IAEA-TECDOC-1868

MEDICAL IRRADIATOR FACILITY CASE STUDY FOR THE NUCLEAR SECURITY ASSESSMENT METHODOLOGIES FOR REGULATED FACILITIES

COORDINATED RESEARCH PROJECT

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2019

CONTENTS

1. INTRODUCTION 1
   1.1. BACKGROUND 1
   1.2. OBJECTIVE 1
   1.3. SCOPE 1
   1.4. STRUCTURE 1

2. TERMS OF REFERENCE 1
   2.1. RATIONALE 1
   2.2. OBJECTIVE 2
   2.3. TASKS AND FUNCTIONS 2
   2.4. OUTCOMES 3

3. PREPARATION AND PLANNING 3
   3.1. REGULATION/POLICIES/GUIDELINES 3
   3.2. REQUIREMENTS 3

4. COLLECTING REQUIRED INFORMATION 3
   4.1. BACKGROUND 3
   4.2. CASE STUDY FACILITY CHARACTERIZATION 4
   4.3. CASE STUDY TARGET IDENTIFICATION 5
   4.4. CASE STUDY THREAT DEFINITION 5

5. CONDUCTING ASSESSMENTS 6
   5.1. PRESCRIPTIVE ANALYSIS 7
      5.1.1. Concept 7
      5.1.2. Radioactive source categorization 7
      5.1.3. Security objectives 7
      5.1.4. Assessment for gamma knife 9
      5.1.5. Assessment for blood bank irradiator 10
      5.1.6. Assessment for the research irradiator 11
      5.1.7. Conclusion for the prescriptive analysis assessment of UMC 13
   5.2. QUALITATIVE ANALYSIS —PAKISTAN NUCLEAR REGULATORY AUTHORITY QUESTIONNAIRE 14
      5.2.1. Concept 14
      5.2.2. Results and analysis 14
      5.2.3. Conclusion for the qualitative analysis assessment of UMC 15
   5.3. SIMPLE PATHWAY ANALYSIS — SIMPLE PATHWAY SPREADSHEET 15
      5.3.1. Concept 15
      5.3.2. Methodology 15
      5.3.3. Assessment for gamma knife 16
      5.3.4. Assessment for blood bank irradiator 17
      5.3.5. Assessment for research irradiator 17
      5.3.6. Analysis 18
      5.3.7. Conclusion for simple pathway analysis assessment of UMC 21

5.4. MODELLING AND SIMULATION ANALYSIS 22
5.4.1. Concept (AVERT) 22
5.4.2. Method (construction of model) 22
5.4.3. Scenarios 22
5.4.4. Results 23
5.4.5. Analysis 24
5.4.6. Conclusion for modelling and simulation analysis 25
5.5. TABLETOP EXERCISE 25
5.5.1. Process for using the tabletop evaluation method 25
5.5.2. Tabletop model and implementation 26
5.5.3. Scenario – adversary and response teams 27
5.5.4. Results – radioactive material unauthorized removal 27
5.5.5. Conclusion for tabletop exercise 29

6. OVERALL ASSESSMENT OF SECURITY ASSESSMENT METHODS 30
6.1. ASSESSMENT METHOD EVALUATION 30
6.2. EVALUATION AND GENERAL TRENDS 32
6.3. CASE STUDY CONCLUSION 34

7. CONCLUSIONS 35

8. RECOMMENDATIONS 36

APPENDIX I UNIVERSITY MEDICAL CENTRE - HYPOTHETICAL FACILITY INFORMATION 37
I.1. GAMMA KNIFE DESCRIPTION 37
I.1.1. Physical protection measures 37
I.2. BLOOD BANK IRRADIATOR DESCRIPTION 39
I.2.1. Physical protection measures 39
I.3. MEDICAL RESEARCH IRRADIATOR DESCRIPTION 40
I.3.1. Physical protection measures 41
I.4. UMC FACILITY - ADDITIONAL DETAILS 42
I.4.1. Facility Background 42
I.4.2. Facility security arrangements 43
I.4.3. Facility staffing 43
I.5. SOURCE CATEGORIZATION 44
I.6. THREAT STATEMENT 44
I.7. ASSUMPTIONS 45
I.8. SCENARIOS 46
I.9. SECURITY AND ADVERSARY CLASSIFICATIONS 48

