แนวทางการตรวจสอบประสิทธิผลของระบบป้องกันทางกายภาพในสถานปฏิบัติการทางรังสีประเภทที่ 1 และ 2

นางสาวจุไรรัตน์ อุตส่าห์ดี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีนิวเคลียร์ ภาควิชาวิศวกรรมนิวเคลียร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2558

INSPECTION GUIDELINE FOR THE EFFECTIVENESS OF PHYSICAL PROTECTION SYSTEM AT CATEGORIES I AND II RADIATION FACILITY

Miss Jurairat Utsadee

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Nuclear Technology
Department of Nuclear Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2015

Thesis Title	INSPECTION GUIDELINE FOR THE EFFECTIVENESS OF PHYSICAL PROTECTION SYSTEM AT CATEGORIES I AND II RADIATION FACILITY
By	Miss Jurairat Utsadee
Field of Study	Nuclear Technology
Thesis Advisor	Dr. Phongphaeth Pengvanich
Thesis Co-Advisor	Dr. Rungdham Takam

Accepted by the Faculty of Engineering, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

.....Dean of the Faculty of Engineering

(Professor Dr. Bundhit Eua-arporn)

THESIS COMMITTEE

.....Chairman

(Associate Professor Dr. Sunchai Nilsuwankosit)

.....Thesis Advisor

(Dr. Phongphaeth Pengvanich)

.....Thesis Co-Advisor

(Dr. Rungdham Takam)

.....Examiner

(Associate Professor Dr. Supitcha Chanyotha)

.....External Examiner

(Assistant Professor Attaporn Pattarasumunt)

จุไรรัตน์ อุตส่าห์ดี : แนวทางการตรวจสอบประสิทธิผลของระบบป้องกันทางกายภาพในสถานปฏิบัติการทางรังสีประเภทที่ 1 และ 2 (INSPECTION GUIDELINE FOR THE EFFECTIVENESS OF PHYSICAL PROTECTION SYSTEM AT CATEGORIES I AND II RADIATION FACILITY) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ดร. พงษ์แพทย์ เพ่งวาณิชย์, อ.ที่ปรึกษาวิทยานิพนธ์ร่วม: ดร. รุ่งธรรม ทาคำ, 136 หน้า.

ปัจจุบันโปรแกรมการตรวจสอบระบบความมั่นคงปลอดภัยของวัสดุกัมมันตรังสีมีการตรวจสอบองค์ประกอบด้านความมั่นคงปลอดภัยเท่านั้น ไม่รวมถึงการตรวจสอบประสิทธิผลของระบบการป้องกันทางกายภาพ การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อพัฒนารายการตรวจสอบที่สามารถใช้ในการประเมินประสิทธิผลของระบบการป้องกันทางกายภาพในสถานปฏิบัติการทางรังสีประเภทที่ 1 และ 2

รายการตรวจสอบที่สร้างขึ้นนั้นได้นำวัตถุประสงค์ของระบบรักษาความมั่นคงปลอดภัยของวัสดุกัมมันตรังสีประเภทที่ 1 ของทบวงการพลังงานปรมาณูระหว่างประเทศมาเป็นตัวกำหนดในการสร้างรายการตรวจสอบ รายการตรวจสอบที่สร้างขึ้นจะอยู่ในรูปของแบบสอบถามเพื่อประเมินระบบรักษาความมั่นคงปลอดภัยซึ่งประกอบด้วย ระบบการตรวจจับ การหน่วงเวลา การตอบสนอง การจัดการความมั่นคงปลอดภัย และวัฒนธรรมความมั่นคงปลอดภัย มีการสร้างเกณฑ์การให้คะแนนในแต่ละคำถาม ระบบรักษาความมั่นคงปลอดภัยจะมีประสิทธิภาพเมื่อแต่ละระบบสามารถตอบสนองวัตถุประสงค์ที่กำหนดได้ กลุ่มตัวอย่างที่ใช้ทดสอบรายการตรวจสอบคือ สถานปฏิบัติการทางรังสีที่มีการติดตั้งอุปกรณ์ระบบความมั่นคงปลอดภัยรวมทั้งหมด 5 กลุ่มตัวอย่าง และประเมินผลรายการตรวจสอบโดยการเปรียบเทียบผลจากรายการตรวจสอบและผลจากโปรแกรมการคำนวณค่าความน่าจะเป็นในการยับยั้งศัตรู (EASI) ผลการวิจัยพบว่าผลที่ได้จากรายการตรวจสอบมีความคล้ายคลึงกันกับผลที่ได้จากโปรแกรมการคำนวณค่าความน่าจะเป็นในการยับยั้งศัตรูในกรณีที่เป็นการขโมย

ภาควิชา วิศวกรรมนิวเคลียร์ ลายมือชื่อนิสิต .....

สาขาวิชา เทคโนโลยีนิวเคลียร์ ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

ปีการศึกษา 2558 ลายมือชื่อ อ.ที่ปรึกษาร่วม .....

5670564021 : MAJOR NUCLEAR TECHNOLOGY
KEYWORDS: CHECKLIST, PHYSICAL PROTECTION, EASI MODEL

JURAIRAT UTSADEE: INSPECTION GUIDELINE FOR THE EFFECTIVENESS OF PHYSICAL PROTECTION SYSTEM AT CATEGORIES I AND II RADIATION FACILITY. ADVISOR: DR. PHONGPHAETH PENGVANICH, CO-ADVISOR: DR. RUNGDHAM TAKAM, 136 pp.

At present the inspection program of security of radioactive materials only looks at the presence of security components, but does not include the measurement of physical protection system effectiveness. This research aims to develop an inspection checklist for evaluating the effectiveness of physical protection system at Categories 1 and 2 radiation facilities.

The checklist is developed based on the security objectives of the IAEA's minimum standard requirements. To meet the objectives, the checklist in the form of questionnaire was created to evaluate each security elements, which are access control, detection, delay, response, security culture, and security management. Scoring criteria are established. The physical protection system will be effective when all security elements meet their objectives. Five samples, which already have the physical protection system installed, are chosen as the test subject for the checklist. The checklist result is compared against the result from the Estimate of Adversary Sequence Interruption (EASI) model, which is a computerized program for evaluating physical protection system effectiveness as the probability of interrupting an adversary in an adversary path. It is found that the checklist result and the EASI result are similar in the case of theft.

Department:	Nuclear Engineering	Student's Signature	.....
Field of Study:	Nuclear Technology	Advisor's Signature	.....
Academic Year:	2015	Co-Advisor's Signature	.....

ACKNOWLEDGEMENTS

The success of this thesis can been attributed to the extensive support and assistance from my advisor, Dr. Phongphaeth Pengvanich. I deeply thank him for his continuous consultation and valuable advice and guidance in this research.

I would also like to thank my thesis committee members, Associate Professor Dr. Sunchai Nilsuwankosit, Associate Professor Dr. Supitcha Chanyotha, Assistant Professor Attaporn Pattarasumunt and my co-advisor, Dr. Rungdham Takam.

I am grateful to all the lecturers and staff in Nuclear Engineering Department of Chulalongkorn University for the support and allowing us to perform this study and also thank to my friends in the Nuclear Security and Safeguard for their kind support.

I would like to give special thank to the EU CBRN Center of Excellence for providing funding to support this research.

CONTENTS

Page

Page

Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Background

Nowadays, nuclear security threats are increasing globally. These are in the form of terrorism, or insurgency, or other malevolent act. There are various purposes of threat, such as to fulfill ideology, to destroy property, to undermine confidence in the economy, or even to destroy life. If the threat is to use radioactive material as a dirty bomb or sabotage, it may have multiple effects on economy, psychology and life. This event should not happen. In order to prevent such event, there must first be common recognition of the security of radioactive materials around the world, including Thailand as well.

Many practices utilizing radiation sources are well established in Thailand today. Co-60, for instance, is used in medical application for the treatment of cancer, and in industrial application for the irradiation of foodstuff. In research, varieties of seal sources are employed. Some consumer products such as smoke detector even make use of radiation sources. According to the information from the Bureau of Radiation Safety Regulation, Office of Atoms for Peace (OAP), there are 971 radiation facilities in Thailand that utilize total of 43,019 radioactive materials. These materials are grouped into Category 1, 2, 3, 4, and 5 based on the risks to human health if not safely and securely managed as shown in Table 1-1. An exposure of only a few minutes to an unshielded Category 1 radioactive material may be fatal. At the lower end of the categorization system, material in Category 5 is the least dangerous.

The Category 1 radioactive material is “extremely dangerous”. If not safely managed or securely protected, it will likely cause permanent injury to the people who handle or are in contact with it for more than a few minutes. The Category 2 radioactive material is “very dangerous”. If not safely managed or securely protected, it can cause permanent injury to the people who handle or are in contact with it for a short period of time (minutes to hours). The Category 3 radioactive material is

“dangerous”. If not safely managed or securely protected, it can cause permanent injury to the people who handle or are in contact with it for some hours.

The Categories 1 and 2 radioactive materials are high risk to human health because exposure to unshielded materials for only a few minutes may be fatal. From Table 1-1, the numbers of radiation facilities that utilize radioactive materials in Categories 1 and 2 are 77 and 89 units respectively. The amount of radioactive materials in Category 1 and 2 are 5,394 and 726 respectively. These radioactive materials should be kept in a safe and secure storage not only to reduce the chance of person coming into contact with them, but also to minimize or eliminate the chance of theft, sabotage, or other malicious acts.

The Office of Atoms for Peace has issued a regulation on security of Categories 1 and 2 radioactive materials, which indicates that the security area (any temporary or permanent area, operation area, or room determined and established by the licensee for the physical protection of Categories 1 or 2 quantities of radioactive materials) must have a physical protection system and alarm system to prevent any intrusion or theft, and the system must not be lower than the regulatory requirement. Such physical protection system and alarm system usually consist of detection, delay, response, security management elements [1].

To ensure that the physical protection system and alarm system are effective, regulators need to have an inspection program to verify that the security of radioactive materials is effectively maintained. However, at present the inspection program only looks at the presence of security components, but does not include the measurement of physical protection system effectiveness. In other words, it cannot tell whether the installed security system will be able to successfully stop or interrupt the adversaries in various potential scenarios.

This research aims to develop an inspection checklist for evaluating the effectiveness of physical protection system at Categories 1 and 2 radiation facilities. The checklist is based on the laws and regulations of Thailand, and the standard recommendations which are derived from the Nuclear Security Series guides published by the International Atomic Energy Agency (IAEA) as well as the security

guidelines of the United States Nuclear Regulatory Commission (U.S. NRC). The issue of security culture is also taken into consideration in the development of the checklist as it is another critical security component that can make or break the physical protection system.

Table 1.1 Number of radiation facility and radioactive material in each category in Thailand

radioactive material category	Number of radiation facility	Number of radioactive material
1	77	5,394
2	89	726
3	255	1,882
4	250	1,408
5	300	43,019
Total	971	52,429

The checklist is compared against the result from a computerized program for evaluating physical protection system effectiveness based on the Estimate of Adversary Sequence Interruption (EASI) model. The model evaluates the effectiveness as the probability of interrupting an adversary in an adversary path. The analysis will identify system deficiencies and help determine the improvement needed. The comparison between the checklist result and the EASI model result ensures that the checklist can be used for evaluating the effectiveness of physical protection system and the limitations of checklist (if any) are accounted for.

1.2 Objective

To develop the inspection guideline for the effectiveness of physical protection system at categories I and II radiation facility

1.3 Scope of Study

1.1 Concentrate on radioactive materials in category I and II in use and storage in radiation facilities.

1.2 Develop checklist as a guideline for inspection.

1.3 Test the checklist at 2 facilities or more (such as hospitals and irradiation centers).

1.4 Expected Benefit

A guideline that can be used by regulatory authorities and those involved with the assessments and inspections of physical protection system at Categories 1 and 2 facilities that use or store radioactive materials in a security area. The guideline would also be useful to licensing applicants in their preparation to submit application for usage authorization of Categories 1 and 2 radioactive materials in order to design the physical protection system that is in compliance with regulatory requirement.

CHAPTER 2
LITERATURE REVIEWS

Concept and theory

2.1 Thai Law and regulation on security of category 1and 2radioactive materials.

The Regulation of Atomic Energy Commission for Peace B.E. 2554 on security of category 1and 2 radioactive materials, indicating that the security area (which means any temporary or permanent area, operation area, or room determined and established to be “security area” by the licensee of Categories 1 or 2 radioactive materials) must be physically and effectively protected. The area must, at a minimum, allow unescorted access only to approved individuals in order to keep the source safe from unauthorized person [1]. And the system should be no less than the following requirements.

Detection of unauthorized access to the storage area, or operation area, or installation area, or source location.

(1) Immediate detection of any unauthorized access to the secured area/source location using equipment such as electronic sensor alarm or continuous surveillance by personnel.

(2) Detection of any attempted unauthorized removal of the source using equipment such as electronic sensor alarm or continuous surveillance by personnel.

(3) Immediate assessment of (1) or (2) using equipment such as CCTV.

(4) Rapid communication to response personnel using equipment such as cell phone or radio communication.

Delay

System has at least 2 layers such as exterior wall or locks to prevent unauthorized removal.

Response

System has immediate initial of response such as personnel with equipment and procedure to interrupt and prevent unauthorized removal.

Security Management

(1) Provide access controls to source location and restrict access to authorized persons only.

(2) Provide background checks for operator personnel.

(3) Provide sensitive information protection system.

(4) Provide security plan.

2.2 Categorization of radioactive material.

IAEA safety standard No. RS-G-1.9 was defined the categorization of radioactive material. The categorization of radioactive material is divided into five categories according to dangerous to the person.

(1) Category 1 is extremely dangerous to the person: This radioactive material, if not safely managed or securely protected, would be likely to cause permanent injury to a person who handled it or who was otherwise in contact with it for more than a few minutes. It would probably be fatal to be close to this amount of unshielded radioactive material for a period in the range of a few minutes to an hour.

(2) Category 2 is very dangerous to the person: This source, if not safely managed or securely protected, could cause permanent injury to a person who handled it or who was otherwise in contact with it for a short time (minutes to hours). It could possibly be fatal to be close to this amount of unshielded radioactive material for a period of hours to days.

(3) Category 3 is dangerous to the person: This source, if not safely managed or securely protected, could cause permanent injury to a person who handled it or who was otherwise in contact with it for some hours. It could possibly — although it would be unlikely — be fatal to be close to this amount of unshielded radioactive material for a period of days to weeks.

(4) Category 4 is unlikely to be dangerous to the person: It is very unlikely that anyone would be permanently injured by this source. However, this amount of unshielded radioactive material, if not safely managed or securely protected, could possibly — although it would be unlikely — temporarily injure someone who

handled it or who was otherwise in contact with it for many hours, or who was close to it for a period of many weeks.

(5) Category 5 is most unlikely to be dangerous to the person: No one could be permanently injured by this source.

And the principle of categorization of radioactive material is divided into two according to prioritization.

2.2.1 Categorization of radioactive material based on practice.

Categorization of radioactive material based on practice for example Co-60 teletherapy is categorized based on practice as Category 1. Categorization of radioactive materials are shown in table 2.1.

2.2.2 Categorization of radioactive material based on A/D.

2.2.2.1 Unlisted radioactive materials in table 2.1, in this case radioactive material is categorized based solely on A/D or activity ratio (A is activity of interested of radioactive material and D is dangerous source, D value). The D value is the radionuclide specific activity of a source and D value can be found in Appendix B.

2.2.2.2 Aggregation of radioactive materials.

In this case, radioactive materials are in close proximity to each other, such as in manufacturing processes (e.g. in the same room or building) or in storage facilities (e.g. in the same enclosure). In such situations, the summed activity of the radionuclide should be divided by the appropriate D value and calculated ratio A/D. If sources with various radionuclides are aggregated, then the sum of the ratios A/D should be used in determining the category, in accordance with the formula:

$$\text{Aggregate } {}^{A}/_{D} = \sum_{n} \frac{\sum_{i} A_{i,n}}{D_n} \qquad \text{Equation 2.1}$$

Where $A_{i,n}$ = Activity of each individual source i of radionuclide n;

D_n = D value for radionuclide n.

Table 2.1 Categorization of radioactive materials [6, 7].

Category	Radioactive materials	A/D
1	Radioisotope thermoelectric generators (RTGs) Irradiators Teletherapy Fixed, multi-beam teletherapy (gamma knife)	A/D≥1000
2	Industrial gamma radiography High/medium dose rate brachytherapy	1000>A/D≥ 10
3	Fixed industrial gauges - Level gauges - Dredger gauges - Conveyor gauges containing high activity sources - Spinning pipe gauges Well logging gauges	10>A/D≥1
4	Low dose rate brachytherapy sources (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity Bone densitometers Static eliminators	1>A/D≥0.01
5	Low dose rate brachytherapy eye plaques and permanent implant X ray fluorescence (XRF) devices Electron capture devices Mossbauer spectrometry Lightening preventor	0.01>A/D

2.3 Security level.

Radioactive material categorized by a risk to human health if not managed safely and securely. Therefore to ensure that the sources are adequately protected, graded approach should be applied to security, thus the concept of security levels should be used. Three security levels (A, B, and C) have been developed to allow specification of security system performance in a graded manner. Security level A requires the highest degree of security while the other levels are progressively lower.

There is a corresponding goal for each security level. The goal defines the overall result that the security system should be capable of providing for a given security level. The goals of each security level as follows:

- Security level A: Prevent unauthorized removal of a radioactive material.
- Security level B: Minimize the likelihood of unauthorized removal of a radioactive material.
- Security level C: Reduce the likelihood of unauthorized removal of a radioactive material.

Each security level goals only address unauthorized removal but malicious act may be in sabotage form, achievement of the goals will reduce the likelihood of a successful act of sabotage. In order to meet the goals, it is necessary to achieve an adequate level of performance for each of the security functions: detection, delay, response, and security management. That level of performance is defined as a set of objectives for each security functions. Security levels and security objectives are shown in table 2.2.

Table 2.2 Security levels and security objectives [4].

Security functions	Security objectives		
	Security Level A Goal: Prevent unauthorized removal[a]	Security Level B Goal: Minimize likelihood of unauthorized removal[a]	Security Level C Goal: Reduce likelihood of unauthorized removal[a]
Detect	Provide immediate detection of any unauthorized access to the secured area/source location		
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider	Provide detection of any attempted unauthorized removal of the source	Provide detection of unauthorized removal of the source
	Provide immediate assessment of detection		
	Provide immediate communication to response personnel		
	Provide a means to detect loss of source through verification		
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal	Provide delay to minimize the likelihood of unauthorized removal	Provide delay to reduce the likelihood of unauthorized removal
Response	Provide immediate response to assessed alarm with sufficient resources to	Provide immediate initiation of response to interrupt the unauthorized	Implement appropriate action in the event of unauthorized

Table 2.2 Security levels and security objectives [4] (continued).

Security functions	Security objectives		
	Security Level A Goal: Prevent unauthorized removal[a]	Security Level B Goal: Minimize likelihood of unauthorized removal[a]	Security Level C Goal: Reduce likelihood of unauthorized removal[a]
	interrupt and prevent the unauthorized removal	removal	removal of a source
Security management	Provide access controls to source location that effectively restrict access to authorized persons only		
	Ensure trustworthiness of authorized individuals		
	Identify and protect sensitive information		
	Provide a security plan		
	Ensure a capability to manage security events covered by security contingency plan		
	Establish security event reporting system		

[a] Achievement of these goals will also reduce the likelihood of a successful act of sabotage.

There are recommended default security levels for commonly used sources by category 1 radioactive materials should have security measures which meet the security objectives of security Level A. Category 2 radioactive materials should have security measures which meet the security objectives of security Level B. Category 3 radioactive materials should have security measures which meet the security objectives of security Level C. And there are general requirements for the security of category 4 and 5 radioactive materials in the International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources (BSS115).

The recommended default security levels for commonly used sources as shown in table 2.3.

