Argonne NATIONAL LABORATORY

The Journal of Physical Security

Volume 7(2), 2014

JPS

THIS ISSUE...

Editor's Comments

NM Waid & MH Nassef, "Preliminary Plan for Reviewing the Physical Protection of Nuclear Facilities in Egypt", pages 1-11

N Terao & M Suzuki, "A Probabilistic Extension of the EASI Model", pages 12-29

MC Echeta, LA Dim, OD Oyeyinka, & AO Kuye, "PPS Evaluation of An Oil Refinery Using EASI Model", pages 30-41

B Nkom, II Funtua, & LA Dim,"Design of an Access Control System: A Paradigm for Small Nuclear Facilities", pages 42-49

M Coole & DJ Brooks, "Do Security Systems Fail Because of Entropy?", pages 50-75

Table of Contents

Journal of Physical Security, Volume 7(2), 2014

Editor's Comments, pages i-ix

Paper 1 - NM Waid and MH Nassef, "Preliminary Plan for Reviewing the Physical Protection of Nuclear Facilities in Egypt", pages 1-11

Paper 2 - N Terao and M Suzuki, "A Probabilistic Extension of the EASI Model", pages 12-29

Paper 3 - MC Echeta, LA Dim, OD Oyeyinka, and AO Kuye, "PPS Evaluation of An Oil Refinery Using *EASI* Model", pages 30-41

Paper 4 - B Nkom, II Funtua, and LA Dim, "Design of an Access Control System: A Paradigm for Small Nuclear Facilities", pages 42-49

Paper 5 - M Coole and DJ Brooks, "Do Security Systems Fail Because of Entropy?", pages 50-76

Editor's Comments

Welcome to volume 7, issue 2 of the Journal of Physical Security. This issue has papers about security evaluations of Egyptian nuclear facilities, a probabilistic model for quantifying the odds of interrupting an attack, a security evaluation for an oil refinery in Nigeria, access control for small nuclear facilities, and entropy as a driver of security failures.

For the last paper in this issue, we had the interesting situation where the reviewers, the editor, and the authors couldn't come to an agreement on possible changes to the paper. This resulted in a discussion at the end of the paper that you won't want to miss because of its larger implications. I hope you find it thought provoking.

As usual, the views expressed by the editor and authors are their own and should not necessarily be ascribed to their home institutions, Argonne National Laboratory, or the United States Department of Energy.

*****

JPS & Peer Review

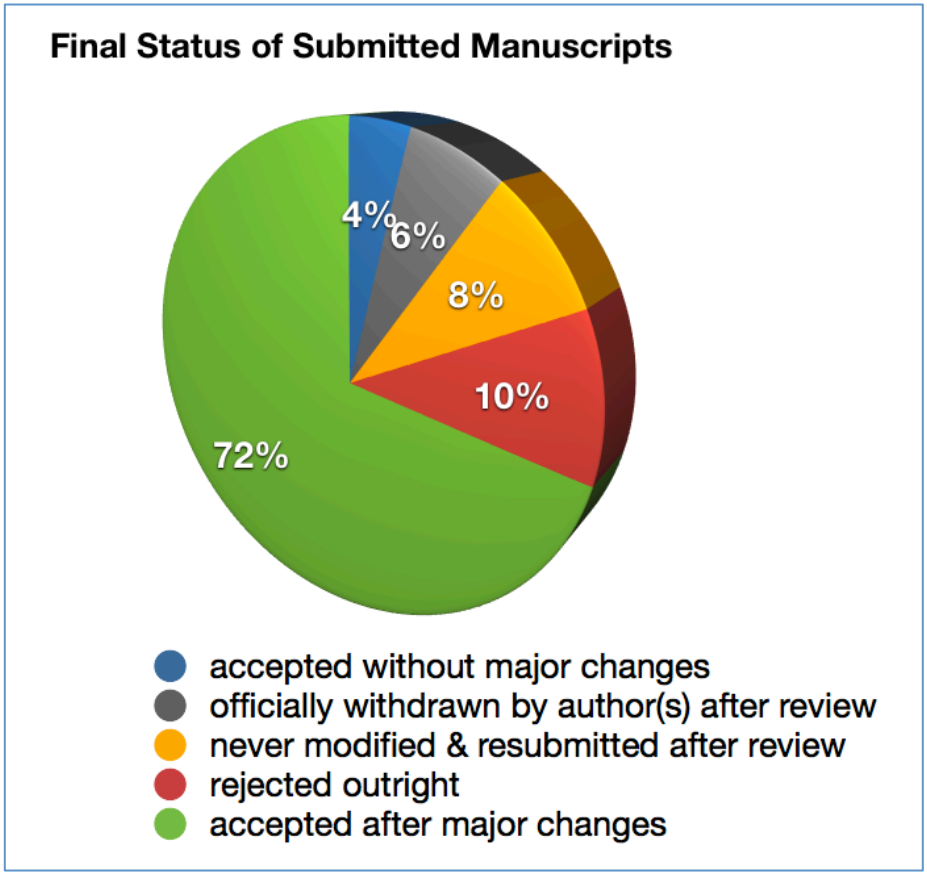
Research manuscripts submitted to this journal are usually reviewed by 2 anonymous reviewers knowledgeable in the subject of the paper. Viewpoint papers are reviewed by 0, 1, or 2 reviewers, depending on the topic and content. (Papers that receive no peer review are clearly marked as such.)

The authors' identities are known to the reviewers, i.e., this journal does not use a double blind review system. This is the case for most peer review journals in other fields. There are pros and cons to this single blind approach.

We are always very grateful to reviewers for their (unpaid) time. Serving as a reviewer is a real service to your security colleagues and to everybody's security. If you are interested in serving as an occasional reviewer, please contact me through Argonne National Laboratory or http://jps.anl.gov.

Dr. Jon Warner of our Argonne Vulnerability Assessment Team serves very capably as Associate Editor.

The pie chart below shows that almost ¼ of manuscripts submitted to JPS do not get printed in the journal. The vast majority of manuscripts that are accepted undergo significant changes or additions suggested by the reviewers and the editor prior to being published. I often assist with editing papers for authors for whom English is not their first language, or who are from the UK.



The standard style of this journal is American English. This includes, among other things, putting a comma before the last item in a list, the so-called "serial comma", also ironically called the "Oxford comma". (Not all Americans do this, however, especially journalists and young people.) Here are 2 examples of where the serial comma can be important:

"*My favorite sandwiches are tuna, ham, and cheese.*" refers to 3 sandwiches, whereas "*My favorite sandwiches are tuna, ham and cheese.*" is focused on 2.

"*I got the idea from talking to my boss, a convicted felon, and a drug addict.*" has quite a different meaning from "*I got the idea from talking to my boss, a convicted felon and a drug addict.*"

While there are counter-arguments, in my mind there are 2 good reasons for use of the serial comma. First, is consistent with the general idea of parallelism, an important element of good writing. Good writing has rhythm and organization, and you don't want to confuse the reader or squander her time by breaking them. One example of good parallelism is writing a list using only nouns or only verbs or only gerunds. Mixing them creates clumsy wording, such as: *"I like to fish, pancakes, and talking to art experts.*" A better sentence might use all gerunds for parallelism: *"I like fishing, eating pancakes, and talking to art experts."*

The second reason the serial comma is useful is that it most closely mimics oral speech, which is really the underlying basis of the written word. To a considerable degree, good writing sounds like good talking. Some writers claim that commas clutter up writing. While commas can certainly be overused, I think they actually make reading easier—and the meaning clearer—when used to mimic the natural pauses in oral speech. Thus, if I really meant 3 sandwiches, the way I say this is "*tuna..ham..and..cheese*", but if I meant 2 sandwiches, "*tuna……ham & cheese*. The comma can help the reader understand where the pauses should be.

*****

Voting for Security Theater

I recently observed a nearly 2-hour training course for election judges. The course was taught by state election officials for a single election jurisdiction. The state and jurisdiction shall go unnamed.

The course was efficient, practical, professionally run, and well tuned to the audience. A lot of useful information was provided to the election judges.

I found it telling that the word "security" made an appearance only once in the 2-hour presentation, and then only in the following context: "Election judges should follow this procedure because it *gives the appearance* of security." [Italics added.]

Now I'm quite familiar with Security Theater. As a vulnerability assessor, I see it all the time in disparate security devices, systems, and programs. But usually Security Theater involves security managers or organizations fooling themselves, or it is busywork deliberately designed to make auditors or the boss happy, or it's something meant to snow customers or the public. Sometimes, Security Theater is used as a form of bluffing, i.e., to make a target falsely look harder than it really is. (Bluffing, however, is usually effective only over the short term.)

The procedure that was being discussed in the course as needing the appearance of security was not one that would be much noted by voters or the public, so it was probably not intended as a bluff. Rather, the apparent attitude among these election officials—which I and others have frequently observed in other contexts, states, and election jurisdictions—is that security is viewed as only being about appearances.

One of the functions of election judges is often to compare voters' signatures on election day with the voter registration records. In this particular state and election jurisdiction, as in most others, election judges are given zero useful instructions on how to compare signatures, not even the brief, rudimentary training often given to cashiers in retail stores on signature verification.

In my view, the veracity of the vote deserves more serious security attention. Election fairness and accuracy are fundamental principles of democracy.

*****

Faking it Artistically

Counterfeit works of art and antiquities are a huge security problem. A new technique has been deployed, based on the anomalously high amount of radioactive carbon-14 found in the atmosphere since the dawn of the nuclear age. A painting attributed to the French cubist painter Fernand Léger was clearly proven to be a forgery. For more information: http://www.chromatographytechniques.com/news/2014/03/carbon-dating-shows-cubist-painting-was-forged?et_cid=3815889&et_rid=396957192&type=headline

*****

Compliance vs. Security

Compliance and Security, of course, are not the same thing. Sometimes they are at odds. In my experience, it is typical for at least a third of compliance rules to actually make security worse. This can occur when compliance wastes time, energy, and resources; distracts security personnel and employees and focuses them on the wrong issues; makes auditors the enemy, instead of the actual adversaries; encourages mindless rule following rather than careful proactive thinking about security; institutionalizes stupid, one-size-fits-all rules mandated by bureaucrats far removed from ground level; fossilizes rules that need to be flexible with changing threats, conditions, and technology; lets the good guys and the existing security infrastructure and security strategies define the problem, not the bad guys (which is the real-world situation); makes security the enemy of productivity and of employees; and engenders cynicism about security.

The best (and funniest and most disturbing) examples I know of compliance harming security can't be openly discussed because of their sensitivity. Here, however, are a few examples I can share.

- Granting access to numerous auditors, overseers, micro-managers, testers, maintenance people for security hardware, and checkers of the checkers increases the insider threat.
- Mandated State of Health (SOH) checks on security hardware increases complexity (bad for security) and hacking opportunities.
- Mandated security devices get in each other's way, or compromise each other's security.
- Specifically mandated security products or anti-malware software preclude the use of better, more up to date products.
- PC security rules applied mindlessly to Macs.
- Compliance makes the best the enemy of the good.
- Almost anybody is considered to have a "Need to Know" if it can help us avoid minor procedural and paperwork errors (or he/she can offer some vaguely plausible story

line), thus creating unnecessary checkers and increasing the insider threat as well as the chances of mishandling sensitive data.
- Government security clearances that require self-reporting of professional counseling and mental health treatment, thus discouraging it.
- Grievance, complaint resolution, and employee assistance programs that increase disgruntlement and target users for retaliation.
- Formal rules requiring overly predictable guard patrols and shift changes.
- Little room allowed for flexibility, individual initiative, proactiveness, questions/concerns, hunches, resourcefulness, observational skills, and people skills.
- Security managers are fearful of installing additional security procedures and hardware (even common sense ones) that can improve security locally because they are not called for by auditors or the compliance documents.
- An over-emphasis on fences (4.5 – 15 sec delay) and entry points as security measures leads to bad security.
- The required complex multitude of security layers ("Defense in Depth") leads to a situation where nobody takes any one layer (or alarm) seriously. See, for example, the Y-12 break-in by an 85-year old nun: http://www.cbsnews.com/news/nun-84-gets-3-years-in-prison-for-breaking-in-nuclear-weapons-complex/ This is a classic, predictable, and very common mode of failure for Defense in Depth ("layered security"). Unfortunately, multiple layers of lousy security rarely add up to good security. And Defense in Depth tends to engender acceptance of lousy layers.
- The wrong mindset is created: Security = Busy Work & Mindless Rule-Following, leading to the idea that the Brass and bureaucrats are responsible for thinking about security, not me.

*****

Criminy!

Recent events in Crimea are a reminder that 2014 is the 160th anniversary of the Crimean War, a conflict between Russia and an alliance of France, Britain, the Ottoman Empire, and Sardinia. It was one of the first "modern" wars in a number of ways.

The Crimean War is probably best remembered for the incompetence and unnecessary loss of life on both sides. At the time, British citizens could buy a commission, i.e., British military leaders were not chosen by merit, intelligence, or experience but by who could cough up big bucks. The poem, "Charge of the Light Brigade" by Alfred, Lord Tennyson based on the Crimean war helped to focus attention on the incompetence of English military leaders, which eventually resulted in ending the practice of selling commissions.

Now, 160 years later, many security professionals are all too familiar with the negative consequences of having leaders who are not chosen based on merit, intelligence, and experience.

*****

Uncommon Common Sense

As of this writing, there is as of yet no solution to the mystery of missing Malaysia Airlines Flight 370.

What has become clear from this incident, however, is that many nations and airlines do not make use of the Interpol database of stolen passports. This database contains data on 40 million lost or stolen travel documents. According to Interpol General Secretary Ronald Noble, "Only a handful of countries worldwide are taking care to make sure that persons possessing stolen passports are not boarding international flights." Even so, the database gets 60,000 hits per year. The United States, UK, and the United Arab Emirates are some of the few countries that do use the database extensively.

A 2011 study found that the database can be an effective tool for counter-terrorism. See http://research.create.usc.edu/cgi/viewcontent.cgi?article=1147&context=published_papers

This countermeasure is quick, simple, inexpensive, and relatively painless. Failure to use it is surely a breakdown of common sense. What is it about security that it is so often divorced from common sense? Or is the problem, as Voltaire thought, more generic? He maintained that the trouble with common sense in general is that it isn't all that common.

*****

Dumber Than the Hardware

A would-be burglar in Chicago defeated the lock on the outside of a bar, but then couldn't manage to get inside because he kept trying to pull the door open. The door was clearly marked, "PUSH". See the video and story at:
http://www.dnainfo.com/chicago/20140115/wicker-park/video-wicker-park-bar-break-in-thwarted-when-man-pulls-door-marked-push

*****

Mexican Threat

Apparently packs of roaming feral Chihuahua dogs are harassing Phoenix. The Phoenix police department reports more than 6,000 complaints. For more information, see http://abcnews.go.com/blogs/headlines/2014/02/chihuahuas-rampage-in-arizona/
Seems like an excellent opportunity to install $10 billion of untested homeland security hardware to monitor the Chihuahua threat!

*****

Canadian Threat

Ottawa police are searching for a man who tried to rob a store while brandishing a hockey stick. The owner of the store grabbed the hockey stick from the suspect, who then fled. See http://www.cbc.ca/news/canada/ottawa/hockey-stick-wielded-in-foiled-ottawa-store-robbery-1.2559383.

Presumably it wasn't a curling broom because curling doesn't exactly have a fierce reputation for bench-clearing brawls. (This might, however, increase the fan base.)

Speaking of Olympic sports, the best suggestion I have ever heard is to require that every Olympic event include one average citizen in the competition, just for comparison.

*****

Bad Joke, Good Security Moral

A young man on a bicycle has a bag of sand slung over his shoulder. He rides up to the border guard who stops him and asks, "What's in the bag?". "Sand," says the young man. The guard doesn't believe him, so makes the young man open the bag and the border guard feels around inside. Sure enough, sand. The guard lets the young man go on his way across the border.

The next day, the same thing happens, only this time, the guard insists the young man empty the bag of sand on the ground so the guard can more carefully examine its contents. Again, nothing but sand. The young man hand shovels the sand back into the bag and pedals across the border. This happens 3 more days in a row.

Growing more and more suspicious, the border guard the next day takes a sample from the young man's bag to be chemically analyzed. For another week, the young man shows up everyday on his bike with the bag of sand slung over his shoulder, and the guard lets him through. Finally, the chemical analysis results come in: 100% sand.

The next day, the guard stops the young man again and says, "Look, son. I know you are smuggling something across the border. I'm dying to know what it is. Just tell me, and I swear on my mother's grave that I won't turn you in. So what are you smuggling?"

"Bicycles," says the young man.

*****

Some Inconvenient Truths About Security

1. If you can't envision security failures, you can't prevent them.

2. If you are not failing in testing your security, you are not learning anything.

3. If you automatically think of "cyber" when somebody says "security", you probably have poor physical security *and* poor cyber security.

4. Most security devices can be compromised in as little as 15 seconds. This can be done at the factory, the vendor, while in transit, while sitting on loading docks, prior to installation, and after installation. This is why a solid chain of custody is needed, starting right at the factory, and why security devices must regularly be carefully examined internally for tampering or counterfeiting. But you have to know what the device is supposed to look like.

5. A chain of custody is a *process* for securing important assets in transit. It is <u>not</u> a piece of paper (never to be examined) that arbitrary people scribble their initials or signatures on!

6. Many manufacturers and vendors of security devices have poor security and poor security culture at their facilities.

7. A mechanical tamper switch or a light detector in a security device is about the same thing as having no tamper detection at all. Moreover, during the time that the device lacks power (such as during shipment), they provide zero security.

8. If you aren't secure before you deploy encryption, you aren't secure after.

9. Encryption has no meaningful role to play in checking product authenticity. It is a red herring.

10. Random, virtual numeric tokens are not the same thing as serialization for detecting counterfeit products. The few companies that use random virtual numeric tokens usually make a number of errors in doing so.

11. Tamper-indicating seals do not magically detect or stop tampering. They take a lot of hard work to be effective.

12. Most organizations ignore or substantially underestimate the insider threat.

13. If you're not making an intense effort to mitigate the disgruntlement of employees, contractors, customers, and vendors, then you are putting yourself at great risk.

14. If the manufacturer or vendor of a security product can't or won't tell you the half dozen most likely ways the device or system can be attacked, you shouldn't buy it.

15. Relatively low tech attacks work well, even on high-tech security devices, systems, and programs.

16. If you think that threats and vulnerabilities are the same thing, or you think that you know all your vulnerabilities (or don't have any), or you think a vulnerability assessment is a test you can pass, then you don't understand vulnerabilities, vulnerability assessments, or your security.

17. Confidence in a security program or security product is almost always wishful thinking. Or as the old adage says, "Confidence is that feeling you sometimes have before you really understand the situation."

18. If you are more worried about compliance than security, you almost certainly have poor security.

19. If people can't question your security without you (or your organization) getting upset, you probably have poor security.

20. "Over-seriousness is a warning sign for mediocrity and bureaucratic thinking. People who are seriously committed to mastery and high performance are secure enough to lighten up." -- Michael J. Gelb

*****

Everybody has a price. If not, everybody has a weakness.
-- Michelle Bulleri

*****

--Roger Johnston
Argonne National Laboratory
LinkedIn: http://www.linkedin.com/in/rogergjohnston
VAT URL: http://www.ne.anl.gov/capabilities/vat
Journal of Physical Security: http://jps.anl.gov
March 2014

Preliminary Plan for Reviewing the Physical Protection of Nuclear Facilities in Egypt

*Nawal M. Said[1,3] and *M.H. Nassef[2,3]

[1]El Taif University, Faculty of Science, Physics Department
[2]King Abdulaziz University, Faculty of Engineering, P.O. Box.80204, Jeddah 21589, Saudi Arabia, Phone: +0567102821, Fax: +26952648
[3]Nuclear and Radiological Regulatory Authority, (NRRA) Cairo, Egypt
*On leave from NRRA-Egypt

Abstract

The main objective of a physical protection system (PPS) is to prevent radiological sabotage of the nuclear facility and theft of nuclear materials. This paper describes a procedure for effective physical protection of nuclear facilities, as will as physical protection of nuclear materials (NMs) in use, storage, and transport. The procedure involves categorizing the nuclear facility targets and how to protect them. We then propose a preliminary plan for a site visit for the purpose of evaluating the PPS, and ensuring that it is in compliance with the International Atomic Energy Agency (IAEA) standards, the International Physical Protection Advisory Service (IPPAS) guidelines, and also meets the necessary conditions set out in Egyptian regulations (licensing) of the facility. The implementation of this plan could strengthen physical protection of Egyptian nuclear facilities.

Key words; *Nuclear facility Physical protection, IAEA- IPASS mission, Inspection plan*

1. Introduction

National practices for what is called "physical protection" of nuclear materials vary widely. Some states have obligated themselves to apply IAEA recommendations for such protection, but others have only agreed to give consideration to those recommendations, or have made no commitment at all. Some have adopted domestic regulations with requirements as high or higher than these recommendations, but others has adopted lower standards, including none at all.[1]

According to Article III of the Non-Proliferation Treaty (NPT), each non-nuclear weapon state that is party to the treaty agrees to accept safeguards as set forth in an agreement to be negotiated and concluded with the International Atomic Energy Agency (IAEA) in accordance with the state's statutes and safeguards system. The purpose of such IAEA safeguards is to verify the fulfillment of the state's obligations under the NPT to prevent diversion of nuclear energy from peaceful uses to nuclear weapons or other nuclear explosive devices. As such, IAEA "safeguards" constitute the most important example of multinational nuclear treaty monitoring.

By the IAEA's own definition, the IAEA safeguards system comprises an extensive set of technical measures by which the IAEA Secretariat independently verifies the correctness and the completeness of the declarations made by states about their nuclear material and activities. While this definition goes a long way in describing the safeguards process from the point of view of the IAEA, it fails to describe concisely and substantively the intentions (and limitations) of IAEA safeguards. To add to the confusion over the term "safeguards", the United States government uses the word "safeguards" in a rather imprecise way, often in combination with "security", to cover a wide range of *domestic* nuclear non-proliferation activities, from physical protection and containment to accounting for nuclear material, grouped under the heading of "Material Protection, Control & Accounting" (MPC&A). It is not surprising, therefore, that many observers complain that a clear, concise, and consistent definition for safeguards is still missing.[2]

As a result, there may be a risk not only of mixing the meaning of the different safeguards terms, but also of confusing the distinct goals of each nuclear security measure implemented. There is a long tradition of the IAEA using domestic (usually U.S.) safeguards technology and approaches with little or no modification for use in IAEA international safeguards.

Domestic and international safeguards—despite both being called "safeguards"—are profoundly dissimilar. Domestic safeguards are primarily concerned with nuclear materials protection, control, and accounting (MPC&A). This includes protecting nuclear weapons or materials from sabotage, vandalism, terrorism, espionage, theft, diversion, or loss. International NPT safeguards, on the other hand, are concerned with obtaining evidence that each state that signed an agreement or treaty is indeed complying with its obligations, declarations, and promises. Most of the "safeguards" currently undertaken by the IAEA involve monitoring under the NPT.[2]

2. Improvement of Nuclear Legislation in Egypt

Egypt started its legal framework to control and regulate the peaceful uses of nuclear energy with Law No. 59 in the year 1960. On 30 March 2010, the Government of Egypt issued a new comprehensive law governing nuclear and radiation related activities (Law No. 7 of 2010). This new law aims to establish a legislative framework for nuclear installations and activities in order to protect individuals, the environment and property. It regulates radiation protection, nuclear safety, radioactive waste management, transport of radioactive material, emergency preparedness and response, nuclear security, nuclear safeguards, import and export controls, and civil liability in the case of nuclear damage. The law also has the power to deal with all activities and financing mechanisms covering the decommissioning process for the nuclear reactors.[3]

According to the new Law, all the radioactive and nuclear activities are controlled under the independent regulatory body, the Nuclear and Radiological Regulatory Authority (NRRA). The NRRA is responsible for issuing licenses and permits for any activity involving radioactive materials, and for controlling and verifying that these activities are performed within the NRRA regulations. In our view, the new law has helped Egypt be in compliance with international safety and security standards.

NRRA Licenses cover the following nuclear activities in Egypt:

- Research Reactors (ET-RR-1 & ET-RR-2)
  - A: Reactor Operator
  - B: Fuel Fabrication Plant for ET-RR-2
- Nuclear Power Plant and Related Activities
- Accelerators (Cyclotron & Linear Accelerator)
  - A. Industrial Irradiator
- Applications of Radioisotopes in Industry, Medicine, Agriculture, and Research
- Radioactive Waste Disposal Facility and Treatment Plant
- Transportation of Radioactive Materials.

The Nuclear safeguards agreements between Egypt and the IAEA have been concluded pursuant to NPT. A state system of accounting for and controlling of nuclear material in Egypt has been established under the title of "A National System of Nuclear Material Accounting and Safeguards (NSNMAS)". [4]

A physical protection system (PPS) for nuclear materials (NMs) in nuclear research reactor (NRR) facilities provides measures for external protection, administrative control, guards, entry and access control, safety, and protection for transport and personnel.[5] These measures are applied during the operation or the decommissioning of the facility. Since the operator is responsible for operational safety and the physical protection of the nuclear facility, the operator must ensure that all nuclear materials belonging to it, including waste, is stored in specially designed containers. The operator is obliged to establish and apply an accounting system for nuclear materials, and to exercise control in accordance with the requirements laid down in the safeguards agreement. Such accounting is a part of the physical protection system.[6]

In this study, the physical protection system (PPS) for one of the two declared nuclear facilities in the Anshas zone in Egypt was investigated. The PPS under investigation belongs to the old Egyptian nuclear reactor (ET-RR-1), which was the first Egyptian nuclear research reactor (NRR) having a material balance area (MBA):ET-A. The ET-RR-1 is a 2 MW research reactor, tank type, with distilled water as a moderator coolant, and utilizing a reflector. The nuclear fuel used in this reactor is type EK-10 of Russian fabrication. The fuel rods are made of uranium dioxide dispersed in magnesium matrix, enriched by 10% ^{235}U in the form of rods cladded by an Al jacket.[7]

3- Basic Concept of Physical Protection

According to the IAEA recommendations and the Egyptian regulations on the physical protection of nuclear materials, PPS's must deal with the following issues:

a- Categorizing of nuclear materials
b- Determining the protected and controlled areas
c- Controlling the access of persons and vehicles
d- Managing the security of workers
e- Providing a data information and analysis unit

A physical protection plan is part of the reviewed documentation necessary for issue of the license given by NRRA. The plan must take in account all requirements related to the PPS according to the specifications of INFCIRC/225/Rev.4 and also the IAEA-IPPAS guidelines, which deal with categorization of the nuclear facilities, nuclear materials, and radioactive waste.[8,9] Because nuclear materials (NMs) can be found in different physical, morphological, and chemical forms, the attractiveness of these materials for theft or sabotage depends crucially on their specific nature and properties. Thus, the primary factors for determining the physical protection measures against unauthorized removal or sabotage of NMs must be the status and nature of the NM itself. Table 1 shows the type of nuclear material as categorized by the IAEA conventions on physical protection, specifically INFCIRC/274/rev.1 and INFCIRC/225/rev.3.[10-12]

3.1. Physical Protection of the NRR

Since the nuclear materials contained in the two Egyptian nuclear research reactors are classified as category II and III, both reactors are protected by designed PPSs involving barriers and inner areas, delay components, access control, and assessment systems to defeat theft or sabotage attempted by one or more persons from outside or inside the plants (MC&A). All the equipment and nuclear materials of category II are located in the controlled area, while the equipment and nuclear materials of category III are located in the protected area.

