureaucrats, manufacturers, vendors, and end users will be equally amazed the next time around.

That's Why They Pay Us the Big Bucks Maxim: Security is nigh near impossible. It's extremely difficult to stop a determined adversary. Often the best you can do is discourage him, and maybe minimize the consequences when he does attack, and/or maximize your organization's ability to bounce back (resiliency).

Throw the Bums Out Maxim: An organization that fires high-level security managers when there is a major security incident, or severely disciplines or fires low-level security personnel when there is a minor incident, will never have good security.

Scapegoat Maxim: The main purpose of an official inquiry after a serious security incident is to find somebody to blame, not to fix the problems.

Eeny, Meeny, Miny Maxim: The scapegoat(s) chosen after a serious security incident will tend to be chosen from among these 3 groups: those who had nothing to do with the incident, those who lacked the authority and resources to prevent it, and those whose warnings about the possibility of this or related incidents went unheeded.

A Priest, a Minister, and a Rabbi Maxim: People lacking imagination, skepticism, and a sense of humor should not work in the security field.

Thinking Outside the Bun Maxim: Any security manager who cannot think of a new place to have lunch oversees a poor security program.

Absence of Evidence As Evidence of Absence Maxim: The fact that any given unimaginative bureaucrat or security manager cannot immediately envision a viable attack scenario will be taken as proof that there are no vulnerabilities.

That's Not My Department Maxim: Any employee who's job primarily entails checking on security compliance will have no interest in (or understanding of) security, will not permit it to interfere with his/her job, and will look at you like you are crazy if you raise any actual security concerns.

Deer in the Headlights (I'm With Stupid) Maxim: Any sufficiently advanced cowardice, fear, arrogance, denial, ignorance, laziness, or bureaucratic intransigence is indistinguishable from stupidity.

Cowboy Maxim: You can lead a jackass to security, but you can't make him think.

Awareness Training: Most security awareness training turns employees against security and/or hypocritically represents the organization as having a good security culture when it does not.

See I (Just Work Here) Maxim 1: (Your security awareness or CI training not withstanding) any given Counter-Intelligence (CI) Officer doesn't want to hear about your CI concerns, and will do nothing about them if they are forced upon him/her.

See I (Just Work Here) Maxim 2: Any bureaucrat sufficiently high up in the Security or Counter-Intelligence Department doesn't get Counter Intelligence (CI).

Mr. Spock Maxim: The effectiveness of a security device, system, or program is inversely proportional to how angry or upset people get about the idea that there might be vulnerabilities.

Double Edge Sword Maxim: Within a few months of its availability, new technology helps the bad guys at least as much as it helps the good guys.

Mission Creep Maxim: Any given device, system, or program that is designed for inventory will very quickly come to be viewed—quite incorrectly—as a security device, system, or program. Comment: This is a sure recipe for lousy security. Examples include RFIDs, GPS, and many so-called nuclear Material Control and Accountability (MC&A) programs.

We'll Worry About it Later Maxim: Effective security is difficult enough when you design it in from first principles. It almost never works to retrofit it in, or to slap security on at the last minute, especially onto inventory technology.

Somebody Must've Thought It Through Maxim: The more important the security application, the less careful and critical thought and research has gone into it. Comment: Research-based practice is rare in important security applications. For example, while the security of candy and soda vending machines has been carefully analyzed and researched, the security of nuclear materials has not. Perhaps this is because when we have a very important security application, committees, bureaucrats, power grabbers, business managers, and linear/plodding/unimaginative thinkers take over.

That's Entertainment Maxim: Ceremonial Security (a.k.a. "Security Theater") will usually be confused with Real Security; even when it is not, it will be favored over Real Security. Comment: Thus, after September 11, airport screeners confiscated passengers' fingernail clippers, apparently under the theory that a hijacker might threaten the pilot with a bad manicure. At the same time, there was no significant screening of the cargo and luggage loaded onto passenger airplanes.

Ass Sets Maxim: Most security programs focus on protecting the wrong assets. Comment: Often the focus is excessively on physical assets, not more important assets such as people, intellectual property, trade secrets, good will, an organization's reputation, customer and vendor privacy, etc.

Vulnerabilities Trump Threats Maxim: If you know the vulnerabilities (weaknesses), you've got a shot at understanding the threats (the probability that the weaknesses will be exploited, how, and by whom). Plus you might even be ok if you get the threats wrong (which you probably will). But if you focus only on the threats, you're likely to be in trouble. Comment: It's hard to predict the threats accurately, but threats (real or imagined) are great for scaring an organization into action. It's not so hard to find the vulnerabilities if you really want to, but it is usually difficult to get anybody to do anything about them.

Vulnerabilities are the Threat Maxim: Security (and emergency response) typically fails not because the threats were misunderstood, but because the vulnerabilities were not recognized and/or not mitigated.

Pink Teaming Maxim: Most so-called "vulnerability assessments" are actually threat assessments, "red teaming", or some other exercise (like auditing, design basis threat, or performance/reliability testing) not well designed to uncover a wide range of security vulnerabilities. Comment: This is much more the case in physical security than in cyber security. Originally, "red teaming" meant doing a vulnerability assessment, but it recent years, it has come to mean a one-off, often rigged "test" of security which may have some value, but is not the same thing as a comprehensive vulnerability assessment looking at a wide range of vulnerabilities.

Risky Business Maxim: Many of the activities involved in developing or evaluating security measures will only have a partial or superficial connection to true Risk Management.

Mermaid Maxim: The most common excuse for not fixing security vulnerabilities is the belief that they simply can't exist. Comment: Often, the evidence offered that no security vulnerabilities exist is that the security manager who expresses this view can't personally imagine how to defeat the security.

Onion Maxim: The second most common excuse for not fixing security vulnerabilities is that "we have many layers of security", i.e., we rely on "Security in Depth". Comment: Security in Depth has its uses, but it should not be the knee jerk response to difficult security challenges, nor an excuse to stop thinking and improving security, as it often is.

Hopeless Maxim: The third most common excuse for not fixing security vulnerabilities is that "all security devices, systems, and programs can be defeated". Comment: This maxim is typically expressed by the same person who initially invoked the Mermaid Maxim, when he/she is forced to acknowledge that the vulnerabilities actually exist because they've been demonstrated in his/her face. A common variant of the hopeless maxim is "sure, we could

implement that inexpensive countermeasure so that the average person on the street couldn't defeat our security with a bobby pin, but then the bad guys would just come up with another, more sophisticated attack".

Takes One to Know One Maxim: The fourth most common excuse for not fixing security vulnerabilities is that "our adversaries are too stupid and/or unresourceful to figure that out." Comment: Never underestimate your adversaries, or the extent to which people will go to defeat security.

Depth, What Depth? Maxim: For any given security program, the amount of critical, skeptical, creative, and intelligent thinking that has been undertaken is inversely proportional to how strongly the strategy of "Security in Depth" (layered security) is embraced.

Waylayered Security Maxim: Layered security will fail stupidly. Comment: See, for example, the 82-year old nun penetrating the Y-12 nuclear facility, or the White House fence jumper.

Redundancy/Orthogonality Maxim: When different security measures are thought of as redundant or "backups", they typically are not. Comment: Redundancy is often mistakenly assumed because the disparate functions of the two security measures aren't carefully thought through.

Tabor's Maxim #1 (Narcissism Maxim): Security is an illusionary ideal created by people who have an overvalued sense of their own self worth. Comment: From Derek Tabor. This maxim is cynical even by our depressing standards—though that doesn't make it wrong.

Tabor's Maxim #2 (Cost Maxim): Security is practically achieved by making the cost of obtaining or damaging an asset higher than the value of the asset itself. Comment: From Derek Tabor. Note that "cost" isn't necessarily measured in terms of dollars.

Buffett's Maxim: You should only use security hardware, software, and strategies you understand. Comment: This is analogous to Warren Buffett's advice on how to invest, but it applies equally well to security. While it's little more than common sense, this advice is routinely ignored by security managers.

Just Walk It Off Maxim: Most organizations will become so focused on prevention (which is very difficult at best), that they fail to adequately plan for mitigating attacks, and for recovering when attacks occur.

Thursday Maxim: Organizations and security managers will tend to automatically invoke irrational or fanciful reasons for claiming that they are immune to any postulated or demonstrated attack. Comment: So named because if the attack or vulnerability was demonstrated on a Tuesday, it won't be viewed as applicable on Thursday. Our favorite example of this maxim is when we made a video showing how to use GPS spoofing to hijack a truck that uses GPS tracking. In that video, the GPS antenna was shown attached to the

side of the truck so that it could be easily seen on the video. After viewing the video, one security manager said it was all very interesting, but not relevant for their operations because their trucks had the antenna on the roof.

Galileo's Maxim: The more important the assets being guarded, or the more vulnerable the security program, the less willing its security managers will be to hear about vulnerabilities. Comment: The name of this maxim comes from the 1633 Inquisition where Church officials refused to look into Galileo's telescope out of fear of what they might see.

Michener's Maxim: We are never prepared for what we expect. Comment: From a quote by author James Michener (1907-1997). As an example, consider Hurricane Katrina.

Black Ops Maxim: If facility security is the responsibility of the Operations Department, then security will be given about as much importance and careful analysis as snow removal or taking out the trash.

Accountability 1 Maxim: Organizations that talk a lot about holding people accountable for security are talking about mindless retaliation, not a sophisticated approach to motivating good security practices by trying to understand human and organizational psychology, and the realities of the workplace.

Accountability 2 Maxim: Organizations that talk a lot about holding people accountable for security will never have good security. Comment: Because if all you can do is threaten people, rather than developing and motivating good security practices, you will not get good results in the long term.

Blind-Sided Maxim: Organizations will usually be totally unprepared for the security implications of new technology, and the first impulse will be to try to mindlessly ban it. Comment: Thus increasing the cynicism regular (non-security) employees have towards security.

Better to be Lucky than Good Maxim: Most of the time when security appears to be working, it's because no adversary is currently prepared to attack.

Success Maxim: Most security programs "succeed" (in the sense of their being no apparent major security incidents) not on their merits but for one of these reasons: (1) the attack was surreptitious and has not yet been detected, (2) the attack was covered up by insiders afraid of retaliation and is not yet widely known, (3) the bad guys are currently inept but that will change, or (4) there are currently no bad guys interested in exploiting the vulnerabilities, either because other targets are more tempting or because bad guys are actually fairly rare.

Rigormortis Maxim: The greater the amount of rigor claimed or implied for a given security analysis, vulnerability assessment, risk management exercise, or security design, the less careful, clever, critical, imaginative, and realistic thought has gone into it.

Catastrophic Maxim: Most organizations mistakenly think about and prepare for rare, catastrophic attacks (if they do so at all) in the same way as for minor security incidents.

I am Spartacus Maxim: Most vulnerability or risk assessments will let the good guys (and the existing security infrastructure, hardware, and strategies) define the problem, in contrast to real-world security applications where the bad guys get to. Comment: Named for the catch-phrase from the 1960 Stanley Kubrick film *Spartacus*. When the Romans captured Spartacus' army, they demanded he identify himself, but all his soldiers claimed to be Spartacus. Not historically accurate, but very Hollywood!

Band-Aid Maxim: Effective security is difficult enough when designed in from scratch. It can rarely be added on at the end, or as an afterthought. Comment: So plan security at the earliest design stages of a security device, system, or program.