Table 2.3 Recommended default security levels for commonly used sources [4]

Category	Source	A/D	security level
1	RTGs Irradiators Teletherapy Fixed, multi-beam teletherapy (gamma knife)	A/D≥1000	A
2	Industrial gamma radiography High/medium dose rate brachytherapy	1000>A/D ≥10	B
3	Fixed industrial gauges that incorporate high activity Well logging gauges	10>A/D ≥1	C
4	Low dose rate brachytherapy sources (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity Bone densitometers Static eliminators	1>A/D ≥0.01	Apply measures as described in Basic Safety Standards (BSS115)
5	Low dose rate brachytherapy eye plaques and permanent implant X ray fluorescence (XRF) devices Electron capture devices Mossbauer spectrometry Positron emission tomography (PET) check sources	0.01>A/D and A>exempt	

2.4 Physical protection system and effectiveness.

A physical protection system (PPS) integrates of people, procedure and equipment for the protection of asset or facilities against theft, sabotage and other malevolent human attacks [3]. The purpose of PPS is to prevent an adversary from successful completion of a malevolent action against a facility. The PPS has primary physical protection functions which are detection, delay, and response but not only these functions, there are other functions to provide the PPS more effective which are access control and security management. It is essential to understanding of the definitions of these functions and the measure of effectiveness of each is required to evaluate the system. The effectiveness of the PPS is the meeting each security objective. All of these functions will explain as follows:

Detection

Detection is the discovery of adversary action which have aimed of unauthorized removal or sabotage of a radioactive material. Detection can be achieved by several measures, including visual observation, video surveillance, electronic sensors, accountancy records, seals and other tamper indicating devices, process monitoring systems, and other measures. The measures of effectiveness for the detection function are the probability of sensing adversary action and the time required for reporting and assessing the alarm [3]. Therefore, the objectives of detection measures could range from immediate detection, assessment and communication of any unauthorized access to subsequent detection of unauthorized removal through tamper indicators or periodic physical checks [4]. The “immediate” is commonly defined as “instant” or “without delay [8].” It should be note that detection will not complete if without assessment and communication.

Assessment of alarm: detection should always be complemented by assessment to determine the cause of the alarm immediately. Alarm assessment requires human observation and judgment, through deployment of response personnel to investigate the cause of the alarm, or through remote closed circuit television (CCTV) systems.

Communication to response personnel: if the assessment confirms that unauthorized access or attempted unauthorized removal has occurred, immediate notification or reporting should be made to response personnel by operator personnel with diverse (at least two) means of communication such as landline telephones, auto-dialers, cellular phones, radios or paging devices.

Example of immediate detection measures: electronics sensor linked to an alarm; continuous visual surveillance personnel (24 hours working); continuous monitoring through CCTV by operator personnel or front guard (24 hours working); functional equipment for assessment and communication. For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of immediate intrusion detection. Note, however, that if continuous surveillance is chosen as a security measure, continuous visual surveillance may require observation by at least two individuals at all times. If the detection is provided by continuous visual surveillance by operator personnel, assessment should be performed concurrently with detection by the operator personnel keeping the source under continuous visual surveillance.

Delay

Delay is the slowing down of adversary progress. The measure of delay effectiveness is the time required by the adversary (after detection) to remove the radioactive material or sabotage. Even the adversary may be delayed prior to detection, this delay is of no value to the effectiveness of the physical protection system, because it does not provide additional time to respond to the adversary. Therefore, the objective of delay measure could range from providing sufficient delay after detection to allow response personnel to interrupt adversary. Delay can be achieved by several measures, generally through multiple barriers or other physical measures, such as locked doors [4]. For security level A, the system must have at least 2 delay layers after detection to be effective. Example of effectiveness for delay measure: a locked device in a locked room to separate the device from unauthorized personnel; a locked and fixed container or a device holding the source

in a locked storage room; for mobile sources, continuous visual surveillance by operator personnel may substitute for one or both layers of barriers.

Response

Response is an action taken by the response force personnel to prevent adversary success. Response consists of interrupt adversary. The interruption is defined as a sufficient number of response force personnel arriving at the appropriate location to stop the adversary's progress. Therefore the objectives of response measures could range from providing immediate response with sufficient resources to interrupt malicious acts to providing alarm notification to allow the appropriate authority to investigate the event. Immediate means that responders should arrive, once notified, in a time shorter than the time required to breach the barriers and perform the tasks needed to remove the source. Adequate means that the response team is of sufficient size and capability to subdue the adversary. Response may be a directly employed security force, a third party security team, local police, or national gendarmerie [4]. Example of effectiveness for response measure: immediate response such as responder know how to action if an event occur; sufficient resource such as the number of responder and equipment is enough to respond i.e. there is at least one responder per allocation area; all responders should have at least one equipment to interrupt adversary and communication device; all responders must be trained.

Access control

Access control refers to allowing access to authorized personnel and detecting the attempted access of unauthorized personnel. Access control can be achieved by several measures, including locked control by swipe card reader, personal identification number (PIN), badge, or key control. The measures of effectiveness of access control are identification and two verification of a person’s access authorization. Example of effectiveness for access control measure: locked control by swipe card reader and PIN; badge and control key; fingerprint and PIN; controlled key and visual verification of identity by other authorized personnel. For

mobile sources in use, continuous visual surveillance by multiple operator personnel may substitute for access control and they have a way to verify if an individual is authorized personnel (e.g. access list, badge type).

Security management

Security management measures, addressing access control, trustworthiness, information protection, development of a security plan and security event reporting.

Access control: access control means a system for allowing only authorized personnel to have unescorted access to the security area and for ensuring that all other person are subject to escorted access. The management in access control can be achieved by development of procedure or method for control an accessing to security area, including key control management, establishment of security area, recording of access control management, establish a list of persons currently approved for unescorted access and measure for authorized personnel have retired.

Trustworthiness: the determination of trustworthiness and reliability is a key measure in mitigating the threat posed by insiders. Trustworthiness can be achieved by background check, including a verification of references to determine the integrity and reliability of each person.

Information protection: accessing to sensitive information should be limit and access by authorized person only. Key elements of information protection include identifying the information that must be protected; designating individuals with authorized access to such information; and protecting such information from disclosure to individuals who do not have this access.

Development of a security plan: a security plan should be develop, implement, test, periodically review, revise as necessary and comply with its provisions. The plan should describe the overall nuclear security system in place to protect the radioactive material and should include measures to address an increased threat level, response to nuclear security events and the protection of sensitive information. The content for a security plan which refers from IAEA Nuclear Security Series No. 11 can be found in Appendix C.

Security event reporting: security event is the event that security-related such as suspected or actual theft of a radioactive source; unauthorized intrusion into a facility or source storage area; loss of control over a radioactive source; unauthorized access to or unauthorized use of a source; failure or loss of security systems that are essential to the protection of radioactive sources. Any absence or discrepancy regarding the presence or amount of radioactive material, particularly during an inventory, should be promptly investigated. Promptly report to the regulatory body and other relevant competent authorities (e.g. law enforcement) should be required.

2.5 Nuclear security culture.

A cultural approach to physical protection involves determining what attitudes and beliefs need to be established in an organization, how these attitudes and beliefs manifest themselves in the behavior of assigned personnel, and how desirable attitudes and beliefs can be transcribed into formal working methods to produce good outcomes. An effective nuclear security culture depends on proper planning, training, awareness, operations and maintenance, as well as on the thoughts and actions of people who plan, operate and maintain nuclear security systems.

The foundation of nuclear security culture is recognition in role and responsibility of security of every position level personnel. This foundation is represented as the basis for the model of an effective nuclear security culture. Nuclear security culture is defined as the assembly of characteristics, attitudes and behavior of individuals, organizations and institutions which serves as a means to support and enhance nuclear security [11], the proper assembly of which leads to more effective nuclear security. The attitudes and behavior of people who have responsibilities for the use, handling, safe-keeping or transport of radioactive material is important to increase effectiveness of physical protection system and the factor that assess the nuclear security culture of individual and organization should include management system, operating system, personnel performance and training as described follows:

Management system: the established nuclear policy and clearly defined roles and responsibilities for all nuclear security positions is represented as awareness of organization culture. Therefore, a well developed management system is an essential feature of effective nuclear security.

Operating system: the established documented procedures which security-related and clearly defined in their job descriptions will improve and understanding of role of person. Therefore, a well developed operating system is an essential feature of effective nuclear security.

Personnel performance: A major part of the nuclear security culture of an organization is. Personnel performance is represented as the characteristic of operator personnel behavior in awareness security-related. The effectiveness of nuclear security depends on the behavior of all personnel, including adhering to procedure or standards.

Training: operator or employees should receive baseline instruction on policies, issues, and incident response/reporting procedures. The training should be tailored to an individual's job within the facility and short enough to be easily comprehensible and it is important to get feedback on the training programs and materials, as well as the trainers themselves. Training can be performed annually, quarterly, or as needed.

2.6 EASI model.

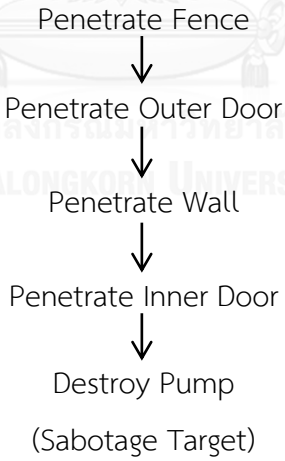
A PPS is a complex configuration of detection, delay, and response elements that can be analyzed to determine system effectiveness. The analysis will identify system deficiencies and help evaluate improvements. The technique that can be used for evaluating either an existing protection system or a proposed system design is the Estimate of Adversary Sequence Interruption (EASI) model, which was developed in the 1970s by Sandia National Laboratories, USA. The most commonly used form of EASI is as a Microsoft Excel application.

EASI is a simple calculation tool that quantitatively illustrates the effect of changing physical protection parameters along a specific path of adversary (only

analyze one adversary path). It uses detection, delay, response, and communication values to compute the probability of interruption (P_I) [3].

EASI use pathway analysis to evaluation of PPS effectiveness. Pathway analysis involves identifying and analyzing the paths (through a facility) that an adversary might take during his theft or sabotage attempt. An adversary path is an ordered series of actions against a target that, if completed, results in successful theft or sabotage. There are many adversary paths into a facility. The critical path or worst path is that path with the lowest P_I, and successful malevolent act by adversary easily. Figure 2.1 illustrates example of a single sabotage path of an adversary who wishes to destroy a pump in an industrial facility.

Note that paths differ depending on the adversary objective. Theft implies the adversary must get into and out of the facility to succeed, while sabotage only requires that the adversary get to the asset and have time to complete the act of sabotage to be successful. This difference is extremely important when performing a quantitative analysis, because it will determine how much time the response force has to interrupt the adversary.



Source: Garcia, Mary Lynn. 2001. The design and evaluation of physical protection systems. pp.242.

Figure 2.1 Example of sabotage path of an adversary who wishes to destroy a pump in an industrial facility.

In EASI model, parameters input for analysis are (1) detection and communication inputs as probabilities (P_C and P_D respectively), and (2) delay and response inputs as mean times and standard deviations for each element. The output will be P_I or the probability of interruption the adversary before any theft or sabotage occurs. The P_I is calculated as:

$$P_I = P_C * P_D \qquad \text{Equation 2.2}$$

Where P_C is Probability of Guard communication,

P_D is Probability of detection.

The value entered into EASI for P_C is at least 0.95, which is from evaluation of many systems designed and implemented by Sandia National Laboratories and the most system operate with this value. This number can be used as a working value during the analysis of a facility.

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 [12, 13].

2.7 Equation for evaluation of effectiveness of physical protection system in the research.

The physical protection system (PPS) requires synergy among various security elements, including access control, detection, delay, response, security management and security culture. All elements are important to the supporting of asset protection -- if one of the elements was to fail, the whole physical protection would fail. For example, if there is no delay system, the responder will not have enough time to stop or interrupt the attack of the adversary even if the adversary has been detected. If there is delay element but it is unacceptable, other elements must compensate for the shortfall. The overall system needs to take into account that each security element can support each other. For such reason, we propose that the overall effectiveness of the system is the multiplication of all the security elements as follow:

$$\sum Acc \times \sum Det \times \sum Del \times \sum Res \times \sum Man \times \sum Cul \leq 1 \qquad \text{Equation 2.3}$$

where $\sum Acc$ is the score of access control normalized to 1

$\sum Det$ is the score of detection normalized to 1

$\sum Del$ is the score of delay normalized to 1

$\sum Res$ is the score of response normalized to 1

$\sum Man$ is the score of security management normalized to 1

$\sum Cul$ is the score of security culture normalized to 1

and the score of 0 means the element is missing, whereas the score of 1 means the element is fully present and sufficient based on the regulatory requirements and standard recommendations.

From equation 2.3, can be further explained as follows:

Considering the access control element. Even though a facility may have very good detection, delay, response, security management and security culture elements, but if there is no control of access to the security area or source location, it would be easy for an unauthorized person to gain access to perform malicious act to the target. Since there is nobody or no measure to restrict accessing, the adversaries can reach the target and achieve their task quickly.

Considering the detection element. Even though a facility may have very good access control, delay, response, security management and security culture elements, but if there is no detection of unauthorized access to security area or source location and there is no detection of unauthorized removal of radioactive source, there would be no way to detect and confirm that there is intrusion, and the response personnel would not be notified about the intrusion. Hence, the adversaries can reach the target and achieve their task without being interrupted.

Considering the delay element. Even though a facility may have very good access control, detection, response, security management and security culture elements, but if there is no delay after detection, the adversary can reach the target quickly. There would be no barrier or other delay system to provide enough time for the response personnel to interrupt and prevent the adversary from accomplishing its task.

Considering the response element. Even though a facility may have very good access control, detection, delay, security management and security culture elements, but if there is no response personnel or the response personnel is not sufficient, the adversary would not be interrupted or defeated.

Considering the security management element. Even though a facility may have very good access control, detection, delay, response and security culture elements, but if there is no good security management implemented, a loophole may open in the system which allows adversary to get in. For example, insufficient background check of an authorized person can lead to insider threat. Once a person is authorized, he or she can get in the security area or source location with ease. No proper security plan would also result in not knowing what action to take when a security incident occurs.

Considering the security culture element. Even though a facility may have very good access control, detection, delay, response and security management elements, but if security culture is lacking, the other security elements would not be used properly. For example, if the manager and staff are not seriously following or aware of security protocols, they may just bypassing any security systems installed at the facility and cause security incidence.

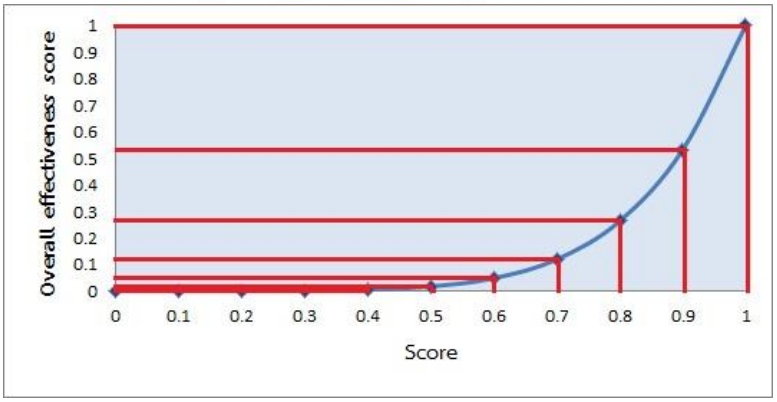


Figure 2.2 The overall effectiveness score is proportion to x^6

From equation 2.3, it is found that the overall effectiveness score is proportion to x^6. It should be noted that even if all of the security elements have a score of 0.9, which is very high score, the overall effectiveness score would still be 0.53 as shown in Figure 2.2. If a regulator decides to implement this checklist, the criteria of

acceptance will depend on what percentage or score will be considered “passing” by the regulator. For instance, if the passing scores of all security elements are set to 0.7 or 70%, the acceptable overall effectiveness score would be 0.12.

Literature Reviews

US.NRC. (2012). Report to Congress on the Security Inspection Program for Commercial Power Reactors and Category I Fuel Cycle Facilities: Results and Status Update. Annual Report for Calendar Year 2012.

U.S.NRC has published report. This report provides both an overview of the NRC’s security inspection and Force-on-Force inspection programs of the commercial nuclear power industry and Category I (CAT I) fuel cycle facilities, and summaries of the results of those inspections. This inspection resides within the “security cornerstone” and the security cornerstone focuses on the following five key licensee performance attributes: access authorization, access control, physical protection systems, material control and accounting (MC&A), and response to contingency events. Through the results obtained from all oversight activities, the NRC determines whether NPP licensees comply with appropriate regulatory requirements and can provide high assurance of adequate protection against the design basis threat (DBT) of radiological sabotage.

A. ŠTEFULOVÁ. (2001). Evaluation of effectiveness of physical protection systems at nuclear facilities in Slovakia. In Proceedings IAEA 2001 of International Conference on Measures to Prevent, Intercept and Respond to Illicit Uses of Nuclear Material and Radioactive Sources, Stockholm, Sweden, 7–11 May 2001. pp. 221-223.

The utilization of the nuclear power in Slovakia is based upon the Act No. 130/1998. The nuclear facilities in the Slovak Republic are supervised by Nuclear Regulatory Authority of the Slovak Republic (UJD SR). The utilization of the nuclear power in Slovakia is based upon the Act No. 130/1998. According to this act, physical protection of the nuclear facilities and nuclear materials is an integral part of measures necessary to ensure the nuclear safety. Before get the license, every

organization which intends to begin construction or operation of the nuclear facility need to submit physical protection plan to the UJD SR. The plan must take into account all requirements imposed upon the physical protection system as stipulated in the UJD SR's Regulation No. 186/1999 which details the physical protection of the nuclear facilities, nuclear materials, and radioactive wastes.

The physical protection of the nuclear facilities and nuclear materials are aimed to prevent unauthorized manipulations, prevent their abuse or damage.

The government of former Czechoslovakia decided that there was a need to create a new physical protection system which would increase the level of the nuclear facilities physical Protection. It was decided that the physical protection would be preferably provided using an Automated Complex of Security Protection of NPPs – AKOBOJE.

The inspectors of UJD SR perform to evaluation of the physical protection system. The main inspection is to assess condition of the physical protection system, assess the training and qualification program of the physical protection team members, and evaluate the plans and procedures. The inspection focus on check of the persons and vehicle entries individual areas, check of the guarded, protected, and inner area barriers, check of the detection element, check of the AKOBOJE control center, check of the performance of the examination and maintenance. In case of employees qualification evaluation, the inspection focus on verify that employee have training: sufficient knowledge and skill. In case of evaluate the system, the inspection focus on effectiveness and functional of the AKOBOJE system by simulation of an incident and the inspection paid attention in functionality check of AKOBOJE system in service, vigilance check of the AKOBOJE control room staff, check of connection and effective communication, and check of response management system.

Based on the inspection performed up to date, it can be satisfactorily stated that the automated security system AKOBOJE installed in the nuclear facilities in Slovakia is fully functional and reliable and it complies with even highest requirements imposed upon the systems of this type in the develop countries.

Hosik Yoo, Jeong-Ho Lee. (2015). Results of nuclear security culture survey on personnel at nuclear power plants. Journals Annals of Nuclear Energy, Volume 85, November 2015, pp. 398-402.

Hosik Yoo and Jeong-Ho Lee have surveyed to evaluate awareness of the nuclear security culture of personnel at nuclear facilities. The survey was done by using the developed questionnaires. The questionnaires were divided into four categories, beliefs and attitude, operating systems, leadership behaviors and staff behaviors. The category on beliefs and attitude was composed of questions that asked plant workers on how much consideration facility personnel give to issues of security when doing his/her work. The section pertaining to operating systems for nuclear security consisted of questions on guidance documents, information security, and education and training. The questions on leadership behaviors were separated into two parts, one for managers and another for staff. These include questions relating to communication between management and staff, surveillance work related to nuclear security and the sharing of information. The last category of questions concerned staff behaviors. It consisted of questions on knowledge, procedures and implementation related to nuclear security. 858 people who work at nuclear power plants in the area of nuclear security were surveyed. Answers to the questions were divided into five categories (strongly disagree, disagree, neutral, agree, strongly agree). The result showed that there was a significant relationship between age and the security awareness score. The awareness score increased with age until employees entered their 50s. In their 60s employees showed lower awareness scores when compared to someone in their 50s. Groups in their 20s and 30s showed quite lower scores, especially in the category of beliefs and attitude.