REFERENCES 51

ABBREVIATIONS 53

LIST OF PARTICIPANTS 55

1. INTRODUCTION

1.1. BACKGROUND

This publication provides Member States with a hypothetical medical irradiator facility case study that demonstrates the standard nuclear security assessment (SA) methodology that was developed by the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP), Nuclear Security Assessment Methodologies (NUSAM) for Regulated Facilities.

1.2. OBJECTIVE

The objective of this publication is to demonstrate the risk informed, performance based methodological framework in a systematic, structured, comprehensive and appropriately transparent manner for a hypothetical medical irradiator facility. While the NUSAM project explored new approaches to nuclear security assessment, the established framework contained in Ref. [1] is consistent with recommendations and guidance provided in current IAEA Nuclear Security Series publications.

1.3. SCOPE

This publication utilizes the methodology framework contained in Ref. [1] to assess the performance of defined protection measures as described in the hypothetical facility description in Appendix I. The emphasis is on the methodological aspects of SA and is illustrated by the application of the methodological framework to hypothetical medical irradiator facility.

It is not appropriate to use this methodology where the security risks to materials and facilities are judged as requiring no more security than similar industrial and technological facilities that do not handle nuclear or radioactive materials.

1.4. STRUCTURE

This publication demonstrates the assessment methodology and compares various methods for assessment security performance for a hypothetical medical irradiator facility. It is intended to be a practical reference. This publication contains seven main sections following the introduction and one appendix.

Section 2 provides the terms of reference for the case study. Section 3 discusses the preparation and planning for an SA. Section 4 discusses the collection of required information for an SA. Section 5 discusses the tools and methods used for the conduct of the SA. Section 6 describes the overall summary of security assessment methods utilized for the SA. Section 7 provides the case study conclusions. Section 8 provides the case study recommendations.

Appendix I provides a hypothetical facility description and additional detailed information that was used to conduct the SA.

References in this publication provide links to important international publications, standards and other guidance publications relevant to NUSAM.

2. TERMS OF REFERENCE

2.1. RATIONALE

In order to illustrate the application of the methodological framework, a number of security case studies were considered. Each security case study had a dedicated working group to develop a model and perform a nuclear security assessment using the recommended methodological framework on that model. This provides Member States with detailed examples to illustrate the nuclear security assessment process.

The highest consequence facilities/activities expected to be relevant for Member States are nuclear power plants (Ref. [2]), spent fuel storage facilities, Category 1 source facilities, transport of Category 1 sources (Ref. [3]) and low enriched uranium fuel cycle facilities. These facilities/activities tend to have significantly different approaches for security. As a result of both of these factors, they were considered for inclusion as security cases for the NUSAM project.

Facilities using radioactive sources, such as medical facilities, are typically less protected than a site dedicated to the use of nuclear material or other radioactive material. This is because typical outcomes from an event of sabotage at a medical facility are less hazardous than outcomes from a nuclear power plant (NPP) or similar. Such facilities typically have more limited security and access control features, alarm stations and on-site guard force. In addition, the guard force is typically intended to protect the staff and civilian users (if any) of the facility rather than for the specific purpose of protecting radioactive material assets on the site. Such facilities exist in virtually every Member State, conveying a clear relevance to NUSAM project members. Adversary targets at such facilities are typically straightforward, usually involving the unauthorized removal or sabotage of a particular radioactive source or machine housing sources. Outcomes from a successful adversary action of sabotage or unauthorized removal will result in financial and psychological impact, as causing direct and significant harm purely from a radioactive source is difficult. Security measures are typically commensurate with this radiological consequence assessment.