Table 1: Categorization of Nuclear Material.

Material	Form	Category I	Category II	Category III
Plutonium	Un-irradiated	≥2 kg	>500 g <2 kg	>15 g ≤500 g
Uranium-235	Un-irradiated Uranium enriched (EU) to 20% ^{235}U	≥5kg	>1 kg <5 kg	>15g ≤1 kg
	EU to 10% but < 20% ^{235}U		≥10 kg	≥1 kg <10 kg
	EU above natural, but < 10% ^{235}U			≥10 kg
Uranium-233	Un-irradiated	≥2 kg	>500 g < 2 kg	>15 g ≤500 g
Irradiated Fuel*			depleted or natural U, Th, or low enriched fuel > 10% fissile	

*The categorization of irradiated fuel in the table is based on the international transport considerations. The state may assign a different category for domestic use, storage, and transport taking all relevant factors into account.

The first Egyptian Nuclear Research Reactor (ET-RR-1) has been in operation since 1961. Provisions were made for the facility geographical location, the safety design, the access to vital areas, and the State's assessment of the threat. The PPS was upgraded and some new technical components were introduced, such as a perimeter barrier: a peripheral fence has been built around the nuclear facility as a second barrier. The first barrier is the original fence of the Nuclear Research Center (NRC-EAEA), where authorized personnel are allowed to entry or exit through the main gate.

In addition to fences, there are intrusion sensors, alarms, a lightning system (in order to ensure functioning of the surveillance 24 hours a day), and entry control (the access of personnel to the NRR facility is controlled through a personnel entry/exit port located near a local security guard). Authorized personnel are granted entry to the NRR facility only after registering and signing in on an registration book. There is also video surveillance to monitor the inner areas, and an integrated alarm system with ultrasonic sensors to detect the movement of an intruder within the interior of a specific inner area inside the NRR facility. The NRR facility fence is provided with a local security control center, guards, communication equipment, and is in direct contact with the main guard and security center. Also, the fence has video cameras allowing complete visibility of the fence zone.[13]

For ET-RR-2, the physical protection system was installed and operational in 1997. As with ET-RR-1, the PPS is maintained by a technical group. The ET-RR-2 facility is monitored 24 hours a day. Also, as part of the upgrades, the PPS responsible staff and regulatory body staff received training in the physical protection of nuclear materials and facilities. This was done via the International Training Course (ITC) on the Physical Protection of Nuclear Facilities and Materials, conducted at Sandia National Laboratories in the USA under the umbrella of IAEA. The course was first offered in 1978. The course focuses on a systems engineering performance–based approach to requirements, definition, design, and evaluation of physical protection systems. In addition to providing important information and experience, the course is helpful in improving the cooperation of facility personnel. During the first 21 presentations of ITC (the years 1987 through 2010), 20 participants from Egypt were trained.[14]

3.2. Procedure for an Effective Physical Protection System

Ensuring the physical protection of NMs during use, storage, and transportation is one of the obligatory requirements to be met in Egypt in order to get licensed for design and operation of nuclear facilities. A physical protection procedure for inspection and for reporting must be submitted. This procedure contains a listing of numerous elements that need to be evaluated in order to improve the existing PPS and help to devise new plans for the physical protection requirements. The procedure that we recommend, which we call our "check list", deals mainly with the following:

- Determining the possible threats to the NRR, NMs, and the fuel manufacturing pilot plant based on Design Basis Threat (DBT) analysis.

- Classifying the NRR and the NMs into individual categories.

- Conducting safety and security analyses, taking into consideration the national threat assessment and assumed adversary model to identify areas that must be protected**.**

- Identifying the protected areas, inner areas, and vital areas for the nuclear facility.

- Describing the technical equipment used in the security or for the monitoring of the NRR and NMs within the PPS.

- Checking the access controls provided for the identification and entry authorization of all incoming personal, materials, and vehicles into the individual categorized areas.

- Erecting barriers to prevent the entry of unauthorized incoming vehicles.

- Establishing the presence of a control room inside the protected area where the security personnel can monitor the condition and status of all PPS equipment. (It is important to mention that the operator inside the control room must have sufficient equipment to communicate with the security personnel and also communicate with external response forces.)

- Equipping the guard forces with sufficient equipment to carry out their task, e.g., communications equipment and weapons.

- Creating a program for measuring the training and practicing of personnel in the implemented physical protection system.

- Developing a program for testing and maintaining PPS equipment.

- Documenting the quality assurance for the design and implementation of the PPS.

- Analyzing the implementation of the physical protection functions during the operation of the nuclear reactor and during theoretical emergency situations.

- Evaluating PPS test results.

- Updating the PPS plan when the facility is modified.

3.3. IAEA IPPAS Mission to Enhance the Level of PPS

The objective of the International Physical Protection Advisory Service (IPPAS) mission to Egypt is to assist and help the NRR to enhance the physical protection system and regulations for the nuclear facilities in Egypt. The products of the mission include detailed technical notes, with recommendations, suggestions, and good practices for upgrading the PPS system through a discussion with the competent authority (NRRA) and the operator's staff at the nuclear research reactors. It is important to mention that all documents generated before, during, and after the mission are treated as *safeguards confidential* documents by the IAEA and the team members according to the IAEA internationally accepted recommendations (INFCIRC/225 Rev. 4 (Corr.).[15]

3.4. Physical Protection During the NMs Transportation

It is widely believed that NMs are most vulnerable to illegal acts and sabotage during transport. As a consequence, a plan for the physical protection of NMs during transportation inside the facility must be prepared by the nuclear facility operator. (External transportation involving "transportation outside the facility" is beyond the scope of our proposed plan).

A permit is needed for any such internal transport, and the plan for each transportation stage requires the following:

- Determining the possible threats to the NRR, NMs, and the fuel manufacturing pilot plant based on Design Basis Threat (DBT) analysis.

- Classifying the NRR and the NMs into individual categories.

- Preparing a physical protection plan.
- Establishing a communication and reporting system for use during transportation.
- Locking and sealing the transport packages.
- Protecting the confidentiality of the physical protection information.
- Establishing an emergency response system.[16]
- [In the case of international transport, the responsibility for ensuring PPS is regulated by an agreement between the states concerned.]

4. Our Proposed Inspections Plan

To evaluate the effectiveness of the PPS plans and procedures, an inspection plan organized by the authors was devised. Our inspection is aimed at a more detailed examination and determination of whether the PPS elements are functional and working according to plan. This check-up of the system would ideally be conducted at least once a year by representatives of the NRRA, jointly with a facility operator.

The elements of our proposed inspection include:

Routine Inspection: The main aim of this is to assess and evaluate the conditions of the PPS, and also to assess the training and qualifications of the physical protection team (and how they may have changed from the previous inspection.)[17] This involves a routine check and verification of the PPS elements. Routine inspection activities are undertaken either at fixed time intervals or at variable time intervals in conjunction with specific tasks, e.g., pre-operation, nuclear materials transport from or to the nuclear facility, etc.[18]

Stimulation of an security incident: This is an in-service inspection of the physical protection elements and the facility's capability to detect, communicate, and respond to an intruder's progress towards the target in the shortest possible time. Specific checklists for each type of practice inspection help facilitate this review. Regardless of the type of inspection, the following systems require checking: the exterior intrusion detection system; the entry control system for personnel and vehicles; the entry control barriers (fences, personnel gate, vehicle gate, etc.); the interior detection system; the communication system; and the manual response of security personnel.

4.1. Proposed Inspection Report

In our view, the inspection reports should be done and submitted by the nuclear facility operator directly to the NRRA. The proposed inspection report includes**:**

1. Name and code of the nuclear facility.
2. Names of inspection team members (personnel), and their responsibilities during the inspection.
3. Date and type of inspection, including weather conditions.
4. Classification of the nuclear material.

5. Resources used for the inspection (personnel, time, materials, equipment, etc.).
6. The inspection techniques used (running the system, revision, check and measure, verification, etc.)
7. Inspection findings and recommendations.
8. Assessment of the physical facilities from the viewpoint of physical protection.
9. Type(s) of analyses used to evaluate the PPS.
10. A list of crucial corrective actions.
11. A list of possible areas for improvement.
12. The response times for security guards.
13. Overall findings and test results.
14. Recommendations specific to the facility operator.
15. Recommendations specific to the regulatory organization.

Conclusions and Recommendations

The nuclear materials in Egyptian research reactors have been categorized according to their fuel amount, type, and enrichment. This is important information for both safety and security planning.

We believe our proposed preliminary inspection plan, which includes an inspection checklist (Section 3.2) and proposed report content (Section 4.1), could assist the regulatory organization (NRRA) in evaluating the physical protection systems at nuclear facilities. The plan might also help the NRRA systematically follow up on inspection findings to ensure that all aspects of legislation, including the license conditions, are fully compliant with national and international obligations. This approach can also help the operator of the nuclear facility improve facility safety and security.

When our inspection checklist was applied to the studied NRR, we came to the following major conclusions:

1) The PPS in the NRR should be modified to incorporate new construction and repair.

2) It is important to have a sufficient stock of spare parts of PPS components because most of these spare parts are produced abroad and in the majority of cases, cannot be substituted by local products so as to ensure uninterrupted operation of the PPS.

3) The performance of the security response force to an emergency situation should be examined to understand its response time and reliability.

Acknowledgments

We are grateful to the editor and anonymous reviewers for useful suggestions, and for assistance with editing and reviewing the English.

Acronyms

IAEA	The International Atomic Energy Authority
PPS	Physical Protection System
DBT	Design Basis Threat
IPPAS	International Physical Protection Advisory Service
NPT	The Treaty on the Non-Proliferation of Nuclear Weapons
NRR	Nuclear Research Reactor
NRRA	Nuclear and Radiological Regulatory Authority
NRC	Nuclear Research Center
NM	Nuclear Materials
EU	Enriched Uranium
ET-RR-1	Egyptian First Research Reactor
ET-RR-2	Egyptian second Research Reactor

References

1. George Bunn, Frtiz Steinhausler, and Lyudmila Zaitesva, "Strengthening Nuclear Security Against Terrorists and Thieves Through Better Training", *Nonproliferation Review* (Fall/Winter 2001), http://cns.miis.edu/npr/pdfs/83bunn.pdf

2. Roger G. Johnston and Morten Bremer Maerli, "International vs. Domestic Nuclear Safeguards: The Need for Clarity in the Debate over Effectiveness", *Disarmament Diplomacy*, issue 69, pp 1-6 (2003), http://www.acronym.org.uk/dd/dd69/69op01.htm

3. OECD, *Nuclear Law Bulletin* No.85, volume 2010/1, Nuclear Energy Agency, (2010).

4. Ismail Badawy, "The National System of Nuclear Material Control, Developments and Challenges", *Sixth Conference on Nuclear Sciences and Applications*, Cairo, Egypt, 15-20 March, volume 111 (1996).

5. A. A. Hamed, Wael A. El-Gammal, and I. Badawy, "A Proposed Nuclear Safeguards System for A Decommissioned Nuclear Research Reactor", *International Eighth Conference on Nuclear Sciences & applications*, volume II, Cairo, Egypt, 7-12 February (2004).

6. S. Kursels, "Development of a Legal and Organizational Basis for Physical Protection of Nuclear Material and Nuclear Facilities in Lithuania", *International Conference on Physical Protection of Nuclear Materials*, Vienna, Austria, 10-14 November (1997).

7. E.A. Saad, E. M. El Sherbiny, M. Sobhy, and S. I. Mahmoud, "Spent Fuel Storage Experience at the ET-RR-1 Reactor in Egypt", International Atomic Energy Agency, IAEA-TECDOC-786, *Experience with Spent Fuel Storage at Research and Test Reactors*, Proceedings of an Advisory Group meeting held in Vienna, Austria, 5-8 July (1993).

8. IAEA-INFCIRC/225/rev.4, *The Physical Protection of Nuclear Material and Nuclear Facilities*, International Atomic Energy Agency, Vienna, Austria (1999).

9. *IAEA-IPPAS Guidelines*, IAEA International Physical Protection Advisory Service. IAEA Services Series No.3. Feb. (1999).

10. IAEA-INFCIRC/274/Rev.1, *The Convention on the Physical Protection of Nuclear Material*, IAEA, Vienna, Austria (1981).

11. IAEA-INFCIRC/225, *The Physical Protection of Nuclear Material*, International Atomic Energy Agency, Vienna , Austria (1975).

12. IAEA-INFCIRC/225/Rev.3, *The Physical Protection of Nuclear Material*, International Atomic Energy Agency, Vienna, Austria (1993).

13. I. Badawy, "Upgrading of Physical Protection of Nuclear Materials in an Old Nuclear Research Reactor Facility", IAEA-CN-86/9, Proceedings, International Conference held in Stockholm, Sweden, 7-11 May (2001).

14. John C. Matter, "The International Training Course on the Physical Protection of Nuclear Facilities and Materials", Topical paper, *Journal of Nuclear Materials Management*, vol. XXXVIII, No.4, p 4-11, (2010).

15. IAEA-INFCIRC/225/Rev.4(Corrected), *The Physical Protection of Nuclear Material and Nuclear Facilities*, 29 pages, IAEA, June, (1999).

16. H. Kawai, H. Kurihara, M. Kajiyoshi, "Physical Protection of Nuclear Material in Japan", *International Conference on Physical Protection of Nuclear Materials*, Vienna, Austria, 10-14 November (1997).

17. A. Stefulova, "Evaluation of Effectiveness of Physical Protection System at Nuclear Facilities in the Slovak Republic", *International Conference on Security of Material, Measures to Prevent, Intercept and Respond to Illicit Uses of Nuclear Material and Radioactive Sources*, Stockholm, Sweden 7-11 May 2001, IAEA-Cn_86-47, p84-86, (2001).

18. M.A. Shiniashin, Regulatory inspection of plane of nuclear facilities, private communication.

Journal of Physical Security 7(2), 12-29 (2014)

A Probabilistic Extension of the EASI Model

Norichika Terao* and Mitsutoshi Suzuki

Japan Atomic Energy Agency
* terao.norichika@jaea.go.jp

Abstract

The probability of an adversary's interruption, P_I, in a specific scenario can be evaluated using a calculation code, EASI. The purpose of this study is to devise a quantification method for P_I by considering the influence of uncertainty and variability. Specifically, we attempt to devise a new calculation method for three components of P_I: the probability of detection, $P(D_i)$; the probability of successful communication to the response force, $P(C_i)$; and the probability of the response force arriving prior to the end of the adversary's completion of the attack, $P(R|A_i)$. In addition, we design a hypothetical nuclear facility and an adversary attack scenario, and then assess the P_I value using our new method. We set the performance parameters of the facility as temporary, hypothetical values without a real performance test. We attempt to express the uncertainty and variability of each element of the facility using the Monte Carlo method.

Introduction

The September 11, 2001 attacks increased our understanding of the importance of considering adversarial attacks. After a speech in Prague in 2009, President Obama hosted the first Nuclear Security Summit (NSS) in 2010 in Washington D.C. aimed at global nuclear terrorism prevention. The second NSS was held in Seoul in 2012, and the third will be held in Hague in 2014. Regarding the physical protection regime in Japan, a relevant ministerial ordinance was revised in 2012 that considered both INFCIRC/225/Rev.5 and the lessons of the Fukushima Daiichi nuclear power plant accident.[1] Because of heightened interest in nuclear security, it is useful to establish an evaluation method to calculate the risks to a hypothetical nuclear facility.

Nuclear security is founded on a number of issues, but 3 of the most important are physical protection (PP) [2], illegal trafficking [2], and protection of radioisotopes [2]. Other issues are important as well, such as mitigating the insider threat, conducting effect threat assessments, providing cyber security, instigating material control and

accounting (MC&A), optimizing security resources, and providing countermeasures to espionage. In this study, we focus on a hypothetical sabotage event in a model nuclear facility. We focus particular attention on PP.

The risk (R) for PP can be defined as $R=P_A\times(1-P_E)\times C$, where P_A is the probability of an adversary attacking during a given period, P_E is the probability of PP system effectiveness, and C is the consequence value of a security failure.[3] The P_A value should be expressed as the possibility of attack against the target facility using the data of events during the scenario, such as sabotage or the theft. Often [4], the value of P_A is set to 1, though this may not be a prudent choice in actual practice.

The probability of system effectiveness is defined as $P_E=P_I\times P_N$, where P_I is the probability of the adversary being interrupted, and P_N is the probability of neutralization.

Now the difference between nuclear security and nuclear safety is the existence of adversaries in nuclear security. Many types of adversaries exist for reasons such as politics and religion. Various factors affect the adversaries' probability of success, including skills, equipment, knowledge, and motivation. It is necessary to consider the detailed characteristics of adversaries individually in order to accurately express the nuclear security risk. Here, we include only one type of adversary in our scenarios.

In general, risk is determined using two factors: the magnitude of possible adverse consequences, and the likelihood of occurrence of each consequence. Probabilistic risk assessment (PRA) uses probability distributions to characterize variability or uncertainty in risk estimates.[5] In the nuclear safety field, PRA is conducted using factors such as the frequency of an accident sequence, the probability that sensors cease functioning, and human error.[6] The frequencies with which an accident sequence or random sensor errors occur are typically expressed using actual measured values. Thus, sensor problems or human errors are well quantified in nuclear safety. By contrast, many of the frequencies and probabilities for nuclear security are unknown or cannot be revealed for security reasons. Therefore, PRA for nuclear security is a more challenging problem.

In this study, we focus on quantifying the value of P_I. The P_I value in a specific scenario can be evaluated using an Estimate of Adversary Sequence Interruption (EASI), a calculation code developed by Sandia National Laboratory (SNL) in the United

States.[7] In the EASI model, errors caused by uncertainty and variability are ignored when expressing the performance of sensors and communications. The purpose of this study is to devise a quantification method for P_I by considering the influence of uncertainty and variability. In addition, we seek to design a hypothetical nuclear facility as well as an adversary's attack scenario, and then assess the P_I value using our new method.

Conventional Expression of P_I Using EASI

We conduct a risk assessment of the interruption probability P_I under a specific scenario using EASI developed by SNL. EASI is a simple and easy-to-use method for evaluating the performance of a PP system along a specific adversarial path and with specific conditions of threat and system operation, and is a traditional tool used worldwide.

A simple calculation describing P_I in EASI when an adversary intrudes into a nuclear facility is shown in figure 1. The left side of this figure indicates the simplified diagram of an event tree for the P_I calculation at the n point barriers, and the right side indicates the calculation components of P_I. The summation of the calculation components of P_I becomes the P_I value. The P_I value is represented [7] by equation (1).

$$P_I = P(\mathrm{D}_1)\times P(\mathrm{C}_1)\times P(\mathrm{R}|\mathrm{A}_1) + \sum_{i=2}^{n} P(R|A_i)\times P(C_i)\times P(D_i)\times \prod_{i=1}^{i-1}(1 - P(D_i)), \quad (1)$$

where $P(\mathrm{D}_i)$ is the probability of a detection alarm for the facility equipment, e.g., infrared (IR) sensors; $P(\mathrm{C}_i)$ is the probability that the facility guard successfully understands the alarm condition using the facility's equipment and successfully communicates it to the response force; and $P(\mathrm{R}|\mathrm{A}_i)$ is the conditional probability that, given a recognized alarm, the response force arrives prior to the end of the adversary's action sequence. In the calculation of P_I using the EASI method, both $P(\mathrm{D}_i)$ and $P(\mathrm{C}_i)$ values are taken as the evaluated values without uncertainty and variability errors, and the $P(\mathrm{R}|\mathrm{A}_i)$ value is calculated using a normal distribution.

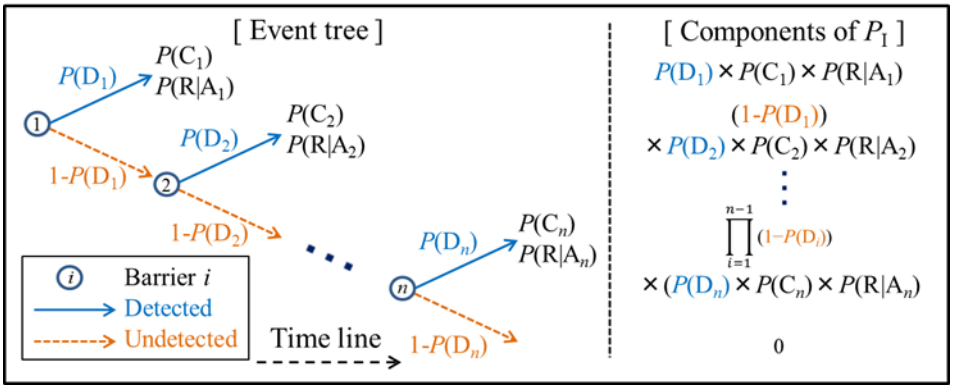


Figure 1 - Schematic of the EASI method.

New Quantification Method for P_I

In this study, we devise a new calculation method for the three components of P_I: $P(D_i)$, $P(C_i)$, and $P(R|A_i)$. Specifically, we express $P(D_i)$ and $P(C_i)$ as probability distributions that include errors caused by uncertainty and variability. Uncertainty means incompleteness of knowledge, such as failure to set conditions or wrong operation procedures, and variability means fluctuations in nature, such as weather conditions, environmental conditions, or presence of wild animals. Furthermore, we express a new calculation method of $P(R|A_i)$ using a Bernoulli trial.

Calculation of $P(D_i)$

The performance of sensors in a nuclear facility provide the value of $P(D_i)$ for the EASI computation, which is used as the evaluated value without any errors.[7] There are many types of sensors used in the facility, such as active and passive IR sensors, microwave sensors, sonic sensors, vibration sensors, and video cameras. In this study, we consider only IR and microwave sensors.

It is possible to express the influence of a sensor's uncertainty and variability as a probability distribution by examining the statistical false positive error rates (type I error, or α) and false negative error rates (type II error, or β). A graph of $P(D)$ and P_{fa} of a hypothetical sensor against the signal strength in dB is shown in figure 2. $f_{s+n}(R)$ indicates the probability density function (PDF) of a signal plus noise, and $f_n(R)$ indicates the PDF of noise, respectively, as a function of signal intensity, R. The threshold (V_T) separates the sensor's detectable region and the undetectable region of

$f_{s+n}(R)$ and $f_n(R)$. The blue dashed area, 1-β, indicates the P(D) value, and the orange dashed area, α, indicates the P_{fa} value. Determining a proper $f_{s+n}(R)$ can help us calculate the P(D) value.

First, we consider $f_{s+n}(R)$ and $f_n(R)$ for the IR sensors. There are basically two types of IR sensors, active and passive. Active IR sensors emit infrared light and detect changes to the reflected or scattered infrared light indicative of intrusion. Passive IR sensors detect changes to the thermal infrared light emitted by warm bodies, including people. For simplicity, we assume that $f_{s+n}(R)$ for both kinds of IR sensors is the same as $f_n(R)$.

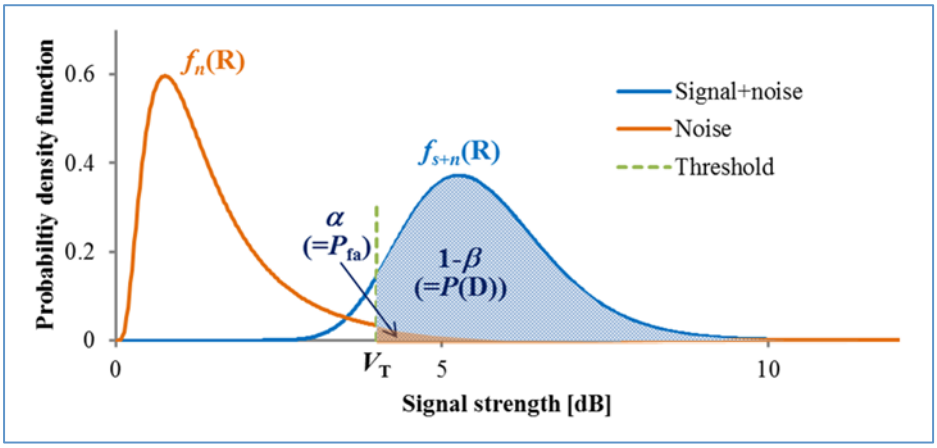


Figure 2 - Probability distribution functions P(D) and P_{fa} for a hypothetical sensor.