M.C. Echeta; L.A. Dim; O.D. Oyeyinka; and A.O. Kuye. (2014). PPS Evaluation of An Oil Refinery Using EASI Model. Journals of Physical Security, Vol.7(2), pp.30-41.

M.C. Echeta L.A. Dim, O.D. Oyeyinka, and A.O. Kuye 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. To use EASI in this work, they followed 2 steps: step 1,

collection of critical Asset (Target) and Site Assessment information and step 2, design possible adversary paths and action sequences. Critical Asset (Target) and Site Assessment information is about the target, which is an oil refinery, the plant layout of the oil refinery with its most likely adversary paths, the detail of physical security of oil refinery such as what type of gate, or fence, or wall, or pipeline. Possible adversary paths and action sequences is the most likely adversary paths to the critical asset. Three possible adversary action sequences were developed to evaluate the PPS of oil refinery. All obtained information was put in EASI model. Results obtained from the analysis of the most likely adversary paths showed that the values of probability of interrupting the adversaries (P_I) were very low. But by upgrading the physical security systems with certain measures and equipment, the values of P_I increased significantly, improving security.

CHAPTER 3
METHODOLOGY

The methodology of this research has 3 steps as follows:

3.1 Establish the checklist

3.1.1 Collect information that is related to physical protection system.

3.1.2 Study and analyze laws and regulations of Thailand and standard recommendation from the Nuclear Security Series guidelines set by the International Atomic Energy Agency (IAEA), the United States Nuclear Regulatory Commission (US NRC), the National Nuclear Security Administration (NNSA), the Center of International Trade and Security (CITS), or World Institute for Nuclear Security (WINS).

3.1.3 Create a checklist (Appendix A) as a guideline for inspection based on the IAEA minimum standard requirements [4, 11]. The checklist consisted of three parts as follows:

Part I: General information about facility including name, address, radiation safety officer name, email, and telephone number.

Part II: Radioactive material information about type, total activity, serial number, date of calibration, manufacturer.

Part III: Physical protection system information which consists of six security elements: access control, detection, delay, response, security management, and security culture. To create the checklist in this part, one should:

- Determine security element. Six security elements which are access control, detection, delay, response, security management and security culture.
- Determine the security objective and security measure of each security element as shown in table 3.2.
- Determine the questionnaire and scoring criteria for the security element to evaluate whether these objectives are properly fulfilled.
- Determine inspection guidance for each security element.

An example of created checklist in access control element as shown in table 3.1.

Table 3.1 An example of created checklist in access control element.

Security element	Questionnaire	Inspection guidance
<u>Access</u> Provide access controls to source location that effectively restrict access to authorized persons only <u>*Measures*</u>: Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control. (A combination of two or more verification measures should be required, e.g. the use of a swipe card and a PIN; or the use of a swipe card and a controlled key; or a PIN and a	1. There is restricting access to security area, which are source location or operation area for only authorized persons 2= Has restricting access measure for only authorized persons 1= Has restricting access measure but not only authorized persons 0= No measure for restricting access to source location or secure area	Inspect to verify that there is real existing measure or equipment and functional and inspect by interview operator personnel that who can access to security area and how. And inspect the measure or functional of equipment by ask operator personnel access to security area or source location then observe
	2. There are 2 verification measures for access to security area or source location 2= Has 2 verification measures e.g. swipe card and PIN; or controlled key and visual verification of identity by other authorized personnel 1= Has only one verification measures e.g. swipe card; or controlled key; authorized personnel 0= No verification measure	
	3. Those measures/equipment can identify and verify person correctly and reject entry if input false identities or cannot identify and verify person 2= measures/equipment can identify and verify all person correctly and reject all entry if input false identities or cannot identify and verify person 1= measures/equipment can identify and verify some person correctly and reject all entry if input false identities or cannot identify and verify person 0= measures/equipment cannot identify and verify person and cannot reject all reject all entry if input false identities or cannot identify and verify person	

Table 3.1 An example of created checklist in access control element (continued).

Security element	Questionnaire	Inspection guidance
computer keypad; or the use of a controlled key and visual verification of identity by other authorized personnel)	4. If there is unauthorized person access to security area or source location, they are escorted and are under constant surveillance by authorized person (in case of medical exposure or mobile source) 2= All time unauthorized persons are escorted and are under constant surveillance by authorized person 1= Sometime unauthorized persons are escorted and are under constant surveillance by authorized person or unauthorized persons are escorted but are not under constant surveillance by authorized person 0= No escorted unauthorized persons and no constant surveillance	

Table 3.2 Minimum requirements of physical protection system for Categories 1 and 2 radioactive materials [4, 11].

Security element	Objective	Security measure
Access control	Provide access controls to source location that effectively restrict access to authorized persons only	Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control.
Detection	Provide immediate detection of any unauthorized access to the secured area/source location.	Electronic intrusion detection system and/or continuous surveillance by operator personnel.
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider.	Electronic tamper detection equipment and/ or continuous surveillance by operator personnel.

Table 3.2 Minimum requirements of physical protection system for Categories 1 and 2 radioactive materials [4, 11] (continued).

Security element	Objective	Security measure
	Provide immediate assessment of detection.	Remote monitoring of CCTV or assessment by operator / response personnel.
	Provide immediate communication to response personnel.	Rapid, dependable, diverse means of communication such as phones, cell phones, pagers, radios.
	Provide a means to detect loss through verification.	Daily checking through physical checks, CCTV, tamper indicating devices, etc.
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal.	System of at least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal.	Capability for immediate response with size, equipment, and training to interdict.
Security management	Provide access controls to source location that effectively restrict access to authorized persons only.	Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control.
	Ensure trustworthiness of authorized individuals.	Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.
	Identify and protect sensitive information.	Procedures to identify sensitive information and protect it from unauthorized disclosure

Table 3.2 Minimum requirements of physical protection system for Categories 1 and 2 radioactive materials [4, 11] (continued).

Security element	Objective	Security measure
	Provide a security plan.	A security plan which conforms to regulatory requirements and provides for response to increased threat levels.
	Ensure a capability to manage security events covered by security contingency plans.	Procedures for responding to security-related scenarios.
	Establish security event reporting system.	Procedures for timely reporting of security events.
Security culture	There is established nuclear security policy for organization	
	There are written documents related to guidelines or procedures for nuclear security that workers can easily follow	
	Personnel is aware of follow the procedure and know their responsibility	
	There are training course security-related in order to improvement of professional	

3.2 Test the checklist at facilities.

The checklist was test in 2 parts: first, test in security area during day time in all samples study and second, test in security area during night time in all samples study. The checklist was completed during the inspection process which included inspection by review documents; inspection by interview radiation safety officer (RSO) and front guards; inspection by test the performance of equipment; and inspection by observation.

Two sample facilities, which already have the physical protection system installed through the support of the United States Department of Energy (U.S. DOE), are chosen as the test subject for the checklist.

These two facilities, which hereinafter shall be called Facilities A and B, possess Categories 1 and 2 radioactive materials. Facility A possesses Categories 1 and 2 radioactive materials in use or shall be called “Asset 1 and Asset 2”; and Facility B

possesses Categories 1 and 2 radioactive materials in use or shall be called “Asset 3 and Asset 4”, and Category 2 radioactive materials in storage or shall be called “Asset 5.” Asset 1- 5 is the target for adversary. In total, five samples have been studied. The checklist was tested in two security area, security area during day time and security area during night time. The PPS at security area should be able to perform 3 functions: detection, delay, and response. The PPS for our five samples are shown in follows:

Asset 1: The sensors and monitoring include one balance magnetic switch (BMS) on the source location door and the control room door, one tamper switch on the target. 3 motion sensors inside the source used room, one motion sensor inside the control room, one CCTV in conjunction with operating personnel for monitoring in front of security area, 2 CCTV in conjunction with operating personnel for monitoring inside the source used room. For access control, one fingerprint with keypad is in front of the security area and control room. Only authorized personnel can go inside the security area. The system has 2 high security padlocks on the source location door and one high security padlocks on the control room door. If a sensor detects an adversary, the guard will be able to arrive in 120 seconds. The PPS of Asset 1 is shown in Figure 3.1.

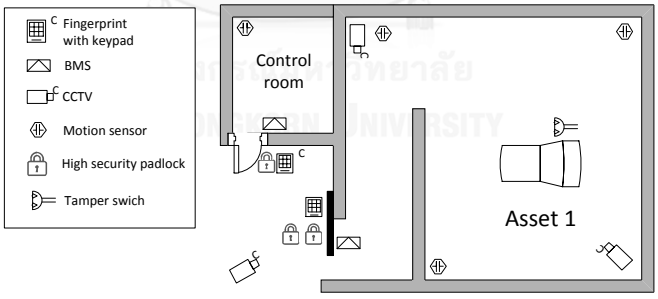


Figure 3.1 The layout of the security area and the PPS of Asset 1.

Asset 2: The sensors and monitoring include one balance magnetic switch (BMS) on the source location door, one tamper switch on the target, 3 motion sensors inside the source used room. For access control, one fingerprint with keypad in front of the security area. Only authorized personnel can go inside the security area. The system has 2 high security padlocks on the source location door and 2 high

security padlocks on the source device. If a sensor detects an adversary, the guard will be able to arrive in 120 seconds. The PPS of Asset 2 is shown in Figure 3.2.

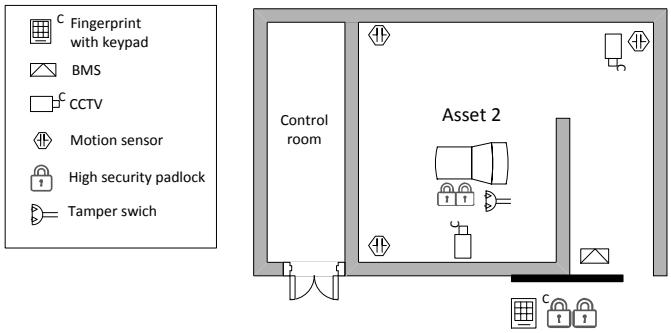


Figure 3.2 The layout of the security area and the PPS of Asset 2.

Asset 3: The sensors and monitoring include one balance magnetic switch (BMS) on the source location door and the control room door, one tamper switch on the target. 2 motion sensors inside the source used room, one CCTV in conjunction with operating personnel and front guard for monitoring in front of security area, one CCTV in conjunction with operating personnel for monitoring inside the source used room. For access control, one fingerprint with keypad in front of the security area. Only authorized personnel can go inside the security area. The system has 2 high security padlocks on the source location door and one high security padlocks on the control room door. If a sensor detects an adversary, the guard will be able to arrive in 120 seconds. The PPS of Asset 3 is shown in Figure 3.3.

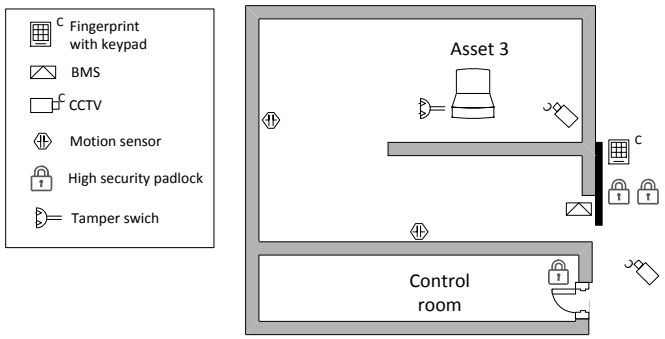


Figure 3.3 The layout of the security area and the PPS of Asset 3.

Asset 4: The sensors and monitoring include one balance magnetic switch (BMS) on the source location door and the control room door, one tamper switch on the target, 2 motion sensors inside the source used room, one motion sensor inside the control room, one CCTV in conjunction with operating personnel for monitoring in front of security area, inside source used room, and inside the control room. For access control, one fingerprint with keypad in front of the security area and in front of the control room. Only authorized personnel can go inside the security area. The system has 2 high security padlocks on the source location door and on the source device, one high security padlocks on the control room door. If a sensor detects an adversary, the guard will be able to arrive in 120 seconds. The PPS of Asset 4 is shown in Figure 3.4.

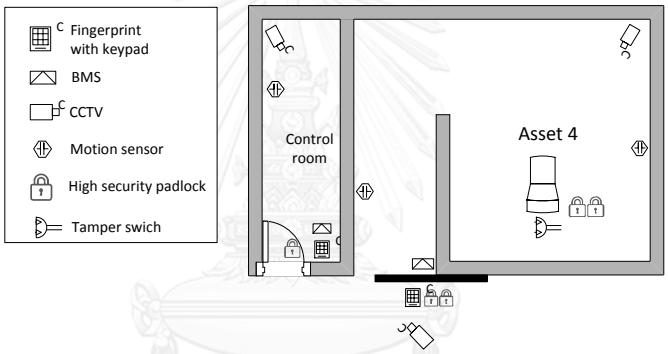


Figure 3.4 The layout of the security area and the PPS of Asset 4.

Asset 5: The sensors and monitoring include one balance magnetic switch (BMS) on the source location door and the control room door, one tamper switch on the target, 2 motion sensors inside the source storage room, one CCTV in conjunction with operating personnel for monitoring in front of the security area, 2 CCTV in conjunction with operating personnel for monitoring inside the source storage room. For access control, one fingerprint with keypad in front of the security area and the control room. Only authorized personnel can go inside the security area. The system has 2 high security padlocks on the source location door and on the source device. If a sensor detects an adversary, the guard will be able to arrive in 120 seconds. The PPS of Asset 5 is shown in Figure 3.5.

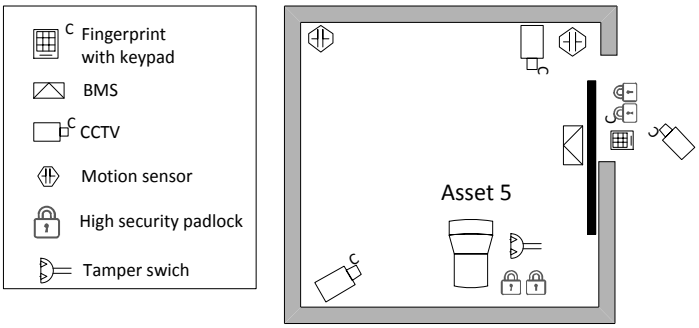


Figure 3.5 The layout of the security area and the PPS of Asset 5.

3.3 Compare the checklist result against the result from the Estimation of Adversary Sequence Interruption (EASI) Model.

The obtained checklist results have been compared against the results from the EASI model. In order to the checklist result is in term of score but the EASI is in term of probability. The comparison cannot do directly. However, the comparison can be done by two parts. First is comparison of effectiveness of each security elements, which are detection, delay and response. Because the EASI model use detection, delay, response to compute the probability of interruption [3], while the access control, security management and security culture elements are assumed to be 100% effective, i.e. EASI model does not take them into consideration. Second is comparison of the correlation between overall effectiveness score (multiplication of detection, delay and response) from the checklist result and the probability of interruption (P_I) from the EASI result. The potential scenarios should be assumed to use in EASI and to find limitations of the checklist.

The potential scenarios used in the EASI model.

Using adversary path and the EASI model, potential scenarios can be evaluated against the existing PPS and can be found the limitation of checklist. Three scenarios have been assumed with 2 adversary's goal, sabotage and theft and focus on two action of intruder, hitting door and cutting door. Cutting door with cutting torch.

Hitting door with sledgehammer. Sabotage by using 2 kilograms of explosives. Three assumed scenarios are shown as follows:

(1) Intruder hits the door and sabotages target

(2) Intruder cuts through the door and sabotages target.

(3) Intruder cuts through the door and steals target.

These 3 scenarios were applied into Asset 1, 2, 3, 4, and 5 and applied in both security areas during day time and night time. The adversary path of each scenario is shown in Figure 3.6.

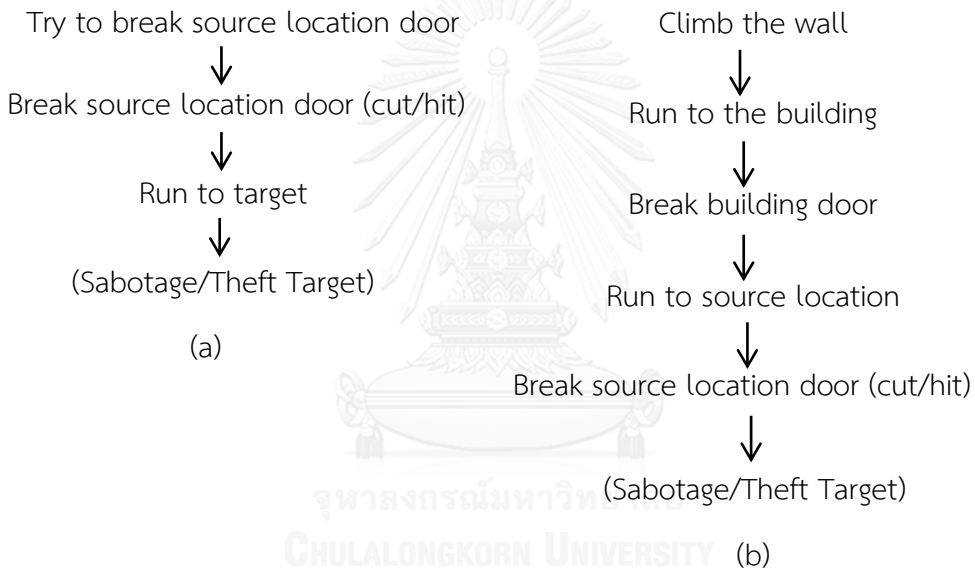


Figure 3.6 Adversary paths for sabotage and theft aimed in action of cutting and hitting door, (a) During day time, (b) During night time

In this research, there are 2 types of results. First, the checklist result from the inspection survey; and second, the calculation result using the EASI model. In each result consists of 2 parts: the result of physical protection system in the security area during day time of Asset 1-5, and second, the result of physical protection system in the security area during night time of Asset 1-5. The 2 types of results are compared. The summary result obtained in this research is shown in Table 3.3.

Table 3.3 The obtained result in the research.

	Result of Physical Protection System Effectiveness Based on the Checklist and the EASI model	
	Checklist result	EASI result
Security area during day time	Asset 1-5	(1) Intruder hits the door and sabotages target of Asset 1-5. (2) Intruder cuts through the door and sabotages target of Asset 1-5. (3) Intruder cuts through the door and steals target of Asset 1-5.
Security area during night time	Asset 1-5	(1) Intruder hits the door and sabotages target of Asset 1-5. (2) Intruder cuts through the door and sabotages target of Asset 1-5. (3) Intruder cuts through the door and steals target of Asset 1-5.

CHAPTER 4
RESULTS AND DISCUSSIONS

In this chapter, there are 4 sections are shown follows:

(1) Result of Physical Protection System Effectiveness Based on the Checklist in security area during day time and night time.

(2) Result of Physical Protection System Effectiveness Based on the EASI model in security area during day time and night time.

(3) Comparison and discussion of checklist result to EASI result in security area during day time and night time.

(4) Improving the PPS using EASI model.

4.1 Result of Physical Protection System Effectiveness Based on the Checklist.

The checklist result has 2 parts: result of security area during day time and night time. The security areas of investigation at day time are the source storage room or the source use room. The results from checklist are shown in Table 4.1. The security area of investigation at night time is the building that the source is located. The results from checklist are shown in Table 4.2.

4.1.1 Result of Physical Protection System Effectiveness in security area during day time.

Table 4.1 The scoring result of each security element and the overall effectiveness score of the system of all assets during day time.