2.2. OBJECTIVE

The medical irradiator facility case study working group needed to develop a detailed model of the facility to demonstrate the use and applicability of the NUSAM methodological framework, and the recommended information, tools and approaches developed by the methodological working groups. The development of security cases provides a basis for discussion of the many practical issues encountered when undertaking a nuclear security assessment, with the aim to reach broad consensus in as many areas as possible.

The purpose of this medical irradiator facility case study is to demonstrate to an operator how different assessment methods of radioactive source security compare, and consequently whether a performance-based approach is appropriate for their requirements. A performance-based approach is not a recommended requirement for radioactive sources, as documented in Ref. [4]. However, the Member State could use this method for high consequence materials, under a high-threat level, or in order to ensure the effectiveness of prescriptive measures against the threat.

2.3. TASKS AND FUNCTIONS

To realize the objectives of the medical irradiator facility case study working group within the overall objectives of the NUSAM project, the following broadly defined activities included:

- Defining each security case study in more detail and list the Guidelines/Regulations/Policies applicable to the case study;
- Compiling and describing the information needed for the security assessment;
- Developing detailed models and facility/activity specific information in a report based on the recommendations of the methodological working groups;
- Encouraging participation from each security case study working group in a methodological working group;
- Defining, considering and documenting information security concerns;
- Performing the security assessment for each security case study;
- Documenting lessons learned in terms of the application of the methodological framework to each security case study.

Throughout the project, the working group proposed and communicated any potential enhancements to the methodological framework to the Coordinating Group.

2.4. OUTCOMES

In order to produce the expected outcome, the medical irradiator facility case study working group:

- Produced a detailed model and information for the facility/activity; and
- Documented the assessment of the nuclear security system using the NUSAM methodological framework, including assumptions and rationales used in the assessment process.

3. PREPARATION AND PLANNING

3.1. REGULATION/POLICIES/GUIDELINES

Ref. [2] provides information on the specific security responsibilities for the State and for the operator. The State should create an independent regulatory infrastructure, supported by effective national legislature, to provide for the responsible, safe and secure usage of nuclear and other radioactive material.

Typically, the independent regulatory body and the country's legislature would codify regulation and policies for the State.

For this case study, the Republic of Lagassi has such a legislative infrastructure, which is primarily designed around the principles and guidance contained in Refs [5– 7] and the supporting Implementing Guides in order to adequately protect both radioactive and nuclear materials.

Ref. [5] describes a vulnerability assessment as follows:

> "A vulnerability assessment, also known as a security survey or security assessment, is a method for evaluating protective security systems. It is a systematic appraisal of the effectiveness of a security system for protection against an assessed threat (or DBT if one exists). The vulnerability assessment can be specific or general in nature, can be conducted locally by the operator or by the State/regulatory body, and can be used to help the development of regulations by the State/regulatory body or for demonstrating regulatory compliance of the operator."

Further information on vulnerability assessments is provided in Appendix III of Ref. [5].

3.2. REQUIREMENTS

The recommended requirement to protect facilities using radioactive material against a radiological sabotage act is based on Refs. [4–6]. The main security measures to be assessed in this case study are the abilities of the physical protection system (PPS) to prevent unauthorized removal of radioactive materials and ensure that unacceptable radiological consequences (URC) do not occur through sabotage acts at the hypothetical facility.

The purpose of this case study is to examine the applicability of five different assessment methods (prescriptive, qualitative, simple pathway analysis, modelling and simulation, and tabletop exercise) and to assess their suitability for purpose.

4. COLLECTING REQUIRED INFORMATION

4.1. BACKGROUND

Assessment of an effective nuclear security system includes the determination of the nuclear security system objectives, the proposed design or characterization of an existing nuclear security system, the evaluation of the design, and possibly a redesign or refinement of the system. To assess the objectives, facility/activity characterization must be completed and requires gathering information about facility/activity operations and conditions, such as a comprehensive description of the facility/activity, operating conditions, and nuclear security requirements as well as regulatory requirements. The

assessment would consider the effectiveness of a system of elements that work together to ensure protection rather than regarding each element separately.