Methodist Maxim: While vulnerabilities determine the methods of attack, most vulnerability or risk assessments will act as if the reverse were true.

Rig the Rig Maxim: Any supposedly "realistic" test of security is rigged.

Tucker's Maxim #1 (Early Bird & Worm Maxim): An adversary is most vulnerable to detection and disruption just prior to an attack. Comment: So seize the initiative in the adversary's planning stages. From Craig Tucker.

Tucker's Maxim #2 (Toss the Dice Maxim): When the bullets start flying, it's a crapshoot and nobody can be sure how it'll turn out. Comment: So don't let it get to that point. From Craig Tucker.

Tucker's Maxim #3 (Failure = Success Maxim): If you're not failing when you're training or testing your security, you're not learning anything. Comment: From Craig Tucker.

Gunslingers' Maxim: Any government security program will mistakenly focus more on dealing with force-on-force attacks and brute force methods than on more likely attacks involving insider threats and subtle, surreptitious approaches.

Fool-On-Fool Maxim: The incompetence of any security program is proportional to the degree of obsession with idea that the major threat is a small band of stupid, unprepared adversaries who mindlessly attack straight on, using force and zero insiders. Comment: Somehow, the number of envisioned attackers is always less than the number the security program can purportedly neutralize.

3D Maxim: The incompetence of any security program is proportional to how strongly the mantra of "Deter, Detect, Delay" is embraced. Comment: This philosophy, while theoretically having some merit, is (as a practical matter) strongly correlated with unimaginative, non-proactive security.

D(OU)BT Maxim: If you think Design Basis Threat (DBT) is something to test your security against, then you don't understand DBT and you don't understand your security application. Comment: If done properly—which it often is not—DBT is for purposes of allocating security resources based on probabilistic analyses, not judging security effectiveness. Moreover, if the threat probabilities in the DBT analysis are all essentially 1, the analysis is deeply flawed.

It's Too Quiet Maxim: "Bad guys attack, and good guys react" is not a viable security strategy. Comment: It is necessary to be both proactive in defense, and to preemptively undermine the bad guys in offense.

Nietzsche's Maxim: It's not winning if the good guys have to adopt the unenlightened, illegal, or morally reprehensible tactics of the bad guys. Comment: "Whoever fights monsters should see to it that in the process he does not become a monster." Friedrich Nietzsche (1844-1900), *Beyond Good and Evil.*

Patton's Maxim: When everybody is thinking alike about security, then nobody is thinking. Comment: Adapted from a broader maxim by General George S. Patton (1885-1945).

Kafka's Maxim: The people who write security rules and regulations don't understand (1) what they are doing, or (2) how their policies drive actual security behaviors and misbehaviors.

30% Maxim: In any large organization, at least 30% of the security rules, policies, and procedures are pointless, absurd, ineffective, naïve, out of date, wasteful, distracting, or one-size-fits-all nonsense, or they may even actively undermine security (by creating cynicism about security, or by driving bad behaviors that were not anticipated).

By the Book Maxim: Full compliance with security rules and regulations is not compatible with optimal security. Comment: Because security rules and regulations are typically dumb and unrealistic (at least partially). Moreover, they often lead to over-confidence, waste time and resources, create unhelpful distractions, engender cynicism about security, and encourage employees to find workarounds to get their job done—thus making security an "us vs. them" game.

Aw Ditz Maxim: Mindlessly auditing if bureaucratic security rules are being followed will usually get confused with a meaningful security review, or a vulnerability assessment.

Cyborg Maxim: Organizations and managers who automatically think "cyber" or "computer" when somebody says "security", don't have good security (including good cyber or computer security).

Caffeine Maxim: On a day-to-day basis, security is mostly about paying attention.

Any Donuts Left? Maxim: But paying attention is very difficult.

Wolfe's Maxim: If you don't find it often, you often don't find it. Comment: Perceptual blindness is a huge problem for security officers.

He Who's Name Must Never Be Spoken Maxim: Security programs and professionals who don't talk a lot about "the adversary" or the "bad guys" aren't prepared for them and don't have good security. Comment: From *Harry Potter*.

Mahbubani's Maxim: Organizations and security managers who cannot envision security failures, will not be able to avoid them. Comment: Named for scholar and diplomat Kishore Mahbubani. He meant to apply this general principle to politics, diplomacy, and public policy, but it is also applicable to security.

Hats & Sunglasses Off in the Bank Maxim: Security rules that only the good guys follow are probably Security Theater.

Merton's Maxim: The bad guys don't obey our security policies. Comment: This maxim is courtesy of Kevin Sweere. It is named after Thomas Merton (1915-1968), a theological writer and philosopher.

Sweere's Maxim (Merton's Corollary): It's worse than that. The bad guys will analyze our security policies and regulations to find exploitable vulnerabilities, including those not envisioned by the good guys.

Wall Street Maxim: Every good idea is eventually a bad idea.

Dumbestic Safeguards Maxim: Domestic Nuclear Safeguards will inevitably get confused with International Nuclear Safeguards (treaty monitoring), including by people and organizations claiming to fully appreciate that the two applications are very different. Comment: Domestic Nuclear Safeguards is a typical security application, just for very important assets. With International Nuclear Safeguards, in contrast, the bad guys own the assets and facilities of interest, and they fully understand the surveillance, monitoring, and safeguards equipment being used (and may even build, control, and/or install it). It is especially common to overlook or ignore the fact that the adversary in International Nuclear Safeguards is a country, with national- to world-class resources available to defeat the safeguards. [Note: It's sometimes misleading called "International Nuclear Safeguards" when one country or organization, or group of countries try to help a nation improve its own domestic nuclear safeguards, but this is still just Domestic Nuclear Safeguards for the country of interest.]

Werther's Maxim: The security of encrypted (or digitally authenticated) information has less to do with the sophistication of the cipher than with the competence, intelligence, diligence, and loyalty of the people who handle it. Comment: From a quote by Waldemar Werther that "The security of a cipher lies less with the cleverness of the inventor than with the stupidity of the men who are using it."

Tobias's Maxim #5: Encryption is largely irrelevant. Comment: From Marc Weber Tobias.

Red Herring Maxim: At some point in any challenging security application, somebody (or nearly everybody) will propose or deploy more or less pointless encryption, hashes, or data authentication along with the often incorrect and largely irrelevant statement that "the cipher [or hash or authentication algorithm] cannot be broken".

Comment: For many security applications, people forget that "it's no more difficult to copy *encrypted* data than it is to copy *unencrypted* data."

Product anti-counterfeiting tags and International Nuclear Safeguards are two security applications highly susceptible to fuzzy thinking about encryption and data authentication.

With anti-counterfeiting tags, it is no harder for the product counterfeiters to make copies of encrypted data than it is to make copies of unencrypted data. They don't have to understand the encryption scheme or the encrypted data to copy it, so that the degree of difficulty in breaking the encryption (usually overstated) is irrelevant. Indeed, if there was a technology that could preventing cloning of encrypted data (or hashes or digital authentication), then that same technology could be used to prevent cloning of the unencrypted original data, in which case the encryption has no significant role to play. (Sometimes one might wish to send secure information to counterfeit hunters in the field, but the security features and encryption typically employed on cell phones or computers is good enough.)

What makes no sense is putting encrypted data on a product, with or without it including encrypted data about an attached anti-counterfeiting tag; the bad guys can easily clone the encrypted data without having to understand it. When there is an anti-counterfeiting tag on a product, only the degree of difficulty of cloning it is relevant, not the encryption scheme. The use of unique, one-of-a-kind tags (i.e., complexity tags) does not alter the relative unimportance of the encryption as an anti-counterfeiting measure.

Sometimes people promoting encryption for product anti-counterfeiting vaguely have in mind an overly complicated (and usually incomplete/flawed) form of a virtual numeric token ("call-back strategy"). ([See RG Johnston, "An Anti-Counterfeiting Strategy Using Numeric Tokens", *International Journal of Pharmaceutical Medicine* **19**, 163-171 (2005).]

Encryption is also often thought of as a silver bullet for International Nuclear Safeguards, partially for reasons given in the Dumbestic Safeguards Maxim. The fact is that encryption or data authentication is of little security value if the adversary can easily break into the equipment holding the secret key without detection (as is usually the case), if there is a serious insider threat that puts the secret encryption key at risk (which is pretty much always the case), and/or if the surveillance or monitoring equipment containing the secret key is designed, controlled, inspected, maintained, stored, observed, or operated by the adversary (as is typically the case in International Nuclear Safeguards).

Anti-Silver Bullet Maxim: If you have poor security before you deploy encryption or data authentication, you will have poor security after.
Comment: Sometimes, you'll have worse security because the encryption/authentication provides a false sense of security, or causes distractions.

It's Standard Maxim: As a general rule of thumb, about two-thirds of security "standards" or "certifications" (though not "guidelines") make security worse.

Alice Springs Maxim: Organizations will be loathe to factor in local, on-the-ground details in deciding what security resources to assign to a given location or asset. One-size-fits-all will be greatly preferred because it requires less thinking.
Comment: This maxim is named after the standard reassurance given to worried tourists in Australia that "there aren't a lot of shark attacks in Alice Springs".

Follow the Money Maxim: Security attention and resources will usually be doled out in proportion to the absolute dollar value of the assets being protected, not (as it should be) in proportion to the risk.

Oh, the Lovely Colors! Maxim: High-level corporate executives will be convinced the organization has good security if they are shown lots of detailed, colorful graphs, spreadsheets, and calendars concerning security policies, planning, documentation, and training.

The MBA Maxim: At high levels in an organization, lots of detailed work on security policies, planning, documentation, scheduling, and charts/graphs/spreadsheets will be preferred over actually thinking carefully and critically about security, or asking critical questions.

Fallacy of Precision Maxim 1: If security managers or bureaucrats assign a number or a ranking to some aspect of security (e.g., probability of attack, economic consequences of the loss of an asset, etc.) they will incorrectly think they really understand that aspect and the related security issues.

Fallacy of Precision Maxim 2: If there are n bits in the attribute measurement of a given object, then security end users can be easily (wrongly) convinced that 2^{-n} is: (1) the probability that a similar object matches this one, and/or (2) the probability that somebody can fool the attribute reader, including by "counterfeiting" or mimicking the object so that it has essentially the same attribute measurement. Comment: End users of security products (especially biometrics or tag readers) will often be fooled by this fallacy. Why is it a fallacy? Among other reasons: Because the bits are not uncorrelated, because they don't all have relevance to the security or authenticity problem (maybe none of them do!), because the degree of correlation between similar objects has not been inputted into the problem, because the type 1 and type 2 errors and tradeoffs haven't been carefully measured or analyzed, because the ease or difficulty of counterfeiting involves many outside factors not included here, and because the ease or difficulty of otherwise spoofing the reader has not been considered.

Apples and Oranges Maxim: Anyone trying to sell you a counterfeit detector, will make a big show of how different objects have different signatures (attribute measurements), but will ignore, oversimplify, or misrepresent the far more important question of how hard it is to fool the reader, including by "counterfeiting" or mimicking the object so that it has

essentially the same signature. Comment: Manufacturers, vendors, and promoters of biometrics products and tag readers are very fond of doing this.

I Second That Motion Maxim: "Security by Committee" is an oxymoron.