Generally, IR sensors are easily affected by noise and variability. We assume that their sensitivity to anomalies is proportional to their variability. Because the risk evaluation formula is a multiplicative function, the distribution of the risk that takes only a positive value generally uses a log-normal distribution. We assume that $f_{s+n}(R)$ obeys a log-normal distribution. If the evaluation values are usable, a best-fit probability distribution is most useful. The detection probability is equal to the distribution function of $f_{s+n}(R)$.

$$P(D_{i\_\text{IR}}) = (1-\beta) = \int_{V_{\text{T}\_i\_IR}}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_{s\_i\_IR}R} \exp\left(-\frac{(\ln R-\mu_{s\_i\_IR})^2}{2\sigma_{s\_i\_IR}{}^2}\right) dR, \qquad (2)$$

where $V_{\text{T}\_i\_IR}$ is the threshold value and $\mu_{s\_i\_IR}$ and $\sigma_{s\_i\_IR}$ are the mean and standard deviation of the signal-plus-noise performance of the IR sensors, respectively. Similarly, we assume that $f_n(R)$ obeys a log-normal distribution. The false alarm probability is equal to the distribution function of $f_n(R)$:

$$P_{fa\_i\_\mathrm{IR}} = \alpha = \int_{V_{\mathrm{T}\_i\_IR}}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_{n\_i\_IR}R} \exp\left(-\frac{(\ln R - \mu_{n\_i\_IR})^2}{2\sigma_{n\_i\_IR}^2}\right) dR, \quad (3)$$

where $\mu_{n\_i\_IR}$ and $\sigma_{n\_i\_IR}$ is are the mean and standard deviation of the noise of the IR sensors, respectively.

Next, we consider $f_{s+n}(R)$ and $f_n(R)$ for the microwave sensors. The microwave sensors typically detect changes in reflected or scattered microwaves, including amplitude or Doppler frequency shifts. Microwaves are electromagnetic waves with wavelengths between 1 cm and 10 cm. The intensity of microwaves can be weakened by rain or fog; we will assume that the variability of the microwave sensors is mainly caused by air conditions. For microwave sensors, some concrete statistical models of $f_{s+n}(R)$ and $f_n(R)$ have been proposed.[8, 9] In this study, we assume that the main source of background noise is thermal noise. $f_{s+n}(R)$ obeys a Rice distribution [10], and the detection probability is equal to the distribution function of $f_{s+n}(R)$.

$$P(D_{i\_\mathrm{M}}) = (1-\beta) = \int_{V_{\mathrm{T}\_i\_M}}^{\infty} \frac{R}{\sigma_{n\_i\_M}^2} \exp\left(-\frac{R^2+\sigma_{s\_i\_M}^2}{2\sigma_{n\_i\_M}^2}\right) I_0\left(\frac{\sigma_{s\_i\_M}R}{\sigma_{n\_i\_M}^2}\right) dR, \quad (4)$$

where $V_{\mathrm{T}\_i\_M}$ is the threshold value, $\sigma_{s\_i\_M}$ is the standard deviation of the signal plus the noise, and $\sigma_{n\_i\_M}$ is the standard deviation of the noise of the microwave sensors. In addition, $I_0(Z)$ is a modified Bessel function of the first kind with order zero. If clutter becomes dominant in the background noise, the Rice distribution is not used due to its large error; $f_n(R)$ obeys a Rayleigh distribution in that case. The false alarm probability is equal to the distribution function of $f_n(R)$:

$$P_{fa\_i\_\mathrm{M}} = \alpha = \int_{V_{\mathrm{T}\_i\_M}}^{\infty} \frac{R}{\sigma_{n\_i\_M}^2} \exp\left(-\frac{R^2}{\sigma_{n\_i\_M}^2}\right) dR. \quad (5)$$

If the clutter becomes dominant in the background noise, a log-normal distribution [8] or Weibull distribution [9] is appropriate instead of a Rayleigh distribution.

Calculation of P(C_i)

In the EASI model, the value of $P(C_i)$ ignores errors.[7] In our model, two human characters come into play: a facility guard and a responder from the response force. In this study, two communication processes are considered for calculating the probability. The first process occurs when the guard understands the anomalous signal from the sensors and recognizes the events that occurred in the facility. The second process is when thae guard correctly communicates information to the responder, who, in turn,

comprehends the complete sequence of events from such information. Communication effectiveness is influenced by uncertainty and variability because of human errors such as failure to act, fear, inattention, memory lapses, and rule-based or knowledge based mistakes. In contrast, the influence of insider threats such as violations or sabotage is not considered here. Generally, the human error probability (HEP) is quantified using various human reliability analysis (HRA) methods.[11, 12] In our model, the $P(C_i)$ value is expressed using a probability distribution that represents human errors.

In the first communication process, the HEP is influenced by both uncertainty (e.g., the guard's condition and lack of perception) and variability (e.g., bad environmental conditions). We assume that the HEP of the first process is proportional to the degree of uncertainty and variability. Because the log-normal distribution is used frequently in safety studies as the epistemic distribution of failure rates [13], the HEP is represented as a log-normal distribution function. Furthermore, we suppose that the unit of a variable is expressed using its error rate, that is, the number of errors per command. The $P(C_{type1\_i})$ value indicates the communication probability of the first process, and it is expressed in equation (6) by deducting the HEP from the whole.

$$P\left(C_{\text{type1\_}i}\right) = 1 - \int_0^{V_{F1\_i}} \frac{1}{\sqrt{2\pi}\sigma_{C1\_i}R} \exp\left(-\frac{\left(\ln R - \mu_{C1\_i}\right)^2}{2{\sigma_{C1\_i}}^2}\right) dR, \quad (6)$$

where the V_{F1_i} is quantity of uncertainty and variability, and μ_{c1_i} and σ_{c1_i} are the mean and standard deviation of the first communication process, respectively.

In the second communication process, the HEP is influenced by both uncertainty (e.g., the guard's or the responder's condition and lack of perception) and variability (e.g., bad environmental conditions). We assume that the HEP of the second process is proportional to the quantity of uncertainty and variability. The HEP is represented as a distribution function of log-normal type, as with the first communication process. The $P(C_{type2\_i})$ value indicates the communication probability of the second process and is expressed in equation (7) by deducting the HEP from the total probability.

$$P\left(C_{\text{type2\_}i}\right) = 1 - \int_0^{V_{F2\_i}} \frac{1}{\sqrt{2\pi}\sigma_{C2\_i}R} \exp\left(-\frac{\left(\ln R - \mu_{C2\_i}\right)^2}{2{\sigma_{C2\_i}}^2}\right) dR, \quad (7)$$

where the V_{F2_i} is quantity of uncertainty and variability, and the μ_{c2_i} and σ_{c2_i} are the mean and standard deviation of the second communication process, respectively.

Finally, the $P(C_i)$ value is calculated as the product of the $P(C_{type1\_i})$ value and the $P(C_{type2\_i})$ value for each i.

Calculation of P(R|A$_i$)

The value of $P(R|A_i)$ for EASI is calculated using the normal distribution by including both the delay time of the barrier for the facility and the arrival time of the response force.[7] Approximately 99.7% of phenomena occur within ±3 sigma for the normal distribution. Therefore, it is clear whether the response force can reach the adversary in time. Because the actions of the response force should have considerable flexibility, a gradually decreasing probability distribution, rather than the normal distribution, needs to be considered. In this section, $P(R|A_i)$ is expressed using a different method than EASI.

The $P(R|A_i)$ value is expressed using a Bernoulli trial, focusing on whether the response force can get the situation under control before the adversary finishes the attack. The probability distribution of the Bernoulli trial is described using a binominal and a Poisson distribution. An adversary attack is a major problem for nuclear security. The binominal distribution is assumed to occur for the target event multiple times, and hence, the Poisson distribution is more suitable than the binominal distribution for representing $P(R|A_i)$.

A Poisson distribution is a discrete probability distribution expressed in equation (8).

$$P(X = k) = \frac{\lambda^k e^{-\lambda}}{k!}, \tag{8}$$

where k is natural number and λ is a positive constant. In other words, a Poisson distribution is the probability that an event that arises λ times on average occurs k times during a given period. In this section, we assume that λ_i at the i^{th} barrier is a calculated value that indicates the frequency of the response force arriving in time before the adversaries obtain their goal. The λ_i value is given in equation (9).

$$\lambda_i = \frac{TR_i}{RFT_i}, \tag{9}$$

where TR_i is the residual time at the i^{th} barrier, and RFT_i is the response force's arrival time at the i^{th} barrier. If λ is greater than 1, the response force can reach the event on

time. By subtracting the probability when k is equal to 0 from the total probability, 1, the value of $P(\mathrm{R}|\mathrm{A}_i)$ for each barrier is given as:

$$P(\mathrm{R}|\mathrm{A}_i) = 1 - e^{-\lambda_i}. \tag{10}$$

Trial of Risk Assessment

We assess the value for P_I in the case of an adversary's attack against a hypothetical nuclear facility using the new quantification method proposed above. An overview of the designed hypothetical facility and the adversary's attempt are shown in figure 3. The circled numbers in this figure indicate the barriers of the facility, and the dashed line indicates the adversary's attempt to sabotage the target nuclear material. Sensors in this facility are assumed to be IR and microwave detectors. The assumed delay values (Delay_i) and response force time (RFT_i) of the barrier i are shown in table 1. Delay_i means the time that the adversaries need in order to pass through each barrier i, and RFT_i indicates the time required for the response force to arrive at the facility in case of an attack.

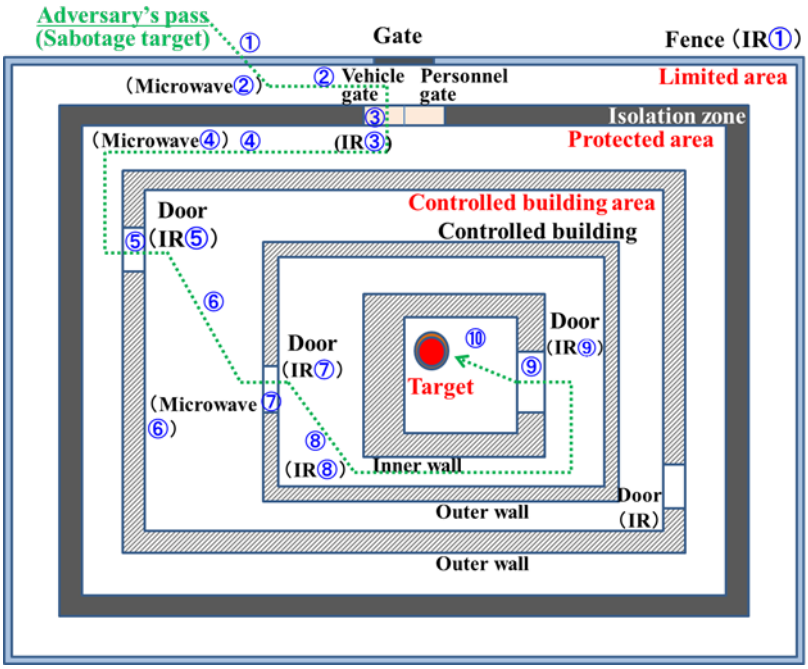


Figure 3 - Overview of the designed hypothetical nuclear facility and adversary's pass.

The temporary performance levels of the sensors, guards, the adversary, and the response force are given approximate numerical values in order to assess the P_I value, because we cannot use actual values for security reasons. It is necessary to consider the influence of uncertainty and variability of $P(D_i)$, $P(C_i)$, and $P(R|A_i)$. In this study, the uncertainty and variability of each element of the facility are expressed using a Monte Carlo method.

Table 1 - Some parameters of the hypothetical nuclear facility.

i	$Delay_i$ [sec]		RFT_i [sec]	
	Mean	Standard deviation	Mean	Standard deviation
1	40.0	4.00	220	22.0
2	30.0	3.00	220	22.0
3	20.0	2.00	220	22.0
4	50.0	5.00	220	22.0
5	50.0	5.00	220	22.0
6	40.0	4.00	220	22.0
7	60.0	6.00	220	22.0
8	50.0	5.00	220	22.0
9	60.0	6.00	220	22.0
10	120	12.0	220	22.0

Table 2 - Some parameters to calculate the $P(D_i)$ value and result.

i	Infrared sensors					Microwave sensors			$P(D_{\_i\_IR})$ or $P(D_{\_i\_M})$	$P_{fa\_i\_IR}$ or $P_{fa\_i\_M}$
	$V_{T\_i\_IR}$	$\mu_{s\_i\_IR}$	$\sigma_{s\_i\_IR}$	$\mu_{n\_i\_IR}$	$\sigma_{n\_i\_IR}$	$V_{T\_i\_M}$	$\sigma_{s\_i\_M}$	$\sigma_{n\_i\_M}$		
1	5.00	2.00	0.400	1.10	0.500	-	-	-	0.84	0.15
2	-	-	-	-	-	1.50	2.00	0.500	0.87	0.12
3	4.50	2.00	0.400	1.00	0.400	-	-	-	0.89	0.10
4	-	-	-	-	-	1.50	2.00	0.500	0.87	0.12
5	4.50	2.00	0.400	1.00	0.400	-	-	-	0.89	0.10
6	-	-	-	-	-	1.50	2.00	0.500	0.87	0.12
7	4.00	2.00	0.400	0.900	0.300	-	-	-	0.94	0.05
8	4.00	2.00	0.400	0.900	0.300	-	-	-	0.94	0.05
9	4.00	2.00	0.400	0.900	0.300	-	-	-	0.94	0.05
10	-	-	-	-	-	-	-	-	0.00	0.00

First, $P(D_i)$ is expressed using the Monte Carlo method. The $P(D_i)$ values are expressed using equation (2) and equation (4). For the IR sensors, the $P(D_i)$ values are calculated using the $V_{T\_i\_IR}$, the $\mu_{s\_i\_IR}$, and the $\sigma_{s\_i\_IR}$ values. For the microwave sensors, the $P(D_i)$ values are calculated using the $V_{T\_i\_M}$, the $\sigma_{s\_i\_M}$, and the $\sigma_{n\_i\_M}$ values. These values are set freely and shown in table 2 together with the calculated $P(D_i)$ values.

If the operational performance of the sensors is directly influenced by errors caused by uncertainty and variability, a focus on the fluctuations of the variables $\sigma_{s\_i\_IR}$, $\sigma_{s\_i\_M}$, and $\sigma_{n\_i\_M}$ is warranted. We assume that these values are randomly affected by uncertainty and variability, and that they are expressed using a normal random number. We generated a normal random number using the following two processes: A uniform random number sequence between 0–1 was generated using the RAND function of Microsoft Excel and was then translated into a normal random number, N(0, 1], using the Box-Muller transform.[14]

The trial run was repeated 5,000 times using a random number sequence. The same random number sequence was used for all barriers, *i*. For the IR sensors, the variation of $\sigma_{s\_i\_IR}$ was assumed to fluctuate by 0.01 from the value set in table 2. Similarly, for the microwave sensors, we assumed that the variation of $\sigma_{s\_i\_M}$ and $\sigma_{n\_i\_M}$ fluctuate by 0.005 and 0.01, respectively, from the values set in table 2. The histograms of the 5,000 calculated $P(D_i)$ values are shown in figure 4 for every $P(D_i)$ value. The data interval of the $P(D_i)$ values was 0.001.

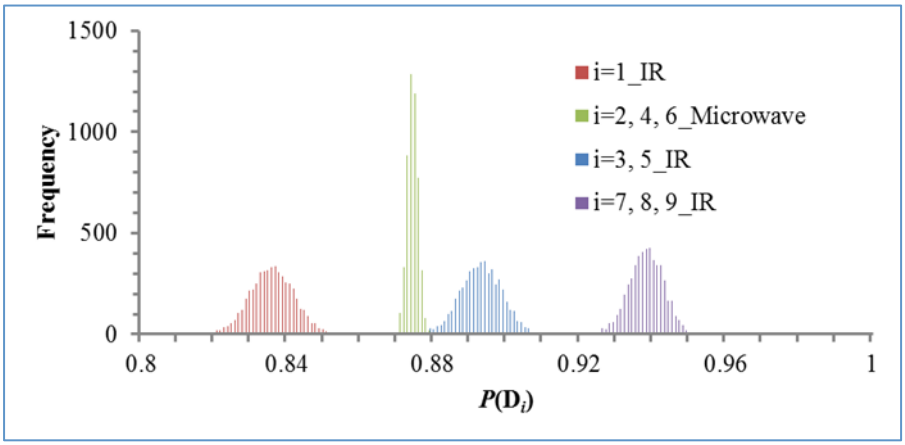


Figure 4 - Probability distribution of $P(D_i)$ using 5,000 normal random numbers.

Next, $P(C_i)$ was expressed using the Monte Carlo method. The $P(C_i)$ values were calculated by multiplying equation (6) by equation (7). In the first communication

process, the $P(C_{type1\_i})$ values are calculated from the V_{F1_i}, μ_{c1_i}, and σ_{c1_i} values. Similarly, in the second communication process, the $P(C_{type2\_i})$ values are calculated using the V_{F2_i}, μ_{c2_i}, and σ_{c2_i} values. These values are set freely and shown in table 3, together with the calculated $P(C_{type1\_i})$, $P(C_{type2\_i})$, and $P(C_i)$ values.

Table 3 - Some parameters to calculate the $P(C_i)$ value and result.

i	Path 1				Path 2				$P(C_i)$
	V_{F1_i}	μ_{C1_i}	σ_{C1_i}	$P(C_{type1\_i})$	V_{F2_i}	μ_{C2_i}	σ_{C2_i}	$P(C_{type2\_i})$	
1	0.0500	1.00	3.00	0.909	0.0200	1.00	2.00	0.993	0.90
2	0.0400	1.00	3.00	0.920	0.0200	1.00	2.00	0.993	0.91
3	0.0300	1.00	3.00	0.933	0.0100	1.00	2.00	0.997	0.93
4	0.0300	1.00	3.00	0.933	0.0100	1.00	2.00	0.997	0.93
5	0.0100	1.00	3.00	0.969	0.0100	1.00	2.00	0.997	0.97
6	0.0200	1.00	3.00	0.949	0.0100	1.00	2.00	0.997	0.95
7	0.0100	1.00	3.00	0.969	0.0100	1.00	2.00	0.997	0.97
8	0.0200	1.00	3.00	0.949	0.0100	1.00	2.00	0.997	0.95
9	0.0100	1.00	3.00	0.969	0.0100	1.00	2.00	0.997	0.97
10	0.0100	1.00	3.00	0.969	0.0100	1.00	2.00	0.997	0.97

If $P(C_{type1\_i})$ and $P(C_{type2\_i})$ are directly influenced by errors caused by uncertainty and variability, a focus on the fluctuations of the variables V_{F1_i} and V_{F2_i} is warranted. We thus assume that these values are randomly affected by both uncertainty and variability. These values were expressed using a normal random number, N(0, 1]. The sequence of the 5,000 normal random numbers was generated using the same method as that of $P(D_i)$. A different random number sequence was used in the $P(C_{type1\_i})$ and $P(C_{type2\_i})$ calculation.

The trial run was repeated 5,000 times using a different random number sequence. The same random number sequence, i, was used for all barriers. We assumed that the variations of both V_{F1_i}, and V_{F2_i} fluctuate by 0.01 from the value set in table 3. The histograms of the 5,000 calculated $P(C_{type1\_i})$ and $P(C_{type2\_i})$ values are shown in figure 5. The data interval of the $P(C_{type1\_i})$ and $P(C_{type2\_i})$ values are 0.001 and 0.0005, respectively. The histograms of the 5,000 calculated $P(C_i)$ values are shown in figure 6. The data interval of the $P(C_i)$ values was 0.001.

Finally, $P(R|A_i)$ was determined using the Monte Carlo method. The $P(R|A_i)$ values come from equation (10) as a function of the variable λ_i. The λ_i values were calculated using the TR_i and RFT_i values, similar to what was done for equation (9). The TR_i values can be calculated from the delay values shown in table 1. The RFT_i values are also shown in table 1. The standard deviation values of TR_i and λ_i can be calculated using the propagation of errors technique. These values are shown in table 4 along with the calculated $P(R|A_i)$ values.

If $P(R|A_i)$ is influenced by errors caused by uncertainty and variability directly, focusing on the fluctuations of the λ_i variables is warranted. We assume that these values are affected by uncertainty and variability at random. These values were expressed using a normal random number, N(0, 1]. The sequence of 5,000 normal random numbers is generated in the same manner in $P(D_i)$ and $P(C_i)$.

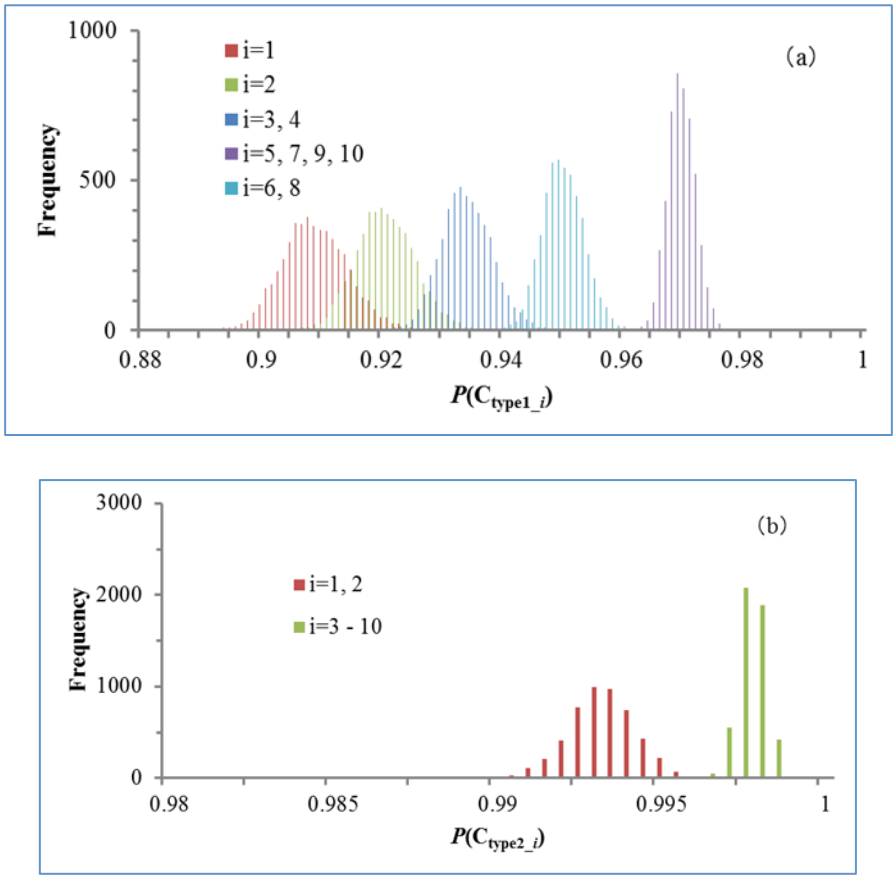


Figure 5 - (a) Probability distribution of $P(C_{type1\_i})$ using 5,000 normal random numbers. (b) Probability distribution of $P(C_{type2\_i})$ using 5,000 normal random numbers.

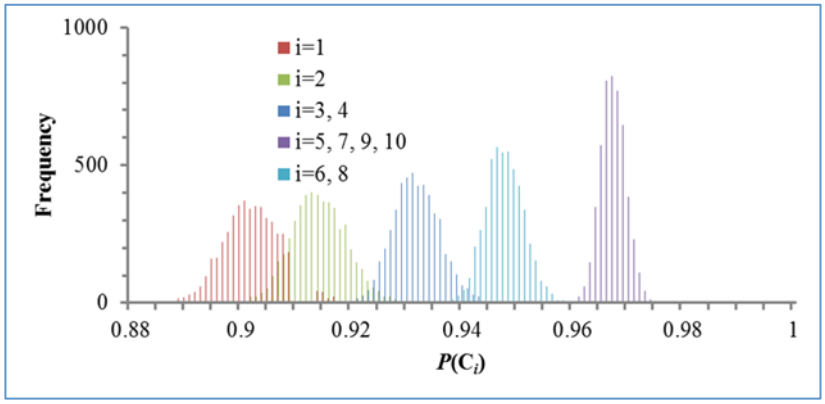


Figure 6 - Probability distribution of $P(C_i)$ using 5,000 normal random numbers.

Table 4 - Some parameters to calculate the $P(R|A_i)$ value and result.

i	TR_i [sec]		RFT_i [sec]		λ_i		$P(R|A_i)$
	Mean	Standard deviation	Mean	Standard deviation	Mean	Standard deviation	
1	520	18.3	220	22.0	2.36	0.251	0.91
2	480	17.9	220	22.0	2.18	0.233	0.89
3	450	17.6	220	22.0	2.05	0.220	0.87
4	430	17.5	220	22.0	1.95	0.211	0.86
5	380	16.8	220	22.0	1.73	0.189	0.82
6	330	16.0	220	22.0	1.50	0.167	0.78
7	290	15.5	220	22.0	1.32	0.150	0.73
8	230	14.3	220	22.0	1.05	0.123	0.65
9	180	13.4	220	22.0	0.818	0.102	0.56
10	120	12.0	220	22.0	0.545	0.0771	0.42

The trial run was repeated 5,000 times using the random number sequence. The same random number sequence was used for all barriers, i. We assumed that the variations of λ_i fluctuate by the standard deviation values set in table 4. The histograms of the 5,000 calculated $P(R|A_i)$ values are shown in figure 7. The data interval of the $P(R|A_i)$ values is 0.01.

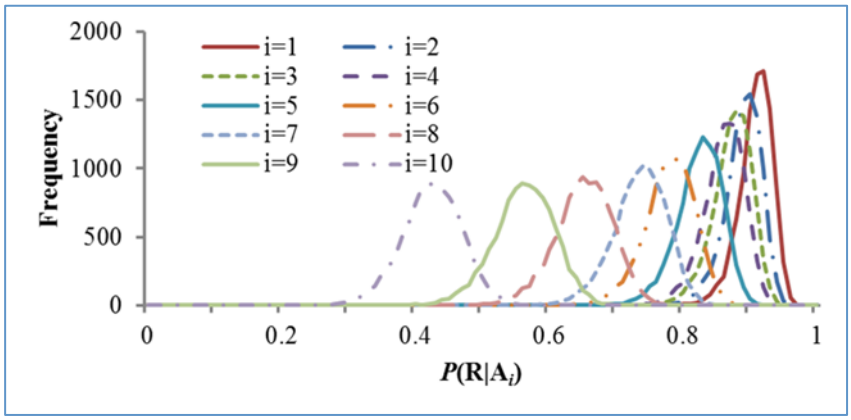


Figure 7 - Probability distribution of $P(R|A_i)$ using 5,000 normal random numbers.