The assessor identifies targets including vital areas. Determination of whether nuclear/radioactive materials are attractive targets is based mainly on the type of material and the ultimate goal of the adversary threat. This allows the assessor to know the objectives of the nuclear security system (what to protect against whom).

Following the facility characterization and target identification processes, the assessor uses the threat defined by the competent authority and other considerations, such as local conditions and factors about potential adversaries, including: intent, motivation, types, capabilities and the range of tactics.

4.2. CASE STUDY FACILITY CHARACTERIZATION

The University Medical Centre (UMC), a hypothetical facility using radioactive sources within the Republic of Lagassi, is located in a downtown city region alongside a large state university. The UMC employs approximately 500 people. The city has a population of 500,000, and the university has more than 20,000 students enrolled. There are several residences and apartment buildings located within 100 metres of the south-east side of the site. Other commercial park businesses occupy two of the other three sides as shown in Fig. 1.

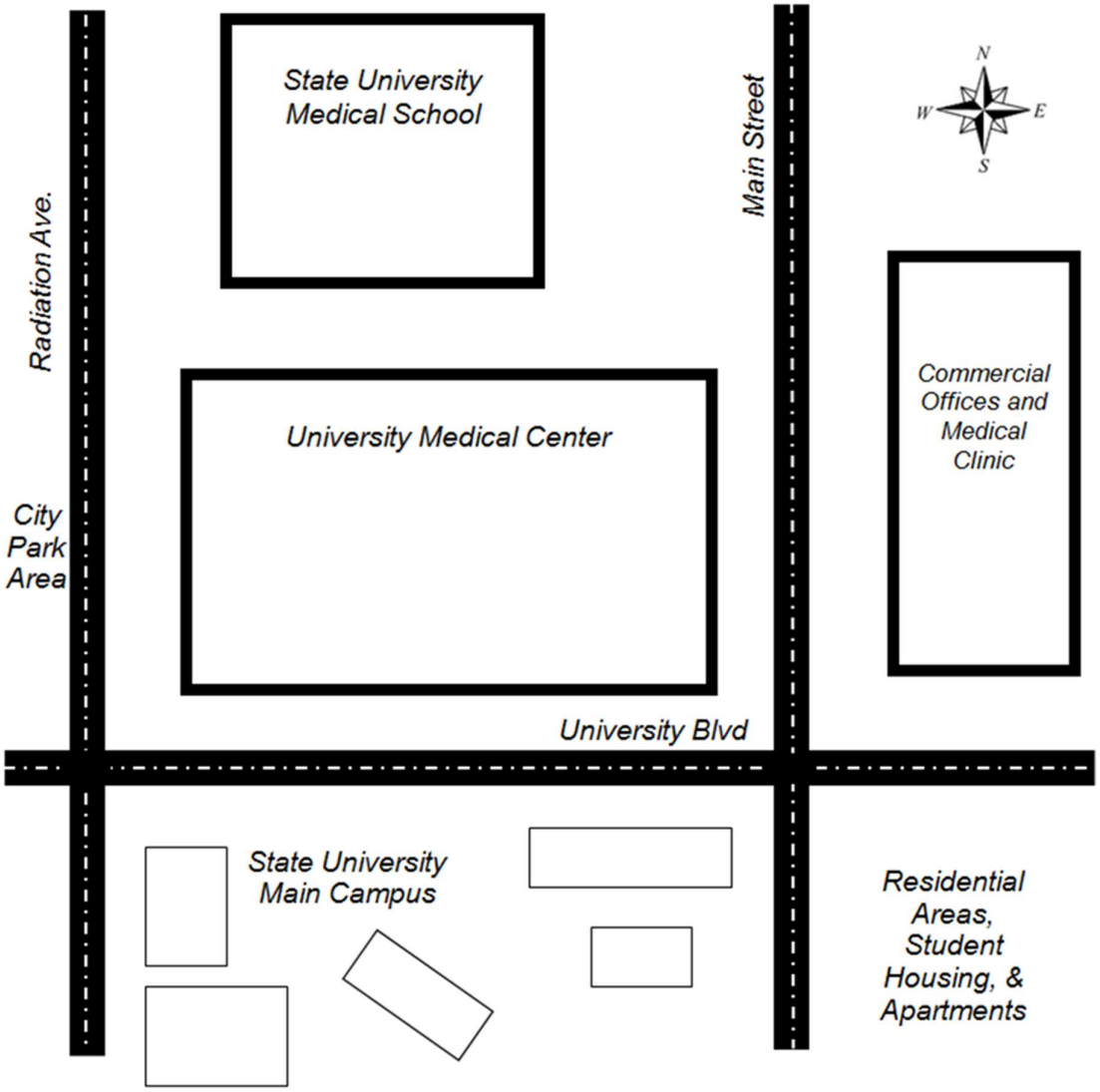


FIG. 1. Map of the University Medical Centre and the surrounding area

The UMC is located on a 200 metre^2 plot on the corner of Main Street and University Blvd as shown in Fig. 1. The hospital grounds are an open area with nearly direct vehicle access to the building on all sides. There is a landscaped 'sidewalk' (trees and the occasional boulder) along both University Blvd and Main Street, and city bus stops are located there as well. UMC is a multi-story hospital, but the research wing has only one floor and a basement. Nearly all research activity in the research wing is conducted in the basement.