The following are general "laws" that also apply to security:

Fudd's Law: If you push on something hard enough, it will fall over.

First Law of Revision: Information necessitating a change of design will be conveyed to the designers after—and only after—the plans are complete.

Hellrung's Law: If you wait long enough, it will go away.

Grelb's Law: But if it was bad, it will come back.

Brien's First Law: At some time in the life cycle of virtually every organization, its ability to succeed in spite of itself runs out.

Bucy's Law: Nothing is ever accomplished by a reasonable person.

Stewart's Law: It is easier to get forgiveness than permission.

Horngren's Law: The Real World is a special case.

Glazer's Law: If it says "one size fits all", then it doesn't fit anybody.

Gold's Law: If the shoe fits, it's ugly.

Firestone's Law: Chicken Little only has to be right once.

Shaw's Law: Build a system that even a fool can use, and only a fool will want to use it.

Byrne's Law: In any electrical circuit, appliances and wiring will burn out to protect the fuses.

Ginsberg's Laws from the beat poet Allen Ginsberg (1926-1997):
The First Law of Thermodynamics: "You can't win."
The Second Law of Thermodynamics: "You can't break even."
The Third Law of Thermodynamics: "You can't quit."

Putt's Law: Technology is dominated by two types of people: those who understand what they do not manage, and those who manage what they do not understand.

Clarke's First Law: When a distinguished but elderly scientist states that something is possible, he is almost certainly right. When he states that something is impossible, he is probably wrong.

Hawkin's Law: Progress does not consist of replacing a theory that is wrong with one that is right. It consists of replacing a theory that is wrong with one that is more subtly wrong.

Schryver's Law: Sufficiently advanced incompetence is indistinguishable from malice.

Kernighan's Law: Debugging is twice as hard as writing the software in the first place. Therefore, if you write the software as cleverly as possible, you are (by definition) not smart enough to debug it.

Life Cycle of a Good Idea Law: If you have a good idea: first they ignore you, then they ridicule you, then they claim to have thought of it first, then it's declared to be obvious.

Not Invented Here Law: If it wasn't invented here, it's a bad idea (unless we can steal the idea and make it look like we thought of it first).

Glass Houses Law: The people most obsessed with the work quality of others will typically be among the most incompetent, deadwood screw-ups in the whole organization.

Tacitus's Law: To show resentment at a reproach is to acknowledge that one may have deserved it. Comment: From Tacitus (55-117 AD).

Sallinger's Law: All morons hate it when you call them a moron. Comment: From J.D. Sallinger (1919-2010).

Modeling a Physical Protection System for the 444 TBq ^{60}Co Irradiation Source at the Center for Applied Radiation Science and Technology, Mafikeng, South Africa

C. C Arwui[1], V. M Tshivhase,[1] and R. M Nchodu[2]

1. North-West University (Mafikeng Campus), Faculty of Agriculture Science and Technology. Centre for Applied Radiation Science and Technology, Private Bag X2046, Mmabatho 2735, South Africa, arwui2000@yahoo.com.

2. Ithemba Laboratory for Accelerator Based Sciences. Old Faure Road, Faure, 7131, Cape Town, South Africa.

Abstract

This study models a physical protection system (PPS) for a ^{60}Co irradiation source which will be used at the Centre for Applied Radiation Science and Technology of the North-West University (Mafikeng Campus). The model PPS was analyzed and evaluated quantitatively by the use of the Estimate of Adversary Sequence Interruption (EASI) to determine the effectiveness of the PPS. This evaluation was done to calculate the Probability of interruption (P_I) of a potential adversary attack scenario along a specific path. The P_I values show the extent to which the security system is effective; the results indicate low values of P_I for the existing protection system, and high values of P_I for the proposed new physical protection system. The values increase from 0 to a range of 0.51 – 0.84 for a sabotage scenario, and 0.55 – 0.90 for a theft scenario—indicating stronger overall security for the proposed PPS compared to the original PPS.

Keywords: Physical Protection Systems, Probability of Detection, Probability of Guard Communication, Probability of Interruption, Detection, Delay, Response, South Africa nuclear.

1. Introduction

Nuclear security is defined by the International Atomic Energy Agency (IAEA) as the measures put in place for the prevention, detection of, and response to theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material, other radioactive material, or their associated facilities and activities.[1] The IAEA has grouped nuclear security risks into four potential categories, but only two are relevant to this facility: the malicious use of radioactive sources in (for example) dirty bombs, and radiological hazards caused by the attack on, or the sabotage of, a facility or a transport vehicle.[2] The aim of the measures is to protect persons, property, society, and the environment from harmful consequences of a unauthorized nuclear event.[3]

Nuclear security of any State will only be successful if it has a good, functional, and effective Nuclear Security Regime. This regime is made up of legislative and regulatory framework, administrative systems, and measures that govern the security of nuclear material or other radioactive material and their associated facilities and associated activities. These systems and measures are part of a physical protection regime which is an essential part of the overall nuclear security regime.

A physical protection regime should have the objectives to protect against unauthorized removal of nuclear material or any radioactive material, and to locate and recover missing nuclear material or radioactive material.[4] The development of a national detection strategy which relies upon an effective nuclear security detection architecture contributes to the protection of persons, property, society, and the environment, and it is one of the necessary elements for establishing an effective nuclear security regime.[4] In order to sustain the nuclear security detection architecture, significant planning and commitment of resources, both financial and human, are needed to ensure the long term operational effectiveness of national capabilities for detection of nuclear and other radioactive material out of regulatory control.[5]

Figure 1.1: Google Map showing the layout of the North-West University (NWU).

Figure 1.1 shows the location of the Centre for Applied Radiation Science and Technology (CARST) on the university premises. The yellow markers in the upper right hand corners indicate the three buildings of the Centre. One of the buildings houses the ^{60}Co irradiation source. CARST is one of the Centres under the Faculty of Agriculture Science and Technology of the North – West University, and is also one of the Centres mandated to train nuclear scientists at the postgraduate level to work in the nuclear industry of South Africa. The university is located between two towns of one of the province of South Africa. The Province has seventy 78 towns and cities. The two towns nearest the University are always found in the top 10 precincts in terms of crime, and this poses a serious threat to the facility due to the nature of the specific type of crimes.[6]

In a threat assessment, tactics, capabilities, potential actions, and motivations of adversaries should be taken into account. Adversaries can be outsiders or insiders, or a combination, as well as passive or active in an attack. Adversaries employ 3 main types of tactics, namely Deceit, Stealth, and Force in their effort to gain unauthorized access to their target locations.[7] Extortion, blackmail, kidnapping, coercion, etc. can arise from these 3 tactics. The nature and type of crimes in the two towns surrounding the facility are such that local criminals do indeed use all three types of tactics in different crimes.

The capabilities of local criminals in committing the crimes are high because they have arms and ammunitions, as well as different kinds of hand tools. They also have means of

transportation. It should be noted that the emerging capabilities of the criminals might not be used against all facilities, but because they are emerging, we need to plan for them in our security designs—especially with the insurgency of Boko Haram and Al-Shabaab militants in Eastern and Western Africa.

Adversaries' actions depend mainly on their goals in an attack. These goals can include theft, sabotage, terrorism, and political protest. Considering the threat the facility is exposed to and the crimes committed around the facility, the above mentioned actions can be linked to the different crimes such as unlawful possession of fire arms and ammunition, robbery at both residential and non-residential premises, malicious injury to properties, kidnapping, stalking, and burglary at both residential and non-residential premises. Motivations of adversaries could be ideological, economical (financial benefits), revenge by disgruntled former or current employees or personal. Looking at the different crimes committed, we believe that the main motivation of local criminals is economic.

A Physical Protection System (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage or other malevolent attacks which can lead to negative consequences. This system typically has a number of elements namely, deterrence, detection, delay, and response.[8] A security management system incorporated into the design addresses access control, trustworthiness, information protection, preparation of a security plan, training and qualification, accounting, inventory, and event reporting issues.[9] Hence, this work is aimed at evaluating the current status of the PPS for the ^{60}Co radioactive source to be used in the irradiation facility, developing a Design Basis Threat (DBT) based on the threat the facility is exposed to, and proposing a new PPS model for the facility based on the proposed DBT. The process will utilize a performance-based system to model the PPS. Finally, we performed an analysis and evaluation of the PPS effectiveness for the protection of the radioactive source using the EASI computer code.

2. Methodology

2.1 Assessment of Assets

The main asset of the facility is the ^{60}Co irradiation source. This source and its shielding was manufactured in 1987 with an activity of 93 TBq or 2500 Curie. It was used by Ithemba Laboratories of South Africa for Teletherapy treatment of cancer. A memorandum of understanding (MOU) between Ithemba Laboratories and the Center for Applied Radiation Science and Technology of the North-West University (Mafikeng Campus) was signed in November 2013.[10] However, the source can only be transferred to the Centre after the proposed PPS is implemented completely. Based on the value of the initial activity of the source and the year of manufacture, calculations determined that the current activity is 2.5 TBq or 67.6 Curie as at June 2015. The center intends to upgrade the source to the maximum the source head can accommodate to enhance research. Checking the manufacturer's specifications contained in the MOU indicates that the Eldorado 78 which houses the ^{60}Co can accommodate a total activity of 444 TBq or 12000 Curie. The higher activity of the source makes it more prudent to have an effective PPS in place because when the source is upgraded, it becomes more harmful if it gets out of regulatory control.[10]

The extent of harmful effects that the radioactive source could cause was derived from the introduction of a new IAEA categorization system in October 2003 for radioactive sources [11]. This information is needed to ensure that the source is maintained under control commensurate with the radiological risks. This categorization system is based on the potential for radioactive sources to cause deterministic effects, i.e., health effects which do not appear until threshold values are exceeded, and for which the severity of effect increases with the dose beyond the threshold. This system categorizes radioactive sources beginning from sources with their associated practices causing the highest consequences being category one (1) followed by two (2), three (3), four (4) and five (5) in that order.

Before a source is put under a category, the risk factor is first obtained by dividing the activity (A) of the source by the dangerous value (D) of the source. Category 1 sources have a ratio of A/D that is greater or equal to 1000. Category 2 sources a ratio of A/D less than 1000 but greater or equal to 10. Category 3 sources have a ratio of A/D less than 10 but greater or equal to 1. Category 4 sources have a ratio of A/D less than 1 but greater or

equal to 0.01, and finally category 5 sources have a ratio of A/D less than 0.01 but greater or equal to Exemption activity/D.

A D value is the quantity of radioactive material which is considered a dangerous source.[12] A dangerous source is one which could cause permanent injury or be immediately life-threatening if not managed safely and contained securely.[11] Our study made use of the current and upgraded activities of the source and the D value of ^{60}Co to calculate the risk factor of the source in order to ascertain the appropriate level of security.

2.2 Assessment of Risk to the Facility

Most facilities conduct routine risk assessment for their security or protection system in order to verify whether they are adequately protecting their assets. These routine assessments help to identify areas that may need additional attention. This study assessed the likelihood of a negative event, in this case a security incident and its consequences. The quantitative security risk was measured through the use of the following equation:

$$R = P_A \times (1 - P_E) \times C \qquad (1)$$

where R is the risk to the facility in the event of an adversary getting access to, or stealing critical assets; P_A is the probability of an adversary attack during a period of time; P_E is the effectiveness of the PPS; $(1 - P_E)$ is the vulnerability of the PPS to the identified threat; and C is the consequence value.[13]

The probability of adversary attacking during a period of time (P_A) can be very difficult to determined, but the probability ranges from 0 (no chance of an attack) to 1.0 (certainty of an attack). Critical assets that are valuable and whose consequence of loss will be high if a security event occurs in the facilities, will certainly require protection, even if the P_A is low.