Finally, values of P_I considering uncertainty or variability can be calculated using equation (1). The values of $P(D_i)$, $P(C_i)$, and $P(R|A_i)$ allowing for uncertainty or variability are shown in figures 4, 6, and 7, respectively. By using the 5,000 temporary data points of $P(D_i)$, $P(C_i)$, and $P(R|A_i)$ generated using the Monte Carlo method, the 5,000 data points of the P_I were calculated. The histogram of the 5,000 calculated P_I values is shown in figure 8. The data interval of the P_I values was 0.005, and the mean and standard deviation value of P_I were 0.81 and 0.02, respectively.

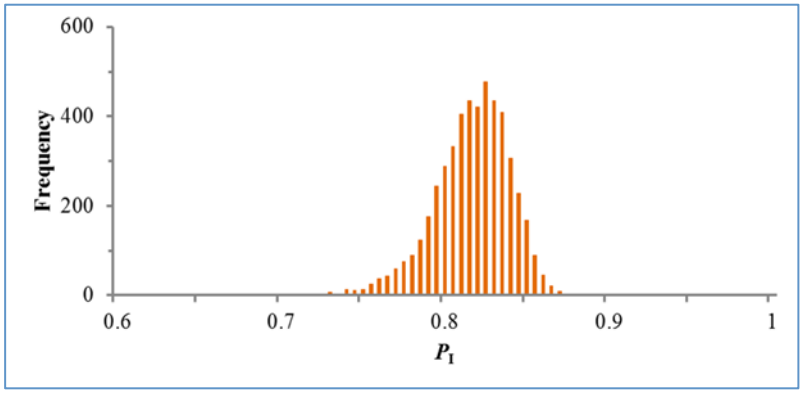


Figure 8 - Probability distribution of P_I calculated from a probability distribution of $P(D_i)$, $P(C_i)$, and $P(R|A_i)$.

We can assess the probabilistic P_I values using a temporary value set when an adversary attacks a hypothetical nuclear facility. Because the random numbers used in this paper are independent of the real performance of sensors, guards, adversary, and

response force, the assessment result does not reveal the real fluctuations caused by uncertainty or variability. If the random numbers are represented by real performance data, the real-world P_I values can be calculated.

Conclusions

The P_I value in a specific scenario can be calculated using a method such as EASI developed by SNL in the United States. In the EASI calculation, errors caused by uncertainty and variability are not considered in expressing the performance of sensors and communication.

We attempted to devise a new calculation method for three components of P_I: $P(D_i)$, $P(C_i)$, and $P(R|A_i)$. Specifically, the new calculation method for $P(D_i)$ and $P(C_i)$ is expressed as a probability distribution that includes errors caused by uncertainty and variability. We assumed that $f_{s+n}(R)$ obeys a log-normal distribution in the case of IR sensors, and a Rice distribution in the case of microwave sensors. The $P(D_i)$ values are equal to the distribution function of $f_{s+n}(R)$. Moreover, two communication processes are considered to calculate the $P(C_i)$ value. We assumed that the HEP of these processes is represented as a long-normal distribution function. The communication probability for the first and second processes, $P(C_{type1\_i})$ and $P(C_{type2\_i})$, respectively, are expressed by deducting the HEP from the total probability. In contrast, the new calculation method of $P(R|A_i)$ is expressed using a Bernoulli trial, specifically a Poisson distribution. We assumed that λ_i at the i^{th} barrier is the frequency at which the response force can arrive in time before the adversaries obtain their goal. By subtracting the probability when k is equal to 0 from the total probability, 1, the $P(R|A_i)$ value for each barrier is expressed as an exponential form.

We calculated the P_I value using the new quantification method in the case of an adversary's attack against a hypothetical nuclear facility. The temporary performance of sensors, guards, adversary, and the response force were assigned numerical values in order to assess the P_I value, because real values cannot be used for security reasons. The influence of uncertainty and variability are expressed using a Monte Carlo method.

If the sensor's operational performance is directly influenced by errors caused by uncertainty and variability, focusing on the fluctuations of the variables $\sigma_{s\_i\_IR}$, $\sigma_{s\_i\_M}$, and $\sigma_{n\_i\_M}$ in the case of $P(D_i)$, that of V_{F1_i} and V_{F2_i} in the case of $P(C_i)$, and that of λ_i in the case of $P(R|A_i)$ is warranted. We assumed that these values are affected by uncertainty

and variability at random. Therefore, we expressed these values using a normal random number, N(0, 1]. By using 5,000 temporary performance data points of $P(D_i)$, $P(C_i)$, and $P(R|A_i)$ generated by the Monte Carlo method, the 5,000 performance data points of P_I were calculated. The mean and standard deviation value of P_I were found to be 0.81 and 0.02, respectively.

We can assess the probabilistic P_I value by using a temporary value set when an adversary attacks a hypothetical nuclear facility. Because the random numbers of this study are independent to the real-world performance of the sensors, guards, adversary, and response force, the assessment result does not reveal the actual fluctuations caused by uncertainty or variability. If the random numbers were represented by real performance data, the real P_I value can be calculated.

References

1. The Sasakawa Peace Foundation, *The Fukushima Nuclear Accident and Crisis Management*, pp 63-80, (2012).
2. Kazutomo Irie, *Redefining Interrelationship between Nuclear Safety, Nuclear Security and Safeguards*, Journal of Power and Energy Systems **6**(2), 109-117, (2012).
3. Mary Lynn Garcia, *EASI Model*, The Design and Evaluation of PHYSICAL PROTECTION SYSTEMS 2nd edition, Butterworth-Heinemann, p. 9-10, (2007).
4. Mary Lynn Garcia, *EASI Model*, The Design and Evaluation of PHYSICAL PROTECTION SYSTEMS 2nd edition, Butterworth-Heinemann, p. 292, (2007).
5. 60 FR 42622, *Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement*, Washington, DC, (1995).
6. INSAG-12, Basic Safety Principles for Nuclear Power Plants, *75-INSAG-3* Rev. 1, IAEA, (1999).
7. Mary Lynn Garcia, *EASI Model*, The Design and Evaluation of PHYSICAL PROTECTION SYSTEMS 2nd edition, Butterworth-Heinemann, pp 319-323, (2007).
8. G. R. Valenzuela and M. B. Laing, *On the Statistics of Sea Clutter, NRL REPORT 7349.*
9. D. A. Shnidman, *Generalized radar clutter model*, IEEE Trans., Aerospace and Electronic Systems, **35**(3), 857-865, (1999).
10. S. O. Rice, *Mathematical Analysis of Random Noise*, Bell System Tech. J., **23**, 282-332, (1994), and **24**, 46-156, (1945).
11. A. D. Swain, & H. E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, (1983).

12. E. Hollnagel, Cognitive Reliability and Error Analysis Method – CREAM, Oxford: Elsevier Science, (1998).
13. Michael Stamatelatos, and Homayoon Dezfuli, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, 2nd edition, pp. 6-8 to 6-11, (2011).
14. G. E. P. Box and Mervin E. Muller, *A Note on the Generation of Random Normal Deviates*, The Annals of Mathematical Statistics, **29**(2), 610–611, (1958).

PPS Evaluation of An Oil Refinery Using *EASI* Model

M.C. Echeta[1], L.A. Dim[2], O.D. Oyeyinka[1], and A.O. Kuye[1]

1. Centre for Nuclear Energy Studies, University of Port-Harcourt, P.M.B 5323, Port Harcourt, Nigeria
2. Centre for Energy Research and Training, Ahmadu Bello University, Zaria, Nigeria

Abstract

This paper attempts to quantitatively analyze the effectiveness of a Physical Protection System (PPS) designed for an oil refinery using the Estimate of Adversary Sequence Interruption (EASI) model. The output from the model is the Probability of Interruption (P_I) of a potential attack scenario along a specific path. The effectiveness of a security system is dependent on the value of the Probability of Interruption. Results obtained show that the values of the probability of interruption of the adversaries for the most likely adversary paths are very low. But by upgrading the protection elements, the values of probability of interruption increase from 0 to a range of 0.66 to 0.89, strengthening overall security.

Keywords: Physical Protection System; PPS Evaluation; Oil Refinery Security

Introduction

A Physical Protection System (PPS) integrates people, procedures, and/or equipment for the protection of assets or facilities against theft, sabotage, and other malevolent human acts. A PPS can be applied to either fixed or moving assets. The ultimate objective of a PPS is to prevent the accomplishment of overt or covert malevolent actions. A PPS accomplishes its objectives by either deterrence or a combination of detection, delay, and response (Garcia, 2001). For these objectives to be achieved, the PPS must be evaluated or analyzed to determine its effectiveness. For a system to be effective, there must be awareness of an attack (detection) and the slowing of adversary progress to the targets (delay), thus allowing a response force enough time to interrupt or stop the adversary (response).

In the design, evaluation, and selection of security systems, Doyon (1981) presents a probabilistic network model for a system consisting of guards, sensors, and barriers. He determines analytic representations for determining probabilities of intruder apprehension in different zones between site entry and a target object. Schneider and Grassie (1989) and Grassie et al. (1990) present a methodology in which countermeasures

are developed in response to asset-specific vulnerabilities. They discuss issues relating to cost-effectiveness tradeoffs for individual countermeasures, but fail to give an overall security system evaluation scheme. They do allow for a "system level impression of overall cost and effectiveness" created by considering the interaction of the selected countermeasures.

Garcia (2001) gives an integrated approach to designing physical security systems, evaluation and analysis of protective systems as well as risk assessment. A cost-effectiveness approach is presented, and the measure of effectiveness employed for a physical protection system is the probability of interruption, which is defined as "the cumulative probability of detection from the start of an adversary path to the point determined by the time available for response". Whitehead et al. (2007) suggest that a quantitative analysis is required for the protection of assets with unacceptably high consequence of loss, even if the probability of an adversary attack is low.

A PPS can be evaluated for its effectiveness using available software tools and techniques. A number of software tools are available for evaluating the effectiveness of a PPS. These include EASI, SNAP, SAVI, and SAFE.

Describing these software tools, Swindle (1979) refers to Safeguard Network Analysis Procedure (SNAP) as an NRC-sponsored methodology developed by Prisker and Associates, Inc., through subcontract to Sandia National Laboratories, for evaluating the effectiveness of the physical security measures of a safeguards system**.** He emphasizes that SNAP employs the network modeling approach to problem solving. Garcia (2001) also states that SNAP employs the network modeling approach to problem-solving. It requires the analyst to model the facility, the guard force, and the adversary force. SNAP is highly scenario-dependent and uses an assumed attribute method to give a measure of the PPS effectiveness within a certain scenario. For applications in which force-on-force battles are not expected, EASI is the preferred analysis tool.

Garcia (2001) opines that the System Analysis of Vulnerability to Intrusion (SAVI) model provides a comprehensive analysis of all adversary paths into a facility. This was developed in 1980 (Sandia National Laboratories, 1989). Once data on the threat, target, facility, site-specific PPS elements, and response force time are entered, the SAVI code computes and ranks the ten most vulnerable paths for up to ten response force times. This model uses the EASI algorithm to predict system performance and also uses Adversary Sequence Diagram (ASD) Model for multi-path analysis (Jang et al. 2009).

Engi and Harlan (1981) and Chapman et al. (1978) describe Safeguards Automated Facility Evaluation Methodology (SAFE) as a Sandia-developed, NRC-sponsored methodology for evaluating the effectiveness of the physical security aspects of a safeguards system. SAFE consists of a collection of functional modules for facility representation, component selection, adversary path analysis, and effectiveness evaluation. The technique has been implemented on an interactive computer time-sharing system and makes use of computer graphics for the processing and presentation of information.

For the purpose of this work, Estimate of Adversary Sequence Interruption (EASI) is the preferred analysis tool. This is because the model is simple to use, easy to change, and it quantitatively illustrates the effect of changing physical protection parameters. This paper is focused on using EASI for the evaluation of the effectiveness of the current physical protection system of an oil refinery.

Methodology

A- EASI Model

EASI is a fairly simple calculation tool developed by Sandia National Laboratories, USA. It quantitatively illustrates the effect of changing physical protection parameters along a specific path. It uses detection, delay, response, and communication values to compute the probability of interruption P_1. Since EASI is a path-level model, it can only analyze one adversary path or scenario at a time. It can also perform sensitivity analyses and analyze physical protection system interactions and time trade-offs along that path.

In this model, input parameters representing the physical protection functions of detection, delay, and response are required. Communication likelihood of the alarm signal is also required for the model. Detection and communication inputs are in form of probabilities (P_D and P_C respectively) that each of these total functions will be performed successfully. Delay and response inputs are in form of mean times (T_{delay} and RFT respectively) and standard deviation for each element. All inputs refer to a specific adversary path (Garcia, 2001). The output is P_1, the probability of interrupting the adversary before any theft or sabotage occurs. After obtaining the output, any part of the input data can be changed to determine the effect on the output. If there is one sensor on the path, this probability is calculated as:

$$P_1 = P_C \times P_D \quad (1)$$

Where, P_C is probability of guard communication, and P_D is probability of sensor detection.

One of the input parameters of this model was changed to suit the relevant environment. This parameter was the probability of guard communication, P_C. Evaluation of many systems designed and implemented by Sandia National Laboratories indicates that most systems operate with a P_C of at least 0.95. This number can be used as a working value during the analysis of a facility, unless there is reason to believe that this assumption is not valid. If actual testing at a facility yields a different P_C, this number should be used; if guard communication appears to be less dependable, a lower value can be substituted in the model. Factors that may influence P_C include lack of training in use of communication equipment, poor maintenance, dead spots in radio communication, or the stress experienced during an actual attack. This flexibility allows the analyst to vary Pc as needed to correctly represent the function. Based on expert judgement, the probability of guard

communication of 0.9 was used as the input value in this work to fit our own specific environment. This is because the guard response forces do not receive adequate training in the use of communication gadgets, and these gadgets are not properly maintained, thereby passing incomplete information or instituting delay in disseminating information. The values of probability of detection are based on the availability/non-availability of sensor(s) on the adversary paths. Delay and response values, in form of mean times and standard deviation for each element are purely expert opinion based on security guards' drills.

To use EASI in this work, we followed the steps listed below.

B- Critical Asset (Target) and Site Assessment

The refinery complex consists of two refineries and it occupies an area of 900 hectares. It is bounded on the south by muddy vegetation and sea, and on the north, east, and west by dry ground. There are many streams, creeks, residential buildings, and shops near the complex. These two refineries have combined processing capacity of 210,000 barrels of crude oil per day. This refinery complex houses different assets such as the administrative and technical buildings, oil pipelines, refined petroleum products storage tanks, refining processing units, and power plants. Of all these assets, the most critical asset is the 7½ km refined petroleum products pipelines that run from the inside of the refinery to the jetty where ships and fuel tankers load/offload products for import and export. Some parts of these pipelines run on top of the ground, on top of saline water, and underneath residential buildings.

The refinery complex is doubled fenced in some areas while others are singled-fenced. The complex has 8 entrance and exit gates, but only four major gates lead directly into the oil facilities. Gate 1 is an entrance gate for employees and visitors, gate 2 is for vehicles entering the facility complex, gate 3 is the exit for vehicles and persons, while gate 5 leads to the restricted area (which houses the crude oil refining facilities). These gates are constantly locked except when vehicles and human movements are required. The plant layout of the oil facility is shown in figure 1.

The heights of the concrete and electric fences are roughly 4-5 meters and there are 2 closed-circuit televisions (CCTVs) at gates 2 and 3. The videos recorded by these CCTVs are sent to and monitored by the control room. There are security operatives' posts at the entrance and exit gates of the refinery complex and at some distances along the 7½ km refined petroleum products pipelines. There are no sensors on the fences, gates, or pipelines. The 7½ km pipelines are partly exposed without any external fence protecting the part of the pipelines on land. There is also no fencing or other protective measures for the underground parts of the pipelines, or the parts in saline water.

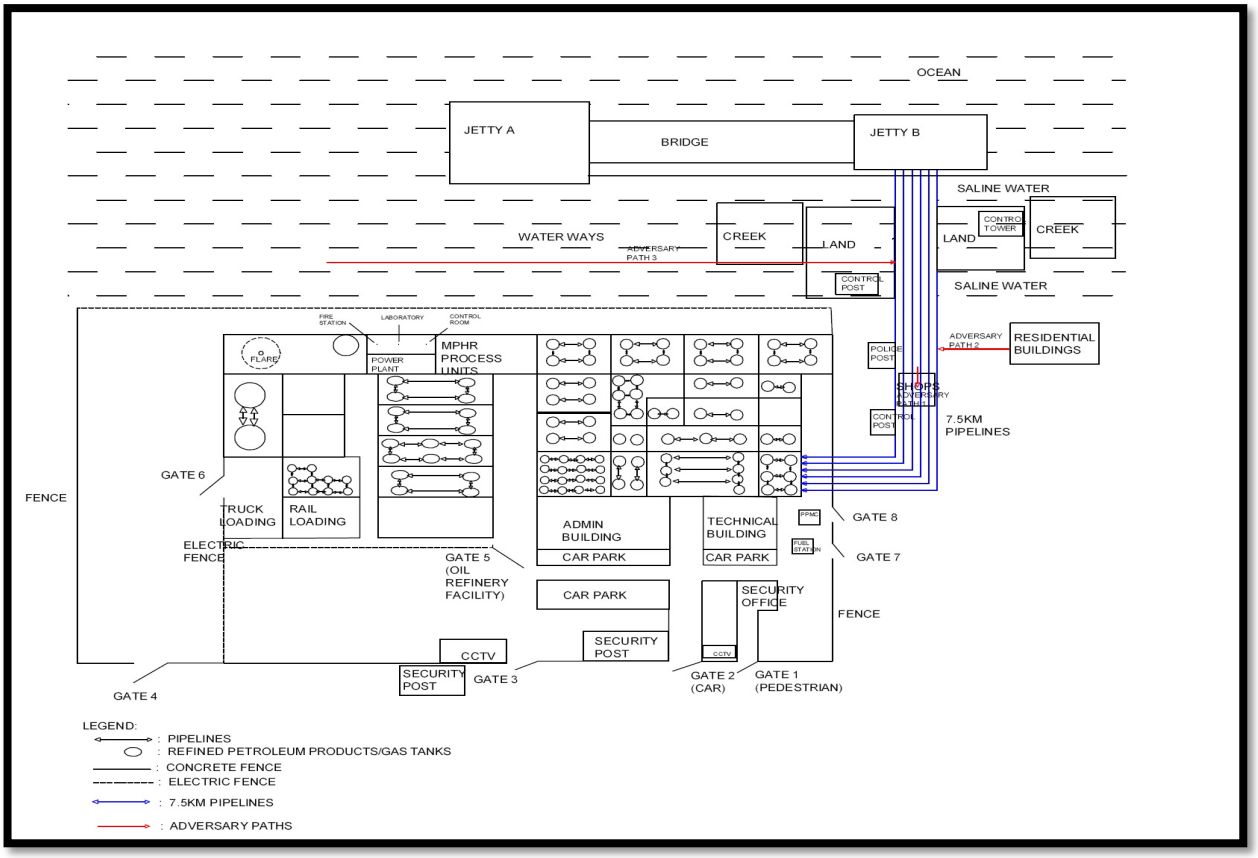


Figure 1 - The plant layout of the oil refinery with its most likely adversary paths and target.

The *Design Basis Threat* for critical assets must consider the attributes, characteristics, and motivations of potential insider and/or external adversaries who might attempt to damage or seek unauthorized removal of refined petroleum products, against which the PPS is designed and evaluated. This paper is limited to attack from external adversaries because EASI model does not handle insider attacks. Past hostilities that have occurred on the oil pipelines were all believed to be from the outside. Presently, there is no record of internal attacks on the oil pipelines. The possibility of an insider attack is not being ruled out completely, however.

The most likely adversaries of the oil facility are militants and local vandals. Other kinds of outside adversaries represent a lower probability of attack. In the past, adversaries have attacked the facility from outside of the refinery complex using equipment such as plasma cutters, welding machines, pliers, valves, and rubber pipes. From the information gathered, they appeared to be intent on oil pipeline sabotage and theft of refined petroleum products from the pipelines. The adversaries are motivated by the financial gain from the sale of refined petroleum products, or by their desire for resource control for their communities.

C- Possible adversary paths and action sequences

The most likely adversary paths to the critical asset are shown in figure 1. Adversary path 1 is from the shop on top of the 7½ km oil pipelines. Adversary path 2 runs from the residential buildings to the pipelines. Adversary path 3 runs through the water-ways, creek and on land to the oil pipelines. The possible adversary action sequences corresponding to the paths are shown in Fig. 2.

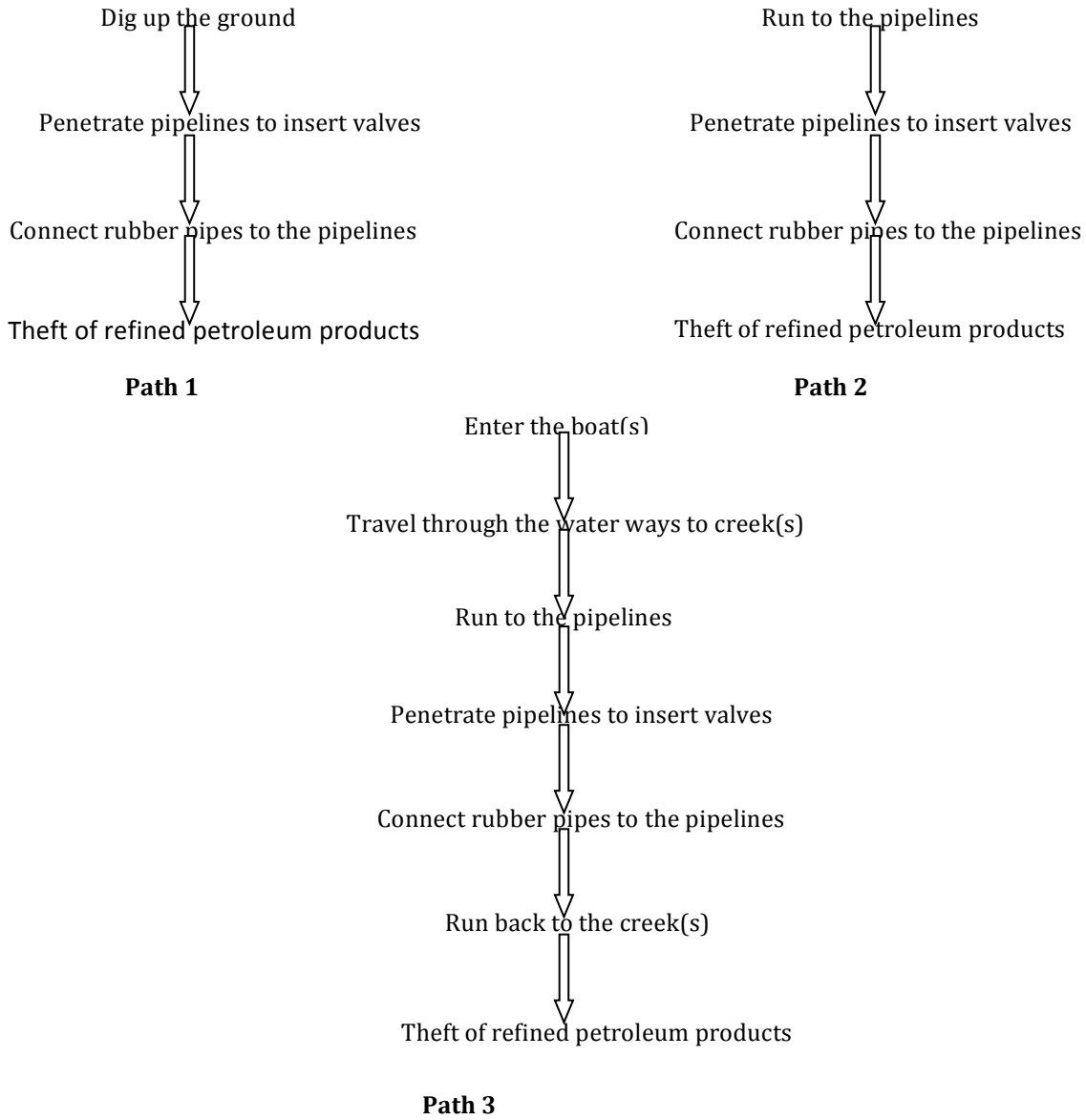


Figure 2 - Possible adversary action sequences.

Results and Discussion

Baseline paths

A computerized EASI model was used to calculate the probability of interruption (P_I) of all the most likely adversary paths using the input values obtained from the experts at the refinery site. Figure 3 shows the result of the EASI analysis of adversary path 3. The results of EASI analyses of adversary paths 1 and 2 produced the same output as path 3.

Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Mean Response Force Time (RFT) (secs)	Standard Deviation of RFT (secs)
0.9		720	216

Task	Description	P (Detection)	Location	Delays (Seconds): Mean	Standard Deviation
1	Enter Boat	0	B	6	1.8
2	Travel to the Creek	0	B	480	144
3	Run to Pipelines	0	B	10	3
4	Penetrate Pipelines	0	B	600	180
5	Connect Rubber Pipes	0	B	150	45
6	Run back to the Creek	0	B	10	3
7	Theft Target	0	B	120	36

Probability of Interruption:	0.000

Figure 3 - Results of EASI analysis for adversary path 3.

The results of the EASI analysis of the entire common adversary paths show the probability of interruption to be 0.000. This shows that the adversary cannot be interrupted until the refined petroleum products have been stolen from the pipelines or if an accident occurs during pipeline vandalism.