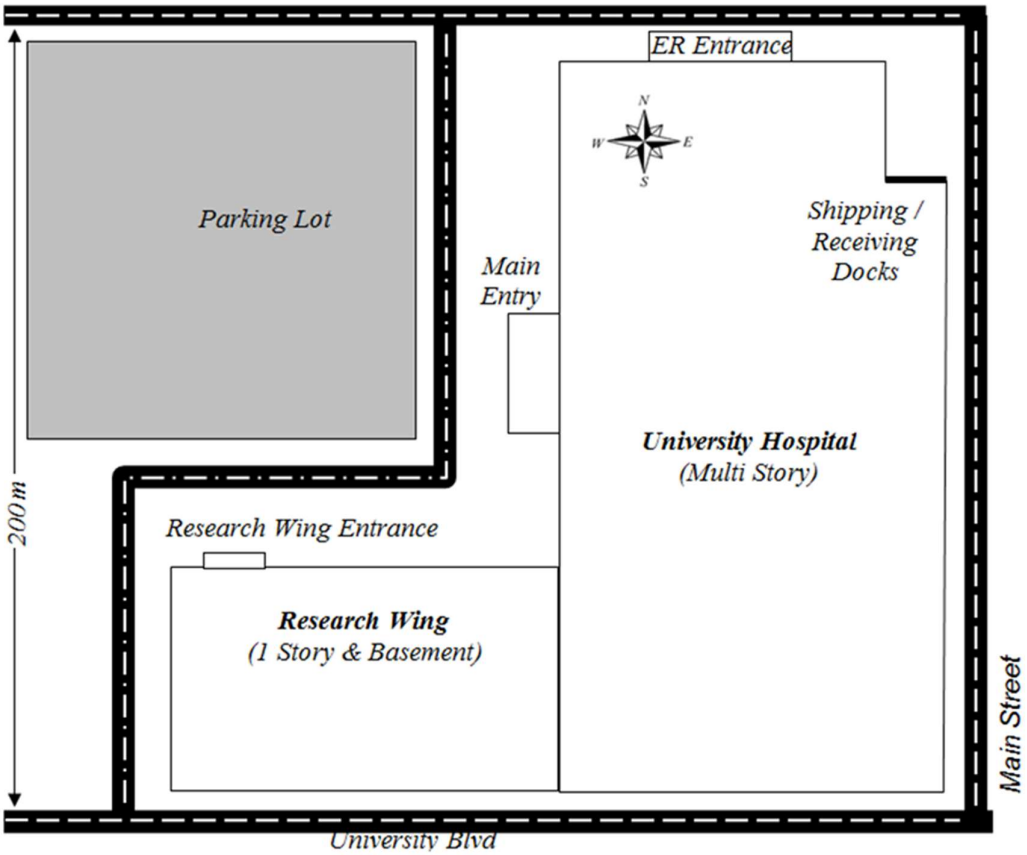


FIG 2. Map of the University Medical Centre site layout

A detailed facility characterization used in the various analyses methods is contained Appendix I and II. This includes specification of the protection and security features assessed in subsequent sections of this report.

4.3. CASE STUDY TARGET IDENTIFICATION

The purpose of the malicious act would be to steal radioactive material with the intention to use it maliciously elsewhere, or sabotage in-situ; to cause unacceptable radiological consequences, remove capability and equipment availability, or a combination of reasons. The exact target for any malicious action would be determined by the individual adversary's goals and therefore not wholly predictable – each source is potentially a target. Further details are available in Appendix I.5.

4.4. CASE STUDY THREAT DEFINITION

The State should have created a design basis threat (DBT) document following the guidance in Ref. [8] that provides advice on the potential malicious capabilities that the PPS should be designed to counter. Although most countries do not have a DBT specifically for the protection of radioactive sources, the same approach can be used to develop a realistic and credible threat definition. Appendix I.6 details the threat for this case study.

Insider threats based upon Ref. [9] need to be considered as part of a complete assessment.

Some competent authorities create generic potential adversarial forces documents that provide guidance on developing the scenarios describing the attack methodology of the potential adversaries. Full details of the assumptions made in target identification are detailed in Appendix I.7. The scenarios for the case study are detailed in Appendix I.8.

Infiltration and exfiltration times, as well as the time required to access or sabotage a source, were determined based on the type of adversary (see Appendix I.9).