Security element	Asset 1	Asset 2	Asset 3	Asset 4	Asset 5
Access control	1.00	1.00	1.00	1.00	1.00
Detection	0.96	0.96	0.96	0.96	0.96
Delay	1.00	1.00	1.00	1.00	1.00
Response	0.72	0.72	0.79	0.79	0.79
Security management	0.58	0.58	0.58	0.58	0.58
Security culture	0.63	0.63	0.62	0.62	0.62
Overall effectiveness of the system	0.25	0.25	0.27	0.27	0.27

4.1.2 Result of Physical Protection System Effectiveness in security area during night time.

Table 4.2 The scoring result of each security element and the overall effectiveness score of the system of all assets during night time.

Security element	Asset 1	Asset 2	Asset 3	Asset 4	Asset 5
Access control	1.00	1.00	1.00	1.00	1.00
Detection	0.96	0.96	0.96	0.96	0.96
Delay	1.00	1.00	1.00	1.00	1.00
Response	0.72	0.72	0.79	0.79	0.79
Security management	0.58	0.58	0.58	0.58	0.58
Security culture	0.63	0.63	0.62	0.62	0.62
Overall effectiveness of the system	0.25	0.25	0.27	0.27	0.27

The results for each security element and the overall effectiveness score of the system of all assets during day time and night time are similar. The scoring result are obtained by using equation 2.3. The result has 2 acceptant levels. First, acceptant level score at 0.7 or 70% for each security level. Second, acceptant level score at 0.12 for overall effectiveness of the system. The results show that

- All assets receive a score of 0.96 for their detection system, which is acceptable. During day time, all asset use balance magnetic switch (BMS) linked to an alarm as a detection. Detection and assessment of the cause of an alarm through CCTV and communication to response are performed by operator personnel. During night time, all assets use continuous surveillance personnel as first detection and BMS as second detection but assessment and communication are performed by surveillance personnel. It is found that the detection comply with regulatory requirement and minimum standard requirement, which means that the systems meet the security objective to provide immediate detection of unauthorized access/removal, immediate assessment of detection and immediate communication to response personnel. Therefore, the detection systems at all assets are effective and acceptable during day time and night time.

- All assets also receive a score of 1.00 for their delay system, which is acceptable. During day time, after detection, all asset use source location door as first delay and the source holder or locked device as second delay, which means that the systems meet the security objective to provide at least 2 delay layers after detection for the response personnel to interrupt unauthorized removal attempt. The detection at this point can be performed through CCTV monitored by operator personnel. For Asset 2, there is no CCTV in front of security area but the detection at this point can be performed by operator personnel at source location. During night time, all assets have several delay layers. Because the security area during night time is bigger than during day time. The detection at this point can be performed by surveillance personnel patrolling around the source building. Therefore, the delay systems at all assets are effective and acceptable during day time and night time.

- For the response system, receive a score of 0.72 while Assets 3, 4, and 5 receive 0.79, which is acceptable. Because Assets 1 and 2 are in facility A, and Asset 3, 4, and 5 are in facility B, the response personnel in Asset 1 and 2 is the response system in facility A. The response personnel in Asset 3, 4, and 5 is the response system in facility B. The Response personnel A and B are performed by guard. During day time, all assets have at least one response personnel per allocation area. During night time, all assets have 2 response personnel patrol around the source building. All response personnel in all assets have baton and radio communication. There is no exercise or procedure in nuclear security-related but they knows how to action if event occur. The different between response personnel in facility A and B is all response personnel in facility B have trained in the responding to event, while some of response personnel in facility B have trained. However, the response system in facility A and B meet the security objective to provide immediate response to assessed alarm with sufficient resources to interrupt and prevent unauthorized removal attempt. Therefore, the response systems at all assets are effective and acceptable during day time and night time.

- All assets receive a score of 1.00 for their access control system, which is acceptable. During day time, all assets use fingerprint with password for restrict

accessing to security area. Accessing to security area, operator personnel need to put personnel Identification Number (PIN) or swipe card and biometric measure such as fingerprint. This is 2 verification measures. During night time, all assets use visual surveillance personnel for restrict access and the source building was locked. To access to security area, the person need to have key and badge to verifying. Thus, the access systems meet the security objective to provide access control to source location that effectively restricts access to only authorized persons. Therefore, the access control systems at all assets are effective and acceptable.

- All assets also receive a core of 0.58 for their security management system. The low number reveals that the existing system does not meet the security objective. The procedures, policies, records, and plan for securing the source and for sensitive information appear to be lacking. Therefore, the security management systems at all assets are ineffective and unacceptable.

- For the security culture system, Assets 1 and 2 receive a score of 0.62, while Assets 3, 4, and 5 receive 0.63. The security culture system of all assets do not meet the security objective which requires that all personnel are aware of security-related system, follow the procedure, and know their responsibility. Therefore, the security culture systems at all assets are ineffective and unacceptable.

The overall effectiveness of the system based on Equation 4.1 is 0.25 for Asset 1, 0.25 for Asset 2, 0.27 for Asset 3, 0.27 for Asset 4, and 0.27 for Asset 5. Therefore the overall effectiveness of the systems at all assets is acceptable.

Even though there are some unacceptable security elements, the overall effectiveness score of the system for all assets are still acceptable. Thus, the physical protection systems at all assets are effective.

4.2 Results of the Calculation of Physical Protection System Effectiveness of All Assets Based on EASI model

The EASI result has 2 parts. First is result of physical protection system effectiveness in security area during day time. Second is result of physical protection system effectiveness in security area during night time.

For all assets, the EASI model has been applied three scenarios to each asset: (1) intruder hits door and sabotage target, (2) intruder cuts door and sabotage target, and (3) intruder cuts door and steals the target. Cutting door is performed using torch, while hitting door is performed with sledgehammer.

4.2.1 Result of Physical Protection System Effectiveness in security area during day time.

4.2.1.1 Result for Asset 1.

The EASI model results for three scenarios (hitting the door and sabotage, cutting through the door and sabotage, and cutting through the door and steal) are shown in Tables 4.3, 4.4, and 4.5 respectively.

Table 4.3 Probability of Interruption (P_I) of Asset 1 in the security area during day time in case that the intruder hits the door and sabotages the target.

		Probability of Interruption:			0.86
Estimate of Adversary Sequence Interruption		Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0.8	E	800	240.0
3	Run to target	0.9	E	2.3	0.7
4	Sabotage target	0.9	E	40	12.0

Table 4.4 Probability of Interruption (P_I) of Asset 1 in the security area during day time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:			0.45
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Run to target	0.9	E	2.3	0.7
4	Sabotage target	0.9	E	40	12.0

Table 4.5 Probability of Interruption (P_I) of Asset 1 in the security area during day time in case that the intruder cuts through the door and steals the target.

	Probability of Interruption:			0.97
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0

Table 4.5 Probability of Interruption (P_I) of Asset 1 in the security area during day time in case that the intruder cuts through the door and steals the target (continued).

	Probability of Interruption:			0.97
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Run to target	0.9	E	2.3	0.7
4	Steals the target	0.9	E	300	90.0

In Table 4.3, when the intruder penetrates to source location by hitting the door, the probability of interruption (P_I) is 0.86 which is rated high-very high. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. The intruder takes more time to break the source location door (800 seconds) than the security response time (120 seconds). Thus, the response personnel can interrupt the intrusion in time. The time it takes to break in by hitting the door depends on the equipment's that the intruder uses, which is based on the threat evaluation result.

In Table 4.4, the intruder will likely succeed the goal of penetrating to the source location by cutting through door and sabotaging the target because P_I = 0.45, which is low. The response force is unlikely to be able to interrupt the intruder. The intruder may take on average 122.3 seconds to complete the task, while the response needs 120 seconds. The physical protection system of Asset 1 is not effective in this case. In addition, the balanced magnetic switch (BMS) on the door would not trigger because the door was not opened, but rather cut. From the

calculation, cutting through the door should be the case to concern in the security area during day time.

In Table 4.5, there are 2 delay layers after detection. It would take the thief 300 seconds to remove the target from the holder, allowing sufficient time for the response force to take action. The P_I is 0.97; the PPS of Asset 1 is therefore effective against theft.

4.2.1.2 Result for Asset 2.

The EASI model results for three scenarios (hitting the door and sabotage, cutting through the door and sabotage, and cutting through the door and theft) are shown in Tables 4.6, 4.7, and 4.8 respectively.

Table 4.6 Probability of Interruption (PI) of Asset 2 in the security area during day time in case that the intruder hits the door and sabotages the target.

		Probability of Interruption:			0.20
Estimate of Adversary Sequence Interruption		Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.2	E	0	0.0
2	Break source location door	0.8	E	800	240.0
3	Run to target	0.9	E	1.53	0.5
4	Sabotage target	0.9	E	40	12.0

Table 4.7 Probability of Interruption (P_I) of asset 2 in security area during day time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:			0.11
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.2	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Run to target	0.9	E	1.53	0.5
4	Sabotage target	0.9	E	40	12.0

Table 4.8 Probability of Interruption (P_I) of asset 2 in security area during day time in case that the intruder cuts through the door and steals the target.

	Probability of Interruption:			0.76
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.2	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Run to target	0.9	E	1.53	0.5

Table 4.8 Probability of Interruption (P_I) of asset 2 in security area during day time in case that the intruder cuts through the door and steals the target (continued).

		Probability of Interruption:			0.76
Estimate of Adversary Sequence Interruption		Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
4	Steals the target	0.9	E	180	54.0

In Table 4.6, it is found that if an intruder penetrates to the source location by hitting the door, the success rate will be high because the P_I = 0.20. Even though the response time is 120 seconds, which is much less than time to break source location door (800 seconds), the probability of detection while trying to break the door is merely 0.2. This affects to the capability of detection, assessment and communication to response personnel. When the detection system cannot detect early, the delay mechanism before the detection happens does not have any effect on the intruder. Late detection results in late assessment and communication to response personnel late.

In Table 4.7, in case a intruder cuts through the door and sabotages the target, it is found that the P_I is 0.11, which is less than in the case of intruder hitting the door. This low probability is also because the low probability of detection at the first delay layer (P_D = 0.2). From the calculation, cutting through the door should be the case to concern in the security area during day time.

In Table 4.8, in case a intruder cuts through the door and theft the target shows that there are 2 delay layers after the first detection point: the source location door and the locked source holding device with 2 high security padlocks. From the result, PI is 0.77, meaning that the response personnel has high probability of arriving

and interrupting intruder in time. Thus, the PPS of Asset 2 is effective in case of intruder cutting through the door and steals the target.

From all EASI results of Asset 2, it is found that there is a weak point in the PPS. It is system has low probability of detection (P_D = 0.2). Asset 2 does not have CCTV in front of the security area. Even though the system has a balanced magnetic switch (BMS) or an operating personnel for detection, the BMS would be bypassed if the intruder cutting through the door.

The score of delay and detection elements in the checklist for Asset 2 are 1.00 and 0.96 respectively. The number indicates that the detection system in the facility is in compliance with the regulatory requirement, which requires immediate detection of unauthorized access or removal, immediate assessment of detection, and immediate communication to response personnel. However, the detection element in asset 2 is a BMS and the operating personnel, and the BMS can be bypassed in the case of intruder cutting through the door. In such case, the operating personnel at the source location would solely serve as the detection element. Even though the operating personnel at the source location is working continuously, the probability of detection is low because of the human factor. This would decrease the overall effectiveness of the system as shown earlier in the EASI result.

There is another detection element which is the motion sensor within the operating room, which is used in case that the operating personnel and the BMS are not active. Although the motion sensor serves as a detector, the location that it is installed is after the delay layer. Thus, the detection would be too late from the timely response point-of-view. It is clear that this is one of the limitations of the checklist and the current requirement.

The delay objective from the regulatory requirement is that the system must have at least 2 delay layers after the detection point. However, depending on the goal of the adversary, there may be only one delay element after detection that would be effective at Asset 2. If sabotage is the goal of the intruder, i.e. no need to remove the target, the source holder would not act as effective delay layer. But if theft is the goal, the source holder can be effective. Table 4.8 shows the result for

the theft case when the intruder cuts through the door (less time for penetrate to target than hitting the door).

4.2.1.3 Result of Asset 3

The EASI model results for three scenarios (hitting the door and sabotage, cutting through the door and sabotage, and cutting through the door and theft) are shown in Tables 4.9, 4.10, and 4.11 respectively.

Table 4.9 Probability of Interruption (P_I) of asset 3 in security area during day time in case that the intruder hits the door and sabotages the target.

		Probability of Interruption:			0.86
Estimate of Adversary Sequence Interruption		Probability of Alarm Communication		Response Force Time (in Seconds)	
				Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0.8	E	800	240.0
3	Run to target	0.9	E	2.3	0.7
4	Sabotage target	0.9	E	40	12.0

Table 4.10 Probability of Interruption (P_I) of asset 3 in security area during day time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:			0.45
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Run to target	0.9	E	2.3	0.7
4	Sabotage target	0.9	E	40	12.0

Table 4.11 Probability of Interruption (P_I) of asset 3 in security area during day time in case that the intruder cuts through the door and steals the target.

	Probability of Interruption:			0.97
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Run to target	0.9	E	2.3	0.7
4	Steals the target	0.9	E	300	90.0

In Table 4.9, when the intruder penetrates to source location by hitting the door, the probability of interruption (P_I) is 0.86 which is rated high-very high. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. The intruder takes more time to break the source location door (800 seconds) than the security response time (120 seconds). Thus, the response personnel can interrupt the intrusion in time. The time it takes to break in by hitting the door depends on the equipment's that the intruder uses, which is based on the threat evaluation result.

In Table 4.10, in case a intruder cuts through the door and sabotages the target, it is found that the P_I is 0.45, which is less than in the case of intruder hitting the door. From the calculation, cutting through the door should be the case to concern in the security area during day time.

In Table 4.11, in case an intruder cuts through the door and steal the target, there are 2 delay layers after detection. It would take the thief 300 seconds to remove the target from the holder, allowing sufficient time for the response force to take action. The P_I is 0.97; the PPS of Asset 3 is therefore effective against theft.

4.2.1.4 Result of Asset 4

The EASI model results for three scenarios (hitting the door and sabotage, cutting through the door and sabotage, and cutting through the door and theft) are shown in Tables 4.12, 4.13, and 4.14 respectively.

Table 4.12 Probability of Interruption (P_I) of asset 4 in security area during day time in case that the intruder hits the door and sabotages the target.

	Probability of Interruption:		0.86	
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0.8	E	800	240.0
3	Run to target	0.9	E	1.02	0.3
4	Sabotage target	0.9	E	40	12.0

Table 4.13 Probability of Interruption (P_I) of asset 4 in security area during day time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:		0.44	
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Run to target	0.9	E	1.02	0.3

Table 4.13 Probability of Interruption (P_I) of asset 4 in security area during day time in case that the intruder cuts through the door and sabotages the target (continued).

		Probability of Interruption:			0.44
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
4	Sabotage target	0.9	E	40	12.0

Table 4.14 Probability of Interruption (P_I) of asset 4 in security area during day time in case that the intruder cuts through the door and steals the target.

		Probability of Interruption:			0.94
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Run to target	0.9	E	1.02	0.3
4	Steals the target	0.9	E	180	54.0

In Table 4.12, in case of intruder penetrates to source location by hitting the door and sabotaging, the probability of interruption (P_I) is 0.86 which is rated high-very high. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. The intruder takes more time to break the source location door (800 seconds) than the security response time (120 seconds). Thus, the response personnel can interrupt the intrusion in time.

In Table 4.13, in case of intruder penetrates to source location by cutting the door and sabotaging, the probability of interruption (P_I) is 0.44, which is less than in the case of intruder hitting the door. The chance of response personnel is low to be able to interrupt the intruder. From the calculation, cutting through the door should be the case to concern in the security area during day time.

In Table 4.14, in case of intruder penetrates to source location by cutting the door and stealing, the probability of interruption (P_I) is 0.94. There are 2 delay layers after detection, allowing sufficient time for the response force to take action. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. The intruder may take on average 261 seconds to complete the task, while the response needs 120 seconds. The intruder takes more time to stealing. Thus, the PPS of Asset 4 is effective in case of intruder cutting through the door and steals the target.

4.2.1.5 Result of Asset 5

The EASI model results for three scenarios (hitting the door and sabotage, cutting through the door and sabotage, and cutting through the door and theft) are shown in Tables 4.15, 4.16, and 4.17 respectively.

Table 4.15 Probability of Interruption (P_I) of asset 5 in security area during day time in case that the intruder hits the door and sabotages the target.

	Probability of Interruption:			0.86
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0.8	E	800	240.0
3	Run to target	0.9	E	1.02	0.3
4	Sabotage target	0.9	E	40	12.0

Table 4.16 Probability of Interruption (P_I) of asset 5 in security area during day time in case that the intruder cuts through the door and sabotage the target.

	Probability of Interruption:			0.44
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0

Table 4.16 Probability of Interruption (P_I) of asset 5 in security area during day time in case that the intruder cuts through the door and sabotage the target (continued).

	Probability of Interruption:		0.44	
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Run to target	0.9	E	1.02	0.3
4	Sabotage target	0.9	E	40	12.0

Table 4.17 Probability of Interruption (P_I) of asset 5 in security area during day time in case that the intruder cuts through the door and steals the target.

	Probability of Interruption:		0.94	
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Run to target	0.9	E	1.02	0.3
4	Steals the target	0.9	E	180	54.0

In Table 4.15, in case of intruder penetrates to source location by hitting the door and sabotaging, the probability of interruption (P_I) is 0.86 which is rated high-very high. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. The intruder takes more time to break the source location door (800 seconds) than the security response time (120 seconds). Thus, the response personnel can interrupt the intrusion in time.

In Table 4.16, in case of intruder penetrates to source location by cutting the door and sabotaging, the probability of interruption (P_I) is 0.44, which is less than in the case of intruder hitting the door. The chance of response personnel is low to be able to interrupt the intruder. From the calculation, cutting through the door should be the case to concern in the security area during day time.

In Table 4.17, in case of intruder penetrates to source location by cutting the door and stealing, the probability of interruption (P_I) is 0.94. There are 2 delay layers after detection, allowing sufficient time for the response force to take action. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. The intruder may take on average 261 seconds to complete the task (180 seconds for remove the target from the 2 high security padlocks), while the response needs 120 seconds. The intruder takes more time to stealing. Thus, the PPS of Asset 5 is effective in case of intruder cutting through the door and steals the target.

4.2.2 Result of Physical Protection System Effectiveness in security area during night time.

The checklist result has 2 parts: result of security area during day time and night time. The security areas of investigation at day time are the source storage room or the source use room. The results from checklist are shown in Table 4.1. The security area of investigation at night time is the building that the source is located. The results from checklist are shown in Table 4.2.

4.2.2.1 Result for Asset 1

The EASI model results for three scenarios (hitting the door and sabotage, cutting through the door and sabotage, and cutting through the door and steal) are shown in Tables 4.18, 4.19, and 4.20 respectively.

Table 4.18 Probability of Interruption (P_I) of asset 1 in security area during night time in case that the intruder hits the door and sabotages the target.

		Probability of Interruption:			0.36
Estimate of Adversary Sequence Interruption		Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	51.11	15.3
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	5.11	1.5
5	Break source location door	0.8	E	800	348.0
6	Run to target	0.9	E	2.3	0.7
7	Sabotage target	0.9	E	40	12.0

Table 4.19 Probability of Interruption (P_I) of asset 1 in security area during night time in case that the intruder cuts through the door and sabotage the target.

	Probability of Interruption:		0.27	
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	51.11	15.3
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	5.11	1.5
5	Break source location door	0	E	80	24.0
6	Run to target	0.9	E	2.3	0.7
7	Sabotage target	0.9	E	40	12.0

Table 4.20 Probability of Interruption (P_I) of asset 1 in security area during night time in case that the intruder cuts through the door and steals the target.

	Probability of Interruption:		0.89	
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	51.11	15.3

Table 4.20 Probability of Interruption (P_I) of asset 1 in security area during night time in case that the intruder cuts through the door and steals the target (continued).