The effectiveness of the PPS to an identified threat (P_E) is related to the probability of interruption by the respondents (P_I), and the probability of neutralizing the adversary by interruption (P_N), via:

$$P_E = P_I \times P_N \qquad (2)$$

2.2.1 Assessment of Risk due the ^{60}Co irradiation source

The risk to the public from an uncontrolled dangerous source is calculated through equation (3) below. For all materials, the risk factor is calculated by the equation:

$$\text{Aggregate } \frac{A}{D} = \sum_i \frac{A_i}{D_i} \qquad (3)$$

where Aggregate A/D is the risk factor, A_i is the activity (in TBq) of each radionuclide over which control could be lost during an emergency/event, and D_i is the D value for the radionuclide.[11]

2.3 Evaluation of the Existing Protection Systems

Figure 2.1 – Layout of the Irradiation Facility at the Centre of Applied Radiation Science and Technology of the North – West University.

An evaluation of the existing PPS was done to ascertain whether it makes use of the three functions of a PPS—detection, delay and response—for ensuring the security of the radioactive source. Modeling a new PPS or upgrading the existing PPS is necessary if the required main functions of a PPS are not employed by the existing PPS.

2.4 Design Basis Threat (DBT)

A DBT was developed based on the threat assessment to the facility's major asset (radioactive source). The purpose of doing a Design Basis Threat (which is a way to identify threats) was to use it as a tool to provide a common basis for planning for physical protection by the operator, as well as for approval of the physical security plan by the competent authority for nuclear security. The use of a DBT methodology is recommended by the IAEA as the best method for designing the security measures for specific sources.[14] The higher the risk, the more capability will be required from the security systems to protect the sources.[15]

2.5 Modeling the New PPS

In designing the PPS, this study took into consideration a performance-based design. In terms of the performance-based design, intrusion sensors performance will depend on the probability of detection (P_D), nuisance alarm rate (NAR), and their vulnerabilities and the ability by adversaries to defeat them. The effectiveness of a sensor will depend on P_D and the confidence level (C_L) of the sensor.[13] The PPS will operate in two protection areas, controlled and supervised areas.

The modeling was done in the stages of detection, delay and response. Duties were allocated to each individual or group involved in providing response to interrupt adversarial actions. These procedures were documented to prevent conflict during response.[16] Administrative procedures were developed to integrate with interior intrusion sensors, access controls, and material and equipment monitoring. These administrative procedures can be effective against insider threats.

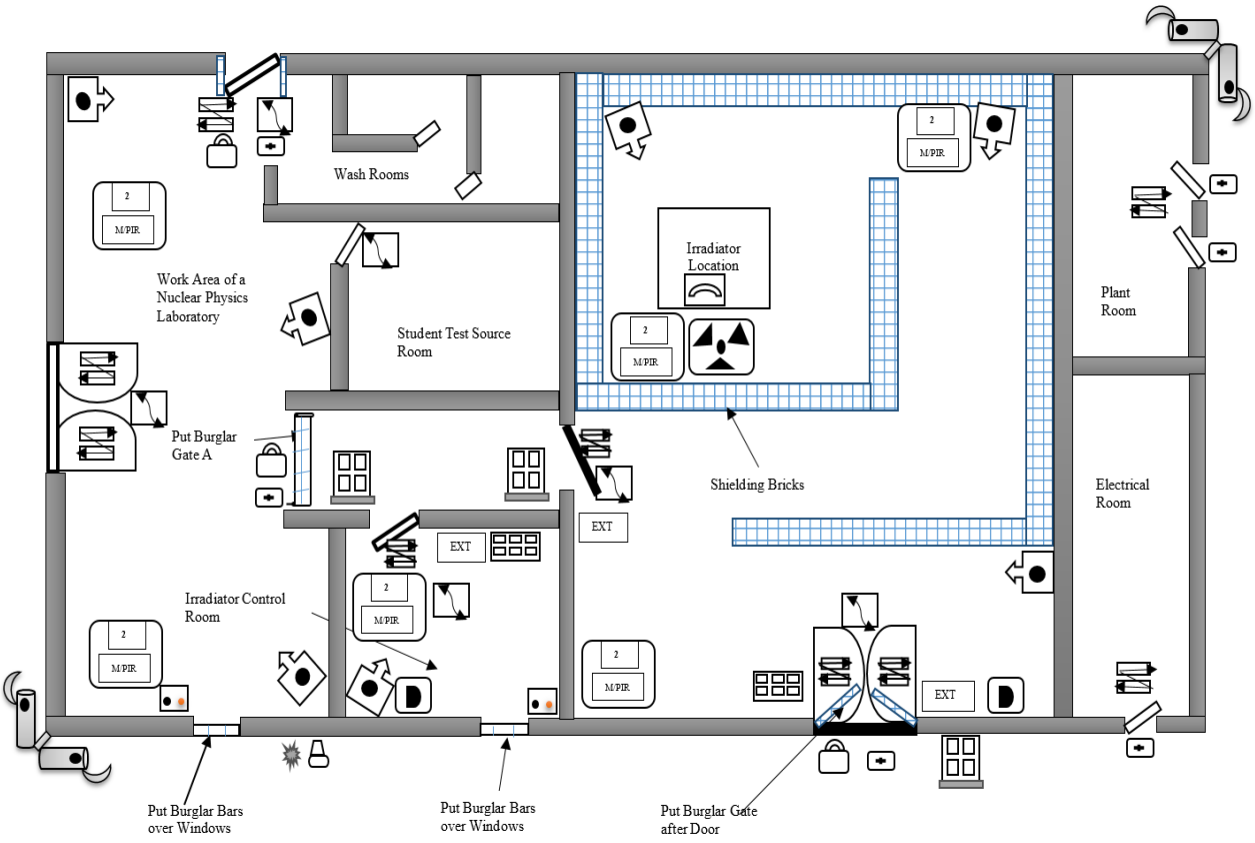

Figure 2.2 – A schematic of the proposed PPS for the ^{60}Co Irradiation Facility.

2.6 Evaluation of the New PPS

The computer model EASI (Estimate of Adversary Sequence Interruption) [7] was used to analyze the proposed model in terms of attack detection, delay, and response. Input parameters representing the physical protection functions of detection, delay, and response were fed into EASI to calculate the Probability of interruption (P_I). The likelihood of effective communication via an alarm signal is also required.

EASI makes use of inputs of probabilities for both Communication and Detection on the assumption that all functions will be performed successfully.[7]. In terms of Delay and Response inputs, mean times and standard deviations for each element are required. Inputs fed into the model represent a specific adversary path. Because EASI works for one specific adversary path at a time, fourteen (14) adversary paths were identified to be used for the analyses.

3 Results

3.1 Risk due the ^{60}Co Irradiation Source

From equation (3) the risk factor A/D was calculated to be 83.3 This falls under the range 1000 > A/D ≥ 10, which makes this source with its current activity a Category 2 source.[11] As such, there will be a high consequence of an unauthorized security event. This source should have security measures that will meet the objectives of security level B.[17]

Because the facility's intention is to upgrade the source activity from 2.50 TBq to the maximum activity of 444 TBq, the risk factor was calculated to be 14800, which falls under the range A/D ≥ 1000 [11] for a Category 1 source. This represents the highest consequence in an unauthorized security event. Therefore, it requires security measures that meet the objectives of security level A.[17]

The risk (R) to the Centre was found from equation (1) to be 0.95 or 95%. This was because the probability of adversary attack was assign the value 1 or 100% due to the high activity of the source. The effectiveness of the PPS to a defined threat (P_E) was calculated using equation (2), and the value was zero because there were no detection parameters along the various adversary paths for the existing PPS. Thus, the probabilities of interruption and neutralization were all zero, resulting in P_E being zero. For the risk computation, the consequence value, C, was assigned a value of 0.95 or 95% due to the high consequences of a security event involving the source.

The next 5 tables indicate the adversary pathways considered in the model. It should be noted that these tables consider only the most likely and conventional adversarial pathways, not other, more imaginative pathways such as using helicopters, tunneling, demolition, etc. that could be employed.

Table 3.1 – Identified Adversary Pathways for the Irradiation Facility.

Path 1	**Path 2**	**Path 3**
Jump Fence	Jump Fence	Jump Fence
Run to Building	Run to Building	Run to Building
Open Outer Burglar Gate	Open Door 4	Open Door 3
Open Door 1	Open Inner Burglar Gate	Open Inner Burglar Gate
Open Inner Burglar Gate	Run to Controlled Area	Walk to Controlled Area
Walk through Maze	Open Inner Burglar Gate A	Open Inner Burglar Gate A
Remove or Sabotage Target	Open Door 2	Open Door 2
	Walk through Maze	Walk through Maze
	Remove or Sabotage Target	Remove or Sabotage Target

Table 3.2 – Continuation of Identified Adversary Pathways for the Irradiation Facility.

Path 4	**Path 5**	**Path 6**
Jump Fence	Jump Fence	Jump Fence
Run to Building	Run to Building	Run to Building
Remove Outer Window Burglar Bars	Open Door 10	Open Door 8
Break Window Glass	Break Wall	Remove Roof
Remove Inner Window Burglar Bars	Break Ceiling	Break Ceiling
Jump into Room	Jump into Room	Jump into Room
Run to Controlled Area	Walk through Maze	Walk through Maze
Open Inner Burglar Gate A	Remove or Sabotage Target	Remove or Sabotage Target
Open Door 2		
Walk through Maze		
Remove or Sabotage Target		

Table 3.3 – Continuation of Identified Adversary Pathways for the Irradiation Facility.

Path 7	**Path 8**	**Path 9**
Jump Fence	Jump Fence	Jump Fence
Run to Building	Run to Building	Run to Building
Open Door 3	Open Door 4	Open Door 4
Open Inner Burglar Gate	Open Inner Burglar Gate	Open Inner Burglar Gate
Run to Controlled Area	Run to Controlled Area	Run to Controlled Area
Open Door 7	Enter Wash Rooms	Open Inner Burglar Gate A
Break Double Ceiling	Break Double Ceiling	Open Door 5
Jump into Room	Jump into Room	Remove or Sabotage Target
Remove or Sabotage Target	Remove or Sabotage Target	

Table 3.4 – Continuation of Identified Adversary Pathways for the Irradiation Facility.

Path 10	**Path 11**	**Path 12**
Jump Fence	Jump Fence	Jump Fence
Run to Building	Run to Building	Run to Building
Open Door 3	Remove Outer Burglar Bars	Remove Outer Burglar Bars
Open Inner Burglar Gate	Break Window Glass	Break Window Glass
Enter Wash Room	Remove Inner Burglar Bars	Remove Inner Burglar Bars
Break Double Ceiling	Jump into Room	Jump into Room
Jump into Room	Open Door 5	Walk through LAB
Remove or Sabotage Target	Open Door 2	Remove Target
	Walk through Maze	
	Remove or Sabotage Target	

Table 3.5– Continuation of Identified Adversary Pathways for the Irradiation Facility.