Proposed/Improved PPS

In re-designing the security system at the oil facility, new security measures and equipment were proposed to improve the three key functions (detection, delay, and response) of PPS. The suggested upgrades have the ability to achieve desired security principles. These include detection early in the path and prior to delay; effectiveness of delay at the asset; the relationship among detection, delay, and response functions; timely

detection; and the principles of protection-in-depth and balanced protection. The upgrades are as follows:

Upgrades for adversary path 1

A. Demolition of shops on top of the pipelines, erecting an external fence with a fence sensor system, and ensuring that buildings are erected beyond a mandatory distance of 25 m from one side of the pipelines;

B. Installation of sensors on oil pipelines;

C. Relocation of guards closer to the pipelines;

D. Enclosing the pipelines in a more hardened case with a stronger alloy.

Upgrades for adversary path 2

A. Erection of external fence with a fence sensor system and ensuring that buildings are erected beyond a mandatory distance of 25 m from one side of the pipelines;

B. Installation of sensors on oil pipelines;

C. Relocation of guards closer to the pipelines;

D. Enclosing the pipelines in a more hardened case with a stronger alloy.

Upgrades for adversary path 3

A. Destruction of creeks, and mounting of sea/water surveillance equipment;

B. Installation of sensors on oil pipelines;

C. Relocation of guards closer to the pipelines;

D. Enclosing the pipelines in a more hardened case with a stronger alloy.

We assigned values to the probability of detection of the proposed upgrades on each adversary path in order to see the effects of these upgrades on the output, i.e., probability of interruption. The effects of these upgrades were analyzed using the EASI model to show the new values of output, P_1. The results of some selected EASI analysis of the upgrades on each of the adversary paths 1, 2 and 3 are shown below. The result of EASI analysis of upgrade A on adversary path 1 is shown in figure 4.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Mean Response Force Time (RFT) (secs)	Standard Deviation of RFT (secs)
	0.9		420	126

Task	Description	P (Detection)	Location	Delays (Seconds): Mean	Standard Deviation
1	Dig Up Ground	0.9	B	240	72
2	Penetrate Pipelines	0	B	360	108
3	Connect Rubber pipes	0	B	60	18
4	Theft Target	0	B	120	36

Probability of Interruption:	0.789

Figure 4 - Result of EASI analysis of upgrade A on adversary path 1.

The result of EASI analysis of upgrade B on adversary path 2 after upgrade A has been executed is shown in figure 5.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Mean Response Force Time (RFT) (secs)	Standard Deviation of RFT (secs)
	0.9		420	126

Task	Description	P (Detection)	Location	Delays (Seconds): Mean	Standard Deviation
1	Run to the pipelines	0.9	B	10	3
2	Penetrate Pipelines	0.9	B	360	108
3	Connect Rubber pipes	0	B	120	36
4	Theft Target	0	B	120	36

Probability of Interruption:	0.768

Figure 5 - Result of EASI analysis of upgrade B on adversary path 2.

The result of EASI analysis of upgrade C on adversary path 3 after upgrades A and B have been carried out is shown in figure 6.

Estimate of Adversary Sequence Interruption	**Probability of Guard Communication**		**Mean Response Force Time (RFT) (secs)**	**Standard Deviation of RFT (secs)**
	0.9		600	180

				Delays (Seconds):	
Task	**Description**	**P (Detection)**	**Location**	**Mean**	**Standard Deviation**
1	Enter Boat	0	B	6	1.8
2	Travel to the Creek	0.75	B	480	144
3	Run to Pipelines	0	B	10	3
4	Penetrate Pipelines	0.9	B	600	180
5	Connect Rubber Pipes	0	B	150	45
6	Run back to the Creek	0	B	10	3
7	Theft Target	0	B	120	36

Probability of Interruption:	0.845

Figure 6 - Result of EASI analysis of upgrade C on adversary path 3.

Table 1 shows the summary of the values of the output, i.e., the probability of interruption (P_1) after the all proposed security upgrades have been implemented.

Table 1 - Summary of values of Probability of interruption (P_1) after Proposed upgrades.

Paths / **Suggested Upgrades**	**Path 1**	**Path 2**	**Path 3**
A	0.789	0.699	0.660
B	0.850	0.768	0.805
C	0.886	0.874	0.845
D	0.890	0.877	0.874

From table 1 it can be seen that the values of the output (the probability of interruption) increased after each proposed upgrade was applied to the adversary paths. The table shows that the final value of P_1 at the end of the entire upgrade (Suggested Upgrade D) on each adversary path is approximately 0.9. When the P_1's along all paths are approximately equal after the upgrades, the physical protection system is said to be "balanced", i.e., all paths are equally difficult for the adversary to achieve their goal. Note that balance is achieved by mixing detection, delay, and response components, and that there are a number of possible combinations that will result in acceptable system performance. This provides the opportunity to select combinations that meet cost and operational requirements without compromising system effectiveness.

Conclusions

This work involved evaluating the effectiveness of the current physical protection system for an oil refinery using the Computerized EASI model. Results obtained from the analysis of the most likely adversary paths showed that the values of probability of interrupting the adversaries (P_1) were very low. But by upgrading the physical security systems with certain measures and equipment, the values of P_1 increased significantly, improving security.

Acknowledgments

The authors are grateful to the Nigeria Atomic Energy Commission (NAEC) for sponsoring this research work.

References

Chapman, L.D., Grady, L.M., Bennett, H.A., Sasser, D.W. and Engi, D., (1978): "Safeguards Automated Facility Evaluation (SAFE) Methodology," Sandia Laboratories report SAND 78-0378, NUREG/CR-0296.

Doyon, L.R., (1981): "Stochastic Modeling of Facility Security-Systems for analytical solutions," Computers & Industrial Engineering, vol. 5, no. 2, pp. 127–138.

Engi, D. and Harlan, C.P., (1981): "Brief Adversary Threat Loss Estimator (BATLE) User's Guide," Sandia National Laboratories report SAND 78-1136, NUREG/CR-1432.

Garcia, M.L., (2001): "The Design & Evaluation of Physical Protection Systems", Butterworth-Heinemann, pp. 251-259.

Grassie, R.P., Johnson, A.J. and Schneider, W.J., (1990): "Countermeasures Selection and Integration: A delicate balancing act for the security designer," in Proceedings IEEE 1990 International Carnahan Conference on Security Technology: Crime Countermeasures, Lexington, Kentucky, pp. 116–123.

Schneider, W.J and Grassie, R.P., (1989): "Countermeasures Development in the Physical Security design process: An Anti-terrorist perspective," Proceedings of 1989 International Carnahan Conference of IEEE on Security Technology, Zurich, Switzerland, pp. 297–302.

Jang, S.S., Kwak, S., Yoo, H., Kim, J and Yoon, W.K., (2009); "Development of a Vulnerability Assessment code for a Physical Protection System", Journal of Nuclear Engineering and Technology, Vol. 41, No. 5, pp. 747-752.

SAVI, (1989): Systematic Analysis of Vulnerability to Intrusion, V1, SAND89-0926, Sandia National Laboratories, pp. 1-8.

Swindle, D.W., (1979): "The Use of Effectiveness Evaluation in the Design of a Physical Protection System for the Consolidated Fuel Reprocessing Program's Hot Experimental Facility," 20th Annual Meeting of the Institute of Nuclear Materials Management, Albuqueraue, NM; Nuclear Materials Management VIII, 761, pp. 1-20.

Whitehead, D.W., Potter, C.S and O'Connor, S.L (2007): "Nuclear Power Plant Security Assessment Technical Manual", SAND2007-5591, Sandia National Laboratory, pp. 1-63.

Journal of Physical Security 7(2), 42-49 (2014)

Design of an Access Control System: A Paradigm for Small Nuclear Facilities

B. Nkom[1], I.I. Funtua[2], and L.A. Dim[3]

Centre for Energy Research and Training (CERT), Ahmadu Bello University, P. M. B. 1014, Zaria, Nigeria
[1]b.nkom@ieee.org; [2]iifuntua@yahoo.com; [3]lawrenceanikwedim@yahoo.com

Abstract - This paper describes the design of a Radio Frequency Identification (RFID) personnel access control/anti-intruder system, using an active Quad Tag (RWD-QT) Reader/Writer module in direct conjunction with a Microchip™ PIC18F4550 microcontroller, which provides control, non-volatile memory, data processing, and external communication functions. The system obtains signals from an RFID module, motion detectors and vibration sensors to effectively control a dot-matrix LED display, alarm sounders, and an electric door strike, thereby providing a low-cost, power-efficient, reliable means of supplementing traditional methods of providing physical protection for research reactor buildings. Relevant IAEA documents such as INFCIRC/225/Rev. 4 and TECDOC 967 (Rev. 1) were duly consulted for the necessary guidance in this research and development effort.

Keywords - Physical Protection, Low Cost, Radio Frequency Identification (RFID), Access Control System, Microcontroller.

I. INTRODUCTION

Since 2011, lingering terrorist threats have required the global nuclear industry to constantly reaffirm its commitment to ensuring nuclear security.[1-2] By factoring in the present globalization trends, nuclear security has evolved into an issue that positive-thinking individuals, organizations, and governments worldwide now realize concerns and affects them, due to the potential for huge consequences for everyone if a large scale breach occurs in any part of the world.[3]

Physical protection is an integral part of nuclear security. Guidance note G101 of [4] states the need for a physical protection system and points out that a system based on a combination of personnel, hardware, procedures, and facility design should be established to achieve the desired protection, bearing in mind the overall safety of the facility. This paper is concerned with protection using hardware, specifically electronic hardware. The term "facility" used here may be viewed in broad terms to include fixed facilities such as reactors and spent fuel repositories, as well as in-transit facilities that refer to special facilities used in transporting nuclear material, (e.g., trucks or railcars) which are sometimes not properly secured.[2] The access control/anti-intruder system described in this paper is primarily meant to supplement existing fixed facility protection, specifically at university-based research reactors. The terms "asset" and "threat" used here may also be viewed in broad terms. An asset refers to anything that is being protected (personnel, equipment, nuclear and non-nuclear material) that aids nuclear security. A threat refers to anything that compromises the security of a nuclear material or facility (natural disasters, adversaries). This paper is concerned with the means of protection against adversaries, which include protestors (demonstrators, activists, and extremists), terrorists, and criminals from outside; as well as internal employees, regular visitors, and contractors/suppliers with grudges, criminal tendencies, or psychological/drug-related issues.[5,18]

University-based research reactors are mostly located in fairly dense locations, sometimes inside campuses, and thus may be perceived as easy targets by adversaries. A lot of reactors experience a large influx of students, visitors, and clients on a daily basis, which may cause laxity in security protocols when juxtaposed with long periods of absence of security-related incidences. Long shutdown periods as a result of school calendars and national holidays are also common. In addition, most of these reactors are used for non-profit, non-commercial purposes that offer little financial gains to justify elaborate physical protection schemes, giving rise to a high risk scenario.[6] Furthermore, such reactors that are located in politically unstable, technologically unprepared, and economically disadvantaged countries are at greater risk due to lean budgets, financial incentives to engage in criminal activities, and lack of understanding of physical protection technology.[7]

This paper seeks to show that with the advancement of physical protection technology in general, and electronics technology in particular, acquiring electronic physical protection systems does not necessarily require big budgets. In addition, we will try to show that managers of such facilities can be actively involved in the rudimentary design process in order to tailor the electronic systems to suit their individual circumstances, taking national, regional, and

international regulations and advice into consideration. This is actually expected in physical protection considerations, as expressly indicated in guidance note G427 of [4].

The rest of this paper is organized as follows: Section Two gives an overview of a few modern electronic devices that function in accordance with the primary requirements for physical protection systems, and also provides a brief description of microcontrollers. Section Three mentions a few hardware considerations necessary for successful electronic physical protection system design and outlines the design process for the control and data processing centre for our system. Section Four covers final system implementation and verification considerations, including a few factors to consider when actually carrying out security system installations. Concluding statements are given in Section Five.

II. OVERVIEW OF ELECTRONIC PHYSICAL PROTECTION DEVICES

An effective physical protection system should perform the following primary functions: Deter, Detect, Assess, Delay, and Respond.[4] G103 states that the physical protection sub-system first encountered by adversaries in any facility should serve as a huge deterrent by presenting a difficult obstacle to penetrate. These obstacles are usually non-electronic systems such as steel gates, but in recent times there have been increased use of electrified fences and armored floodlights as the first line of defense.[8]

Attempts to breach a protected area are to be detected by a physical protection system, and this is mostly achieved by the use of electronic sensors. These are typically devices that detect changes in a physical quantity (heat, motion, vibration) and convert them to electrical signals. These signals are then made readily available for indication and/or annunciation at the central alarm station via transmission sub-systems. Providing a supplementary means of indication at the point of detection may also serve as a deterrent. Motion sensors are used in the system described in this paper; the type and specifications cannot be stated here as required by confidentiality clauses in sections 4.3.1 and 4.3.2 of [9], and G444 and 445 of [4]. If a fixed nuclear facility has been well designed, its vital areas will have a small number of entrances/exits, windows, and other vulnerable access points as recommended by G610 of [4], which will reduce the number of such devices to be used at each point, and hence lower costs.

Best practice highly recommends that assessment should go hand in hand with detection, so that confirmation of an intrusion may be done at the central alarm station when detection occurs. This is best achieved by visual means via CCTV systems [8] in conjunction with guards, as recommended in G108 and G615 of [4]. This is already in adequate use in the facility where the access control/anti-intruder system is to be installed.

In order to delay an adversary, the entrance and perimeter to the vital or inner area of the facility should be difficult to breach, even by the use of force, and this is a function of the facility design. Good access control systems should also be capable of controlling the physical barrier at the entrance/exit point automatically by preventing access to the vital area until authorization is granted, thus contributing to the delay function. This is mostly achieved by electromechanical sub-systems such as door strikes and rotating doors.

A well-designed physical protection system should always assume a threat of sabotage, as stated in 7.1.1 of [9] and G104 and G110 of [4], thus a rapid human intervention to an intrusion may be achieved by the access control/anti-intruder system's ability to respond quickly and effectively by promptly alerting response teams through communications sub-systems, by the use of aural and visual alarm indicators such as sirens and strobes. Additional response measures such as initiating a lock-down by electromechanical means may also be carried out by the system.

Assuming category I nuclear material as classified in [9], in the case of protection against removal of nuclear material, or protection against sabotage of nuclear power reactors, access to the protected area will be only by positive identification through photo badge ID's. Since a more stringent and reliable access control measure is required for the vital area, electronic access control systems that use one or more means of identification are recommended, as stated in 6.2.2 and 7.2.3 of [9], and G601 of [4]. At system design stage, these means of identification come as electronic device modules that are added unto a control and power sub-system to make them functional. A few of such identification modules are numeric keypad modules, biometric fingerprint modules, and biometric iris modules. RFID is the identification scheme for the system described in this paper. Due to its wide availability and susceptibility for spoofing and counterfeiting, infrared detectors and proximity switches were also incorporated in the implementation as extra breach detection barriers.

Placing a combination of the devices described above in a physical protection system, based on primary function and principles of operation, is necessary to obtain an acceptable level of protection. Thus, a way to coordinate the functions of all these devices is needed. Traditionally, pre-manufactured off-the-shelf alarm control panels, typically costing between $80 and $560, depending on level of sophistication, robustness, and communications technology employed, are used.[10] The access control/anti-intruder system described in this paper uses a microcontroller chip to achieve the coordination function. These, together with their programming kits, typically cost between $5 and $240 [11] depending on manufacturer, number and type of on-board modules, and semiconductor technology used. Choosing and

using a suitable one sensibly will drastically reduce the cost associated with the control function.

The microcontroller is a handy device that continues to gain popularity amongst electronic systems developers. It is a computer on a chip that emphasizes self-sufficiency and cost effectiveness; and as the name implies, it is optimized for controlling other devices/components via on-board modules such as ADC's, counters, CCP's, analog comparators, and communications. In recent times, microcontrollers have become vital components in virtually all electrical/electronic equipment and systems, such as home entertainment systems and vending machines; where they are used in controlling the functions of these equipment, and in processing and transferring data into and out of external units connected to them.[12-14] Electronic access control systems are certainly not left out.

Microcontrollers have the advantage of being software configurable and software driven, thus a carefully designed program will reduce the need for external support chips such as digital clock/calendars, thereby offering a low component count. They offer a high level of versatility in design since changing a design parameter mostly just requires changing an aspect of the program. This is vital for physical protection systems, where conditions are highly dynamic. Also, a microcontroller may be directly interfaced with a suitable display, thereby providing a means of creating a menu-based user interface for the system; which will make it more user-friendly. Very importantly also, a microcontroller can be interfaced with a PC for the purpose of data transfer, which is vital for any access control system. No less importantly, a typical microcontroller is a small-sized, lightweight, low-power device, thereby offering the advantage of a small, energy-efficient control panel. In addition, there are various opportunities provided by the development platforms of these microcontrollers to simulate, debug, emulate, and generally troubleshoot your application even before the microcontroller is programmed. This is obviously a time saving tool. The development platforms themselves are deployed on regular PC systems, thereby providing the most important advantage of executing projects completely in-house.

The choice of which microcontroller to use is influenced by popularity of the general family and particular device, suitability for intended application as regards number of input/output ports and on-board peripherals, availability in locality, cost, device architecture, and the device manufacturer, which also has a bearing on its ease of use.[13] By taking these factors into consideration, we narrowed down to the PIC18F4550 microcontroller from Microchip™. This is a 40-pin 16-bit nanoWatt device with 32 kilobytes of self-programmable flash program memory, 256 bytes of flash EEPROM memory, 34 input/output pins with individual direction control, four 16-bit timer/counter peripherals, USB/EUSART/I²C communications, 12 interrupt sources including interrupt on port change for RB<4:7>, multiple selectable oscillator peripherals, four addressing modes, 8-level deep hardware stack, and a large general purpose register pool. It employs an advanced Harvard RISC architecture, featuring 76 single-word instructions for writing assembly code for 18xxx devices. It requires 2 to 5 V DC and consumes less than 200 μA under any condition, with core speeds of zero to 20 MHz valid for operation.[19]

III. SYSTEM DESIGN CONSIDERATIONS

System Design refers to the process of planning a system so that it functions in accordance with a predetermined concept. This concept will only be successfully actualized by considering numerous factors (page 2, paragraph 4 of [15]), some of which are described below:

1) Characteristics of Physical Protection Systems:

These are outlined in G 112 to G118 of [4], the ones that concern us most are:

1. Defense in Depth: This refers to the practice of placing multiple levels of protection sub-systems in sequence along all the probable paths that adversaries will follow in the facility to get to the asset. As previously mentioned, the access control/anti-intruder system described in this paper is to serve as a sub-system in an already existing physical protection system, so it helps the larger system to achieve this requirement. However, defense in depth can be incorporated into the sub-system itself, as will be shown subsequently.
2. Minimum Consequence of Component Failure: This refers to the requirement that the entire physical protection system at the facility should not fail as a result of the failure of a component or sub-system. Measures will be taken to ensure that the failure of the system described in this paper will not cripple the entire physical protection system at a facility by making it entirely independent so that it can serve as a redundant system. However, it will be shown that a good choice of hardware components and design concepts for the access control/anti-intruder system can reduce the odds of total failure going unnoticed.
3. Balance with Other Considerations: An overall balance must be achieved between the physical protection system and other considerations such as safety of personnel at the facility, cost of the system, and structural integrity of the facility itself. These three factors in particular have been positively addressed in the process of designing the system.

2) Functional Conformity:

A physical protection system must be designed with basic functional logic so that it is effective, efficient, and easy to use but not necessarily easy to

figure out. In the case of electronic systems, the functions of the user interfaces should be straightforward, to reduce any confusion pertaining to the operation of the system and thus instill confidence in it. However, the particular manner in which the sensors and actuators interact with the control system should be kept confidential. The entire system should be as energy-efficient as possible, because it should be able to function for a reasonable length of time on battery power, in case the mains supply is unavailable for any reason. All the components that make up the system should be easy to troubleshoot and maintain, so as to reduce down time in case of breakdowns.

3) Vulnerability assessments:

All physical protection systems must be subjected to vulnerability tests, to judge how effective they will be in warding off attacks from adversaries. Some of the types of attacks that should be considered when designing such systems are as follows.[16]

1. False Alarming: This refers to the situation where the adversary induces random, multiple false alarms in a system in order to undermine its usefulness and the confidence placed in it.
2. Fault analysis: This refers to the situation where an adversary, mostly with technically savvy, makes a system function in an abnormal manner by altering its operational parameters, in order to obtain useful information that can be exploited. An example is changing the ambient temperature around a sensor.
3. "Poke the System": This refers to the situation where an adversary probes the system without tampering with it and observes its responses, in order to obtain useful information. An example is taking note of how near one can get to a motion sensor before it detects a presence.

4) Forms of Adversaries:

A few examples of adversaries were given in the introduction, but the point of interest here is the fact that adversaries can come from within the facility organization itself, or at least be aided by people within it. Thus a physical protection system should be designed with the possibility that a legitimate member of the facility may become an adversary at any time. [16-18]

Our concept in this case is an electronics system that will carry out the following general functions:

1. Sense the movement of an animate object already in a protected area towards possible access points to a vital area such as entrances/exits, ducts, and windows, and relay this information to the central alarm station, i.e., Detect. This will be achieved by using motion detectors.
2. Sense the prolonged presence of an animate object in close proximity to an access point to the vital area, and set off a soft alarm capable of being heard at that point, i.e., Deter. This will be achieved by enabling a false alarm time period once an animate object is detected, during which a mini piezo-electric sounder is activated.
3. Monitor all possible access points to the vital area, including designated entrances/exits, to determine when an intrusion occurs or is attempted, and set off a general alarm. This will be achieved by the use of vibration/ultrasonic transducers to detect attempted forced entry, non-magnetic proximity switches to determine door position for likely intrusion, high-intensity sirens to provide a general alarm, and Ethernet communications to relay the situation to the central alarm station.
4. Monitor designated entrances/exits to authorize unhindered access to persons bearing valid RFID tags, and to keep records of instances of entrances and exits for reference and analysis purposes.

The desired system functions stated above served as the main guidelines in creating a flowchart, which completely describes the functions of the access control/anti-intruder system in relation to the sensors and actuators to be used in the system. This is shown in figure 1. It serves as the basis of the firmware to be implemented in our microcontroller of choice, which was developed by translating the structure, instructions, and variables specified in the flowchart into a computer program written in Microchip MPLAB assembly language to influence designated outputs in response to signals from designated inputs, on-board peripherals, and changes in internal registers. The predominant reasons for choosing the PIC 18F4550 microcontroller were its program memory space, on-board peripheral devices, and number of input/output pins; however, this was done after some preliminary design considerations. The firmware development process actually started with the identification and procurement of a motion detector, a vibration detector, an Avago HCMS 2975 serial input 8-character dot-matrix LED display [22], and an RFID module. The best firmware routines needed to run these devices had to be first established by initially working with each of them separately, before integrating the routines in the firmware.

The Microchip MPLAB Integrated Development Environment version 7.52 was used to design, debug, and simulate the firmware, and thereafter insert it into the PIC 18F4550 microcontroller via a PICStart Plus Device programmer in order to make it a functional piece of hardware, which is specifically the control and data processing center for all the devices that constitute the access control/anti-intruder system. A study of the microcontroller's data sheet will show that its peripheral resources are more than adequate to support a fully conformal implementation of the system flowchart.[19] To ensure a low component count for

the system, the firmware was developed to also run a clock/calendar routine in concordance with the multiple functions desired of the access control/anti-intruder system, which placed large constraints on loop timing in order to ensure accuracy. This was effectively resolved by using flags for all desired actions, with the actions actually being managed within the main firmware loop containing the clock/calendar routine. Additional flags may in turn be generated within the main loop to influence actions within the interrupt service routine.

It can be observed from the flowchart that a reasonable level of defense in depth has been achieved by the provision of routines for motion detectors and vibration/proximity sensors in the firmware.

Connecting and mounting these devices correctly will increase the odds that adversaries will have to defeat the protection provided by them in sequence, starting with the detection of motion towards an access point, followed by the detection of attempted forced entry, and then the forced entry. The detection of motion itself triggers a soft alarm at the point of detection as well as at the central alarm station (CAS) to serve as a deterrent to the adversaries by indicating that their presence at that location has been observed. Since at this time the adversaries are not yet at the access point, a visual confirmation of the presence of adversaries will allow the response teams ample time to take action, hopefully before any significant damage is done. Additional defense in depth has been made available by the inclusion of a routine for an electric door strike, lock, rotating bar or door, which will normally prevent access to the vital area until authorization is granted via the RFID module.

The access control/anti-intruder system, even if used without redundancy, will have low consequence of component failure because provision has been made for regular transmission of the status of the system to the CAS via state of health (SOH) data, which will include data about the power situation of the system. In addition, all devices connected to the system provide a definite electrical signal when operational, thus the absence of such signals will be interpreted by the system as an alarm condition.

Provisions for minimizing the impact of false alarms have also been provided in the flowchart. The CAS is alerted when motion detection occurs in order for an assessment of the situation to be made. Even when vibration detection occurs, the general alarm, which may consist of a number of actuators (strobes, sirens) is activated intermittently in accordance with the detector/sensor signal. A predetermined number of "false" alarms within a fixed time period will be interpreted by the system as a "poke" and thus the general alarm will be fully activated. This time period should be adequate for guards to carry out a thorough investigation of the situation to ascertain if adversaries may be responsible for it.

Data pertaining to login/logout attempts, whether successful or not, are relayed to the CAS for reference and analysis purposes. This may aid in identifying potential insider threats in a timely manner.

IV. SYSTEM IMPLEMENTATION CONSIDERATIONS

System Implementation refers to actual construction, verification, installation, and commissioning of the system. The construction of the system required the consideration of a number of issues in general hardware design and implementation that were necessary to ensure functional harmony between the programmed microcontroller and all other hardware components specified for the data logger on integration; first on a breadboard for hardware troubleshooting purposes, and then onto a PCB. A few of these considerations, in turn, required the use of additional hardware components, for overall system effectiveness and efficiency.

Even though we opted to use one of the available internal oscillator speeds for the microcontroller, we chose to also use the crystal clock option with a speed of 32.768 KHz for the timer 1 module, which was configured to run as a real-time clock for our clock/calendar routine. This necessitated the addition of a crystal of like specification and two 30 picoFarad ceramic capacitors necessary to form a crystal oscillator, to our hardware. We also opted for normally open, spring-loaded PCB button switches as our user input interfaces for exit request by regular users and menu-based system operation for the administrator of the system. To avoid interference from electrical noise due to floating inputs at normally open switch contacts, a simple buffering arrangement using TTL inverter gates was used. This called for the addition of a 74L04 IC to our hardware.[20]

A battery backed-up power source was deemed an ideal choice for the data logger because the microcontroller's volatile memory, in the form of its general purpose registers, is used for keeping all timing counts. In addition, the access control/anti-intruder functions must withstand fault analysis attacks from adversaries, and disrupting power to a facility falls under this category; thus, the microcontroller must be kept powered when the system is in use. This necessitated the acquisition of a switch-mode battery-backed power supply module costing $124. However, a transformer power supply with similar specifications may be built for far less.