	Probability of Interruption:			0.89
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	5.11	1.5
5	Break source location door	0	E	80	24.0
6	Run to target	0.9	E	2.3	0.7
7	Steals the target	0.9	E	300	90.0

In Table 4.18, in case of intruder penetrates to source location by hitting the door and sabotaging, the probability of interruption (P_I) is 0.37 which is rated low-medium. The response force is unlikely to be able to interrupt the intruder. Even though the BMS is triggered due to the door was opened and even there is immediate communication to response personnel, but the time to achieve the goal (sabotage) after alarm triggered is 42.3 seconds, which is less than response time (120 seconds). And even though an intruder takes more time to break the source location door (800 seconds) than the security response time (120 seconds), but the first detection is surveillance personnel which has low probability of detection. The detection may be bypassed. The intruder can achieve the task. From the calculation, hitting the door should be the case to concern in the security area during night time.

In Table 4.19, in case of intruder penetrates to source location by cutting the door and sabotaging, the probability of interruption (P_I) is 0.27, which is less than in

the case of intruder hitting the door. Because of the time used for cutting door is 80 seconds, less than hitting door (800 seconds) and also the BMS would be bypassed if the intruder cutting through the door. The trigger alarm and communication to response personnel would be bypassed as well. Delay time was performed by running to target and time for set up explosive (42.3 seconds), while a response personnel needs 120 seconds. The chance of response personnel is low to be able to interrupt the intruder. From the calculation, cutting through the door should be the case to concern in the security area during night time.

In Table 4.20, in case of intruder penetrates to source location by cutting the door and stealing, the probability of interruption (P_I) is 0.89. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. This case is similar to the case of intruder cutting the door, but different goal, which is theft. Even though the probability of detection is low (P_D = 0.2) but the intruder takes more time to remove the target from the holder (300 seconds), allowing sufficient time for the response force to take action. Thus, the PPS of Asset 1 is effective in case of intruder cutting through the door and steals the target.

In addition, Asset 1 uses CCTV in conjunction with operating personnel for continuous monitoring but only during day time. During night time, there is no operator personnel for monitoring.

4.2.2.2 Result for Asset 2

The EASI model results for three scenarios (hitting the door and sabotage, cutting through the door and sabotage, and cutting through the door and steal) are shown in Tables 4.21, 4.22, and 4.23 respectively.

Table 4.21 Probability of Interruption (P_I) of asset 2 in security area during night time in case that the intruder hits the door and sabotages the target.

	Probability of Interruption:		0.36	
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	23.0
2	Run to building	0.2	E	76.67	0.8
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.28	0.4
5	Break source location door	0.8	E	800	240.0
6	Run to target	0.9	E	1.53	0.5
7	Sabotage target	0.9	E	40	12.0

Table 4.22 Probability of Interruption (P_I) of asset 2 in security area during night time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:		0.26	
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	23.0
2	Run to building	0.2	E	76.67	0.8

Table 4.22 Probability of Interruption (P_I) of asset 2 in security area during night time in case that the intruder cuts through the door and sabotages the target (continued).

		Probability of Interruption:			0.26
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.28	0.4
5	Break source location door	0	E	80	24.0
6	Run to target	0.9	E	1.53	0.5
7	Sabotage target	0.9	E	40	12.0

Table 4.23 Probability of Interruption (P_I) of asset 2 in security area during night time in case that the intruder cuts through the door and steals the target.

		Probability of Interruption:			0.80
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	23.0
2	Run to building	0.2	E	76.67	0.8
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.28	0.4

Table 4.23 Probability of Interruption (P_I) of asset 2 in security area during night time in case that the intruder cuts through the door and steals the target (continued).

		Probability of Interruption:			0.80
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
5	Break source location door	0	E	80	24.0
6	Run to target	0.9	E	1.53	0.5
7	Steals the target	0.9	E	180	54.0

In Table 4.21, in case of intruder penetrates to source location by hitting the door and sabotaging, the probability of interruption (P_I) is 0.36 which is rated low-medium. The response force is unlikely to be able to interrupt the intruder. Due to the detection at first layer has low probability of detection (P_D=0.2), an intruder would be access to source location without detected by the surveillance personnel. Even though the BMS triggered due to the door was opened and immediate communication to response personnel is performed, but the time to achieve the goal (sabotage) after alarm triggered is 41.53 seconds, which is less than response time (120 seconds). The intruder can achieve the task. The detection would be bypassed. The intruder can achieve the task. From the calculation, hitting the door should be the case to concern in the security area during night time.

In Table 4.22, in case an intruder cuts through the door and sabotages the target, it is found that the P_I is 0.26. This low probability is also because the low probability of detection at the first delay layer (P_D = 0.2). In addition, the balanced magnetic switch (BMS) on the door would not trigger because the door was not opened, but rather cut. Even though, there are several delay layers after detection,

but may not allowing sufficient time for response personnel due to low probability of detection. From the calculation, cutting through the door should be the case to concern in the security area during night time.

In Table 4.23, in case of intruder penetrates to source location by cutting the door and stealing, the probability of interruption (P_I) is 0.80. Adversary's goal is theft. Even though the probability of detection is low (P_D = 0.2) but a intruder needs time to remove the target from the 2 high security padlocks (180 seconds), allowing sufficient time for the response force to take action. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. Thus, the PPS of Asset 1 is effective in case of intruder cutting through the door and steals the target.

In addition, Asset 2 does not have CCTV in conjunction with operating personnel or front guard for continuous monitoring both during day time and night time.

4.2.2.3 Result for Asset 3

The EASI model results for three scenarios (hitting the door and sabotage, cutting through the door and sabotage, and cutting through the door and steal) are shown in Tables 4.24, 4.25, and 4.26 respectively.

Table 4.24 Probability of Interruption (P_I) of asset 3 in security area during night time in case that the intruder hits the door and sabotages the target.

		Probability of Interruption:			0.91
Estimate of Adversary Sequence Interruption		Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to door1	0.2	E	2.56	0.8

Table 4.24 Probability of Interruption (P_I) of asset 3 in security area during night time in case that the intruder hits the door and sabotages the target (continued).

	Probability of Interruption:		0.91
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Response Force Time (in Seconds) Mean	Standard Deviation
	0.95	120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.53	0.5
5	Try to break source location door	0.9	E	0	0.0
6	Break source location door	0.8	E	800	240.0
7	Run to target	0.9	E	2.3	0.7
8	Sabotage target	0.9	E	40	12.0

Table 4.25 Probability of Interruption (P_I) of asset 3 in security area during night time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:		0.55
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Response Force Time in Seconds) Mean	Standard Deviation
	0.95	120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to door1	0.2	E	2.56	0.8

Table 4.25 Probability of Interruption (P_I) of asset 3 in security area during night time in case that the intruder cuts through the door and sabotages the target (continued).

	Probability of Interruption:		0.55
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Response Force Time in Seconds) Mean	Standard Deviation
	0.95	120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.53	0.5
5	Try to break source location door	0.9	E	0	0.0
6	Break source location door	0	E	80	24.0
7	Run to target	0.9	E	2.3	0.7
8	Sabotage target	0.9	E	40	12.0

Table 4.26 Probability of Interruption (P_I) of asset 3 in security area during night time in case that the intruder cuts through the door and steals the target.

	Probability of Interruption:		0.98
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Response Force Time in Seconds) Mean	Standard Deviation
	0.95	120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6

Table 4.26 Probability of Interruption (P_I) of asset 3 in security area during night time in case that the intruder cuts through the door and steals the target (continued).

	Probability of Interruption:			0.98
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time in Seconds) Mean	Standard Deviation
	0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
2	Run to door1	0.2	E	2.56	0.8
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.53	0.5
5	Try to break source location door	0.9	E	0	0.0
6	Break source location door	0	E	80	24.0
7	Run to target	0.9	E	2.3	0.7
8	Steals the target	0.9	E	300	90.0

In Table 4.24, in case of intruder penetrates to source location by hitting the door and sabotaging, the probability of interruption (P_I) is 0.91 which is rated very high. The response force has high chance to be able to interrupt the intruder. Even though the system has low probability of detection but there is CCTV in front of source use room performed as next detection. CCTV is in conjunction with front guard for continuous monitoring, assessment, communication, and response to event (P_D=0.9). After the detection, there is enough time (842.3) for response personnel to take an action. Thus, the PPS of Asset 3 is effective this case.

In Table 4.25, in case of intruder penetrates to source location by cutting the door and sabotaging, the probability of interruption (P_I) is 0.55 which is rated medium, which is less than in the case of intruder hitting the door. Even though the system has high probability of detection from CCTV in conjunction with front guard, but a intruder use shorter time to cutting the source location door (80 seconds) than hitting door (800 seconds). Delay time was performed by breaking source location door, running to target and time for set up explosive (122.3 seconds), while response personnel needs 120 seconds. Even though the time response personnel action and intruder action were nearby, but the sabotaging is goal of adversary. The chance of response personnel is medium to be able to interrupt the intruder. From the calculation, cutting through the door should be the case to concern in the security area during night time.

In Table 4.26, in case of intruder penetrates to source location by cutting the door and stealing, the probability of interruption (P_I) is 0.98. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. Because of the system has front guard performed as immediate detection, assessment, communication, and response to the intruder. And removing the target is needed by the intruder due to theft aimed. Thus, the PPS of Asset 3 is effective in case of intruder cutting through the door and steals the target.

4.2.2.4 Result for Asset 4

The EASI model results for three scenarios (hitting the door and sabotage, cutting through the door and sabotage, and cutting through the door and steal) are shown in Tables 4.27, 4.28, and 4.29 respectively.

Table 4.27 Probability of Interruption (P_I) of asset 4 in security area during night time in case that the intruder hits the door and sabotages the target.

	Probability of Interruption:			0.36
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to door1	0.2	E	10.22	3.1
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.53	0.5
5	Break source location door	0.8	E	800	240.0
6	Run to target	0.9	E	1.02	0.3
7	Sabotage target	0.9	E	40	12.0

Table 4.28 Probability of Interruption (P_I) of asset 4 in security area during night time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:			0.26
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to door1	0.2	E	10.22	3.1

Table 4.28 Probability of Interruption (P_I) of asset 4 in security area during night time in case that the intruder cuts through the door and sabotages the target (continued).

	Probability of Interruption:			0.26
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds)	
			Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.53	0.5
5	Break source location door	0	E	80	24.0
6	Run to target	0.9	E	1.02	0.3
7	Sabotage target	0.9	E	40	12.0

Table 4.29 Probability of Interruption (P_I) of asset 4 in security area during night time in case that the intruder cuts through the door and steals the target.

	Probability of Interruption:			0.80
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds)	
			Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to door1	0.2	E	10.22	3.1
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.53	0.5

Table 4.29 Probability of Interruption (P_I) of asset 4 in security area during night time in case that the intruder cuts through the door and steals the target (continued).

	Probability of Interruption:		0.80	
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
5	Break source location door	0	E	80	24.0
6	Run to target	0.9	E	1.02	0.3
7	Steals the target	0.9	E	180	54.0

In Table 4.27, in case of intruder penetrates to source location by hitting the door and sabotaging, the probability of interruption (P_I) is 0.36 which is rated low-medium. The response force is unlikely to be able to interrupt the intruder. The first detection is surveillance personnel which has low probability of detection. The detection may be bypassed due to human factor error and BMS will be performed as next detection. Even though an intruder takes more time to break the source location door (800 seconds) than the security response time (120 seconds), but the system cannot protected against the intruder. Because of it is late detection. The time to achieve the goal (sabotage) after BMS triggered is 41.02 seconds, which is less than response time (120 seconds). The intruder can achieve the task. From the calculation, hitting the door should be the case to concern in the security area during night time.

In Table 4.28, in case of intruder penetrates to source location by cutting the door and sabotaging, the probability of interruption (P_I) is 0.26, which is rated low. The chance of response personnel is low to be able to interrupt the intruder. Because of the BMS would be bypassed when the intruder cutting through the door.

The trigger alarm and communication to response personnel would be bypassed as well. Delay time was performed by running to target and time for set up explosive (41.02 seconds), while a response personnel needs 120 seconds. From the calculation, cutting through the door should be the case to concern in the security area during night time.

In Table 4.29, in case of intruder penetrates to source location by cutting the door and stealing, the probability of interruption (P_I) is 0.80. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. This case is similar to the case of intruder cutting the door, but different goal, which is theft. Even though the probability of detection is low (P_D = 0.2) and BMS would not triggered but the intruder takes more time to remove the target from the 2 high security padlocks (180 seconds), allowing sufficient time for the response force to take action. Thus, the PPS of Asset 1 is effective in case of intruder cutting through the door and steals the target.

In addition, Asset 4 uses CCTV in conjunction with operating personnel for continuous monitoring but only during day time. During night time, there is no operator personnel for monitoring.

4.2.2.5 Result for Asset 5

The EASI model results for three scenarios (hitting the door and sabotage, cutting through the door and sabotage, and cutting through the door and steal) are shown in Tables 4.30, 4.31, and 4.32 respectively.

Table 4.30 Probability of Interruption (P_I) of asset 5 in security area during night time in case that the intruder hits the door and sabotages the target.

	Probability of Interruption:		0.36
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Response Force Time (in Seconds) Mean	Standard Deviation
	0.95	120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to door1	0.2	E	12.78	3.8
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.28	0.4
5	Break source location door	0.8	E	800	348.0
6	Run to target	0.9	E	1.02	0.3
7	Sabotage target	0.9	E	40	12.0

Table 4.31 Probability of Interruption (P_I) of asset 5 in security area during night time in case that intruder cuts through the door and sabotages the target.

	Probability of Interruption:		0.26
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Response Force Time (in Seconds) Mean	Standard Deviation
	0.95	120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to door1	0.2	E	12.78	3.8

Table 4.31 Probability of Interruption (P_I) of asset 5 in security area during night time in case that intruder cuts through the door and sabotage the target (continued).

	Probability of Interruption:			0.26
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.28	0.4
5	Break source location door	0	E	80	24.0
6	Run to target	0.9	E	1.02	0.3
7	Sabotage target	0.9	E	40	12.0

Table 4.32 Probability of Interruption (P_I) of asset 5 in security area during night time in case that intruder cuts through the door and steals the target.

	Probability of Interruption:			0.80
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to door1	0.2	E	12.78	3.8

Table 4.32 Probability of Interruption (P_I) of asset 5 in security area during night time in case that intruder cuts through the door and steals the target (continued).

	Probability of Interruption:			0.80
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Break door1	0.2	E	60	18.0
4	Run to source location door	0	E	1.28	0.4
5	Break source location door	0	E	80	24.0
6	Run to target	0.9	E	1.02	0.3
7	Steals the target	0.9	E	180	54.0

In Table 4.30, in case of intruder penetrates to source location by hitting the door and sabotaging, the probability of interruption (P_I) is 0.36 which is rated low-medium. The response force is unlikely to be able to interrupt the intruder. The first detection is surveillance personnel which has low probability of detection. The detection may be bypassed due to human factor error and BMS will be performed as next detection. Even though an intruder takes more time to break the source location door (800 seconds) than the security response time (120 seconds), but the system cannot protected against the intruder. Because of it is late detection. The time to achieve the goal (sabotage) after BMS triggered is 41.02 seconds, which is less than response time (120 seconds). The intruder can achieve the task. From the calculation, hitting the door should be the case to concern in the security area during night time.

In Table 4.31, in case of intruder penetrates to source location by cutting the door and sabotaging, the probability of interruption (P_I) is 0.26, which is rated low. The chance of response personnel is low to be able to interrupt the intruder. Because of the BMS would be bypassed when the intruder cutting through the door. The trigger alarm and communication to response personnel would be bypassed as well. Delay time was performed by running to target and time for set up explosive (41.02 seconds), while a response personnel needs 120 seconds. From the calculation, cutting through the door should be the case to concern in the security area during night time.

In Table 4.32, in case of intruder penetrates to source location by cutting the door and stealing, the probability of interruption (P_I) is 0.80. The response personnel have a high chance to be able to interrupt the intruder before the task is completed. This case is similar to the case of intruder cutting the door, but different goal, which is theft. Even though the probability of detection is low (P_D = 0.2) and BMS would not triggered but the intruder takes more time to remove the target from the 2 high security padlocks (180 seconds), allowing sufficient time for the response force to take action. Thus, the PPS of Asset 1 is effective in case of intruder cutting through the door and steals the target.

In addition, Asset 5 uses CCTV in conjunction with operating personnel for continuous monitoring but only during day time. During night time, there is no operator personnel for monitoring.

4.3 Comparison and discussion of the checklist result and the result from the Estimation of Adversary Sequence Interruption (EASI) Model.

The physical protection system of all assets in security area would not be effective if the intruder penetrates to source location by cutting through the door. The case of intruder cutting through the door is the worst case in this studied. The comparison between the checklist result and the EASI result is divided into 2 parts as follows:

(1) Comparison of detection, delay and response between the checklist and the EASI results in security area during day time and night time.

(2) Comparison of overall effectiveness of the system between the checklist and the EASI results in security area during day time and night time.

4.3.1 Comparison of detection, delay and response between the checklist and the EASI results in security area during day time and night time.

The comparison of detection, delay and response between the checklist and the EASI results in security area during day time are shown in Table 4.33 and during night time are shown in Table 4.34.

Table 4.33 The checklist result of detection, delay and response of all assets in the security area during day time.

Security element	Asset 1	Asset 2	Asset 3	Asset 4	Asset 5
Detection	0.96	0.96	0.96	0.96	0.96
Delay	1.00	1.00	1.00	1.00	1.00
Response	0.72	0.72	0.79	0.79	0.79
Overall effectiveness score	**0.69**	**0.69**	**0.75**	**0.75**	**0.75**

The security area during day time is the source operating room or source storage room. For detection, the score from checklist is 0.96, which is acceptable. This is because of all assets use BMS as detection, and it is linked to an alarm so that the detection can provide immediate detection, assessment, and communication. From the EASI result, in the case of intruder cutting through the door, it is found that the system can detect very fast but the detection is not performed by the BMS. BMS will not trigger because the door is not open. The fast detection is performed by operator's continuous monitoring through the CCTV (P_D=0.9). This is sufficiently effective.

For delay, the score from the checklist is 1.00. All assets have at least 2 delay layers after detection, which are the source location door and the device holding the

source. However, this is only applicable to the theft case. The latter layer does not work in case of sabotage.

For response, the score from checklist is 0.72-0.79 which is acceptable. There are adequate response personnel and equipment to interrupt the intruder. However, there is no document procedure to follow although all response personnel know what action to take in case a security event occurs. The response time is 120 seconds, which is the average time to arrive at the location after an alarm is triggered. The response time can be further reduced if a drill for responding to security event is performed annually.

The score for the overall effectiveness of the system are 0.69 for Assets 1 and 2, and 0.75 for Assets 3-5. And the comparison of the overall effectiveness of the system between the checklist and the EASI results will be compared in Section 4.3.2.

Table 4.34 The checklist result of detection, delay and response of all assets in the security area during night time.

Security element	Asset 1	Asset 2	Asset 3	Asset 4	Asset 5
Detection	0.96	0.96	0.96	0.96	0.96
Delay	1.00	1.00	1.00	1.00	1.00
Response	0.72	0.72	0.79	0.79	0.79
Overall effectiveness score	**0.69**	**0.69**	**0.75**	**0.75**	**0.75**

The security area during night time is the building that the source is located. For detection, the score from checklist is 0.96 (same as the score during day time) which it is acceptable score. The detection is the continuous surveillance personnel, which is in compliance with the regulatory requirement that requires continuous surveillance. In the EASI model, the probability of detection of surveillance personnel is low (P_D = 0.2) due to human factor error, and this low P_D affects the effectiveness of the system. The checklist does not take into account the performance of the detection measure that is used, while the EASI model does.

For delay, the score from the checklist is 1.00 (same as the score during day time). All assets have 3 delay layers after detection, which are the exterior door, the

source location door, and the device holding the source or locked device with high security padlock. The last layer does not affect the intruder in case of sabotage.

For response, the score from checklist is 0.72-0.79, which is acceptable score and is the same as the score during day time.

Even though the results from the checklist and the EASI model agree with each other in the case of theft, but the checklist does not take into account in performance or effectiveness of equipment or measure that is being used. This is the limitation of checklist, which makes it inefficient in the case of sabotage.

4.3.2 Comparison of the overall effectiveness of the system between the checklist and the EASI results.

The comparison of the overall effectiveness of the system between the checklist and the EASI results in security area during day time and night time are shown in Table 4.35 and 4.37 respectively.