Path 13	**Path 14**
Jump Fence	Jump Fence
Run to Building	Run to Building
Open Door 10	Climb Building
Break Double Wall	Remove Roof
Walk through Maze	Break Ceiling
Remove or Sabotage Target	Jump into Room
	Walk through Maze
	Remove or Sabotage Target

3.2 Evaluation Results for the Existing PPS

Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0	E	15	4.5
3	Open Outer Burglar Gate	0	E	94	28.2
4	Open Door 1	0	E	148.5	44.55
5	Open Inner Burglar Gate	0	E	159.8	47.94
6	Walk through Maze	0	E	10.3	3.09
7	Remove Target (Equipment)	0	E	281.3	84.39
8					
9					
10					
11					
12					

Probability of Interruption:	0.00

Figure 3.1 – Result of EASI analysis for adversary path 1.

Figure 3.1 above shows the EASI analysis of the existing protection system. This analysis and the results for the other 13 adversary paths all gave a P_I value of zero. This means that the probability of detection (P_D) for the existing protection system is zero, or that there are

no detection devices along the adversary paths. Thus, the probability of interruption will be zero in any security event involving either removing the ^{60}Co source, or sabotaging it—resulting in detrimental consequences.

3.3 Evaluation Results for Proposed PPS for Sabotage Scenario

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Outer Burglar Gate	0	E	94	28.2
4	Open Door 1	0.9	E	148.5	44.55
5	Open Inner Burglar Gate	0	E	159.8	47.94
6	Walk through Maze	0	E	10.3	3.09
7	Sabotage Target (Equipment)	0.9	E	118	35.4
8					
9					
10					
11					
12					

Probability of Interruption:	0.51

Figure 3.2 – Sabotage result of EASI analysis for adversary path 1.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 4	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Run to Controlled Area	0.9	E	7.6	2.28
6	Open Inner Burglar Gate A	0	E	159.8	47.94
7	Open Door 2	0.9	E	148.5	44.55
8	Walk through Maze	0	E	10.3	3.09
9	Sabotage Target (Equipment)	0.9	E	118	35.4
10					
11					
12					

Probability of Interruption:	0.77

Figure 3.3 – Sabotage result of EASI analysis for adversary path 2.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 3	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Run to Controlled Area	0.9	E	7.6	2.28
6	Open Inner Burglar Gate A	0	E	159.8	47.94
7	Open Door 2	0.9	E	148.5	44.55
8	Walk through Maze	0	E	10.3	3.09
9	Sabotage Target (Equipment)	0.9	E	118	35.4
10					
11					
12					

Probability of Interruption:	0.77

Figure 3.4 – Sabotage result of EASI analysis for adversary path 3.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Remove Outer Window Burglar Bars	0	E	128.4	38.52
4	Break Window Glass	0.9	E	30	9
5	Remove Inner Window Burglar Bars	0	E	89.1	26.73
6	Jump into Room	0	E	18.3	5.49
7	Run to Controlled Area	0.9	E	7.6	2.28
8	Open Inner Burglar Gate A	0	E	159.8	47.94
9	Open Door 2	0.9	E	148.5	44.55
10	Walk through Maze	0	E	10.3	3.09
11	Sabotage Target (Equipment)	0.9	E	118	35.4
12					

Probability of Interruption:	0.81

Figure 3.5 – Sabotage result of EASI analysis for adversary path 4.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 10	0.9	E	56.5	16.95
4	Break Wall	0	E	323.1	96.93
5	Break Ceiling	0	E	79.5	23.85
6	Jump into Room	0	E	18.3	5.49
7	Walk through Maze	0	E	10.3	3.09
8	Sabotage Target (Equipment)	0.9	E	118	35.4
9					
10					
11					
12					

Probability of Interruption:	0.68

Figure 3.6 – Sabotage result of EASI analysis for adversary path 5.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 8	0.9	E	56.5	16.95
4	Remove Roof	0	E	306.7	92.01
5	Break Ceiling	0	E	79.5	23.85
6	Jump into Room	0	E	18.3	5.49
7	Walk through Maze	0	E	10.3	3.09
8	Sabotage Target (Equipment)	0.9	E	118	35.4
9					
10					
11					
12					

Probability of Interruption:	0.65

Figure 3.7 – Sabotage result of EASI analysis for adversary path 6.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds)	
			Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 3	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Run to Controlled Area	0.9	E	7.6	2.28
6	Open Door 7	0.9	E	56.5	16.95
7	Break Double Ceiling	0	E	159	47.7
8	Jump into Room	0	E	18.3	5.49
9	Sabotage Target (Equipment)	0.9	E	118	35.4
10					
11					
12					

Probability of Interruption:	0.64

Figure 3.8 – Sabotage result of EASI analysis for adversary path 7.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds)	
			Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 4	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Run to Controlled Area	0.9	E	7.6	2.28
6	Enter Wash Room	0	E	6	1.8
7	Break Double Ceiling	0	E	159	47.7
8	Jump into Room	0	E	18.3	5.49
9	Sabotage Target (Equipment)	0.9	E	118	35.4
10					
11					
12					

Probability of Interruption:	0.53

Figure 3.9 – Sabotage result of EASI analysis for adversary path 8.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 4	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Run to Controlled Area	0.9	E	7.6	2.28
6	Open Inner Burglar Gate A	0	E	159.8	47.94
7	Open Door 5	0.9	E	148.5	44.55
8	Sabotage Control Room (Equipment)	0.9	E	118	35.4
9					
10					
11					
12					

Probability of Interruption:	0.76

Figure 3.10 – Sabotage result of EASI analysis for adversary path 9.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 3	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Enter Wash Room	0	E	6	1.8
6	Break Double Ceiling	0	E	159	47.7
7	Jump into Room	0	E	18.3	5.49
8	Sabotage Target (Equipment)	0.9	E	118	35.4
9					
10					
11					
12					

Probability of Interruption:	0.52

Figure 3.11 – Sabotage result of EASI analysis for adversary path 10.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Remove Outer Window Burglar Bars	0	E	128.4	38.52
4	Break Window Glass	0.9	E	30	9
5	Remove Inner Window Burglar Bars	0	E	89.1	26.73
6	Jump into Room	0	E	18.3	5.49
7	Open Door 5	0.9	E	148.5	44.55
8	Open Door 2	0.9	E	148.5	44.55
9	Walk through Maze	0	E	10.3	3.09
10	Sabotage Target (Equipment)	0.9	E	118	35.4
11					
12					

Probability of Interruption:	0.79

Figure 3.12 – Sabotage result of EASI analysis for adversary path 11.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 10	0.9	E	56.5	16.95
4	Break Double Wall	0	E	646.2	193.86
5	Walk through Maze	0	E	10.3	3.09
6	Sabotage Target (Equipment)	0.9	E	118	35.4
7					
8					
9					
10					
11					
12					

Probability of Interruption:	0.84

Figure 3.13 – Sabotage result of EASI analysis for adversary path 13.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Climb Building	0.9	E	35.1	10.53
4	Remove Roof	0	E	306.7	92.01
5	Break Ceiling	0	E	79.5	23.85
6	Jump into Room	0.9	E	18.3	5.49
7	Walk through Maze	0	E	10.3	3.09
8	Sabotage Target (Equipment)	0.9	E	118	35.4
9					
10					
11					
12					

Probability of Interruption:	0.62

Figure 3.14 – Sabotage result of EASI analysis for adversary path 14.

3.4 Evaluation Results for Proposed PPS for Theft Scenario

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Outer Burglar Gate	0	E	94	28.2
4	Open Door 1	0.9	E	148.5	44.55
5	Open Inner Burglar Gate	0	E	159.8	47.94
6	Walk through Maze	0	E	10.3	3.09
7	Remove Target (Equipment)	0.9	E	281.3	84.39
8					
9					
10					
11					
12					

Probability of Interruption:	0.76

Figure 3.15 – Theft result of EASI analysis for adversary path 1.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 4	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Run to Controlled Area	0.9	E	7.6	2.28
6	Open Inner Burglar Gate A	0	E	159.8	47.94
7	Open Door 2	0.9	E	148.5	44.55
8	Walk through Maze	0	E	10.3	3.09
9	Remove Target (Equipment)	0.9	E	281.3	84.39
10					
11					
12					

Probability of Interruption:	0.89

Figure 3.16 – Theft result of EASI analysis for adversary path 2.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 3	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Run to Controlled Area	0.9	E	7.6	2.28
6	Open Inner Burglar Gate A	0	E	159.8	47.94
7	Open Door 2	0.9	E	148.5	44.55
8	Walk through Maze	0	E	10.3	3.09
9	Remove Target (Equipment)	0.9	E	281.3	84.39
10					
11					
12					

Probability of Interruption:	0.89

Figure 3.17 – Theft result of EASI analysis for adversary path 3.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Remove Outer Window Burglar Bars	0	E	128.4	38.52
4	Break Window Glass	0.9	E	30	9
5	Remove Inner Window Burglar Bars	0	E	89.1	26.73
6	Jump into Room	0	E	18.3	5.49
7	Run to Controlled Area	0.9	E	7.6	2.28
8	Open Inner Burglar Gate A	0	E	159.8	47.94
9	Open Door 2	0.9	E	148.5	44.55
10	Walk through Maze	0	E	10.3	3.09
11	Remove Target (Equipment)	0.9	E	281.3	84.39
12					

Probability of Interruption:	0.90

Figure 3.18 – Theft result of EASI analysis for adversary path 4.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 10	0.9	E	56.5	16.95
4	Break Wall	0	E	323.1	96.93
5	Break Ceiling	0	E	79.5	23.85
6	Jump into Room	0	E	18.3	5.49
7	Walk through Maze	0	E	10.3	3.09
8	Remove Target (Equipment)	0.9	E	281.3	84.39
9					
10					
11					
12					

Probability of Interruption:	0.85

Figure 3.19 – Theft result of EASI analysis for adversary path 5.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 8	0.9	E	56.5	16.95
4	Remove Roof	0	E	306.7	92.01
5	Break Ceiling	0	E	79.5	23.85
6	Jump into Room	0	E	18.3	5.49
7	Walk through Maze	0	E	10.3	3.09
8	Remove Target (Equipment)	0.9	E	281.3	84.39
9					
10					
11					
12					

Probability of Interruption:	0.84

Figure 3.20 – Theft result of EASI analysis for adversary path 6.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 3	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Run to Controlled Area	0.9	E	7.6	2.28
6	Open Door 7	0.9	E	56.5	16.95
7	Break Double Ceiling	0	E	159	47.7
8	Jump into Room	0	E	18.3	5.49
9	Remove Target (Equipment)	0.9	E	281.3	84.39
10					
11					
12					

Probability of Interruption:	0.84

Figure 3.21 – Theft result of EASI analysis for adversary path 7.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 4	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Run to Controlled Area	0.9	E	7.6	2.28
6	Enter Wash Room	0	E	6	1.8
7	Break Double Ceiling	0	E	159	47.7
8	Jump into Room	0	E	18.3	5.49
9	Remove Target (Equipment)	0.9	E	281.3	84.39
10					
11					
12					