The only components vital to the control and data processing function of the access control/anti-intruder system are the microcontroller and RFID module. This is desirable because a low component count improves the systems reliability and energy-efficiency, and keeps the complexity of the system, and hence its maintenance costs, low; which in turn will ensure that the system stays in fairly regular service.

The access control/anti-intruder system went

through some basic tests for functionality, durability, power consumption, and safety. Power consumption was found to be 38 mA while running. Heat dissipation was barely noticeable, thus no heat sink and/or fan is required for the system; however, vent slots are necessary in any casing considered for the system if a transformer power supply is used, to ensure it is adequately cooled by air convection. At this stage, the data logger was considered to be verified.[13]

The installation and commissioning of any physical protection system is subject to ratification and approval by the regulatory body of the state in question (4.2.4.2. of [9] and G424 of [4], thus the access control/anti-intruder system described in this paper has not yet been installed. However, a few factors to consider when carrying out an installation of this kind are [21]:

1. Integration with existing system: In our case, the system was designed to be independent of any existing access control/anti-intruder system and thus requires no extensive integration with existing systems at the facility where it is to be installed, save for power sources. Structurally the system's control unit is rather small to constitute much of a problem. However, safety analysis, especially in relation to emergency procedures will be carried out in due course.
2. Location of system devices: In our case, the system is meant to be installed at a pre-existing facility as a redundant electronic physical protection system, and thus the final positions of all devices that make up the system will be easy to locate since the vital area, protected area, and possible access points are already known. The unit housing the microcontroller and RFID module, and battery backed-up power supply should naturally be installed in the vital area (G 601 of [4]).
3. Security of Installation: Parts of the system that will be located outside the vital area such as the motion detectors, RFID antenna, and the transmission sub-system in our case, need to be protected. In-wall conduits or armored surface trunking are necessary for cables, with dummy cables added as further precaution (6.2.16 and 7.2.16 of [9]).
4. Inclusion of dummy devices: It is a good security system installation practice to install a number of dummy devices together with the actual ones, as a ruse to intruders.

V. CONCLUSION

The design, implementation, and use of any physical protection system or sub-system involve processes that address the question of how to effectively protect assets from threats. This is highly multidimensional and thus makes physical protection a bit difficult because, while an adversary only needs to find and exploit one vulnerability in a physical protection system to succeed, designers of such systems must identify, understand, and factor-in all possible vulnerabilities. Also, adversaries mostly need to attack from just one point, while security managers must protect entire facilities. Another serious challenge for physical security is the fact that success is equated with non-incidences, which does not permit effective cost/benefit analysis and often results in inadequate resources being allocated. Thus, security budgets decay over time as long as there are no incidences, thereby affecting the security level, mostly due to reduced quality and quantity of paid security personnel and lack of upgrades to systems to keep up with technological advancements. Personnel factors also contribute a lot to general security, thus it is not advisable to rely solely on guards to protect access points that are merely locked.[16]

Since no two facilities are the same, in order to properly design an effective physical protection system, designers and managers must work closely together, and this is easiest when the designers are an integral part of the facility, particularly its engineering wing. Thus, the main objective of this paper is to promote the method of system development suggested herein, which may be used in acquiring an effective electronic physical protection system of a reasonable level of sophistication for organizations that are hampered by low budgets.[15] The microcontroller, display, RFID module and tags, motion detector, vibration sensor, and all sundry items added subsequently, cost a total of $220 (power supply excluded). Labor time was approximately 135 man-hours. There may exist pre-manufactured access control/anti-intruder systems that cost less, but a high level of customization is inherent in designing and implementing in-house, which offers better control of all circumstances that may arise subsequently. This method is highly recommended, especially in creating electronic physical protection system redundancy. The two main constraints identified are the ready availability of embedded system hardware programmers within the facility, and the availability of the development kits to effect the designs; however, making these available where they may be lacking is an investment in the engineering capabilities and infrastructure of that facility, and is highly encouraged.

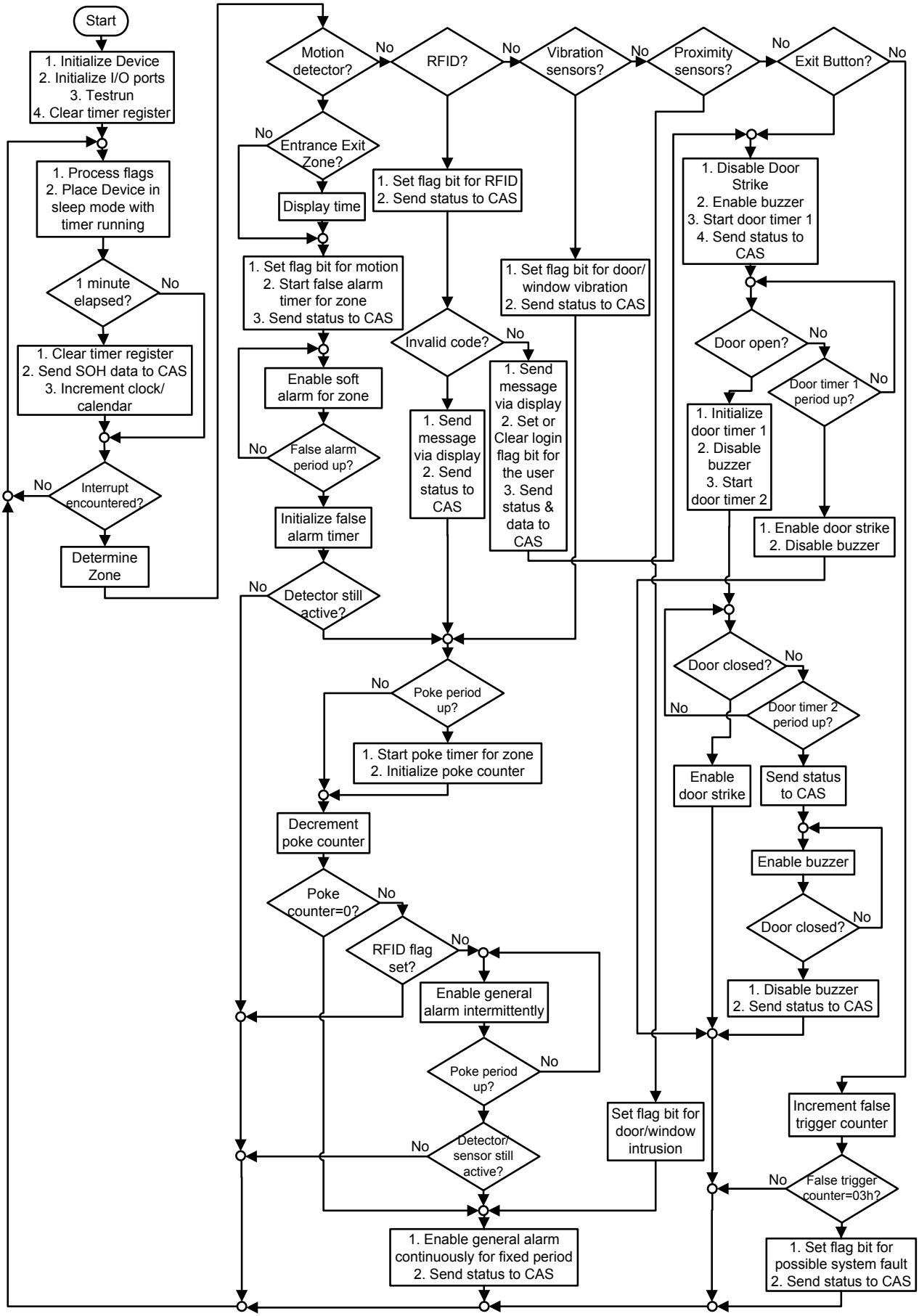


Figure 1 - Flowchart for the access control/anti-intruder system.

REFERENCES

1. *Nuclear Terrorism;* Report by the Director-General to the 46th Regular Session of the General Conference of the IAEA (Items 2,3, 21, 28 and 29 of the Activity Areas); Vienna, Austria, 12th August 2002.
2. *Asymmetrical Sabotage Tactics; Nuclear Facilities/Materials and Vulnerability analysis;* J. D. Ballard, NUMAT Conference Proceedings; Salzburg, Austria, 08 – 13 September 2002.
3. *Nuclear Security Report 2008 – Measures to Protect against Nuclear Terrorism;* Report by the Director-General to the 52nd IAEA Board of Governors General Conference (Items 1 and 18); Vienna, Austria, 22nd August 2008.
4. IAEA-TECDOC-967 (Rev. 1).Guidance and Considerations for Implementation of INFCIRC/225/Rev.3, The Physical Protection of Nuclear Materials and Facilities
5. *International Standard for Design Basis Threat (DBT);* J. Blankenship, NUMAT Conference Proceedings; Salzburg, Austria, 08 – 13 September 2002.
6. *Nuclear Terrorism Potential: Research Reactors vs Power Reactors?* (Page 7 Paragraph 4)*;* G. Bunn et al, NUMAT Conference Proceedings; Salzburg, Austria, 08 – 13 September 2002.
7. *International Terrorists Threat to Nuclear Facilities* (Page 7)*;* C. Braun et al, NUMAT Conference Proceedings; Salzburg, Austria, 08 – 13 September 2002.
8. *Enhanced Physical Protection Measures and the Agency's Plan of Action for Protection against Nuclear Terrorism;* T. Rauf, presented at the 2003 NPT PrepCom, 6th May 2003.
9. *IAEA-INFCIRC/225/Rev. 4.*
10. *Components Catalogue*, RS components website. [Online]. Available: http://www.rs-components.com
11. *Microchip™ Catalogue*, Microchip™ website. [Online]. Available: http://www.microchip.com
12. *An Introduction to PIC Microcontrollers;* R. A. Penfold, Bernard Babani Ltd, 1997.
13. *Integrating Hardware and Software for the Development of Microcontroller-based Systems;* A. H. G. Al-Dhaher, Elsevier Science Journal, Microprocessor and Microsystems 25 (2001), pages 317 – 328.
14. *Introduction to Embedded Systems;* Wiki website. [Online]. Available: http://en.wikibooks.org/wiki/
15. *Nuclear Materials and Facilities – Security Systems and Technology R & D Trends;* D. Ellis et al, NUMAT Conference Proceedings; Salzburg, Austria, 08 – 13 September 2002.
16. *Effective Vulnerability Assessments for Physical Security Devices, Systems, and Programs;* R. G. Johnston et al, NUMAT Conference Proceedings; Salzburg, Austria, 08 – 13 September 2002.
17. *An Integrated Approach to Adapt Physical Protection to the New International Terrorism Threats;* F. Steinhausler et al, NUMAT Conference Proceedings; Salzburg, Austria, 08 – 13 September 2002.
18. *Nuclear Security Series 8 – Preventive and Protective Measures against Insider Threats.*
19. *Microchip™ PIC18F4550 Data Sheet.*
20. *Practical Electronics Handbook (2nd Edition);* I. Sinclair, Heinemann Newnes, 1988.
21. *Nuclear Security Series 4 – Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage.*
22. *Avago HCMS-29 Series Dot-Matrix LED Display Data Sheet.*

Do Security Systems Fail Because of Entropy?*

Michael Coole and David J. Brooks

School of Computer and Security Science, Edith Cowan University
m.coole@ecu.edu.au and d.brooks@ecu.edu.au

ABSTRACT

Security is implemented to mitigate an organisation's identified risks, linking layered elements into a *system* to provide countermeasure by the functions of deter, detect, delay, response and recovery. For a system to maintain its effectiveness these functions must be efficaciously performed in order; however, such systems may be prone to decay leading to security failures. This study used a three-phase qualitative methodology to develop an entropic theoretical foundation and to present a model of entropic security decay.

Security decay is defined as degradation of the microscopic constituents propagating through the security system as a result of knowledge, cultural or economic factors. Security management should be primarily concerned with managing the entropic processes against commissioned security system levels; however, when decay occurs it is as a bottom-up factor. This study suggests security controls should be measurable and be designed, applied, and managed to maintain security system efficacy.

Key words: *Decay, entropy, defence-in-depth, layered security, system, physical security, security management*

INTRODUCTION

Security risk management may be implemented in an open system approach, using the strategy of defence-in-depth (DiD). Nevertheless, it is proposed that DiD strategies can be impeded by the characteristics of disorganization and decay underpinning entropy. For an organisation to maintain a sound security profile, all DiD elements and their constituents must be maintained at their optimum level of commissioning performance. This study argues that the scholarly area of Security Science should draw on the concept of entropy to establish the concept of security decay. Security decay results in a reduction in overall system performance, which could be avoided through effective risk identification at the design stage, and the active monitoring and reviewing of treatment strategies.

Background of the study

Underwood stated that "the provision of effective security is paradoxically the first step towards decay, as an effective system will not only repel successful attacks, but also prevent the attacks being made … an illusion is then created that the established security is unnecessary suggesting decay will follow until the degree of security falls to the point where an attack will succeed" (1984, pp. 249-250).

*Editor's Note: Be sure to see the reviewers' comments at the end of the references.

Early literature on the concept of security decay suggested that the cause was the attitude of apathy, which led to poor compliance to security procedures (McClure, 1997). Nevertheless, decay is a far broader concept, and has to encompass the whole security system and its interrelated constituents. In addition, external factors such as the environment and dynamic threats also affect the security system. Each of these internal and external constituents is prone to some degree of decay. For example, if…

- the operator receives many false intrusion alarms, their trust in the system will diminish to a point where they will be unlikely to assess/discriminate an actual true alarm event.
- a detector fails, physical delay is significantly reduced or eliminated as an effective measure.
- an attacker gains access to firearms, the ability to counter-respond by the guard force will be significantly reduced.
- a security incident occurs, then resources are likely to be directed towards that latest breach, taking the focus away from other parts of the security system (Smith & Brooks, 2013, p. 47) which may require greater attention.
- there is a cultural view that the organisation is not exposed to a given threat, then it won't be prepared for that threat.
- the security manager does not understand the security system and how small changes may affect the greater system, serious security incidents may occur.

Security decay is often misunderstood so that after an incident, the immediate reaction is often to increase the established security resources. However, this reaction is not usually necessary, as all that may be required is the re-establishment of the designed or commissioned level of protection. Responding to decay in this fashion results in security becoming reactive, rather than being proactive. Thus, resources are used ineffectively to provide ad-hock or a piece-meal security mitigation strategies (Smith & Brooks, 2013, p. 47). Conceptually this view was supported in the works of Garcia, who wrote "it is unlikely that a complex system will ever be developed and operated that does not experience some component failure ... it is important to know the cause of component failure to restore the system to normal operations" (2001, p. 59). Therefore, understanding the security system as a *system* and its likely decay factors will lead to improved security.

Study Objectives

The objectives of this study were to present a model that develops the concept of *entropic security decay*, establishing where security decay integrates into the security risk management cycle and stimulating academic discourse into the concept of security decay. To achieve these objectives, a discrete Research Question was put forward, namely:

> *Do security experts support the theoretical validity of entropic decay theory, which states that security decay is represented by the degradation of the microscopic quantities (constituents), and, or, the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system?*

In addition to the primary Research Question, a number sub-questions were addressed. These sub-questions considered whether security experts support the systems approach to implementing effective security controls, whether security systems suffer from decay, and if experts support the view that security decay lies within the

system constituents and their interrelationship. Finally, a security management system was put forward to allow the development of system metrics that can more readily measure the performance level of security systems.

STUDY DESIGN

A three-phase qualitative approach incorporating a Delphic poll was adopted to explore the concept of security decay from a systems approach (figure 1), making reference to relevant theories and laws. Such an innovative approach was considered the most appropriate over more traditional methodologies, as at this stage the body of knowledge encompassing the concept of security decay is still relatively new.

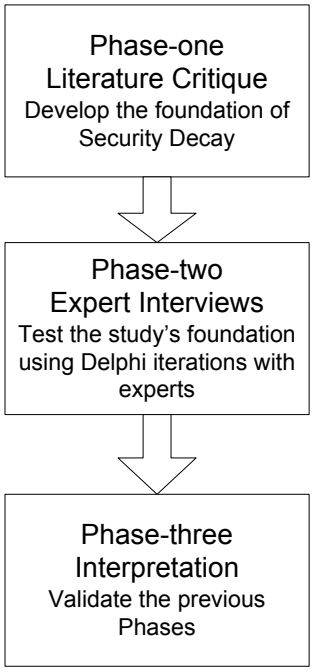


Figure 1 - Study design, using a three-phase developmental approach

Phase-one involved developing a conceptual literature benchmark for framing security decay by drawing on theories, including the strategy of defence-in-depth (DiD) and General Systems Theory (GST). Phase-two used semi-structured expert interviews using the Delphi technique to obtain the participant's thoughts and understanding of security decay within a systems approach to implementing effective physical security, where transcripts were analysed for underlying themes. The Delphi technique is a structured communication approach, developed as a systematic and interactive forecast method that uses a panel of experts who answer questionnaires in two or more rounds. After each round, the researcher provides an anonymous summary of the experts' forecasts from the previous round to encourage revision to their earlier answers. Finally, Phase-three provided a response to the posed Research Question based, in-part, on the proceeding phases. Themes were identified by drawing on key words and phrases in participants' responses.

Security experts were solicited to participate in the study, forming a non-probability sample (N=9) that included a pilot panel and two research panels. As highlighted by Brooks (2010), expert participants were selected based on the criteria that they were

employed or solicited to provide security knowledge advice across the varied security related occupations. In addition, selection was based on their extensive knowledge, experience, occupation, education, training, and that others peer revered their professional opinion within the multi-disciplined security industry.

Reliability and validity

This study used a number of controls to ensure reliability and validity. These controls included the principle of triangulation, with data inputs from multiple participant sources. Expert participants formed research panels, where consistent views were reflected and consensus achieved to demonstrate a high level of confidence to infer support of the core themes and principles.

Triangulation was also used to establish consensus support to each separate panel of experts. Member checking was incorporated into the panel design, where during the second round feedback process, each participant was presented with a transcript of their interview responses. Furthermore, each panel participant was asked whether they supported the interpretations drawn from the data, and were provided with the opportunity to respond to these interpretations. This approach aimed to establish a level of trust towards the inductive analysis prior to moving forward to the deductive analysis phase.

A THEORETICAL FOUNDATION TO DEVELOP SECURITY DECAY

Phase-one explored the literature in order to develop a theoretical foundation of security decay from the perspectives of defence-in-depth (DiD) and General Systems Theory (GST) (Bertalanffy, 1950). The concept of security decay is a significant risk to any security program (Underwood, 1984); however, there has been restricted research conducted into this area and this provides limited insight. Nevertheless, Underwood (1984, p. xi) states that it is "important that security is seen as a whole, both designed and operated as a system". As Garcia (2001, p. 6) stated, DiD should be implemented in security management using a systems approach. Such views indicate that security should be designed, implemented, and managed as a system.

The systems approach in management and a lesser degree, security, is a well supported concept. Therefore, it is reasonable to argue that any discussion in relation to a holistic approach to security decay must consider a systems approach. That is, a holistic approach to security decay must encompass both the processes in establishing the system and the ongoing management processes that aim to ensure the system reliably delivers, over time, the output for which it was commissioned. This study supports the concept of security decay; however, we aregue that the concept of security decay must be considered, defined, and applied congruous with the systems approach used to employ the strategy of DiD.

DiD has been applied to the protection of assets for centuries, based on the argument that a protected asset should be enclosed by a succession of barriers that restricts penetration of unauthorised access to provide time for an appropriate response (Smith, 2003, p. 8). Such barriers must encompass the physical, technological, and human element. The preventative functions of DiD may be considered as deter, detect, delay, response (D^3R) and recovery, implemented systematically to achieve a desired level of

security. As such, General Systems Theory (GST) provides a salient supporting strategy to DiD.

General Systems Theory

General Systems Theory (GST) is the interdisciplinary study of a system, with the formulation and deduction of principles. These principles "apply to systems in general, whatever the nature of their component elements, or of the relations or forces between them" (Bertalanffy, 1950, p. 139). In applying a system approach to DiD, Garcia (2001, p. 6) defines a system as an "integrated collection of components or elements designed to achieve an objective according to plan". However, there are many different types of systems (Midgley, 2003, p. xix) with a number of dictomies, each drawing attention to particular aspects of systems thinking (Barton & Haslett, 2007, p. 151) The most significant development in scientific method towards systems thinking has arisen from the open versus closed dictomy.

Closed systems are those considered isolated from their environment, meaning concrete systems (Midgley, 2003, p. 182). For a closed system, whatever matter-energy happens to be within that system is finite and over time, that energy gradually becomes disordered. Closed systems theory therefore emphasises the tendency towards equilibrium (Keren, 1979, p. 312), where according to the laws of thermodynamics, closed systems attain a time-independent equilibrium state, with maximum entropy and minimum free energy (Bertallanffy, 1950, p. 23).

In contrast, other systems are not isolated from their environment. According to Bittel (1978, p. 1130), open systems theory considers the system's interaction with its environment as crucial to the adoption and evolution of complex systems. Keren (1979, p. 316) explains that open systems depend on their environment for resources and are constrained by its influence. For an open system, the ability to change in response to environmental pressures ensures the system's long-term viability. In contrast to closed systems that eventually attain a time-independent equilibrium state, an open system may attain (certain conditions presumed) a stationary state where the system remains constant as a "whole", referred to as a steady state condition (figure 2) (Bertalanffy, 1950, p. 23).

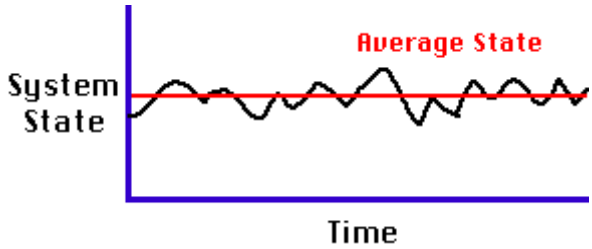


Figure 2 - Example of a steady state system (average condition) over time (Pidwirny, 2006).

While in a closed system, the final state depends on the components given at the beginning of the process, steady state systems (open systems) show equifinality (figure 3), where the initial state can change as energy inputs change. As such, if a steady state is reached in an open system, it is independent of the initial conditions and determined by the system's parameters (Bertalanffy, 1950, p. 158). For example in figure 3, path A commences with a high energy input reaching a high point; however, as the system's

energy inputs are reduced, that is, constituent parameters reduced, its level of output is also reduced reaching a steady state condition based on the mean energy inputs. In contrast, paths B and C commence with lower or negative energy inputs.

For a DiD system, as the individual constituent parameters that achieve the elements of detect, delay and response increase, the systems macro-state output increase. As constituent levels decrease, so does the macro-output of the system. Change, accordant with the provision or reduction of resources makes open systems, and specifically physical protection systems, scalable. Therefore accordant with the principle of equifinality, the system may be tuned to deliver a higher or lower output, or maintained at a predetermined level accordant with the perceived threat driving the system.

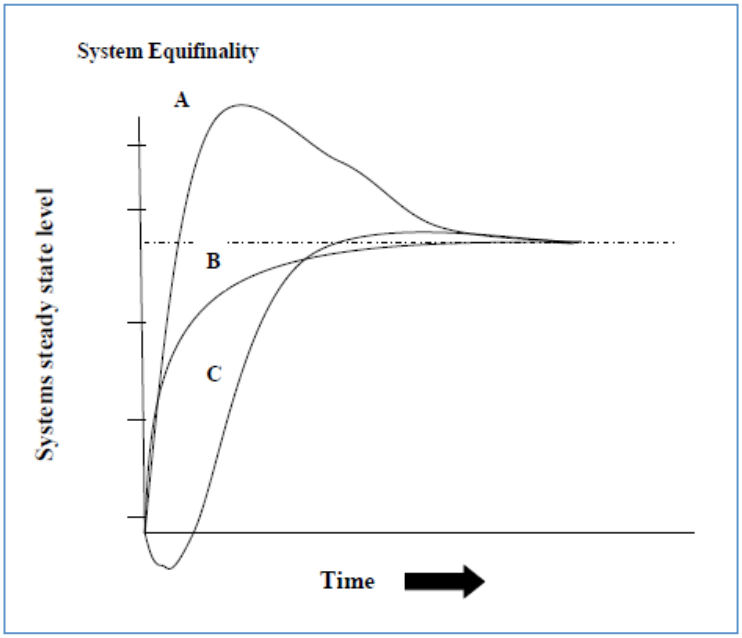


Figure 3 - System equifinality (Bertalanffy, 1968, p. 143).
There are different possible paths to the same state.

According to Checkland (1981, p. 83), the steady state in an open system may create and/or maintain a high degree of order. Steady states in open systems are not defined by maximum entropy, but by the approach of minimum entropy production. Entropy is a concept derived from a metric, defined as a measure of disorder in a system and a process characterised with decay, disintegration, running down and becoming disordered (Bohm & Peat, 2000, p. 137; Herman, 1999, p. 86; Bertalanffy, 1968, p. 42). In all irreversible processes, entropy must increase (Bertalanffy, 1968, pp. 41-42). For a system, as entropy increases its (entropy level) capability decreases, based on the argument that systems rely on order and cohesion.

The isomorphism of entropy

Entropy as a concept is a state function of a system (Roos, 1997, p. 5), a description of the system in terms of its properties at any instant of time. When a system changes from one state to another, the difference in properties depend solely on the states and not on the manner or pathway by which the change occurred. According to Midgley (2003, p. 39), traditional physics only deals with closed systems, and as such, physicists

argue the laws of thermodynamics only apply to closed systems, in particular, the second law (Entropy law) (Bertalanffy, 1968, p. 39). For example, as a closed system moves towards equilibrium, energy is converted to work; however, as it approaches equilibrium the available energy decreases, eventually removing the systems capability until the system is reenergized.

The concept of entropy has been seen as a foundational concept in contemporary systems theory. Although the term originated in the field of thermodynamics, it has both theoretical and mathematical interpretations, as well as widespread applications in other disciplines (Byeon, 2005, p. 224). According to Byeon (2005, p. 224), a large number of useful terms and concepts have been transported into other disciplines from their original discipline. Since its original inception by Clausius in classical thermodynamics, entropy has witnessed a series of subsequent incarnations. As such, the term "entropy" can be used as long as it is qualified by a prefix, as in "social entropy" (Bailey, 1990 cited in Byeon, 2005, p. 224). This prefix enables various isomorphic applications of entropy to be differentiated from Clausius' entropy, or Boltzmann's' entropy, or biological entropy, or any other concept which lacks a certain prefix.