Table 4.35 Comparison of the result of overall score from checklist and the P_I from EASI model in security area during day time

Assets	Checklist	EASI: Probability of Interruption (P_I)		
	(Overall score)	(hit/sabotage)	(cut/sabotage)	(cut/theft)
Asset 1	0.69	0.86	0.45	0.97
Asset 2	0.69	0.20	0.11	0.77
Asset 3	0.75	0.86	0.45	0.97
Asset 4	0.75	0.86	0.44	0.94
Asset 5	0.75	0.86	0.44	0.94

In Table 4.35, all assets have high P_I in case of intruder cuts door and steal target. This is similar to checklist result (high score).

For sabotage case, all assets have low P_I in case of intruder cuts through door. But checklist result has high score, which is similar to in case of intruder hits door in EASI result (except Asset 2). Asset 2 has no CCTV in conjunction with

operating personnel for continuous monitoring, while other assets had. If CCTV was added into asset 2, the P_I is 0.86 as shown in Table 4.50. It is found that after CCTV was added to the system, the result is same result to other assets. Therefore, in sabotage case, the checklist can be used to evaluate the PPS effectiveness in case of intruder hits door but not cuts door. However, hitting door is not the worst case but cutting door is and we cannot know what intruder action is.

Table 4.36 Probability of Interruption (P_I) of Asset 2 in security area during day time after added CCTV in front of security area in case that the intruder hits the door and sabotages the target.

	Probability of Interruption:			0.86
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	800	240.0
3	Open source location door	0.8	E	0	0.0
4	Run to target	0.9	E	1.53	0.5
5	Sabotage target	0.9	E	40	12.0

Table 4.37 Comparison of the result of overall score from checklist and the PI from EASI model in security area during night time

Assets	Checklist	EASI: Probability of Interruption (P_I)		
	(Overall score)	(hit/sabotage)	(cut/sabotage)	(cut/theft)
Asset 1	0.69	0.36	0.27	0.86
Asset 2	0.69	0.36	0.26	0.80
Asset 3	0.75	0.91	0.55	0.98
Asset 4	0.75	0.36	0.26	0.80
Asset 5	0.75	0.36	0.26	0.80

In Table 4.37, in all assets, the probability of interruption goes up to acceptable level in case of theft (P_I = 0.80-0.98). Even there is no CCTV installed at source room in asset 2, but P_I=0.80. This is because of the system has more delay layers, which provide more delay time for adversary to do the task.

There is one sabotage case in EASI result has very high P_I and similar to checklist result. It is case of intruder hits door. Asset 3 has P_I=0.9. Because of Asset 3 has CCTV in conjunction with front guard for continuous monitoring during night time. Other asset also has CCTV in front of source location room but it is not conjunction with front guard, but conjunction with operating personnel.

If consider only Asset 3 in all scenario (except the worst case, intruder cuts door and sabotages target), it is only one asset which has high probability of interruption (P_I) whether during day time or night time. Even in the worst case and during night time, the Asset 3, P_I is 0.55, which is rated medium probability of interruption. It is interesting that security measures were used in Asset 3 is can be a best practice for design and installing the physical protection equipment.

4.4 Improving the PPS using EASI model.

It is found that the existing PPS in all assets are not effective against sabotage case, whether it is during day time or night time, and whether it is in the case of cutting or hitting door. Improving the PPS can be done by (1) in the security area during day time, add a door inside the security area with one high security

padlock (delay time is 90 seconds), and (2) in the security area during night time, add a CCTV in conjunction with a front guard (P_D=0.9) in front of the security area. Table 4.38 shows the P_I of all assets after improving the system. In all assets, the P_I increase whether adding door (P_I=0.82) or adding CCTV (P_I=0.91-0.99). It should be noted that even if the PPS were to be improved, the checklist result would still not change. The P_I after improving of all assets are shown in Table 4.39-4.53.

Table 4.38 Probability of Interruption (P_I) of all assets after improving the system.

Assets	Checklist (Overall score)	P_I in security area during day time	P_I in security area during night time	
		(cut/sabotage)	(hit/sabotage)	(cut/sabotage)
Asset 1	0.69	0.82	0.91	0.81
Asset 2	0.69	0.82	0.91	0.81
Asset 3	0.75	0.82	0.99	0.85
Asset 4	0.75	0.82	0.91	0.81
Asset 5	0.75	0.82	0.91	0.81

Table 4.39 Probability of Interruption (P_I) of Asset 1 after adding door in the security area during day time in case that the intruder cuts through the door and sabotages the target.

		Probability of Interruption:			0.82
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0

Table 4.39 Probability of Interruption (P_I) of Asset 1 after adding door in the security area during day time in case that the intruder cuts through the door and sabotages the target (continued).

		Probability of Interruption:			0.82
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Location	Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Break added door	0.9	E	90	27.0
4	Run to target	0.9	E	2.3	0.7
5	Sabotage target	0.9	E	40	12.0

Table 4.40 Probability of Interruption (P_I) of Asset 2 after adding door in the security area during day time in case that the intruder cuts through the door and sabotages the target.

		Probability of Interruption:			0.82
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Location	Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Break added door	0.9	E	90	27.0
4	Run to target	0.9	E	1.53	0.5

Table 4.40 Probability of Interruption (P_I) of Asset 2 after adding door in the security area during day time in case that the intruder cuts through the door and sabotages the target (continued).

		Probability of Interruption:			0.82
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Location	Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
5	Sabotage target	0.9	E	40	12.0

Table 4.41 Probability of Interruption (P_I) of Asset 3 after adding door in the security area during day time in case that the intruder cuts through the door and sabotages the target.

		Probability of Interruption:			0.82
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Location	Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Break added door	0.9	E	90	27.0
4	Run to target	0.9	E	2.3	0.5
5	Sabotage target	0.9	E	40	12.0

Table 4.42 Probability of Interruption (P_I) of Asset 4 after adding door in the security area during day time in case that the intruder cuts through the door and sabotages the target.

		Probability of Interruption:			0.82
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Location	Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0
2	Break source location door	0	E	80	24.0
3	Break added door	0.9	E	90	27.0
4	Run to target	0.9	E	1.02	0.3
5	Sabotage target	0.9	E	40	12.0

Table 4.43 Probability of Interruption (P_I) of Asset 5 after adding door in the security area during day time in case that the intruder cuts through the door and sabotages the target.

		Probability of Interruption:			0.82
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Location	Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Try to break source location door	0.9	E	0	0.0

Table 4.43 Probability of Interruption (P_I) of Asset 5 after adding door in the security area during day time in case that the intruder cuts through the door and sabotages the target (continued).

		Probability of Interruption:			0.82
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Location	Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
2	Break source location door	0	E	80	24.0
3	Break added door	0.9	E	90	27.0
4	Run to target	0.9	E	1.02	0.3
5	Sabotage target	0.9	E	40	12.0

Table 4.44 Probability of Interruption (P_I) of Asset 1 after adding CCTV in front of the security area during night time in case that the intruder hits the door and sabotages the target.

		Probability of Interruption:			0.91
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	51.11	15.3
3	Try to break door1	0.9	E	0	0.0
4	Break door1	0.2	E	60	18.0

Table 4.44 Probability of Interruption (P_I) of Asset 1 after adding CCTV in front of the security area during night time in case that the intruder hits the door and sabotages the target (continued).

		Probability of Interruption:			0.91
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
5	Run to source location door	0	E	5.11	1.5
6	Break source location door	0.8	E	800	240.0
7	Run to target	0.9	E	2.3	0.7
8	Sabotage target	0.9	E	40	12.0

Table 4.45 Probability of Interruption (P_I) of Asset 2 after adding CCTV in front of the security area during night time in case that the intruder hits the door and sabotages the target.

		Probability of Interruption:			0.91
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	76.67	23.0
3	Try to break door1	0.9	E	0	0.0

Table 4.45 Probability of Interruption (P_I) of Asset 2 after adding CCTV in front of the security area during night time in case that the intruder hits the door and sabotages the target (continued).

		Probability of Interruption:			0.91
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
4	Break door1	0.2	E	60	18.0
5	Run to source location door	0	E	1.28	0.4
6	Break source location door	0.8	E	800	240.0
7	Run to target	0.9	E	1.53	0.5
8	Sabotage target	0.9	E	40	12.0

Table 4.46 Probability of Interruption (P_I) of Asset 3 after adding CCTV in front of the security area during night time in case that the intruder hits the door and sabotages the target.

		Probability of Interruption:			0.99
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	2.56	0.8

Table 4.46 Probability of Interruption (P_I) of Asset 3 after adding CCTV in front of the security area during night time in case that the intruder hits the door and sabotages the target (continued).

		Probability of Interruption:			0.99
	Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
3	Try to break door1	0.9	E	0	0.0
4	Break door1	0.2	E	60	18.0
5	Run to source location door	0	E	1.53	0.5
6	Try to break source location door	0.9	E	0	0.0
7	Break source location door	0.8	E	800	240.0
8	Run to target	0.9	E	2.3	0.7
9	Sabotage target	0.9	E	40	12.0

Table 4.47 Probability of Interruption (P_I) of Asset 4 after adding CCTV in front of the security area during night time in case that the intruder hits the door and sabotages the target.

Estimate of Adversary Sequence Interruption		Probability of Interruption: 0.91			
		Probability of Alarm Communication		Response Force Time (in Seconds)	
				Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	10.22	3.1
3	Try to break door1	0.9	E	0	0.0
4	Break door1	0.2	E	60	18.0
5	Run to source location door	0	E	1.53	0.5
6	Break source location door	0.8	E	800	240.0
7	Run to target	0.9	E	1.02	0.3
8	Sabotage target	0.9	E	40	12.0

Table 4.48 Probability of Interruption (P_I) of Asset 5 after adding CCTV in front of the security area during night time in case that the intruder hits the door and sabotages the target.

Estimate of Adversary Sequence Interruption		Probability of Interruption: 0.91			
		Probability of Alarm Communication		Response Force Time (in Seconds)	
				Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	12.78	3.8
3	Try to break door1	0.9	E	0	0.0
4	Break door1	0.2	E	60	18.0
5	Run to source location door	0	E	1.28	0.4
6	Break source location door	0.8	E	800	240.0
7	Run to target	0.9	E	1.02	0.3
8	Sabotage target	0.9	E	40	12.0

Table 4.49 Probability of Interruption (P_I) of Asset 1 after adding CCTV in front of the security area during night time in case that the intruder cuts through the door and sabotages the target.

		Probability of Interruption:			0.81
Estimate of Adversary Sequence Interruption		Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
		0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	51.11	15.3
3	Try to break door1	0.9	E	0	0.0
4	Break door1	0.2	E	60	18.0
5	Run to source location door	0	E	5.11	1.5
6	Break source location door	0	E	800	240.0
7	Run to target	0.9	E	2.3	0.7
8	Sabotage target	0.9	E	40	12.0

Table 4.50 Probability of Interruption (P_I) of Asset 2 after adding CCTV in front of the security area during night time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:			0.91
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	76.67	23.0
3	Try to break door1	0.9	E	0	0.0
4	Break door1	0.2	E	60	18.0
5	Run to source location door	0	E	1.28	0.4
6	Break source location door	0	E	80	24.0
7	Run to target	0.9	E	1.53	0.5
8	Sabotage target	0.9	E	40	12.0

Table 4.51 Probability of Interruption (P_I) of Asset 3 after adding CCTV in front of the security area during night time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:			0.85
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	2.56	0.8
3	Try to break door1	0.9	E	0	0.0
4	Break door1	0.2	E	60	18.0
5	Run to source location door	0	E	1.53	0.5
6	Try to break source location door	0.9		0	0.0
7	Break source location door	0	E	80	24.0
8	Run to target	0.9	E	2.3	0.7
9	Sabotage target	0.9	E	40	12.0

Table 4.52 Probability of Interruption (P_I) of Asset 4 after adding CCTV in front of the security area during night time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:			0.81
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	10.22	3.1
3	Try to break door1	0.9	E	0	0.0
4	Break door1	0.2	E	60	18.0
5	Run to source location door	0	E	1.53	0.5
6	Break source location door	0	E	80	24.0
7	Run to target	0.9	E	1.02	0.3
8	Sabotage target	0.9	E	40	12.0

Table 4.53 Probability of Interruption (P_I) of Asset 5 after adding CCTV in front of the security area during night time in case that the intruder cuts through the door and sabotages the target.

	Probability of Interruption:			0.81
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		120	36
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Climb the wall	0	E	12	3.6
2	Run to building	0.2	E	12.78	3.8
3	Try to break door1	0.9	E	0	0.0
4	Break door1	0.2	E	60	18.0
5	Run to source location door	0	E	1.28	0.4
6	Break source location door	0	E	80	24.0
7	Run to target	0.9	E	1.02	0.3
8	Sabotage target	0.9	E	40	12.0

Discussion

Checklist result does not change whether in security area during day time or night time, but the EASI result change. Because the EASI take into account in the boundary of security area, but the checklist does not.

EASI result change when scenario is changed, but checklist result does not change. This is because EASI takes into account in action of intruder, while the checklist does not.

EASI result change when equipment or measure is changed, but checklist result does not change. This is because EASI takes into account in the performance or effectiveness of the equipment or measure used, while the checklist does not.

Even though the checklist is taking into account in compliance with the regulatory requirement and the functional of equipment, it does not consider the quality or effectiveness of the equipment, material, or measure used. Thus, it will be good to add these details into the checklist. From result and discussion found that there are several limitations of checklist.

Limitations of checklist

Even though checklist is easy to use for inspection, but may not be sufficient due to several limitations:

- The checklist does not take into account in action of intruder. In this study, the PPS is found to be effective against theft, but not against sabotage. Hitting and cutting the door also produce different results. This cannot be seen in the checklist result, but appears in the EASI model.
- The checklist does not consider the quality or effectiveness of equipment, material, measure, or method used.

Suggestion

The current checklist can be used to evaluate the compliance with the regulatory requirement on radioactive source security, and may be used in conjunction with the EASI model calculation in order to evaluation of the effectiveness of the physical protection system in sabotage case. However, it is found that even if a PPS was found to be in compliance with the existing regulation and the IAEA minimum standard requirement, it might not be effective against sabotage. To have effective PPS, both the regulation and the minimum requirement should also take into account the prevention of sabotage.

CHAPTER 5
CONCLUSION

5.1 Conclusion

At present the inspection program of security of radioactive materials only looks at the presence of security components, but does not include the measurement of physical protection system effectiveness. This research aims to develop an inspection checklist for evaluating the effectiveness of physical protection system at Categories 1 and 2 radiation facilities. Sample studied is radiation facility, which already have the physical protection system installed through the support of the United States Department of Energy (U.S. DOE), are chosen as the test subject for the checklist. In total 5 samples studied. The developed checklist consist of six security element, access control, detection, delay, response, security management and security culture and provide scoring criteria for each statement of each security element. Then compare the checklist result to result from Estimation of Adversary Sequence Interruption (EASI) model, a computerize calculation which is in the form of probability of interruption (PI) of an adversary action sequence aimed at theft or sabotage.

The result of this research showed that

- The checklist cannot be used to evaluate the effectiveness of the physical protection system in case the intruder cuts through the door and sabotages target whether during day time or night time (P_I=0.11-0.55).
- The checklist cannot be used to evaluate the effectiveness of the physical protection system in case the intruder hits the door and sabotages target during night time (P_I=0.36).
- The checklist can be used to evaluate the effectiveness of the physical protection system in case the intruder cuts through the door and steals target whether during day time or night time (P_I=0.76-0.98).
- The checklist can be used to evaluate the effectiveness of the physical protection system in case the intruder hits the door and sabotages target during day time (P_I=0.86).

In conclusion, the checklist can be used to evaluate the effectiveness of the physical protection system in case the adversary's goal is theft, but there is some limitation of checklist in case of sabotage.

It is hoped that this research will be useful for authority regulatory or those involved in assessments and inspections of physical protection system at Categories 1 and 2 facilities that use or store radioactive materials in a security area. This research is also expected to be useful for licensing applicants in their preparation to submit application for usage authorization of Categories 1 and 2 radioactive materials in order to design the physical protection system that is in compliance with regulatory requirement.

5.2 Recommendations for Future Research

In this study, there are some limitations of checklist. The checklist does not take into account the action of intruder. The checklist does not consider the performance or effectiveness of equipment, measure, or method used. It should be good to further improve the checklist to take into account these limitations. For example, the checklist may include weight factor for each equipment, measure, or method used to verify that it is sufficiently effective to protect the asset against theft, sabotage, or other malevolent acts.

Security culture should also be conducted through self-assessment to ensure that all personnel are aware of security-related system, follow the procedure, and know their responsibility.

REFERENCES

REFERENCES

[1] Regulation of Atomic Energy Commission for Peace on methodology of security of radioactive material B.E. 2554.

[2] Atomic Energy for Peace Act B.E. 2504.

[3] Garcia, Mary Lynn. (2001). The design and evaluation of physical protection Systems. Butterworth-Heinemann. Garcia, M. L (2007). The Design and Evaluation of Physical Protection Systems, Second edition, Sandia National Laboratories.

[4] International Atomic Energy Agency. (2009). NSS 11. Security of Radioactive Sources. Vienna, Austria.

[5] United States Nuclear Regulatory Commission. (2013). NUREG-1885, Rev. 6. Report to congress on the Security Inspection Program for Commercial Power Reactors and Category I Fuel Cycle Facilities: Results and Status Update. Washington, DC, USA.

[6] International Atomic Energy Agency. (2004). Code of Conduct on the Safety and Security of Radioactive Sources. Vienna, Austria.

[7] International Atomic Energy Agency. (2009). RS.G.1.9, Categorization of Radioactive Sources. Vienna, Austria.

[8]United States Nuclear Regulatory Commission. (2013). NUREG-2155. Implementation Guidance for 10 CFR Part 37, “Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material”. Washington, DC, USA.

[9] National Nuclear Security Administration. (2010). NAP 70.2. Physical Protection. USA.

[10] International Atomic Energy Agency. (2011). NSS 14. Nuclear Security Recommendations on Radioactive Material and Associated Facilities. Vienna, Austria.

[11] International Atomic Energy Agency. (2008). NSS 7. Nuclear Security Culture. Vienna, Austria.

[12] Omotoso, O; Aderinto A. A (2012). Assessing the Performance of Corporate Private Security Organizations in Crime Prevention in Lagos State, Nigeria, Journal of Physical Security Vol.6:1, pp.73- 90.

[13] Bakr, W.F; Hamed, A.A (2009). Upgrading the Physical Protection System (PPS) to improve the Response to Radiological Emergencies involving Malevolent Action Journal of Physical Security Vol.3, pp. 9-16.

[14] Hosik Yoo; Jeong-Ho Lee. (2015). Results of nuclear security culture survey on personnel at nuclear power plants. Journals of Nuclear Energy, Vol.85, pp.398-402.

[15] A. ŠTEFULOVÁ. (2001). Evaluation of effectiveness of physical protection systems at nuclear facilities in the Slovak Republic. In proceedings of IAEA 2001 International Conference on Measures to Prevent, Intercept and Respond to Illicit Uses of Nuclear Material and Radioactive Sources, Stockholm, Sweden. pp. 221-223.

[16] Sandia National Laboratory, SAND2007-5591(2007). Nuclear Power Plant Security Assessment Technical Manual, Albuquerque, pp. 3-113.

[17] IAEA-TECDOC-1355(2003).Security of radioactive sources Interim guidance for comment, pp.1.

[18] Center for International Trade and Security. (2004). Nuclear Security Culture: The Case of Russia. University of Georgia, USA.

[19] Nasiru Imam Zakariya; M.T.E. Kahn. (2015). Safety, security and safeguard. Journal of Nuclear Energy Vol.5, pp. 292-302.

[20] Chapman, L.D and Harlon, C.P (1985). EASI (Estimate of adversary sequence interruption on an IBM PC: SAND-85-1105; Sandia Labs: Albuquerque, NM, USA, pp. 1-65.