The physical protection systems of facilities using radioactive sources within the Republic of Lagassi are designed and evaluated to defeat the following adversary acts:

- Radiological sabotage or unauthorized removal through direct physical attack or covert access that could cause unacceptable radiological consequences by a determined violent outsider assault or attack by stealth or deceptive actions. The following capabilities, numbers, equipment and assistance apply:
  - Up to 3 outsiders who are determined and willing to use violence during both day and night;
  - They will be well-trained in criminal trespass and in the use of tools for breaching barriers or facilitating entry;
  - They will be familiar with handling radioactive material;
  - They will be equipped with pistols;
  - They will have a vehicle for transporting radioactive sources from the site;
  - Insider assistance may be provided to the outsider adversary team by an authorized individual (e.g. staff, contractor, guard), in any position or role, through the willingness to participate by, for example, facilitating entrance and exit, disabling alarms and communications, etc. However, this person will not participate in violent activity.
- Insider Threat:
  - An individual (staff, contractor, guard…) in any position or role may try to steal radioactive material.
  - An individual (staff, contractor, guard…) in any position or role may damage or otherwise sabotage a source device to prevent its use.

The potential threats outlined above are manifested in the forms of: an insider, an activist team and an assault squad. Further information on the definition of these threats is contained in Appendix I.6.

5. CONDUCTING ASSESSMENTS

The assessment process has several steps based upon the NUSAM methodology.