The concept of entropy is becoming increasingly popular and used to discuss the state of various systems. For example, the second law of thermodynamics has been applied to many domains including information security (King, 2008), organisational systems (Lovey & Nadkarni, 2007), combat systems (Herman, 1999), communications, biology, economics, sociology, psychology, political science and art (Rifkin, 1982, p. 263). Entropy is a concept conceived to discuss the degradation and disorder within a system relating to a systems ability to carry out work.

Developing entropic security decay

According to King (2008, p. 1), "security system degradation is the result of such systems suffering from natural entropy". Honkasalo (1998, p. 136) explains that degradation measures the irreversible increase of entropy, which is the amount of usefulness lost. That is, a security system is only as effective as its parts; when a single part fails, this failure can cause degradation within the total system (Konicek & Little, 1997, p. 184: King, 2008, p. 1). Garcia (2006) concurs, suggesting that system effectiveness can become degraded through the reduction in effectiveness of individual components. As entropy increases, capability decreases as systems rely on order and cohesion (Smith & Brooks, 2013, p. 47), and a security system is no different.

Even the most effective systems will deteriorate over time and with use (Howlet, 1995, p. 222). The isomorphic application of entropy to DiD or a Physical Protection System (PPS) is supported by Lovey and Manohar (2007, p. 99), who assert that various systems suffer from entropy. The application of the second law of thermodynamics, specifically the concept of entropy to a PPS, reintroduces the concepts of degradation and decay into security. System degradation results from entropy production, which reduces the efficiency and effectiveness within a system that impedes its output goal (Bohm & Peat, 2000, p. 137).

In contrast to closed systems, open systems that have the appropriate feedback or energy input will have decreasing entropy. Such systems, with minimum entropy production, are generally stable and provide a consistent output product. Nevertheless,

if one of the system's variables is negatively altered, the system manifests correlating changes in the opposite direction (Bertalanffy, 1950, p. 26). This property of open systems is in-line with Lorenz's (1963) findings and the "Butterfly" metaphor.

Therefore, it is argued that the macro state of a DiD system is recognised as an expression of the average of the microstate variables collectively, where changes in microstates (constituent elements) directly affect the macro state. Such a process is based on the definition of entropy offered by Bohm and Peat (2000, p. 137), where disorder within and between elements increases, decay increases, and capability decreases, demonstrated by the *systems effectiveness* equation (1):

$$\text{System effectiveness} = \frac{\text{capability}}{\text{entropy}} \quad (1)$$

(Coole & Brooks, 2009, p. 22).

For example if the degree of risk mitigation decreases, that is, the individual constituents which combine to achieve specific outputs of the protection system decay, then the ability of the physical protection or response constituents to counter its commissioned threat level is degraded. For the system to maintain its commissioning levels of effectiveness (counter the threats which pose a risk), it must be provided with the appropriate feedback (energy inputs) to ensure the level of output capability for the system is equal to or exceeds the effects of natural entropy at the constituent level.

Measuring decay in physical security systems

In applying a systems approach to physical security, entropy is an idea born from classical thermodynamics. As such, entropy is a quantitative entity rather than something intuitive and should therefore be defined through an equation. To apply a quantitative approach to physical security, this study drew on the works of Garcia (2001, p. 246) who explained that the effectiveness measure of a Physical Protection System (PPS) is the principle of timely detection. Therefore, the macro-state of a PPS can be represented as its probability of interruption (Pi), where Pi is the probability of interruption or the cumulative probability of detection when there is enough time remaining for the response force to interrupt the adversaries.

Entropy can be quantitatively measured for a DiD system using the Estimated Adversary Sequence Interruption (EASI) equation (2) to quantitatively represent a systems commissioning or operational macro-state level (Garcia, 2001). Accordant with the premises of systems theory, EASI quantitatively presents the various relationships among the constituents and elements performance measures within PPS.

$$P(I) = P(D1) \times P(C1) \times P\,(R/A1) + \sum_{i=2}^{n} P(R/Ai)\,P(Ci)\,P\,(Di) \prod_{j=1}^{i-1}(1 - P(Di)) \quad (2)$$

EASI mathematically demonstrates the relationship among the performance measures of the PPS constituents (table 1). For a PPS, the higher the probability of interruption (Pi), the lower the chances of a successful penetration; whereas, the lower the Pi, the higher the chances of penetration (Garcia, 2001, p. 246).

EASI measures are the cumulative sum of the various sub-systems within a PPS, where accordant with the principles of system theory any changes in these inputs have an overall effect on the output of the probability of interruption. Therefore, congruous with the principles of General Systems Theory, changes in the various sub-system's microstates have a direct effect on the PPS's macro-state.

Table 1 - The Estimated Adversary Sequence Interruption (EASI) components.

Component	Descriptor
Ps	Probability that individual detection constituents will sense abnormal or unauthorised activities
Pt	Probability that the alarm indication will be transmitted to an evaluation or assessment point
Pa	Probability of accurate assessment
PD[1]	Product of the probability that the detection constituents will sense abnormal or unauthorised activities, Pd represents the element of detection
P(C)	Probability of guard communication
P(A)	Probability of alarm
	Mean and standard deviation of delay time
	Mean and standard deviation of response time
P(R | A)	Probability of response force arrival prior to end of adversary's action sequence, given alarm

[1] To account for an adversary getting to the next layer along their path, EASI draws on the probability of non-detection (PI) with a variation where the sensor is located relative to path delay measures, with PI = $1-P_{ND}$.

Achieving a steady state physical protection system

The application of the Estimated Adversary Sequence Interruption (EASI) model within an open systems facilitates the measurement of a physical security program, where the combined elements of detect, delay, and response provide a security system's macro-state measure. That is, EASI provides the means of measuring the system's stable condition stemming from the systematic process which combines people, equipment, and procedures. However, according to Olzak (2006, p. 1), "which security layers to implement and to what extent is a risk management decision". That is, the total cost of the security system is determined within the strategy of DiD. The degree of security control required to achieve the amount of time delay judged necessary after detection to facilitate an appropriate response in relation to the risk of the asset being protected (Post, Kingsbury & Schachtsiek, 1991, p. 89; Garcia, 2001, p. 272), which must be implemented in a manner which achieves a steady state (stable) risk reduction system.

McClure (1997, p. 4) considered that an effective security state exists when the level of risk exposure is reduced, through various means, to a level that is acceptable to the organization. Such risk mitigation can be achieved through a security risk management strategy. Security risk management can be represented in many ways, although one such method is with the use of threat, vulnerability, and criticality components (3) (Standards Australia, 2006). This approach establishes the security risk management

context as a combination of a threat assessment, vulnerability review, and criticality register.

$$\text{Risk} = \text{threat} \times \text{vulnerability} \times \text{criticality} \quad (3)$$

Furthermore, Garcia (2001, p. 272) considers risk may be defined through equation (4). Likelihood considers the probability of an attack, the current level of vulnerability within the security system, the effectiveness of the response force to counter the attacker in a timely manner, and the consequence of the attacker achieving their goal.

$$\text{Risk} = P_A \times [1-(P_I)] \times C \quad (4)$$

Where:

P_A = Likelihood (threat) of an adversary attack measured between 0 and 1.
1 = Vulnerability measured between 0 to1.
P_I = Probability of interruption measured between 0 and 1.
C = Consequences (criticality) value measured between 0 and 1.

This study argues that in a quantitative approach to security the relationship can be summarised with the sum (Σ) of deter, detect, delay and respond (D^3R) over risk (3) to produce the final equation for security (5]. For an effective state of security to be achieved, a security system must demonstrate effectiveness in response to a facility's analysed risk level accordant to its defined threat (Garcia, 2006, p. 30).

$$Security = \frac{\sum 3DR}{Risk\ [Threat \times Vulnerability \times Criticality]} \quad (5)$$

Garcia (2001, p. 277) explains the risk equation (4) and Probability of Interruption (Pi) enables effective cost-benefit decisions to be made towards implementing security controls, which reduces an organisation's risk to an acceptable level. For example, figure 4 presents an open system with the level of implemented security based on the risk equation and PPS system performance measures, whilst being cognizant of maintaining a deterrent value during daily system fluctuations. Congruent with the objectives of open systems (Honkasalo, 1998, p. 135), the overall aim of a PPS is to reach a steady state condition where the flow of energy is constant and the increase of entropy is minimal. Such a steady state condition implies an exchange of either matter or energy within the environment (Roos, 1997, p. 6), which is a balance of inputs, outputs and internal processes, and the system is stable to produce what it was commissioned to achieve.

In contrast to an effectively maintained steady-state security system (figure 4) consistent with the principle of equifinality (figure 3), figure 5 indicates the effects entropy has within the DiD system. Entropy effect the systems macro-steady state condition in relation to its commissioned risk reduction level. In figure 5, the level of implemented protection has decreased based on control constituent reductions at the micro level reducing total system efficacy as a system, yet the system still intuitively presents a steady state condition.

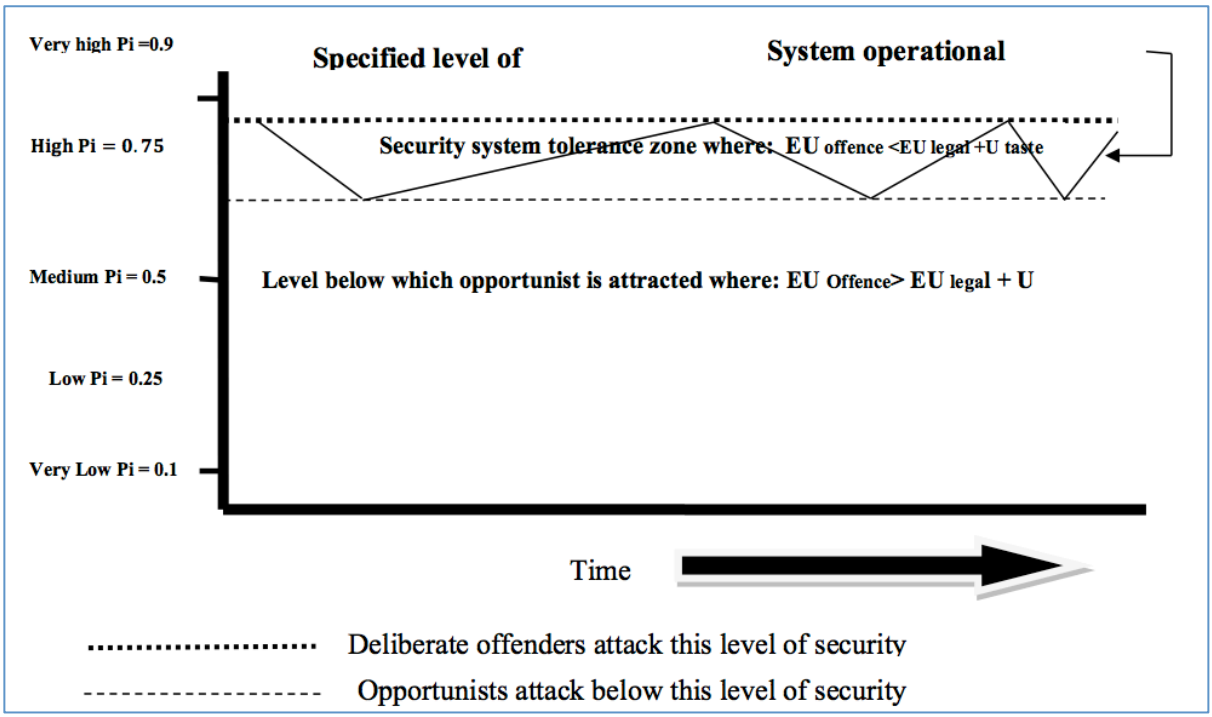


Figure 4 - Effective implemented security levels. (Adapted from Underwood 1984; Martin, 2000, p. 210; Garcia, 2001, 2006; Pidwirny, 2006; Standards Australia HB167 Security Risk Management, 2006).

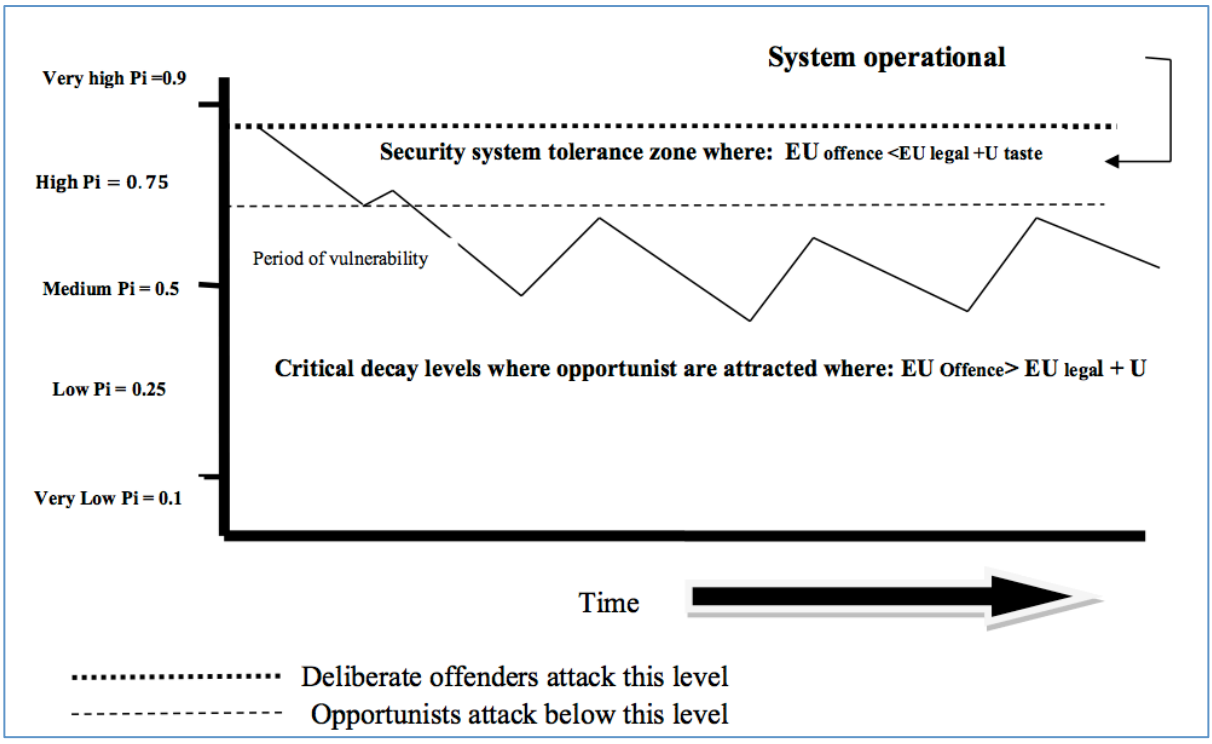


Figure 5 - The effects of decay on the systems commissioning level of effective security when using the Pi and Risk Equation. (Adjusted from Underwood 1984; Martin, 2000, p. 210; Garcia, 2001, 2006; Pidwirny, 2006; Standards Australia HB167 Security Risk Management, 2006).

We argue that this *subtle* degradation results in the system performing below the level of risk control considered necessary for a specific security risk context (figure 5). In addition, as the system is perceived to be degraded by potential adversaries, the deterrence element of DiD is also degraded, leading to the perception by opportunistic offenders that the benefits outweigh the costs leading to a decision within the rational choice framework to attempt penetration.

Entropic security decay conceptually defined

The meaning of entropy is difficult to conceptualise and not well understood outside of academic disciplines, leading to ubiquitous usage and restricted understanding. Whilst various definitions and understandings are applied to entropy, a central theme is how various components of a system relate to one another towards producing a coherent whole. As such, this study has argued that the concept of entropy provides a model towards measuring the gradual degradation of a physical protection system after its commissioning.

The adoption of *security decay* provides a functional definition and therefore, appeal to both security academics and practitioners alike. Study Phase-one, the theoretical foundation of security decay, led to the proposition that security decay can be defined as:

> The gradual degradation of the microscopic quantities (constituents) or the relationship between the microscopic and macroscopic quantities within a security system.

VALIDATING ENTROPIC SECURITY DECAY

Phase-two validated the theoretical foundation of security decay using the Delphi approach. A total of three expert panels were used, where experts were interviewed individually and the sum of their views provided to the other panel experts. Experts were heterogeneous practitioners from across the corporate or commercial security industry (table 2). During the interviews themes were identified by drawing on key-words and phrases in the experts' comments, allowing a response to the posed research sub-questions.

What is the experts' view of entropic security decay?

The systems approach to implementing effective security framed the study's approach in understanding security decay. Considering this view, research sub-question one asked whether *Security experts support the systems approach to implementing effective security controls?*

Congruous with the past authors (Underwood, 1984; Howlet, 1995; McClure, 1997; King, 2008) all the participants supported a systems approach to security. As one of the participant's stated "*a system is a combination of elemental inputs … very much dependant on the correct operation of the effectiveness of each of these elements performing their function and supporting functions of other elements. Therefore, small changes in the elements, particularly where this occurs across many/all elements can have a major impact on system output at the macro level*". Such a view was supported by another participant, who suggested that a "*system ties together a group of elements and*

constituents which maintain a role towards an overall goal, where all aspects are interrelated".

Table 2 - Expert participants.

Expert	Description of security expert
1	20 years experience working with physical protection systems (PPS) in the correctional environment, providing advice on the operational effectiveness of PPS. Qualification: Bachelors Degree in Security.
2	15 years correctional security experience, monitoring and reviewing operational effectiveness of PPS. Qualification: Bachelors Degree in Security.
3	20 years experience in various security roles in customs and correctional environments, providing advice relating to daily management of staff operating and maintaining PPS. Qualification: Bachelors Degree in Business Management.
4	20 years experience in security related projects as a client relations manager for a large security engineering organisation. Facilitates security risk management and leads the design of technical, physical and procedural security controls. Qualification: Diploma of Applied Science.
5	21 years experience in security operations, including the Australian Defence Force, customs and corrections. Coordinates capital works projects focusing on security aspects. Qualification: Bachelors Degree in Security.
6	25 years experience in correctional security and emergency management. Security manager within corrections, coordinating physical and procedural security.
7	20 years experience in special forces, with five years in oil and gas security. Provides security compliance advice to Maritime Transport and Offshore Facilities Security Act (2003) and prepares security and emergency plans. Qualifications: Bachelors Degree in Security, Graduate Certificate in Operations Management.
8	20 years experience in policing and security advisory roles. Principle security consultant, conducting security risk assessments and audits. Qualifications: Bachelors Degree in Security (Honours), Advanced Diploma in Business Management, Diploma in Criminal Investigations.
9	33 years security industry experience as a senior consultant to high level security projects. Published over 60 papers on security issues and has professional qualifications in electrical engineering, building services engineering and holds Certified Protection Professional (CPP) certification.

In general, there was participant acknowledgment that the components of a Physical Protection System (PPS) are interrelated and interdependent, with each sub-system being a system of systems. According to participants, each aspect of a security system has a defined role, where constituents are implemented in a manner where their interrelationships complement and influence each other to reduce security risks. This approach was highlighted by one participant who stated that "*we select individual*

components from their individual key performance indicators, then, combine them together into a designed whole". Where "s*ecurity decay is the degradation in the performance of an element of the security solution, both, as a single element performing a specific function, and the elements role in supporting other elements in their function within the total system"*.

In responding to research sub-question one, results indicated that all participants supported the systems approach to achieving effective security. In addition, their views relating to the implementation of such controls are accordant with the various underpinning principles of General Systems Theory.

Do security systems suffer from decay?

Research sub-question two related to the premises of Underwood (1984) and McClure (1997), asking, *Do security experts support the argument that security systems can suffer from decay*? All research panels reported in the affirmative that they believed security systems suffer from decay. For example, one member stated, "*I do believe that security systems can and do experience decay*", with another stating that, "*yes, … I believe security systems categorically decay"*.

In response to the research sub-question regarding security systems decay, the evidence supported that such decay relates to a failure to maintain security "systems" at their commissioned operating levels of effectiveness, diminishing their ability to deliver the required output goal (risk reduction). As one participant stated "d*ecay relates to the decline in the efficacy and efficiency of the security function, and its correlating increase in risk"*. Another participant summarised decay as when "p*eople who have systems installed do not understand what underpins them, systems are designed with parameters to facilitate for decay, a lack in professional system management, that is, a lack of knowledge to manage these parameters, a lack in education, in formal training leads to decay within physical protection systems"*.

Elements of security decay

Research sub-question three focused on the heterogeneous aspects of the Physical Protection *System* (PPS). As such, this question asked whether *Security experts support that security decay lies within the systems elements, constituents and their interrelationship*? In response, one participant stated that decay "*within a PPS occurs within its individual element, and propagates through the system. Decay occurs at the base level over time. This decay at elemental level occurs through many causes and the effect can result in major system breakdown*". This participant further stated that "*a system is a combination of elemental inputs, the system is very much dependant on the correct operation of the effectiveness of each of these elements in performing their function and supporting functions of other elements*".

Congruous with this viewpoint, one participant stated, *"the effects of decay are directly proportional to the loss of risk management ... Decay occurs in all aspects: management, technology and physical engineering*". This idea was supported by another who suggested that, "*small changes can lead to large security implications, much like a chain. A chain is only as good as its weakest link or point. When the weakest link breaks the results can be large*".

Based on the participants' responses, we argue that security decay lies within the systems elements, constituents, and their interrelationships. That is, decay within a security system occurs at the constituent level, manifests and then expands to incorporate and affect specific sub-system key performance indicators. Such expansion then affects the specific DiD element within the defence in depth strategy for which it is located.

ENTROPIC SECURITY DECAY

Phase-three allowed interpretation to be made in response to the posed Research Question, namely *Do security experts support the theoretical validity of entropic decay theory, which argues that security decay is represented by the gradual degradation of the microscopic quantities (constituents), and/or the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system?* To support the concept of entropic security decay, a number of factors are put forward. An item bank was developed from the expert interviews to consider the components of Physical Protections Systems (PPS). The isomorphic principles of science considered the use of entropy within other systems and how this supports security systems. A security management system approach is shown, detailing how entropic decay can assist in defining process metric system indicators. Finally, we provide a definition for entropic security decay, concluding the conceptual development of this concept.

Entropic security decay item bank

Within a systems approach to physical security, there is a complex interrelationship between the built environment, physical controls, technology, people, and management processes as they achieve the elements of depth-in-depth (DiD). For example, table 3 presents the study's security expert's pool of variables and factors (item bank) associated with the concept of security decay. The item bank is divided into discrete PPS components of technical, people and physical, demonstrating decay conditions, the phenomena and resulting consequence. Such an item bank is underpinned by the expert panel's thoughts, feelings, and experience with degradation within PPS. This study found that within this interrelationship, decay occurs at the constituent level and if left undetected, expands to affect the local sub-system and eventually, the DiD system.

Table 3 - Security decay preliminary item bank for technical, people and physical components.

PPS Components	**Decay Categories**		
	Condition	Phenomenon	Consequence
Technical	Poor detection system maintenance	Increased nuisance alarm rates	Alarms ignored, reducing probability of accurate assessment KPI.
	Incorrect technical maintenance	Causes high nuisance alarm rates.	Blind acceptance of alarms, diminishing accurate assessment as a KPI.

	Degradation of lighting system	Light lamp failure affects the performance of CCTV systems.	Diminished ability to assess (discriminate) alarm sources.
People	Lack of professional management of the security function, as a system.	System decays across all aspects of the management triangle, technological, physical and procedural.	Security events occur due to diminished risk reduction program.
	Poor, or lack of system testing, or, breaches of system testing procedures.	Accurate steady state condition not known.	Sub-system vulnerabilities.
	Poor formal training for new staff, where training occurs through handed down processes.	Incorrect procedures or bad habits passed on to new staff.	Cultural decay within human aspect of the system.
	Lack of qualified staff continuation training.	Decay in response processes for non-routine events.	Staff responses decay.
	System environment environment changed to suit personal requirements.	Changes parameters, discordant with their design specifications.	Triggers small changes in which are not understood until a security event.
	Fluctuations in staff competencies	Reduces sub-system KPI's related to competency reduction.	Staff may not react accordant with system design requirements.
	Poor physical attribute (lighting and air conditioning) within CCR.	Provide inappropriate output conditions.	Staff concentration and focus degrading within CCR.
	Operating procedures modified without reference to holistic system requirements.	Degrades the performance of the operating system as a "whole".	System may not perform accordant with design specifications.
	Poor communication between CCR, and operational staff.	Degradation in efficacy across "whole" system.	System may not perform efficiently against defined threat.

Physical	Lack of maintenance of PPS environments (weeds and feral growth).	Triggers increased nuisance alarm rates	Alarm acceptance reducing probability of accurate assessment KPI.
	Deterioration of delay physical elements.	Barrier time delay degrades against defined threat.	Delay time along an adversary's path is changed altering commissioning Pi.
	Physical components designed without considering physical environment impact.	Leads to premature physical decay.	Physical components may not withstand defined threat stress.

(Adjusted from Gillham, 2000, p. 68)

Isomorphic principles to support entropic security decay

Conforming to the isomorphic principles of science (see Bertalanffy, 1950; 1968), this study considered the laws of thermodynamics (Entropy law) to explain the natural decay occurring in systems of all types, regardless of make-up. We considered this necessary given the variety of different sciences that make a PPS possible, where the one science binds all various sciences to achieve the systems output goal is GST (Bertalanffy, 1950; 1968). As with any physical open or closed system, it will decay overtime if there is restricted or inappropriate input. Entropy is associated with a system's inability to carry out work, transfer useful energy, or maintain orders of activity, and all systems strive towards disorder that when achieved are in a state of equilibrium or death. Therefore, security systems reduce in their efficiency and effectiveness when they, their component elements, or constituents become disordered, run-down, degraded, or decayed.