Probability of Interruption:	0.79

Figure 3.22 – Theft result of EASI analysis for adversary path 8.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 4	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Run to Controlled Area	0.9	E	7.6	2.28
6	Open Inner Burglar Gate A	0	E	159.8	47.94
7	Open Door 5	0.9	E	148.5	44.55
8	Remove Target (Equipment)	0.9	E	281.3	84.39
9					
10					
11					
12					

Probability of Interruption:	0.89

Figure 3.23 – Theft result of EASI analysis for adversary path 9.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds)	
			Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 3	0.9	E	56.5	16.95
4	Open Inner Burglar Gate	0	E	159.8	47.94
5	Enter Wash Room	0	E	6	1.8
6	Break Double Ceiling	0	E	159	47.7
7	Jump into Room	0	E	18.3	5.49
8	Remove Target (Equipment)	0.9	E	281.3	84.39
9					
10					
11					
12					

Probability of Interruption:	0.78

Figure 3.24 – Theft result of EASI analysis for adversary path 10.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds)	
			Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Remove Outer Window Burglar Bars	0	E	128.4	38.52
4	Break Window Glass	0.9	E	30	9
5	Remove Inner Window Burglar Bars	0	E	89.1	26.73
6	Jump into Room	0	E	18.3	5.49
7	Open Door 5	0.9	E	148.5	44.55
8	Open Door 2	0.9	E	148.5	44.55
9	Walk through Maze	0	E	10.3	3.09
10	Remove Target (Equipment)	0.9	E	281.3	84.39
11					
12					

Probability of Interruption:	0.89

Figure 3.25 – Theft result of EASI analysis for adversary path 11.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Remove Outer Window Burglar Bars	0	E	128.4	38.52
4	Break Window Glass	0.9	E	30	9
5	Remove Inner Window Burglar Bars	0	E	89.1	26.73
6	Jump into Room	0	E	18.3	5.49
7	Remove Target (Equipment)	0.9	E	281.3	84.39
8					
9					
10					
11					
12					

Probability of Interruption:	0.55

Figure 3.26 – Theft result of EASI analysis for adversary path 12.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Open Door 10	0.9	E	56.5	16.95
4	Break Double Wall	0	E	646.2	193.86
5	Walk through Maze	0	E	10.3	3.09
6	Remove Target (Equipment)	0.9	E	281.3	84.39
7					
8					
9					
10					
11					
12					

Probability of Interruption:	0.90

Figure 3.27 – Theft result of EASI analysis for adversary path 13.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.93		487	146.1

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Jump Fence	0	E	11.1	3.33
2	Run to Building	0.9	E	15	4.5
3	Climb Building	0.9	E	35.1	10.53
4	Remove Roof	0	E	306.7	92.01
5	Break Ceiling	0	E	79.5	23.85
6	Jump into Room	0.9	E	18.3	5.49
7	Walk through Maze	0	E	10.3	3.09
8	Remove Target (Equipment)	0.9	E	281.3	84.39
9					
10					
11					
12					

Probability of Interruption:	0.82

Figure 3.28 – Theft result of EASI analysis for adversary path 14.

Conclusion

The main goal of a Physical Protection System is to prevent a successful overt or covert malevolent action through deterring, detecting, delaying, and interrupting adversary action by way of a timely response. This study consisted of evaluating the effectiveness of the existing protection system of a ^{60}Co irradiation facility using the EASI model to ascertain whether it is performing the necessary duties. From the evaluations above, it can be seen that only the entry pathways were considered. This was because the protection goal of the model was to interrupt the adversary before removing the target from its location.

The results obtained from the analysis of the existed protection system showed that results of the probability of interruption for the 14 pathways were all zero for the identified adversary pathways. By modeling a new proposed PPS meant to upgrade the system, we found a significant increase in the probability of interruption (P_I). The values increased from 0 for the original PPS to a range of 0.51 – 0.84 for sabotage scenario and 0.55 – 0.90 for theft scenario, indicating stronger security for the proposed PPS.

Lessons Learned

This work further emphasizes that the combination of deterrence, detection, delay and response make up an effective physical protection system. It was also learned that early detection, sufficient delays on adversary paths. and a quick response by respondents are necessary.

Acknowledgements

The authors are very grateful to the managements of National Nuclear Regulator of South Africa, Department of Health, Ithemba Laboratories, and the Centre for Applied Radiation Science and Technology of the North-West University for their technical support and resources for the study.

References

1. International Atomic Energy Agency - International Law Series No. 4, The International Framework for Nuclear Security, Vienna, Austria (2011).

2. ElBaradei M., Nuclear Terrorism, Identifying and Combating the Risks (2005).

3. International Atomic Energy Agency - Nuclear Security Series No. 20, Objectives and Essential Elements of a State's Nuclear Security Regime, Vienna, Austria (2013).

4. International Atomic Energy Agency - Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (Infcirc/225/Revision 5), Vienna, Austria (2011).

5. International Atomic Energy Agency - Nuclear Security Series No. 21, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material Out of Regulatory Control, Vienna, Austria (2013).

6. Crime Stats - Crime Statistics Simplified. www.crimestatssa.com/toptenbyprovince.php?showProvince=North%20West, (2014). Viewed April 1, 2015.

7. Garcia M. L., Design and Evaluation of Physical Protection Systems. Sandia National Laboratories. Second Edition, (2007).

8. The Computer Laboratory - Physical Protection, http://www.cl.cam.ac.uk/-rja14/Papers/Sev2-c11.pdf, Chapter 11 pp (366), (2014).

9. International Atomic Energy Agency - Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, Vienna, Austria, (2011).
10. Ithemba Laboratory - National Research Fund of South Africa, Transfer document of the Eldorado 78 Therapy Head to North-West University Mafikeng Campus, (2013).
11. International Atomic Energy Agency - TECDOC-1344, Categorization of Radioactive Sources. Revision of IAEA-TECDOC-1191, Categorization of Radiation Sources, (2003).
12. International Atomic Energy Agency - Preparedness and Response for a Nuclear or Radiological Emergency. IAEA Safety Standards Series No. GSR-2, Vienna Austria (2002).
13. Garcia M. L., Vulnerability Assessment of Physical Protection Systems. Sandia National Laboratories. First Edition, (2010).
14. International Atomic Energy Agency -TECDOC-1355, Security of Radioactive Sources Interim Guidance for Comment, (2003).
15. International Atomic Energy Agency - Nuclear Security Series No. 10, Development, Use and Maintenance of the Design Basis Threat, Vienna, Austria (2009).
16. Bakr W., F and Hamed A. A., Upgrading the Physical Protection System to Improve the Response to Radiological Emergencies Involving Malevolent Action, Journal of Physical Security 3(1) (2009).
17. International Atomic Energy Agency - Nuclear Security Series No. 11, Security of Radioactive Sources, Vienna, Austria (2009).

A Proposed Regulatory Requirements and Licensing Process for Physical Protection Systems of Nuclear Facilities in Egypt

Zeinab F. Akl

Nuclear Safeguards and Physical Protection Department, Egyptian Nuclear and Radiological Regulatory Authority, P.O. Box 11762, Cairo, Egypt

Abstract

Egypt has taken several steps in enhancing its nuclear regulatory framework, including developing a dedicated law to regulate nuclear and radiation activities, and establishing an independent regulatory body to ensure safe and secure nuclear and radiation activities. This body is called the Egyptian Nuclear and Radiological Regulatory Authority (ENRRA). In order to be consistent with its international commitments and accepted international practice, Egyptian nuclear law clearly states that using nuclear or radiation activities without prior authorization is prohibited. Consequently, the licensing process became an inseparable part of the Egyptian nuclear regulatory and supervisory system.

By law, ENRRA is responsible for granting, amending, suspending, and revoking licenses and setting conditions for granting them. Currently, licensing of nuclear facilities in Egypt is achieved through an integrated licensing system which includes Safety, Security, and Safeguards (the "3Ss").

This paper provides an overview of the nuclear activities and regulatory framework in Egypt, and outlines the regulatory processes which are practiced by ENRRA to regulate nuclear facilities from the nuclear security perspective. The licensing and supervision process of nuclear facilities undertaken by ENRRA, including the required licensing documentation is also described. In addition, I discuss licensing activities in regards to security in nuclear facilities, and the interface between safety and security from a licensing perspective.

Keywords: Licensing, Nuclear facilities, Physical protection systems, Regulatory body.

1- Introduction

Licensing or issuance of an authorization is defined as permission granted in a document by the Regulatory Body (RB) to a legal person who has submitted an application to carry out a practice or any other action.[1-2] The licensing process for nuclear facilities differs from State to State as it stands on the national legislative and regulatory framework as well as the regulatory approaches adopted by the State for a particular activity. The licensing process, however, is based on the common principle that the applicant must demonstrate that the proposed nuclear facility will comply with the established regulations and that it will operate safely and securely without undue risks to the health and safety of facility personnel, the population, and the environment. Depending on the national regulations and laws, the license may be a single document covering all the phases in the facility lifecycle, or a set of consecutive documents requested and issued for different phases.

Each licensing phase requires review and assessment, regulatory inspections, and milestones to proceed from one phase to the other in order to ensure compliance with the license conditions.[3-4] The licensing process enables effective regulatory control of nuclear facilities and activities in a manner that assures the safety and security of nuclear facilities.

The State's physical protection regime is an essential component of its nuclear security regime; it focuses on the prevention, detection, and response to criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities.[5] An effective national nuclear security infrastructure includes a legal, regulatory, and institutional framework; this is vital to ensure that nuclear facilities are secure against the vulnerabilities and threats anticipated, from the very initial phases of development of the nuclear program.[6] The nuclear security regulatory framework should establish applicable physical protection minimums; include a system for evaluation, licensing, and authorization; provide a system of inspection of nuclear facilities to verify compliance with applicable requirements and conditions of the license; and establish a means to enforce applicable requirements and conditions, including effective sanctions.[7]

The national physical protection regime can be established by implementing a system composed of several items including a physical protection system for each nuclear facility; development of technical standards for inspection and review; and establishment of a central control system for physical protection information.[8] A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks.[9] An effective PPS can be designed upon determination of the PPS objectives which needs to be closely related to

existing and anticipating threats. Evaluations of the PPS initial design must be undertaken so that the design can be accepted or redesigned based on the evaluation results.[10-11]

Ensuring the security of nuclear materials and associated facilities is one of the Egyptian priorities. The presence of a robust national nuclear security regulatory regime is critically important. As a result, in recent years significant progress has been made including drafting specific nuclear legislation, and establishing a national regulatory control entity which regulates the whole lifecycle of nuclear facilities.

This paper will describe the current licensing process for nuclear facilities in Egypt, covering issues related to PPS. It will also briefly discuss the physical protection requirements for nuclear facilities and the approaches taken to strengthen the safety-security interface.

2- Overview of the Egyptian Nuclear Program

Beginning in 1955, Egypt's nuclear program has included many nuclear and radiation facilities such as 2 research reactors (2 and 22 MWt), a nuclear fuel manufacturing pilot plant, a radio-isotopes production unit, and research and development facilities for nuclear fuel fabrication and hydrometallurgy.[12] There are additional miscellaneous nuclear and radiation activities as well. Recently, Egypt took concrete steps to establish its first nuclear power plants for electricity generation.