[21] M.C. Echeta; L.A. Dim; O.D. Oyeyinka; and A.O. Kuye. (2014). PPS Evaluation of An Oil Refinery Using EASI Model. Journals of Physical Security, Vol.7(2), pp.30-41.

[22] World Institute for Nuclear Security. (2011). WINS 1.4. Nuclear Security Culture. Vienna, Austria.

APPENDIX

APPENDIX A

Inspection checklist

Part I: General Information

Facility Name			
Address			
Contact Name		Position	
Contact Email		Telephone	
Radiation Safety Officer Name		Position	
Radiation Safety Officer Email		Telephone	

Part II: Source Information

Radionuclide	
Total activity	Ci/GBq
Manufacture	
Serial No.	
Calibration Date	
Storage room	

Part III: Physical Protection System

Security element	Questionnaire	Ref.	Score	Inspection guidance
Access Provide access controls to source location that effectively restrict access to authorized persons only *Measures*: Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control. (A combination of two or more verification measures should be required, e.g. the use of a swipe card and a PIN; or the use of a swipe card and a controlled key; or a PIN and a computer password; or the use of a controlled key and visual verification of identity by other authorized personnel)	1. There is restricting access to security area, which are source location or operation area for only authorized persons 2= Has restricting access measure for only authorized persons 1= Has restricting access measure but not only authorized persons 0= No measure for restricting access to source location or secure area	IAEA NSS11/ NRC10 part37		Inspect to verify that there is real existing measure or equipment and functional. Inspect by interview operator personnel that who can access to security area and how. And inspect the measure or functional of equipment by ask operator personnel access to security area or source location then observe
	2. There are 2 verification measures for access to security area or source location 2= Has 2 verification measures e.g. swipe card and PIN; or controlled key and visual verification of identity by other authorized personnel 1= Has only one verification measures e.g. swipe card; or controlled key; authorized personnel 0= No verification measure	IAEA NSS11		
	3. Those measures/equipment can identify and verify person correctly and reject entry if input false identities or cannot identify and verify person 2= measures/equipment can identify and verify all person correctly and reject all entry if input false identities or cannot identify and verify person 1= measures/equipment can identify and verify some person correctly and reject all entry if input false identities or cannot identify and verify person 0= measures/equipment cannot identify and verify person and cannot reject all reject all entry if input false identities or cannot identify and verify person	IAEA NSS11		
	4. If there is unauthorized person access to security area or source location, they are escorted and are under constant	IAEA NSS11		

Security element	Questionnaire	Ref.	Score	Inspection guidance
	surveillance by authorized person (in case of medical exposure or mobile source) 2= All time unauthorized persons are escorted and are under constant surveillance by authorized person 1= Sometime unauthorized persons are escorted and are under constant surveillance by authorized person or unauthorized persons are escorted but are not under constant surveillance by authorized person 0= No escorted unauthorized persons and no constant surveillance			
	Average			
Detection Provide immediate detection of any unauthorized access to the secured area/source location *Measures*: Electronic intrusion detection system and/or continuous surveillance by operator personnel. **Note:** For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of immediate intrusion detection	1. There is detection system to detect any unauthorized access and it is function for example electronic intrusion detection sensor or monitored intrusion detection system or monitored video surveillance or direct visual surveillance 2= There is detection system to detect unauthorized access and it is function for example electronic intrusion detection sensor or monitored intrusion detection system or monitored video surveillance or direct visual surveillance 1= There is detection system to detect unauthorized access but it is not function 0= No detection system to detect unauthorized access	IAEA NSS11		Inspect to verify that there is detection of unauthorized access and it is function (immediate detection) and inspect by test an alarm of detection system to ensure that it is immediate detection. Or if detection system is monitoring through CCTV monitor or direct visual surveillance personnel, there should be continuous monitoring or continuous direct visual.
	2. The detection system immediate detection of unauthorized access for example electronic intrusion detection sensor linked to an alarm or monitored intrusion detection system linked to onsite or offsite central monitoring or continuous monitored video surveillance or a continuous direct visual surveillance 2= The detection system is immediate detection of unauthorized access for	IAEA NSS11		

Security element	Questionnaire	Ref.	Score	Inspection guidance
	example electronic intrusion detection sensor linked to an alarm or monitored intrusion detection system linked to onsite or offsite central monitoring or continuous monitored video surveillance or a continuous direct visual surveillance (the sensor always linked to an alarm or continuous means 24 hr working) 1= The sensor sometime linked to an alarm or surveillance not continuous 0= The intrusion detection sensor doesn't linked to an alarm or has no continuous monitored surveillance or has no continuous direct visual surveillance			
	3. There is an automatic auxiliary power source for detection systems in case of a power failure (if there is not, direct surveillance need to be provided for continuous detection) 2= There is an automatic auxiliary power source for detection systems and functional, if there is not, direct surveillance need to be provided for continuous detection (work for 24 hours) 1= There is an automatic auxiliary power source for detection systems but not functional or there is direct surveillance but not continues detection 0= No automatic auxiliary power source or no direct surveillance personnel	NRC10 part37		Inspect to verify that there is an automatic auxiliary power source in case of power failure and test the operation of auxiliary power (if any)
Provide immediate detection of any attempted unauthorized removal of the source, including by an insider *Measures*: Electronic tamper detection equipment and/or	4. For category 1, there is detection system to detect any attempted unauthorized removal and it is function for example electronic tamper detection equipment or monitored video surveillance or direct visual surveillance. For category 2, there is measure to verify that the source is present. 2= For category 1, there is detection system to detect any attempted	IAEA NSS11/ NRC10 part37		Inspect to verify that there is detection of unauthorized removal and it is function and inspect by test an alarm of detection system to ensure that it is immediate

Security element	Questionnaire	Ref.	Score	Inspection guidance
continuous surveillance by operator personnel. **Note:** For category2, unauthorized removal can be detected through weekly physical checks, tamper indicating devices, actual use; or other means [NRC10 inspection manual]	unauthorized removal and it is function for example electronic tamper detection equipment or monitored video surveillance or direct visual surveillance. For category 2, there is measure to verify that the source is present such as weekly physical checks and record. 1= For category 1, there is detection system to detect any attempted unauthorized removal but it is not function. For category 2, there is measure to verify that the source is present such as weekly physical checks but not record or there is a physical check but not weekly but check in monthly. 0= For category 1, there is no detection system to detect any attempted unauthorized removal. For category 2, never has physical checks			detection. Or if detection system is monitoring through CCTV monitor or direct visual surveillance personnel, there should be continuous monitoring or continuous direct visual.
	5. For category1, the detection system is immediate detection of any attempted unauthorized removal for example electronic tamper detection equipment linked to an alarm or continuous monitored video surveillance or a continuous direct visual surveillance. For category2, the weekly physical checking is immediate detection system. 2= For category 1, the detection system is immediate detection of any attempted unauthorized removal for example electronic tamper detection equipment linked to an alarm or continuous monitored video surveillance or a continuous direct visual surveillance (the sensor always linked to an alarm or continuous means 24 hr working). For category 2, the weekly physical checking is immediate detection system. 1= For category 1, the sensor sometime	IAEA NSS11/ NRC10 part37		

Security element	Questionnaire	Ref.	Score	Inspection guidance
	linked to an alarm or surveillance not continuous. For category 2, there is weekly physical checks but not record or there is a physical check but not weekly but check in monthly 0= For category 1, there is no detection system to detect any attempted unauthorized removal. For category 2, never has physical checks			
	6. There is an automatic auxiliary power source for detection systems in case of a power failure (if there is not, direct surveillance need to be provided for continuous detection) 2= There is an automatic auxiliary power source for detection systems and functional, if there is not, direct surveillance need to be provided for continuous detection (work for 24 hours) 1= There is an automatic auxiliary power source for detection systems but not functional or there is direct surveillance but not continues detection 0= No automatic auxiliary power source or no direct surveillance personnel	IAEA NSS11/ NRC10 part37		Inspect to verify that there is an automatic auxiliary power source in case of power failure and test the operation of auxiliary power (if any)
Assessment Provide immediate assessment of detection *Measures*: Remote monitoring of CCTV or assessment by operator/ response personnel. **Note:** For mobile or portable sources, where intrusion detection or tamper	7. There is measure of assessment of unauthorized access and it is function such as operator personnel at source location, or CCTV that monitored by operator personnel, or persons immediately deployed to investigate the cause of alarm. 2= There is measure of assessment of unauthorized access and it is function 1= There is measure of assessment of unauthorized access but it is not function 0= No measure of assessment of unauthorized access	IAEA NSS11		Inspect to verify that there is assessment of unauthorized access and it is function (immediate assessment) and inspect by interview operator personnel and see the record of time working of them. And in case of CCTV was used as the assessment, inspect by ask to
	8. The measure is continuous monitoring and provide recording system (in case of	IAEA NSS11/		

Security element	Questionnaire	Ref.	Score	Inspection guidance
detection is provided by continuous visual surveillance by operator personnel, assessment should be performed concurrently with detection by the operator personnel keeping the source under continuous visual surveillance.	CCTV was used as the assessment) 2= There is continuous monitoring through CCTV or there is continuous working of operator personnel at source location (24 hours working) 1= There is not continuous monitoring (not 24 hours working) 0= No measure of assessment of the cause of alarm	NRC10 part37		see the record one period of time.
	9. The assessment measure can classify the object of intrusion (e.g. in case of CCTV was used, no gaps between zones or areas that cannot be assessed because of shadows or object blocking the camera's field of view and can classify if CCTV monitor has at least 6 horizontal TV lines (HTVL) or 6 pixels of resolution to classify an intruder) 2= CCTV monitor display area coverage of assessment zone (75% of monitor area) and can classify the object of intrusion 1= CCTV monitor display some area coverage of intrusion detection zone but cannot classify the object of intrusion. 0= CCTV monitor cannot display area coverage of intrusion detection zone or cannot classify the object of intrusion.	Garcia		Inspect by see a monitor display which can classify the object of intrusion and see clearly in assessment zone or not. For example, one inspector walk around the assessment zone and another inspector watch through monitor display.
	10. There is an automatic auxiliary power source for monitoring systems in case of a power failure (if there is not, direct surveillance need to be provided for continuous monitoring) 2= There is an automatic auxiliary power source for monitoring systems and functional, if there is not, direct surveillance need to be provided for continuous monitoring (work for 24 hours) 1= There is an automatic auxiliary power source for monitoring systems but not functional or there is direct surveillance	NRC10 part37		Inspect to verify that there is an automatic auxiliary power source in case of power failure and test the operation of auxiliary power (if any)

Security element	Questionnaire	Ref.	Score	Inspection guidance
	but not continues monitoring 0= No automatic auxiliary power source or no direct surveillance personnel			
Communication Provide immediate communication to response personnel. *Measures*: Rapid, dependable, diverse means of communication such as phones, cell phones, pagers, radios.	11. There is communicate device and it is function such as phone, radio mobile, auto-dialers, landline telephones 2= There is communicate device and it is function 1= There is communicate device but it is not function 0= No communicate device	IAEA NSS11/ NRC10 part37		Inspect to verify that there is communication device and it is function.
	12. If the assessment confirms that unauthorized access or attempted unauthorized removal has occurred, there is immediate inform to response personnel or police response personnel 2= There is immediate inform to response personnel or police response personnel 1= There is inform to response personnel or police response personnel but not immediately for example direct visual surveillance personnel doesn't has/know mobile number of response personnel or there is another step to inform before response personnel 0= No device to inform response personnel or no procedure to follow or operator personnel doesn't know how to do	IAEA NSS11/ NRC10 part37		Inspect by interview operator personnel and front guard and also review the operation procedure to ensure that there is immediate communication with response personnel
Provide a means to detect loss through verification *Measures*: Daily checking through physical checks, CCTV, tamper indicating devices, etc.	13. For category 1, there is daily checking through physical checks that the source is in place. For category 2, there is weekly checking through physical checks that the source is in place. 2= For category 1, there is recording of daily checking through physical checks that the source is in place. For category 2, there is there is recording weekly checking through physical checks that the source is in place. e.g. observation through CCTV;	IAEA NSS11		Inspect by review a record of physical check

Security element	Questionnaire	Ref.	Score	Inspection guidance
	seal or other tamper evident device; actual use; radiation measurement 1= For category 1, there is daily checking through physical checks that the source is in place. For category 2, there is there is weekly checking through physical checks that the source is in place but not record. Or there is physical checks but not daily for cat.1 or not weekly for cat.2. 0= never has physical checks that the source is in place			
	Average			
Delay Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal *Measures*: System of at least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict **Note:** For mobile sources in use, continuous visual surveillance by operator personnel may substitute for one or both layers of barriers	1. After detection, there is locked room or locked door or other barrier for delay unauthorized personnel and represent the first layer delay (for source in use and storage)=layer 1 after detection 2= After detection, there is locked room or locked door or other barrier for use or store source which separate the source from unauthorized personnel and represent the first layer delay (for source in use and storage)=layer 1 after detection 1= After detection, there is only room for use or store source but the room doesn't lock 0= No locked room that used or stored the source which separate from unauthorized personnel (there is no delay after detection)	IAEA NSS11/		Inspect to verify that there are at least 2 delay layers after detection and inspect by observe and interview operator personnel and verified by inspect onsite
	2. There is locked device which separate the device from unauthorized personnel which and represent the second layer delay (for source in use)= layer 2 after detection 2= After detection, there is locked device which separate the device from unauthorized personnel and represent the second layer delay (for source in use)= layer 2 after detection	IAEA NSS11/ Law		

Security element	Questionnaire	Ref.	Score	Inspection guidance
	1= After detection, there is locked device which can represent the second layer delay within the security area but the lock is not meet standard requirement 0= After detection, there is no locked device which can represent the second layer delay within the security area			
	3. There is locked and fixed container or a device holding the source in a locked storage room (for source in storage)= layer 2 after detection 2= After detection, there is locked and fixed container or a device holding the source in a locked storage room (for source in storage)= layer 2 after detection 1= After detection, there is locked and fixed container or a device holding the source in a locked storage room (for source in storage)= layer 2 after detection but the lock is not meet standard requirement 0= After detection, there is no l locked and fixed container or a device holding the source in a locked storage room	IAEA NSS11/ Law		
	4. There are at least 2 continuous visual surveillance personnel by operator personnel to protect the source (in case of mobile source) 2= There are at least 2 continuous visual surveillance personnel by operator personnel 1= There is one continuous visual surveillance personnel by operator personnel 0= No continue surveillance personnel	IAEA NSS11		In case of visual surveillance personnel is used for delay, interview them to ensure that there are at least 2 person and continuous working
	Average			
Response Provide immediate response to assessed alarm with sufficient	1. There is adequate response force personnel to preliminary interrupt adversary 2= There is at least one response force	IAEA NSS11		Inspect to verify that there are adequate response personnel and

Security element	Questionnaire	Ref.	Score	Inspection guidance
resources to interrupt and prevent unauthorized removal *Measures*: Capability for immediate response with size, equipment, and training to interdict. (Operator personnel or police response)	personnel per allocation area and work for 24 hours 1= There is at least one response force personnel per allocation area but not work for 24 hours. 0= No response force personnel			inspect by observe and interview operator personnel and front guard about and time working and number of response personnel to preliminary interrupt adversary
	2. All response force personnel have trained 2= All response force personnel have trained 1= Some response force personnel have trained 0= No response force personnel have trained	IAEA NSS11		Inspect by interview and review a certificate or evidence to ensure that response force personnel have trained
	3. There is communication device for all response force personnel 2= All response force personnel have communication device such as radio phone 1= Some response force personnel have communication device 0= No response force personnel have communication device	IAEA NSS11		Inspect to verify that there is communication device and it is function.
	4. All response force personnel have adequate equipment to preliminary interrupt adversary 2= All response force personnel have at least one equipment to preliminary interrupt adversary such as a straight baton 1= Some response personnel have at least one equipment to preliminary interrupt adversary 0= all response personnel has no equipment to interrupt adversary	IAEA NSS11		Inspect by interview operator personnel and front guard and verified by inspect onsite
	5. After unauthorized access or	IAEA		Inspect by interview

Security element	Questionnaire	Ref.	Score	Inspection guidance
	unauthorized removal is confirmed, there is immediate deployment order, preparation, travel and deployment of response personnel 2= Has response plan procedure to follow and response personnel know their responsibility 1= Has response plan procedure to follow but response personnel don't know their responsibility. Or has no response plan procedure to follow but response personnel know their responsibility 0= Has no response plan procedure to follow and response personnel know their responsibility	NSS11		operator personnel and front guard about their responsibility and review the response plan procedure
	6. There is drill or exercise in nuclear security-related event or when changes to the facility design and evaluate it (drill or exercise may be performed by table top or force on force) 2= has drill or exercise in nuclear security-related event or when changes to the facility design and evaluate it (drill or exercise may be performed by table top or force on force) 1= has drill or exercise in nuclear security-related event or when changes to the facility design but not evaluate it. Or has drill or exercise but not in nuclear security-related event. 0= No response exercise at least every 12 months or when changes to the facility design or operation adversely affect the potential vulnerability of the licensee's material to theft, sabotage, or diversion	NRC10 part37		Inspect by interview operator personnel and front guard and review the certificate or evidence to ensure that response force personnel have drill in nuclear security-related event
	Average			
Security Management Ensure management of access controls to source location restrict	1. There is established security area for used or stored category 1 and 2 radioactive materials 2= has established security zones for used	NRC10 part37		Inspect by observe and interview operator personnel about established

Security element	Questionnaire	Ref.	Score	Inspection guidance
access to authorized persons only	or stored category 1 and 2 radioactive materials and operators know where security zones is 1= has established security zones for used or stored category 1 and 2 radioactive materials or operators know where security zones is 0= No established security zones for used or stored category 1 and 2 radioactive materials and operators don't know where security zones is			security area and verified by review the security area data and inspect onsite
	2. There is methods for access authorization 2= has method for access authorization and operators know the method 1= has method for access authorization but operators know the method. Or has no method for access authorization but operators know the method 0= No method for access authorization and operators don't know the method	IAEA NSS11		Inspect by observe and interview operator personnel about operation procedure for accessing to security area
	3. There is measure of key control procedure 2= has measure of key control procedure and recording and understood by operators 1= has measure of key control procedure but not recording or operators don't understood 0= No measure of key control procedure and not recording or operators don't understood	IAEA NSS11		Inspect by review a record of key control and accessing to operation procedure for accessing to security area
	4. There is procedure for recording of accessing to source location in abnormal operation time 2= has procedure for recording of accessing to source location in abnormal operation time and record it 1= has procedure for recording of accessing to source location in abnormal	IAEA NSS11		

Security element	Questionnaire	Ref.	Score	Inspection guidance
	operation time but not record it 0= No procedure of recording of accessing to source location in abnormal operation time			
	5. There is establish a list of persons currently approved for unescorted access 2= has document of a list of persons currently approved for unescorted access and the list has picture and detail of persons 1= has document of a list of persons currently approved for unescorted access but the list doesn't has picture or detail of persons 0= No document of a list of persons currently approved for unescorted access	NRC10 part37		Inspect by review a list of persons document
	6. In case of the authorized personnel have retired, there is measure to make them unauthorized personnel 2= has measure to make all authorized personnel to be an unauthorized personnel in case of authorized personnel have retired for example confiscate the identity badge or disconnect the password of card reader 1= has measure to make some authorized personnel to be an unauthorized personnel in case of authorized personnel have retired for example confiscate the identity badge or disconnect the password of card reader 0= No measure to make authorized personnel to be an unauthorized personnel in case of authorized personnel have retired	IAEA NSS11/ NRC10 part37		Inspect by interview operator personnel about operation procedure
Ensure trustworthiness of authorized individuals *Measures*: Background	1. There is fingerprinting and criminal history records check for individuals before allowing unescorted access 2= has measure to verify that there is fingerprinting and criminal history records	IAEA NSS11/ NRC10 part37		Inspect by interview operator personnel about the measure to be an authorized personnel and