In investigating the concept of security decay from a systems approach, contrary to McClure's (1997) work, this study argues that apathy is not the salient factor driving decay. Apathy can be a product of decay manifested from another constituent within the system that has been allowed to propagate. For example, one participant stated, "*all technology decays, as technology decays it constantly false alarms, then staff ignore them, where ultimately they lose confidence in the system and their work decays*". Such a view was also reported by Howlet:

> Even the best system will deteriorate with time and use … from the time of taking a system into use it will start to deteriorate. No system, however well designed, can be completely reliable without proper maintenance. If left without attention it will become unserviceable. A poorly maintained security system will have many unexplained alarms, leading to the guard force losing confidence in the system and eventually ignoring a true alarm as just another false alarm. However, the operator may not be aware of it, but the system will not perform as intended (1995, p. 220).

A security management systems approach

As a result of the heterogeneous nature of a PPS, reduced functionality in one specific area (point disturbance) will result in decay propagating throughout the remainder of the PPS due to interrelationships. For example, a PPS is made from many components that provide the functions of detection, delay and response. If a detection component does not perform to its design parametric, this puts greater stress in the delay component or increased reliance on the following detection components in a layered system. Such propagation ultimately changes the performance (macro-state) of the whole system.

The security management system (figure 6) commences with a top-down approach, where, based on defined or perceived threats, vulnerabilities, and/or criticalities (system purpose), the systems objectives and parameters are established as a desired level of security. Operational deliverables being physical, technological, or procedural are implemented and managed to ensure the system maintains its commissioned measures of performance or key performance indicators over time. However as figure 6 highlights, if the system constituents are allowed to decay, the affect of this decay propagates back up the pyramid in a bottom-up approach. Conceptual decay curves are represented within the constituents. Such propagation of decay constituents diminishes the risk reduction efforts, increasing organisational risk exposure.

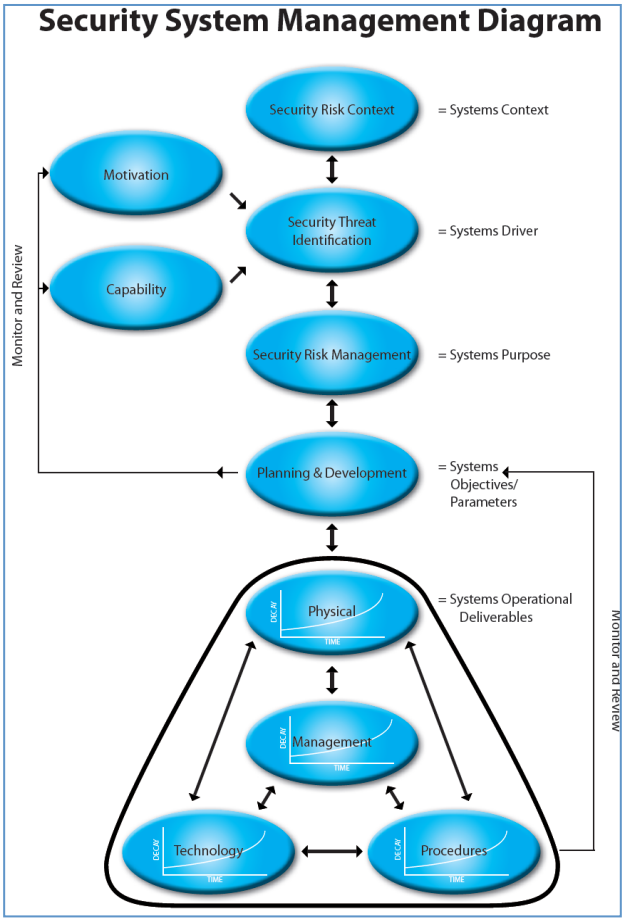


Figure 6 - A security management systems approach, highlighting the decay constitutes curves within the operational deliverables.

McClure highlighted the "complex interrelationship between technology, people, and management processes within a security function" (1997, p. 1). Consistent with such a view, it is the interrelations which integrate the system towards achieving an output goal, rather than a collection or juxtaposition of controls. Coole and Brooks (2009, p. 22) highlighted such a complex relationship within a PPS, arguing that an orderly relationship exists where the space and time distribution of the DiD elements creates a comprehensive state of order in relation to a PPS's macro level of effectiveness.

Defining entropic security decay

In considering the systems approach to achieving DiD, the concept of *entropic security decay* has been presented. DiD is the sum of various elements, namely deterrence, detection, delay, response and recovery. The concept of entropy supported the argument that any change in the efficiency or effectiveness of any of the DiD elements constituents reduces the system's effectiveness. The sum of these concepts collectively form and were referred to as *security decay*, being defined as:

> The gradual degradation of the microscopic quantities (constituents) or the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system.

Such a definition provides rigor and genuine conceptual substance that can be integrated into a PPS performance measures. In addition, such an approach may also be applied to personnel and information security frameworks to encompass the security management functions, ultimately leading to the ability to develop and define system metrics or key performance indicators.

RECOMMENDATIONS

Security decay has been discussed by previous authors (Coole & Brooks, 2009; McClure, 1997; Smith & Brooks, 2013; Underwood, 1984) but has not been explored within systems theory. Therefore, there are a number of recommendations resulting from this study. These include a greater use of applied metrics to measure and record the security constituents, and enhanced efforts to understand and maintain a security system at its commissioned level. Other recommendations include recognizing the dynamic environment that a security system has to operate within, the benefits of a system approach to security, and the need for further research in order to understand the concept of security decay.

Greater use of security metrics

In applying a systems approach to security, there has to be the ability to measure constituents effectiveness, individually and as relationships. Entropy can be quantitatively measured for a DiD system, using the Estimated Adversary Sequence Interruption (EASI) to quantitatively represent a systems commissioning or operational macro-state level (Garcia, 2001). In accordance with the premises of systems theory, EASI quantitatively presents the various relationships among the constituents and elements performance measures within PPS.

Security decay is a quantitative entity, rather than being intuitive. However, all elements or constituents need to be better understood and capable of having metrics applied and recorded.

The commissioned level of security

Security systems are often installed as a reactive action, either over- or under-engineered to mitigate a single risk (Brooks & Smith, In print) and operating as an open system in a dynamic threat environment. Nevertheless, a security system should be understood and maintained at its commissioned level.

Operating with dynamic threat

The dynamic environment should be monitored to allow the security system's steady state to be adjusted to suit the threat, for example the security system should be scalable. As the threat increases, the security system should raise to counter such an increase and, in contrast, lower when threat reduces, thus showing equifinality. The ability to achieve such a dynamic security system requires additional research to gain better understanding of the interrelationship between the functional constituents of security.

Adoption of a security system approach

The adoption of a security systems approach to security management should:

- Define a common lexicon and understanding among stakeholders.
- Act as an aid to defining the security program architecture.
- Generate awareness of system design principles to senior management.
- Provide the basis for conscious divergence from a common philosophy.
- Assist communication across functional management boundaries.
- Promote the regard for security management through adoption of mature concepts.
- Provide flexibility within what might be regarded as an otherwise rigid framework.
- Provide reliability, maintainability, and the ability to be upgraded.
- Be flexibility and resilience.
- Support performance and effective resource allocation.
- Provides explicit senior management support (Smith & Brooks, 2013, pp. 26-27).

A security system should reduce risks consistent with the business appetite. It is security's role to ensure that security is effective, does not waste resources, and uses components to their full potential. The provision of sound security analysis and management allows the business to consider and approve a balanced security plan. Such balance promotes efficient spending to reduce 'under' or 'over' investment in the security system, and provide approved security to counter risks that can impact on the company's reputation, intellectual and physical assets, and to recover from crisis (Cubbage & Brooks, 2012).

Further research in security decay

This study has proposed the model of entropic security decay, providing a theoretical foundation, examples of decay in a physical protection systems, and a concept definition. Past authors have previously discussed security decay (Coole & Brooks, 2009; McClure, 1997; Smith & Brooks, 2013). However, there is still further research

needed to support this preliminary discussion of entropic security decay. Such research should seek to better understand not only the physical or engineering nature of decay, but also how decay is driven through concepts such as a lack of knowledge, economic pressures, and organisational cultural. For example, can decay curves be developed that consider all constituents, and are these transferable within different contexts? How do different domain experts view security decay within different systems? Decay is not only applicable to physical and technical constituents, but also personnel, management, and corporate constituents.

CONCLUSION

This study sought to explore entropic security decay within a systems approach, developing a model of entropic security decay. The initial concept was built from reviewed literature suggesting that all physical systems, if left and with no feedback, will decay. The concept was tested against security expert's views and experience with security systems, supporting the model of entropic security decay.

If a physical protection system is not professionally managed as a system, that is, provided the appropriate feedback, it will decay. In considering such an outcome and consistent with the underpinnings of General Systems Theory (GST), we have argued that, in contrast to Underwood's (1984) and McClure (1997) writings, security decay is primarily concerned with managing the natural entropic processes occurring against commissioned levels of effectiveness within the complex security constitutional relationships. Furthermore, these processes are allowed to manifest due to a lack of professional management of the security function as a *system*. As one of the participating experts stated, "a significant cause of decay is a lack of professional management of the system ... we install systems, but people do not understand what underpins them ... we design in parameters to facilitate for decay; however, a lack of (professional) knowledge and management of these parameters leads to security decay".

Entropic security decay is the degradation of security mitigation strategies within the greater security management system, due to internal or external factors. Security decay is a supportable concept that can be defined as *the gradual degradation of the microscopic quantities (constituents) or the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system*. To effectively manage a security system requires the design, application, and management of security consistent with a security management systems approach. Such an approach allows a system to be applied, with metric operational deliverables ensuring compliance to the security systems objectives. However, further research is required to develop and define this preliminary discussion of security decay and further explore a usable model that supports the general security practitioner.

REFERENCES

Barton, J., & Haslet, T. (2007). Analysis, synthesis, systems thinking and scientific method: rediscovering the importance of open systems. *Systems Research and Behavioural Science*, *24*, 143-155.

Bertalanffy, L., V. (1950). An outline of general systems theory. *The British Society for the Philosophy of Science, 1*(2), 134-165.
Bertalanffy, L., V. (1950). The theory of open systems in physics and biology. *Science, New Series, 111*(2872), 23-29.
Bertalanffy, L., V. (1968). *General systems theory*: foundations, development, application. New York: George Braziller, Inc.
Bittel, L., R. (1978). *Encyclopaedia of professional management*: an authoritative guide to the profitable practice of management. New York: McGraw-Hill.
Borgsdorf, D., & Pliszka, D. (1999). Management your risk or risk your management. *Public Management*, *81*(11), 6-10.
Borodzicz, E., & Gibson, S. D. (2006). Corporate security education: towards meeting the challenge. *Security Journal, 19*, 180-195.
Broder, J. F. (2006). *Risk analysis and the security survey* (3rd ed.). Oxford: Butterworth-Heinemann.
Brooks, D. J. (2010). What is security: Definition through knowledge categorisation. *Security Journal, 23*, 225–239. doi: 101057/sj.2008.18.
Brooks, D. J. (2011). Security risk management: A psychometric map of expert knowledge structure. *International Journal of Risk Management*, *13*(1/2), 17–41. doi: 10.1057/rm.2010.7.
Brooks, D. J., & Smith, C. L. (In print). Engineeirng Principles in the Protection of Assets. In M.Gill (Ed.), *Handbook of Security* (2nd ed.): Palgrave McMillian.
Bohm, D., & Peat, D. (2000). *Science, order, and creativity* (2nd ed.). New York: Routledge.
Byeon, J., H. (2005). A systems approach to entropy change in political systems. *Systems Research and Behavioural Science. 22*, 223-231.
Callister, W. D. (1997). *Materials science and engineering: An introduction* (4th ed.). New York: John Wiley & Sons.
Checkland, P. (1981). Systems thinking, systems practice. Salisbury: John Wiley & Sons.
Clarke, R. V., & Cornish, D. B. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, *50*(4), 933-947.
Collins Australian Pocket Dictionary of English Language. (1994). Melbourne: Harper Collins Publishers.
Coole, M., & Brooks, D. J. (2009). Security Decay: An entropic approach to definition and understanding. *Proceedings of the 2nd Australian Security and Intelligence Conference*, Perth.
Craighead, G. (2003). *High-Rise Security and fire life safety* (2nd ed.). Boston: Butterworth Heinemann.
Cubbage, C., & Brooks, D. J. (2012). *Corporate Security in the Asia Pacific Region: Crisis, Crime, Fraud and Misconduct* Boca Raton: Taylor and Francis.
Denbigh, K. G. (2009). *Note on entropy, disorder and disorganization*. Retrieved April 3, 2009 from http://www.endeav.org/evolut/text/denbig1/denbig1e.htm
Edith Cowan University, (2004). *Physical security*: *Study guide SCY 1101*. Perth: Author.
Felder, G. (2001). *Things fall apart: An introduction to entropy*. Retrieved July 15, 2011 from http://www4.ncsu.edu/unity/lockers/users/f/felder/public/kenny/papers/entropy.html
Fennelly, I. J. (1997). *Effective physical security* (2nd ed.). Amsterdam; Boston. Butterworth-Heinemann.

Garcia, M. L. (2001). *The design and evaluation of physical protection systems*. Boston: Butterworth-Heinemann.

Garcia, M. L. (2006). *Vulnerability assessment of physical protection systems*. Boston: Butterworth-Heinemann.

Hatfield, A. J., & Hipel, K. W. (2002). Risk and systems theory. *Risk Analysis*, *22*(6), 1043-1057.

Herman, M. (1999). *Entropy based warfare: Modelling the revolution in military affairs.* Retrieved April 18, 2010 from http://209.85.173.132/search?q=cache:7Rigu4CTvaAJ:www.au.af.mil/au/awc/awcgate/jfq/1620.pdf+herman+entropy+based+warfare&cd=1&hl=en&ct=clnk&gl=au

Honkasalo, A. (1998). Entropy, energy and steady-state economy. *Sustainable Development. 6*, 130-142.

Howlet, J., F. (1995). Maintenance: The pacifier's influence. *Proceeding of the 1997 International Carnahan Conference on Security Technology*, Institute of Electronic Engineers. pp. 219-224.

Keren, M. (1979). Ideological implications of the use of open systems theory in political science. *Behavioural Science, 24*, 311-324.

King, S. (2008). *Security entropy*. Computer Weekly. Retrieved July 5, 2011 from http://www.computerweekly.com/blogs/stuart_king/2008/09/security-entropy.html

Konicek, J., & Little, K. (1997). *Security, ID systems and locks: The book on electronic access control*. New York: Butterworth-Heinemann.

Liamputtong, P. & Ezzy, D. (2006). *Qualitative research methods* (2nd ed.). Oxford: University Press.

Lovey, I., & Nadkarni, M., S. (2007). *How healthy is your organisation*. Westport, Connecticut: Praeger Publishing.

Manunta, G. (1999). What is security? *Security Journal*. *12*, 57-66.

Manunta, G. (2007). The management of security: How robust is the justification process? *Security Journal*. *20*, 41-43.

Martin, D., W. (2000). *Doing psychology experiments* (5th ed.). Wadsworth.

McClure, S. A. (1997). *Security decay: The erosion of effective security*. Unpublished honours thesis, Edith Cowan University, Perth, Western Australia.

Midgley, G. (2003). *Systems thinking: general systems theory, cybernetics and complexity*. London: SAGE Publications.

Morales-Matamoros, O., Tejeida-Padilla, R., & Badillo-Pina, I (2010). Fractal Behaviour of Complex Systems. *Systems Research and Behavioural Science, 27*, 71-86.

Motz, L., & Weaver, J. H. (1989). *The story of physics*. New York: Plenum Press.

O Block, R. L., Donnermeyer, J., F., & Doeren, S., E. (1991). *Security and crime prevention* (2nd ed.). Boston: Butterworth-Heinemann.

Olzac, T. (2006). Just enough security. *Security*, *43*(9), 114.

Post, R. S., Kingsbury, A. A., & Schachtsick, D. A. (1991). *Security administration: An introduction to the protective services* (4th ed.). Boston: Butterworth-Heinemann.

Pidwirny, M. (2006). "Equilibrium Concepts and Feedbacks". *Fundamentals of Physical Geography, (2nd ed.).* February 3, 2010, from: http://www.physicalgeography.net/fundamentals/4f.html

Pitzer, K., S. (1995). *Thermodynamics*. New York: McGraw-Hill.

Prigogine (1987). Exploring complexity. *European Journal of Operational Research,* 30, 97-103.

Rifkin, J., & Howard, T. (1982). *Entropy*: a new world view. New York: The Viking Press.
Roos, I. (1997). The Debt of Systems Theory to Thermodynamics. Monash University Faculty of Business & Economics. Working paper series 34/97.
Singh, A. M. (2005). Private security and crime control. *Theoretical Criminology*, *9*, 153-174.
Smith, C. L. (2003). *Understanding concepts in the defence in depth strategy*, School of Engineering and Mathematics. Edith Cowan University, Perth, Western Australia.
Smith, S. (1992). Global dumbing: the politics of entropy. *Progressive Review*. Retrieved April 22, 2009 from http://prorev.com/dumbing.htm
Smith, C. L., & Brooks, D. J. (2013). *Security Science: The Theory and Practice of Security* Waltham, MA: Elsevier.
Somerson, I., S. (2009). *The art and science of risk security risk assessment.* Alexandria, VA: ASIS International.
Standards Australia. (2004). *AS/NZS4360:2004 Risk management.* Sydney: Standards Australia.
Standards Australia. (2006). *HB 167:2006 Security risk management*. Sydney: Standards Australia.
Styer, D. F. (2000). Insight into entropy. *American Journal of Physics*, *68*(12), 1090-1096.
The New Oxford School Dictionary (1991). Melbourne: Harper Collins Publishers.
Trusted Information Sharing Network for Critical infrastructure Protection, (2008). *Defence in depth*. Retrieved July 15, 2011 from http://www.dbcde.gov.au/__data/assets/pdf_file/0006/88359/DiD-CIO-15_Oct-2008.pdf
Underwood, G. (1984). *The security of buildings*. London: Butterworths.
Vannini, A. (2005). Entropy and Syntropy: from mechanical to life science. *NeuroQuantology* (2), 88-110.

REVIEWERS' COMMENTS (AS SUMMARZIED BY THE EDITOR WITH THEIR APPROVAL)

The authors are to be congratulated for provided us a fascinating and innovative model for thinking about security. Unfortunately, we have problems with the choice and phrasing of questions to the experts panels, with the degree to which the model was "validated", and with the writing itself. Most importantly of all, we believe the authors are perpetuating a number of myths and oversimplifications about security. These are both unnecessary for their thesis, and a disservice to readers.

The experts chosen for this study were clearly very qualified. While the authors were no doubt simply trying to be thorough and careful, many of the questions posed to the experts were rather mundane and pedantic. Is it really necessary to essentially check whether the experts believe in the 2nd Law of Thermodynamics? More troublesome, the questions to the experts seemed to be framed in a way that did not invite them to find any problems with the model. They don't seem to have been particularly encouraged to think about or raise any objections. In other words, too many softball questions resulted in a missed opportunity to critically examine the model.

One of us (but not so much the other) thinks that the authors' claim that the Delphi exercise "validated" their model may be overreaching, and that perhaps "examining its validity" might be a better way to think about this study.

The authors attempt—and we think with some success—to argue that decay can cause security failure. Unfortunately, they largely ignore other failure mechanisms that should be discussed as alternative or competing mechanisms, e.g., security may have been poorly designed right from the start, security resources may simply be inadequate, security hardware/software products deployed may not be very good or adversaries may have compromised them before deployment, the facility may be badly designed, changing threats and external technology development may make existing security moot or ineffective, the organization's mission or funding may have been modified by external authorities, etc.

Another problem with the paper, and something that impedes the reader's understanding and enjoyment, are the prevalent grammatical errors, pedantic language, clumsy wording, and (especially) the excessive use of the passive voice in much of the writing. If writing isn't the authors' strong suit, perhaps they should seek the assistance of a proficient technical writer in the future.

The biggest issue we have with the paper is that the authors seem overly obsessed with "Defense in Depth" (DiD), and the often mindless mantra "Deterrence, Detection, Delay, Response, and Recovery" (3D2R). The latter is more traditionally thought of as the 5Ds: "Deter, Detect, Deny, Delay and Defend". (DiD is sometimes also called "layered security".) The authors do not need to invoke these concepts to discuss security decay; they would have a more general model (and mislead the reader less) without them, or if they at least used them only tangentially.

It is NOT true, as stated in the abstract, that "...these functions [Deter, Detect, Delay, Response, and Recover] must be ...performed in order". In fact, 3D2R and 5Ds, which tend to be used somewhat interchangeably, aren't even in agreement over the order! More importantly, it's delusional thinking to believe that security managers can force a tightly ordered sequence (or a small number of pre-defined attack paths) on an intelligent and prepared adversary, especially inside attackers. It is also worth noting that in some complex DiD security plans, the various functions (or at least some of them) are meant to go into action simultaneously.

For many security applications, all of the various functions in 3D2R (or 5Ds) aren't relevant. Tamper-evident packaging on drugs, for example, involve detection, but there is little deter, delay, or recovery. When the President of the United States visits a city, Secret Service Agents sometimes "babysit" mentally unbalanced citizens who have made threats in the past as a preventive measure during the visit. This is pure prevention, without 3D2R or 5Ds. As another example, [Deter, Detect, Delay, Response, Recover] are often wholly or partially irrelevant for inside attackers.

By insisting that security can only be thought of in terms of DiD and 3D2R or 5Ds, the authors are perpetuating common, but dangerous myths. By insisting that their model can only be about DiD and 3D2R or 5Ds, they are limited its generality and usefulness.

EDITOR'S COMMENTS

I agree with the reviewers that this is a welcome and interesting paper, and that the authors should be thanked for their diligent efforts and for sharing them with us.

I was surprised at the vehemence with which both *reviewers* rejected the efficacy and orthodoxy of Defense in Depth and 3D2R (or 5D). I thought that was my shtick. I was also surprised at the vehemence with which the *authors* insisted that the only way to think about security or security decay is via Defense in Depth and 3D2R (or 5D).

I certainly have seen many examples of bad DiD security—the security failure at Y-12 with the trespassing 85-year old nun being a classic example of how (stupidly) DiD usually fails. (See the middle of page v at the beginning of this issue for more information about the Y-12 security breach.) I have also frequently seen examples of where an obsession with 3D2R (or 5D) leads to an over-emphasis on unimaginative force-on-force attacks at the expense of not properly defending against more probable, subtle, intelligent, and effective attack scenarios. These include, for example, insider attacks, and tampering with or installing backdoors in security hardware, software, or the facility being defended. In my view, the concepts of DiD and "3D2R (or 5D)—and in particular their "mindless" use (borrowing one reviewer's incendiary term)—have probably caused almost as much harm to security as good.

As a vulnerability assessor, I often ask about the strategy behind the security device, system, or program we are analyzing. If the first thing that the developer, manufacturer, or security manager says is "Defense in Depth", then I know in advance we are going to find a lot of amateurish and egregious vulnerabilities because the security has been incompletely thought through. If, on the other hand, there actually is a security strategy, with DiD merely being part of that strategy, then we will certainly find vulnerabilities but they won't be as numerous or embarrassing.

I have to agree with the reviewers that neither DiD nor 3D2R (or 5D) are necessary in the authors' model, and are indeed something of a red herring. On the other hand, decay is no doubt a bigger problem for complex systems, and DiD is almost always an (overly) complex system. Moreover, DiD and 3D2R (or 5D) are highly relevant to real world security because these are approaches and paradigms commonly used in security—for good or ill. To further side with the authors (at least a little), it is probably unfair for the reviewers and me to gang up on them over the issue of DiD and 3D2R (or 5D). The authors certainly did not invent these concepts nor are they responsible for their often "mindless", knee-jerk implement-tation. Furthermore, the second and third papers in this issue discuss applying and extending the EASI model, yet neither I nor the (different) reviewers of those papers criticized the authors over their use of EASI, DiD, and 3D2R (or 5D).

Though the reviewers did not raise this point, I was disappointed that the authors—having invoked a lot of science—didn't much use their model in a scientific way: to make predictions. Social scientists tend to use models to organize ideas, assist in interpreting the real world, and provide a construct for thinking about the relevant issues. Scientists, in

contrast, typically view the purpose of models as making predictions that can be tested. One prediction that the authors' model would seem to make that the authors did not much pursue is the idea that when security programs are not closed, i.e., when there is a lot of input of fresh "energy" (e.g., money, new ideas, new personnel, improved hardware and software, fresh analysis of threats/vulnerabilities/consequences/strategies), then the system's entropy can decrease.

I also whole-heartedly agree with the reviewers' condemnation of the extensive use of passive voice by the authors. Passive voice is not rigorous or scholarly. Rather, it obscures and it disguises. And it's annoying in excess. I have edited out a good bit of it in the final paper, as is standard practice for the *Journal of Physical Security*.

For any confused readers, here are some examples: "I made mistakes" is much better than the passive and weasely "Mistakes were made." People should write, "The data suggest…", not "It can be inferred from the data…"

For future authors: Here is Stephen King commenting on the passive voice [from *On Writing: A Memoir of the Craft,* Simon and Schuster, (2000), pp. 122- 124]:

> Verbs come in two types, active and passive. With an active verb, the subject of the sentence is doing something. With a passive verb, something is being done *to* the subject of the sentence. The subject is just letting it happen. *You should avoid the passive voice.* I'm not the only one who says so; you can find the same advice in *The Elements of Style.*
>
> Messrs. Strunk and White don't speculate as to why so many writers are attracted to passive verbs, but I'm willing to; I think timid writers like them for the same reason timid lovers like passive partners. The passive voice is safe. There is no troublesome action to contend with…I think unsure writers also feel the passive voice somehow lends their work authority, perhaps even a quality of majesty. If you find instruction manuals and lawyers' torts majestic, I guess it does. …
>
> I won't say there's no place for the passive tense. [But]…two pages of passive voice—just about any business document ever written, in other words, not to mention reams of bad fiction—make me want to scream. It's weak, it's circuitous, and it's frequently tortuous, as well.

Now some might argue that technical writing is somehow different. Poppycock*, I say! It is still done in English, and the principles of good English and good communication still apply, maybe even more so. (And this includes the importance of writing in short, clean, unambiguous sentences.)

Overall—the objections of the reviewers and myself notwithstanding—I think this is a remarkable and laudable paper. It certainly made me think about security (and "entropy") in a different way, and the disagreements were at least exciting, if not illuminating.

---

*"Poppycock" is from the Dutch word "pappekak", literally "soft dung".