3- The Physical Protection Regulatory Framework in Egypt

It is internationally known that establishing and maintaining a legislative and regulatory framework to govern physical protection is the responsibility of the State.[5]. As a result, the Egyptian nuclear and radiation Law No. 7 of 2010, which I will refer to as "the law", has been issued.[13] This law not only covers security and physical protection, but also safety, safeguards, emergency matters, and liability for the whole peaceful applications of atomic energy.

The law establishes a single independent body, known as 'ENRRA', to carry out all regulatory and control functions related to nuclear and radiation facilities, activities, and practices in Egypt. ENRRA is mandated to ensure the safety and security of people, property, society, and the environment from the risks of exposure to ionizing radiation. ENRRA is empowered by the law to do the following:

1- Issue, modify, suspend, renew, withdraw, and rescind all types of licenses for nuclear and radiation facilities and activities in pursuance of the provisions of the law.

2- Enforce administrative closure of facilities that are using ionizing radiation in violation of the provisions of the law, its executive regulation [14], and relevant decrees.

3- Issue binding regulatory decrees and rules for licensees, to enhance and ensure the safe and secure practice, without prejudice the conditions of the granted license.

4- Review and assess the safety analysis, including reports written by the license applicant, and make appropriate regulatory decisions.

5- Carry out regulatory inspection of all nuclear and radiological practices in all phases.
Particularly for nuclear security, the law establishes what is known as "the Egyptian system of nuclear security" within ENRRA's organizational structure to ensure the existence of adequate physical protection for nuclear material and facilities. ENRRA's responsibility includes: participating in defining the anticipated threats of nuclear materials and facilities; reviewing the design of the PPS meant to defeat the anticipated threats; evaluating the performance of these systems; ensuring that appropriate measures for physical protection of nuclear facilities are taken; approving import and export activities; monitoring illicit trafficking of nuclear and radioactive material measures and procedures; and establishing the State's database for nuclear material and radiation sources in all applications.[13-14]

4- The Licensing Process of Nuclear Facilities in Egypt

Licensing of nuclear facilities in Egypt is achieved through an integrated licensing system that covers the entire lifecycle of a facility, from site preparation to decommissioning and release from regulatory control. Before any legal person can prepare a site, undertake construction, operate, decommission a nuclear facility; or possess, use, transport or store nuclear materials, a license must be issued by ENRRA. Any changes to license conditions require prior approval by ENRRA.[13] Procedures for issuing licenses and permits for safe and secure use of nuclear energy have been established by the law, and the licensing phases of the lifecycle of nuclear facilities and the requirements for each phase were defined as well.[13-14].

ENRRA issues only one license for each nuclear facility covering safety, security, and safeguards requirements. A license is conditional on the applicant having appropriate financial, technical, and human resources to meet the defined obligations. The license is issued when ENRRA is convinced of the existence of adequate protection of people and the environment. The ENRRA licensing process for nuclear facilities is depicted in figure 1.

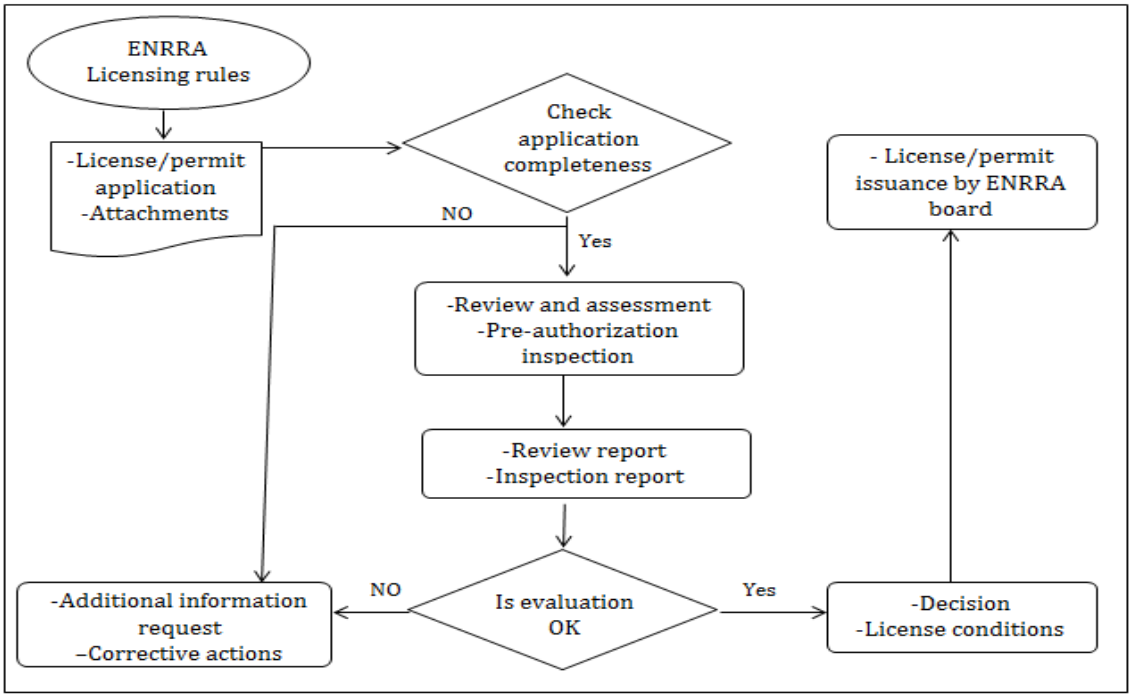

Figure 1: A schematic of the ENRRA licensing process for nuclear facilities.

The licensing process is initiated by an application provided to ENRRA that includes all required documents mandated by ENRRA licensing rules. Upon ensuring the completion of all required documents, the assessment of the information submitted by the applicant is carried out in cooperation with other concerned governmental agencies. A preauthorization inspection may be conducted by ENRRA inspectors, if needed. If the result of the assessment is in support of the application, the license conditions are put in writing and a license is issued by ENRRA board. Separate licenses are issued in sequence for each phase in the lifecycle of the nuclear facility.

ENRRA issues various permits and licenses throughout the lifecycle of the nuclear facility. At each licensing phase, an application has to be submitted to ENRRA with a number of attachments as listed in table 1. This list of needed documents, as mentioned in table 1, is a minimum list, and ENRRA by law has the right to ask for and receive additional documents and/or information to fulfill its function. Each of the different phases in the lifecycle of a nuclear facility, which appear below, are required by the law to have a license or permit.

Site approval permit

Site evaluation is an analysis of the factors that could affect safety and security of the proposed facility. A proposed site has to be adequately investigated with regard to all the site characteristics that could be significant to safety and security, including hazards associated with external natural events and with human-induced events.[15]. Requirements for site evaluation are intended to ensure adequate protection of site personnel, the public, and the environment from the effects of ionizing radiation arising from nuclear facilities. Although there are no specific requirements for physical protection documentation or requirements for facility location in the law, the scope of the investigation made by ENRRA for the proposed site of a nuclear facility covers the adequacy of the site location from a nuclear security perspective.

Construction permit

Construction is the process of manufacturing and assembling the parts of nuclear facility, carrying out civil works, providing the components and equipment, and performing associated tests. The construction processes and methods should take into account the internal and external hazards.[16] In the construction phase, the applicant has to submit a Physical Protection Plan to ENRRA. This Plan is a major document, which justifies the idea that the proposed activities will be implemented in compliance with the regulatory requirements. In the preliminary Physical Protection Plan, the licensee must describe how physical protection requirements for construction will be met. This Plan is considered a confidential document and therefore is not available for public.

Pre-operational testing permit

Pre-operational testing or commissioning is a process during which components and systems of a nuclear facility, having been constructed, are made operational and verified to be in accordance with design and performance criteria. Both nuclear and non-nuclear tests are involved.[17] A detailed program of tests must be prepared, and the responsibility for implementing and reporting on the various parts of the commissioning program has to be clearly defined

Fuel loading and approach to criticality permit

After completion of construction, installation, and commissioning, the applicant has to apply for permission to introduce nuclear material into the system and to approach criticality. This permission covers the progressive loading of fuel into the core, and taking the reactor critical for the first time. The next step is a series of low power tests aimed at demonstrating shutdown systems and the measurement of neutron production.

Table 1: Licensing phases of nuclear facilities and related documents to be submitted at each phase.

Siting	Construction	Pre-operational testing	Fuel loading and criticality approach	Operation	End of service
-Facility data -Identification of the site's legal right -Environmental impact analysis report -Site analysis report -Ministerial and concerned bodies approvals	-Site approval permit -Installation and construction schedule -Data on the companies and bodies that would oversee the installation and construction and their organizational structure -Data on the vendors and constructors -Quality Management systems of vendors and constructors -Radiological protection program -Radioactive waste management system -Preliminary safety analysis report -Preliminary emergency plan -Preliminary physical protection plan -Preliminary NMAC system -Commitment to follow ENRRA requirements	-Construction permit -Any additions or modifications introduced to the approved design - Systems performance tests results -Scheduled pre-operational test programs -Organizational structures of commissioning, testing, operation and maintenance personnel -Any additions or modifications introduced to the physical protection, emergency, NMAC system, radiological protection and radioactive waste management plans	-Construction permit -Any additions or modifications introduced to the approved design -System performance tests results -Systems performance test results -Scheduled fuel loading and criticality approach programs -Organizational structures of the personnel responsible for fuel loading and criticality approach -Data on operators -Any additions or modifications introduced to the physical protection plan, emergency plan, NMAC system, radiological protection program and radioactive waste management system	-Pre-operational testing permit -Fuel loading and approach to criticality permit -Pre-operational testing results -Final safety analysis report -Emergency plan -Physical protection plan -NMAC system -Quality management system -Operation and maintenance documents	-Safe dismantle and removal of radioactive contamination program -Radiological protection program -Radioactive waste management system -Emergency plan -Physical protection plan -NMAC system -Quality management systems -Site future uses report

Operation license

Operation is the product of successful completion of commissioning; it incorporates all activities performed to achieve the purpose for the nuclear facility, such as maintenance, in-service inspection, refueling, and other associated activities.[1] An operational license is granted after confirmation that a sufficient number of adequately trained and qualified operating personnel are available, operating instructions and procedures are issued, an effective PPS is implemented, offsite and onsite response plans have been developed, and emergency preparedness plans are in place and have been tested satisfactorily.

End of service permit

End of service includes decommissioning and release from regulatory control. Decommissioning means that administrative and technical actions had been taken to allow removal of all or some of the regulatory control. Decommissioning of nuclear facility is not just dismantling, it also includes decontamination and final shutdown.[18] In this phase, all nuclear materials are removed from the facility, but there is lot of radioactive waste, so the protection has to be commensurate with the level of the waste.[19] The release of a nuclear facility or a site from regulatory control requires, among other things, the decontamination, dismantling, and removal of nuclear material, nuclear waste, and contaminated components, and facility structures. Safety and security requirements remain in place until radiation dose levels fall below specified levels.

5- ENRRA's Licensing Approach for Physical Protection

Although there is no separate license issued by ENRRA for PPS, a dedicated approach has been taken into account during nuclear facility licensing regarding nuclear security. This is depicted in Figure 2. The cornerstone of this approach is the Design Basis Threat (DBT); ENRRA's physical protection requirements and the licensee's physical protection plan should be based on the DBT, taking into account the graded approach depending on the associated consequences. A DBT is derived from this threat assessment to facilitate the development of physical protection on the basis of a State's evaluation of the threat.[20]

The licensee must establish and implement the PPS, and develop a Physical Protection Plan, in different license phases. The licensee must describe how the PPS is designed, based on the current evaluation of the threat, and then provide the Plan to ENRRA for approval. At each phase of the licensing process, ENRRA reviews and approves the Physical Protection Plan before awarding the license or permit to the facility. Actually implementing the Plan is part of the license conditions.