Security element	Questionnaire	Ref.	Score	Inspection guidance
checks for all personnel authorized for unescorted access to the source location and for access to sensitive information	check before allowing unescorted access and keep recording 1= has measure to verify that there is fingerprinting and criminal history records check before allowing unescorted access but not keep recording 0= No measure to verify that there is fingerprinting and criminal history records check			review the record document
	2. There is verification of true identity for individuals before allowing unescorted access 2= has measure to verify that there is verification of true identity before allowing unescorted access for example review official identification documents (e.g. driver's license; identification; certificate of birth) and compare the documents to personal information data provided by the individual to identify any discrepancy in the information and keep recording 1= has measure to verify that there is verification of true identity but not keep recording 0= No measure to verify that there is verification of true identity	IAEA NSS11/ NRC10 part37		Inspect by interview operator personnel about the measure to be an authorized personnel and review the record document
	3. There is verification of employment history for individuals before allowing unescorted access 2= has measure to verify that there is verification of employment history for individuals before allowing unescorted access and keep recording 1= has measure to verify that there is verification of employment history for individuals before allowing unescorted access but not keep recording 0= No measure to verify that there is verification of employment history	IAEA NSS11/ NRC10 part37		Inspect by interview operator personnel about the measure to be an authorized personnel and review the record document
	4. There is verification of education for	IAEA		Inspect by interview

Security element	Questionnaire	Ref.	Score	Inspection guidance
	individuals before allowing unescorted access 2= has measure to verify that there is verification of education for individuals before allowing unescorted access and keep recording 1= has measure to verify that there is verification of education for individuals before allowing unescorted access but not keep recording 0= No measure to verify that there is verification of education	NSS11/ NRC10 part37		operator personnel about the measure to be an authorized personnel and review the record document
	5. There is determination of character and reputation for individuals before allowing unescorted access 2= has measure to verify that there is determination of character and reputation for individuals before allowing unescorted access for example personal reference (references not supplied by the individual; references not supplied by a close member of the individual's family) and keep recording 1= has measure to verify that there is determination of character and reputation for individuals before allowing unescorted access for example personal reference (references not supplied by the individual; references not supplied by a close member of the individual's family) but not keep recording 0= No measure to verify that there is determination of character and reputation	IAEA NSS11/ NRC10 part37		Inspect by interview operator personnel about the measure to be an authorized personnel and review the record document
	6. Documentation record is kept for at least 3 years after the individual no longer requires unescorted access 2= has keep record of document for at least 3 years after the individual no longer requires unescorted access 1= has keep record of document less than	NRC10 part37		Inspect by interview operator personnel about the period of keep record and review the record document

Security element	Questionnaire	Ref.	Score	Inspection guidance
	3 years 0= No keep record of documentation			
	Average			
Identify and protect sensitive information. *Measures*: Procedures to identify sensitive information and protect it from unauthorized disclosure.	1. There is system of files stored in a locked drawer or file cabinet for the protection of access authorization records and personal information 2= has system of files stored in a locked drawer or file cabinet 1= has system of files stored but the drawer or cabinet is not locked 0= No system of files stored	NRC10 part37		Inspect by observe and interview operator personnel about the method or system of file stored
	2. There is procedures that address the protection of accessing of files stored in a locked drawer or file cabinet 2= has procedures that address the protection of accessing of files stored in a locked drawer or file cabinet and has key control system for example access to file stored by locked key and the locked key was kept in secure place and used by only authorized person 1= has procedures that address the protection of accessing of files stored in a locked drawer or file cabinet but has no key control system for example locked key was not kept in secure place and used by only authorized person 0= No procedures that address the protection of accessing of files stored in a locked drawer or file cabinet and has no key control system	NRC10 part37		Inspect by observe and interview operator personnel about who can access to the file and how
	3. There is system of electronic files stored in computer or other and procedures that address the protection of access authorization records and personal information 2= has system of electronic files stored in computer or other and procedures that address the protection of access	NRC10 part37		Inspect by observe and interview operator personnel about the method of electronic file stored and may ask operator access to the electronic file

Security element	Questionnaire	Ref.	Score	Inspection guidance
	authorization records and personal information for example access to electronic file stored by using password or intranet of authorized person 1= has system of electronic files stored in computer or other but no procedures that address the protection of access authorization records and personal information for example access to electronic file stored by everyone 0= No system of electronic files stored			and observe there is password or not
	Average			
Provide a security plan. *Measures*: A security plan which conforms to regulatory requirements and provides for response to increased threat levels	1. There is developed a written security plan specific to its facilities and operations 2= has development of security plan and operators know what security plan is 1= has development of security plan but operators don't know what security plan is. Or has no development of security plan but operators know what security plan is 0= No development of security plan and operators don't know how to response	IAEA NSS11/ NRC10 part37		Inspect by interview operator personnel about security plan and review a plan that has sufficient detail or not (sufficient detail should be follow all NSS11 requirement) and check the record of periodically exercising and evaluating and updating the plan
	2. The written security plan has sufficient detail 2= The written security plan has sufficient detail which follow all NSS11 requirement. 1= The written security plan has sufficient detail which follow some of NSS11 requirement. 0= No security plan	IAEA NSS11/ NRC10 part37		
	3. There is periodically exercising and evaluating and updating the plan 2= has periodically exercising and evaluating and updating the plan 1= has one of exercising or evaluating or updating the plan 0= No periodically exercising and evaluating and updating the plan	IAEA NSS11/ NRC10 part37		
	Average			
Ensure a capability to	1. There is development of security	IAEA		Inspect by interview

Security element	Questionnaire	Ref.	Score	Inspection guidance
manage security events covered by security contingency plans. *Measures*: Procedures for responding to security-related scenarios.	contingency plan 2= has development of security contingency plan and operators know how to response 1= has development of security contingency plan but operators don't know how to response. Or has no development of security contingency plan but operators know how to response 0= No development of security contingency plan and operators don't know how to response	NSS11		operator personnel about security contingency plan and review a plan that has sufficient detail or not (sufficient detail should be follow all NSS11 requirement) and check the record of periodically exercising and evaluating and updating the plan (security contingency plan may include in security plan)
	2. The written security contingency plan has sufficient detail 2= The written security contingency has sufficient detail which follow all NSS11 requirement. 1= The written security contingency has sufficient detail which follow some of NSS11 requirement. 0= No security contingency	IAEA NSS11		
	3. There is periodically exercising and evaluating and updating the plan 2= has periodically exercising and evaluating and updating the plan 1= has one of exercising or evaluating or updating the plan 0= No periodically exercising and evaluating and updating the plan	IAEA NSS11		
	Average			
Establish security event reporting system. *Measures*: Procedures for timely reporting of security events.	1. There is development of procedures for reporting of security events to the regulatory body, first responders, and others as appropriate 2= has procedures for reporting of security events and operators know what should report 1= has procedures for reporting of security events but operators don't know what should report. Or has no procedures for	IAEA NSS11/ NRC10 part37		Inspect by interview operator personnel about what should report and review a procedure and check a record of suspected or actual security event Security event = suspected or actual

Security element	Questionnaire	Ref.	Score	Inspection guidance
	reporting of security events but operators know what should report. 0= No procedures for reporting of security events and operators don't know what should report			theft of a radioactive source; unauthorized intrusion into a facility or source storage area; loss of control over a radioactive source; unauthorized access to or unauthorized use of a source; failure or loss of security systems that are essential to the protection of radioactive sources
	2. All operators involving in security understand the security events 2= all operators involving in security understand the security events 1= some operators involving in security understand the security events 0= all operators involving in security don't understand the security events	NRC10 part37		
	3. There is record of suspected or actual security event and report to supervisor, regulatory body, first responders, and others as appropriate 2= has record of suspected or actual security event and report to supervisor regulatory body, first responders, and others as appropriate 1= has record of suspected or actual security event but not report to supervisor regulatory body, first responders, and others as appropriate. Or no record but has report. 0= has suspected or actual security event but not record and not report such event to supervisor regulatory body, first responders, and others as appropriate			
	Average			
Security culture **Management system** There is established nuclear security policy for organization	1. There is established nuclear security policy for organization 2= has established nuclear security policy and operators know what nuclear security policy is 1= has established nuclear security policy but operators don't know what nuclear security policy is. Or has no established nuclear security policy but operators know	IAEA NSS7/ WINS 1.4		Inspect by observe and interview operator personnel about nuclear security policy and knowing it

Security element	Questionnaire	Ref.	Score	Inspection guidance
	what nuclear security policy is 0= No established nuclear security policy and operators know what nuclear security policy is			
	2. The nuclear security policy is clearly defined roles and responsibilities for all nuclear security positions 2= has clearly defined roles and responsibilities for all nuclear security positions 1= has defined roles and responsibilities for some nuclear security positions. For example has only responsibility for staff not for manager 0= No defined roles and responsibilities for all nuclear security positions	IAEA NSS7		Inspect by review a nuclear security policy about responsibilities
	3. There is spread and enforce the nuclear security policy to all staff 2= the nuclear security policy is posted in workplace that everyone can see and enforce to all staff (In the event of violations, the sanctions should applied) 1= the nuclear security policy is posted in workplace that everyone can see but not enforce to all staff 0= No nuclear security policy is posted in workplace that everyone can see and enforce to all staff	IAEA NSS7/ CITS		Inspect by observe and interview operator personnel that how to spread and enforce the policy
	4. There is allocate financial, technical and human resources to implement the security system 2= has allocate financial, technical and human resources to implement the security system such as maintenance, training 1= has allocate financial or technical or human resources to implement the security system 0= No allocate financial, technical and human resources to implement the	IAEA NSS7		Inspect by interview operator personnel that there is allocate financial for security system or not

Security element	Questionnaire	Ref.	Score	Inspection guidance
	security system			
	average			
Operating system There are written documents related to guidelines or procedures for nuclear security that workers can easily follow	1. There is a written security plan specific to its facilities and operations 2= has development of security plan and operators know what security plan is 1= has development of security plan but operators don't know security plan is. Or has no development of security plan but operators know security plan is 0= No development of security plan and operators don't know security plan is	IAEA NSS7/ CITS		Inspect by interview operator personnel that there is security plan and knowing it and review the plan
	2. There is instructions, procedure, policy, or normative documents of sensitive information protection 2= has instructions, procedure, policy, or normative documents of sensitive information protection and operators know how to protect sensitive information 1= has instructions, procedure, policy, or normative documents of sensitive information protection but and operators don't know how to protect sensitive information. Or has no instructions, procedure, policy, or normative documents of sensitive information protection but operators know how to protect sensitive information 0= No instructions, procedure, policy, and normative documents of sensitive information protection and operators don't know how to protect sensitive information	IAEA NSS7/ CITS		Inspect by interview operator personnel that there is document of sensitive information protection and knowing of protection and review the document
	3. There is instructions, procedure, policy, or normative documents of access control to secure area or source location 2= has instructions, procedure, policy, or normative documents of access control to secure area or source location and operators know how to control accessing	IAEA NSS7/ CITS		Inspect by interview operator personnel that there is document of accessing to security area and knowing of access and review

Security element	Questionnaire	Ref.	Score	Inspection guidance
	1= has instructions, procedure, policy, or normative documents of access control to secure area or source location but and operators don't know how to control accessing. Or has no instructions, procedure, policy, or normative documents of access control to secure area or source location but operators know how to control accessing 0= No instructions, procedure, policy, and normative documents of sensitive information protection and operators don't know how to control accessing			the document
	4. The roles and responsibilities for staffs are clearly defined in their job descriptions and easily to understand 2= has clearly defined roles and responsibilities and easily to understand and operators know their roles and responsibilities 1= has clearly defined roles and responsibilities and easily to understand but operators don't know their roles and responsibilities 0= No defined roles and responsibilities for staffs	IAEA NSS7/ CITS		Inspect by interview operator personnel about their responsibility and review the document
	5. There is procedure of periodic physical protection equipment maintenance 2= has procedure of periodic physical protection equipment maintenance and operators know the its details and important of maintenance 1= has procedure of periodic physical protection equipment maintenance but operators don't know its details and ignore the important of maintenance. Or has no procedure but know its detail. 0= No procedure of periodic physical protection equipment maintenance and operator don't know about maintenance	IAEA NSS7/ CITS		Inspect by interview operator personnel about physical protection equipment and review the document plan for maintenance

Security element	Questionnaire	Ref.	Score	Inspection guidance
	and ignore the important of maintenance			
	6. There is instructions, procedure, policy, or normative documents in case of security event occurred (contingency plan in security plan) 2= has instructions, procedure, policy, or normative documents in case of security event occurred and operators know its details and know how to action if security event occurred 1= has instructions, procedure, policy, or normative documents in case of security event occurred but operators don't know its details. Or has no instructions, procedure, policy, or normative documents in case of security event occurred but operator know how to action if security event occurred 0= No instructions, procedure, policy, or normative documents in case of security event occurred and operators don't know its details and don't know how to action if security event occurred	IAEA NSS7/ CITS		Inspect by interview operator personnel about how to action if security event occurred and review the document
	average			
Personnel performance Personnel is aware of follow the procedure and know their responsibility	1. Staffs know that there is nuclear security policy or instructions, procedures, policies, and normative documents related to security 2= Staffs know that there is nuclear security policy or instructions, procedures, policies, and normative documents related to security and can describe the details of them 1= Staffs know that there is nuclear security policy or instructions, procedures, policies, and normative documents related to security but cannot describe the details of them 0= Staffs don't know that there is nuclear security policy or instructions, procedures,	IAEA NSS7/ CITS		Inspect by interview operator personnel about the detail of nuclear security policy and review the document

Security element	Questionnaire	Ref.	Score	Inspection guidance
	policies, and normative documents related to security and cannot describe the details of them			
	2. Staffs know their responsibility and assignment which related to security 2= Staffs know their responsibility and assignment which related to security and can describe their responsibility 1= Staffs know their responsibility and assignment which related to security but cannot describe their responsibility 0= Staffs don't know their responsibility and assignment which related to security and cannot describe their responsibility	IAEA NSS7/ CITS		Inspect by interview operator personnel about their responsibility and assignment in security
	3. Staffs usually follow the instructions, procedure or policy 2= Staffs usually follow all of instructions, procedure or policy 1= Staffs usually follow some of instructions, procedure or policy 0= Staffs don't follow all of the instructions, procedure or policy	IAEA NSS7/ CITS		Inspect by interview operator personnel about operation procedure in couple with review the procedure
	4. Staffs know the quantity of physical protection equipment in department and the function of them 2= Staffs know the quantity of physical protection equipment in department and the function of them 1= Staffs know the quantity of physical protection equipment in department but don't know the function of them. Or staffs know some details of physical protection equipment and the function of them 0= Staffs don't know the quantity of physical protection equipment in department and the function of them	IAEA NSS7/ CITS		Inspect by interview operator personnel about the knowledge of function of physical protection equipment
	5. Staffs always attend the training on security 2= Staffs always attend the training on security and aware of security important	IAEA NSS7/ CITS		Inspect by interview operator personnel about how many attend security

Security element	Questionnaire	Ref.	Score	Inspection guidance
	1= Staffs sometime attend the training on security and aware of security important. Or never attend the training on security but aware of security important 0= Staffs never attend the training on security and not aware of security important			training and see a certificate or evidence
	average			
Training There are training course security-related in order to improvement of professional	1. There is periodic of the training programs for nuclear security and evaluation of them 2= has periodic of the training programs for nuclear security and evaluation of them 1= has periodic of the training programs for nuclear security but no evaluation of them 0= No training programs for nuclear security and no evaluation of them	IAEA NSS7/ CITS		Inspect by interview operator personnel about there is security training and review the result or record of training program
	2. There is sufficient details in nuclear security training program 2= has sufficient details in nuclear security training program 1= has details in nuclear security training program but not sufficient or too less 0= No details in nuclear security training program	IAEA NSS7/ CITS		Inspect by review the security program has sufficient detail and period of time and plan for security training in facility (sufficient detail should be follow all NSS11 requirement)
	3. There is contingency plan and conduct drill and evaluate it 2= has contingency plan and conduct drill and evaluate it 1= has contingency plan and conduct drill but not evaluate it. Or has contingency plan and evaluate it but not conduct drill 0= No contingency plan and never conduct drill and never evaluate it	IAEA NSS7/ CITS		Inspect by interview operator personnel about contingency plan drill and review the plan or the result or record of drill
	4. There is assessment of the quality of training and trainers by special surveys or	IAEA NSS7/		Inspect by interview operator personnel

Security element	Questionnaire	Ref.	Score	Inspection guidance
	questionnaires 2= has assessment of the quality of training and trainers by special surveys or questionnaires and report 1= has assessment of the quality of training and trainers by special surveys or questionnaires but not report 0= No assessment of the quality of training and trainers by special surveys or questionnaires	CITS		about assessment of training for improvement in the future and review the result or record of training
	average			

APPENDIX B

Dangerous value, D Value

The *D* value is the radionuclide specific activity of a source which, if not under control, could cause severe deterministic effects and the D value as shown in table B.1.

Table B.1 Dangerous value, D Value [1, 4, 6, 7].

Radionuclide	D value	
	TBq	Ci
Am-241	6.E-02	2.E+00
Am-241/Be	6.E-02	2.E+00
Cf-252	2.E-02	5.E-01
Cm-244	5.E-02	1.E+00
Co-60	3.E-02	8.E-01
Cs-137	1.E-01	3.E+00
Gd-153	1.E+00	3.E+01
Ir-192	8.E-02	2.E+00
Pm-147	4.E+01	1.E+03
Pu-238	6.E-02	2.E+00
Pu-239[(b)]/Be	6.E-02	2.E+00
Ra-226	4.E-02	1.E+00
Se-75	2.E-01	5.E+00
Sr-90 (Y-90)	1.E+00	3.E+01
Tm-170	2.E+01	5.E+02
Yb-169	3.E-01	8.E+00
Au-198*	2.E-01	5.E+00
Cd-109*	2.E+01	5.E+02
Co-57*	7.E-01	2.E+01
Fe-55*	8.E+02	2.E+04
Ge-68*	7.E-01	2.E+01

Table B.1 Dangerous value, D Value. (Cont.)

Radionuclide	D value	
	(TBq)	(Ci)
Ni-63*	6.E+01	2.E+03
Pd-103*	9.E+01	2.E+03
Po-210*	6.E-02	2.E+00
Ru-106 (Rh-106)*	3.E-01	8.E+00
Tl-204*	2.E+01	5.E+02

* These radionuclides are very unlikely to be used in individual radioactive sources with activity levels that would place them within Categories 1, 2 or 3 and would therefore not be subject to the paragraph relating to national registries or the paragraphs relating to import and export control.

APPENDIX C

Content for a security plan

A security plan should include all information necessary to describe the security approach and system being used for protection of the source(s). The following topics should typically be included:

- A description of the source, its categorization, and its use.
- A description of the environment, building and/or facility where the source is used or stored, and if appropriate a diagram of the facility layout and security system.
- The location of the building or facility relative to areas accessible to the public.
- Local security procedures. —The objectives of the security plan for the specific building or facility, including:
  - the specific concern to be addressed: unauthorized removal, destruction, or malevolent use;
  - the kind of control needed to prevent undesired consequences including the auxiliary equipment that might be needed;
  - the equipment or premises that will be secured.
- The security measures to be used, including:
  - the measures to secure, provide surveillance, provide access control, detect, delay, respond and communicate;
  - the design features to evaluate the quality of the measures against the assumed threat.
- The administrative measures to be used, including:
  - the security roles and responsibilities of management, staff and others;
  - routine and non-routine operations, including accounting for the source(s);
  - maintenance and testing of equipment;

- determination of the trustworthiness of personnel;
- the application of information security; • methods for access authorization;
- security-related aspects of the emergency plan, including event reporting;
- training;
- key control procedures.

- The procedures to address increased threat level.
- The process for periodically evaluating the effectiveness of the plan and updating it accordingly.
- Any compensatory measures that may need to be used.
- References to existing regulations or standards.

VITA

Name and Surname Miss Jurairat Utsadee

Date of Birth 7 April 1981

Place of Birth Surin

Background Education

2005 Bachelor of Science in Physics, Kasetsart University

2012 Certificate in Radiation Protection and Safety of Radiation Source, Malaysia.

Position and Organization

Radiation Physicist at Bureau of Radiation Safety Regulation, Office of Atoms for Peace (OAP), Ministry of Science.