The objective of review and assessment is to determine whether the applicant/licensee submissions comply with ENRRA requirements related to physical protection during a particular licensing phase, as well as during the lifetime of the facility. The areas of review for physical protection of the nuclear facility vary depending upon the phase of the licensing and the type of the facility. Joint review and assessment may be conducted by both safety and security personnel to discuss and resolve safety-security interface issues. The licensee should implement the approved Physical Protection Plan and review it regularly to ensure it remains up to date and that it reflects the current operating conditions and PPS.

Licensing nuclear facilities and activities will be useless without the necessary enforcement actions to assure that the licensees actually comply with the terms and conditions of the granted licenses.[21]. Therefore, the law gave ENRRA inspectors the right to have access at any time to any part of the facility, buildings, and other sites at which the nuclear activities are carried out. The executive regulation specifies that the facility's PPS is subject to ENRRA oversight and inspection in order to ensure its effectiveness, and it obliges the licensee to provide all necessary information to ENRRA inspectors, who will deal with such information in a secure manner.

ENRRA conducts inspections on security aspects to verify compliance with requirements, license conditions, and whether processes and procedures are properly implemented. During the regulatory inspections, the licensee is required to demonstrate that the PPS withstands the DBT and/or ENRRA requirements. Inspections are carried out at various phases of the nuclear facility, where results are considered for giving clearances for the subsequent consenting phase. ENRRA performs joint routine inspection activities for security, safeguards and safety aspects in an appropriate manner by regular and/or unannounced inspection.

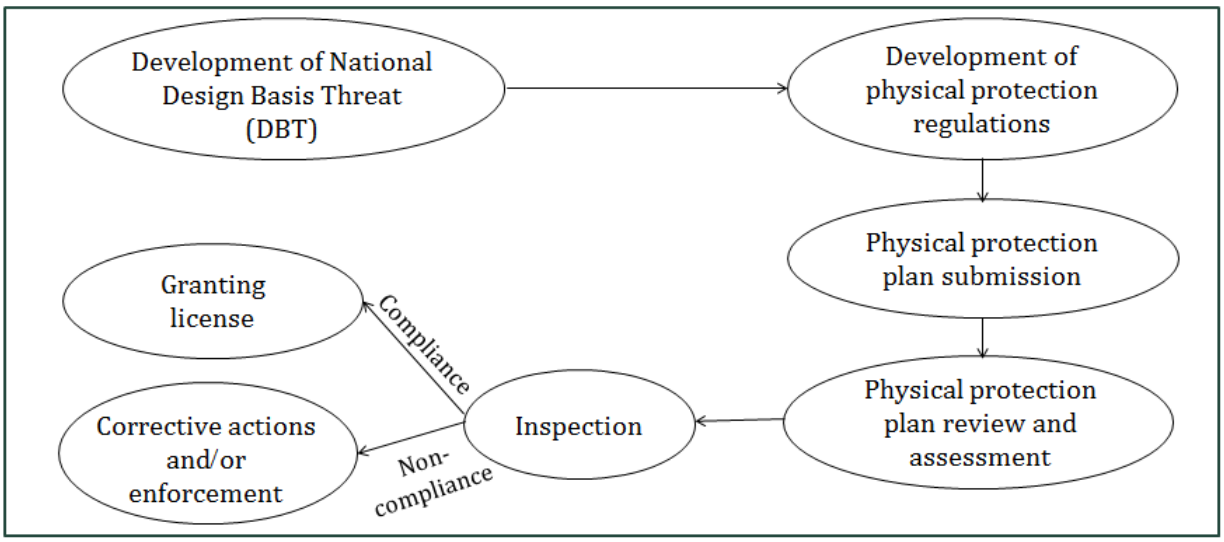

Figure 2: ENRRA physical protection licensing approach.

6- Regulatory Requirements for Physical Protection

According to the law, the license is granted only after completing the safety, physical protection, and emergency plans, which are based on ENRRA requirements for the different phases of the facility lifecycle. ENRRA currently prepares comprehensive physical protection requirements, including the licensing requirement for granting authorization, which will be applicable to all nuclear materials and facilities in the State. These requirements are prepared on the basis of the law which clearly states that ENRRA has the authority to issue binding regulatory decrees and rules for licensees in order to enhance and ensure the safe and secure practice, without prejudicing the conditions of the granted license. In addition, the executive regulation gives ENRRA the right to develop the physical protection requirements for nuclear facilities and materials in order to prevent unauthorized removal of nuclear materials and sabotage of nuclear facilities.

The requirements will be based mainly on the International Atomic Energy Agency (IAEA) recommendations on physical protection of nuclear material and nuclear facilities [7], and will contain provisions and requirements for the following:

- Licensee responsibilities.
- Nuclear material categorization and security levels.
- License applications of each nuclear material category.
- Basic requirements for the physical protection of each nuclear material category in domestic use and storage and nuclear facilities.

- Requirements for high security sites (Design Basis Threat Analysis).
- Requirements concerning protected, inner, and vital areas.
- Protection arrangements, contingency plans, and response force.
- Reports and records.
- Nuclear security culture.
- Nuclear security and nuclear safety interface.
- Information security.
- Security management.
- Security organization.
- Training of security personnel.

7- The Safety - Security Interface from a Licensing Perspective

Complementary safety and security measures have in common the aim of protecting human life/health and the environment. Measures for both safety and security must be designed and implemented in an integrated manner so that they do not compromise each other.[22]. A constant interaction between safety and security during design, construction, installation, manufacturing, operation and final disposal should be taken into consideration. In Egypt, safety and security are regulated by one regulatory authority, ENRRA, which recognizes that safety and security are different disciplines requiring their own unique expertise and methodology. Nevertheless, an understanding of each other's disciplines and requirements is the only way to grantee they will reinforce, rather than hinder each other.

In order to overcome safety- security interface issues, several efforts had been made at ENRRA to identify potentially conflicting requirements resulting from safety and security considerations in the licensing process. These will be carefully analyzed to provide an acceptable solution with respect to both safety and security. Coordination and collaboration mechanisms between safety and security within ENRRA have been established. The coordination and collaboration between safety and security divisions include performing joint inspection on nuclear facilities, and working together in enhancing both nuclear safety and security culture at the national level. When PPS upgrade is required for a nuclear facility, both safety and security personnel work together, and both safety and security requirements are jointly considered. In addition to that, safety and security regulations are developed and reviewed by a joint team before issuance in order to assure there is conflict between them, and to avoid incompatible requirements or contradictory compliance expectations.

Another important area of the safety-security interface is emergency and contingency planning. Emergency Plans are generally generated to deal with the consequences of a radiological event, and are formulated in the context of a radiological release to the environment outside the reactor facility and/or off-site resulting from an accident. A Contingency Plan, in contrast, generally generated to deal with security related events. At ENRRA, a continuous cooperation and discussion between nuclear security and emergency personnel is already in place. Furthermore, the regulatory requirements of each section are investigated by the other. Moreover, at the facility level, joint exercises, which simultaneously test emergency and contingency plans, are carried out at intervals compatible with the level of threat; this is done to assess and validate the adequacy of the interfaces and the response coordination between the safety and security sections.

8- Conclusion

Since 1955, Egypt has owned and operated a number of nuclear facilities including different categories of nuclear materials. A single independent nuclear regulatory body called "ENRRA" is in place performing the whole set of regulatory and control functions covering safety, security, and safeguards. ENRRA established a robust mechanism to license the nuclear facilities and materials from a nuclear security perspective. ENRRA is currently developing physical protection requirements, taking into consideration the IAEA recommendations and international best practices. Coordination and collaboration mechanisms between safety and security sectors are in place to manage issues in the area of the safety-security interface.

References

1- IAEA, Safety Standards Series No. SSG-12, Licensing process for nuclear installations, Vienna, Austria (2010).

2- IAEA, Safety Glossary, Terminology use in nuclear safety and radiation protection, 2007 Edition, Vienna, Austria (2007).

3- IAEA, Safety Series No. 115, International basic safety standards for protection against ionizing radiation and for the safety of radiation sources, Vienna, Austria (1996).

4 - A. Alonso, S.K. Sharma, D.F. Torgerson, Licensing for nuclear power plant siting, construction and operation, infrastructure and methodologies for the justification of nuclear power programmes, A volume in Woodhead Publishing Series in Energy, (2012).

5-IAEA, Nuclear Security Series No. 20, Objective and essential elements of a state's nuclear security regime, Vienna, Austria (2013).

6- IAEA, Nuclear Security Series No.19, Establishing the nuclear security infrastructure for a nuclear power program, Vienna, Austria (2013).

7 - IAEA, Nuclear Security Series No. 13, Nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/Revision 5), Vienna, Austria (2011).

8- Hosik Yoo, Sung-Woo Kwak, Sung Soon Jang, Jae-Kwang Kim, Jung-Soo Kim, Wan-Ki Yoon, A roadmap for establishing the physical protection regime of nuclear materials and facilities, Transactions of the Korean nuclear society spring meeting, Korea, May 10-11, (2007).

9- ML Garcia, Design and evaluation of physical protection systems, Butterworth-Heinemann, USA, (2001).

10- M.L. Garcia, Vulnerability assessment of physical protection systems, Butterworth-Heienmann, USA, 2006

11- P. Xu, Y.Deng, X. Su, X.Chen, S. Mahadevan, An evidential approach to physical protection system design, Safety Science, 65, 125-137 (2014).

12- A. I. M. Aly, The Egyptian experience on nuclear and radiation legislations, International Journal of Nuclear Law, 2, (2009).

13- Egypt, Law no. 7, The law for organizing nuclear & radiation activities, Amiri Presses, Cairo, Egypt (2010).

14- Egypt, Executive regulation of the Law no.7, Amiri Presses, Cairo, Egypt (2011).

15- IAEA, Safety Standards Series No. Ns-R-3, Site evaluation for nuclear installations safety requirements, Vienna, Austria (2003)

16- IAEA, Safety Standards Series No. SSG -38, Construction for nuclear installations, Vienna, Austria (2015).

17- IAEA, Safety Series No. 50-SG-04, Commissioning procedures for nuclear power plants, Vienna, Austria (1980).

18- M. Laraia, nuclear decommissioning: planning, execution and international experience, Woodhead publishing series in energy: number 36, Woodhead publishing limited, UK, (2012).

19 - E. Uspuras, S. Rimkevicius, E. Babilas, Licensing documentation and licensing process for dismantling and decontamination projects in Lithuania, Progress in Nuclear Energy 84, 41-49 (2015).

20- IAEA, Nuclear Security Series No. 10, Development, use and maintenance of the design basis threat, Vienna, Austria (2009).

21- C. Stoiber, A. Bear, N. Pelzer, W. Tonhauser, Handbook on nuclear law, IAEA, Vienna, Austria (2003).

22- IAEA, International nuclear safety group, INSAG-24, The interface between safety and security at nuclear power plants, Vienna, Austria (2010).