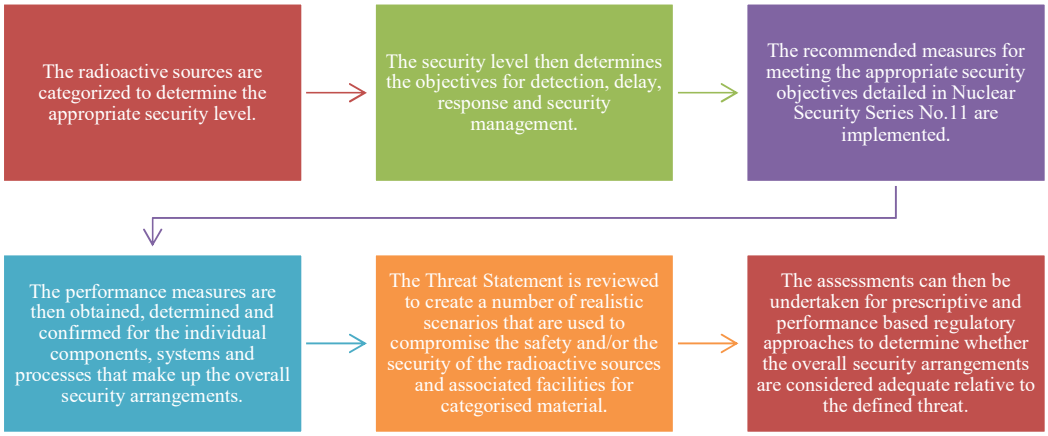


FIG. 5. Assessment process

Five assessment methodologies; prescriptive analysis, qualitative analysis, simple pathway analysis, modelling and simulation, and tabletop exercise are used in this case study. The results from each of the different assessment methods are compared and discussed in Section 6.

The assessment methods progress from simple to complex, increasing in time and effort required. As the complexity of the method increases, the potential learning on where enhancements can be made also increases. Conclusions are reported in Section 7 and recommendations are reported in Section 8.

5.1. PRESCRIPTIVE ANALYSIS

5.1.1. Concept

The prescriptive analysis method used in this instance is based upon Ref. [5]. Appendix I contains details of the protection and security arrangements subject to the assessment in the following sections.

5.1.2. Radioactive source categorization

The gamma knife and blood bank irradiator are Category 1 radioactive sources and are assigned to Security Level A, as detailed in Ref. [5]. The research irradiator is Category 2 and assigned to Security Level B (see Appendix I.1).

Section 4.3.1 and Tables 6 and 7 of Ref. [5] provide the recommended security measures (against unauthorized removal) for Security Level A and B respectively.

According to Table 4 in Ref. [5], the research irradiator is to be classified at Security Level A. However, for the purposes of this case study it was decided to treat it as Security Level B by assuming a certain age of the radioactive sources within. This allowed for variance in the analysis in the case study.

Refer to Appendix I.5 for the source categorization table (See Fig. I.5).

5.1.3. Security objectives

The security objectives cover four aspects of the physical protection system: detection, delay, response, and security management. The additional aspect of deterrence is presented here for completeness, but is not considered in the main body of the analysis due to its intangible nature.

Ref. [5] defines deterrence, detection, delay, response and security management as:

- "***Deterrence*** occurs when an adversary, otherwise motivated to perform a malicious act, is dissuaded from undertaking the attempt. Deterrent measures have the effect of convincing the adversary that the malicious act would be too difficult, the success of the act too uncertain, or the consequence of the act to the adversary too unpleasant to justify the undertaking. Measures designed specifically to deter thus involve communication to the adversary about the presence of measures performing the other security functions. If this communication has the intended effect, deterrence is the result.
- ***Detection*** is the discovery of an attempted or actual intrusion which could have the objective of unauthorized removal or sabotage of a radioactive source. Detection can be achieved by several means, including visual observation, video surveillance, electronic sensors, accountancy records, seals and other tamper indicating devices, process monitoring systems, and other means. Adversary awareness of detection measures can also serve as a deterrent.
- ***Delay*** impedes an adversary's attempt to gain unauthorized access or to remove or sabotage a radioactive source, generally through barriers or other physical means. A measure of delay is the factor of time, after detection, that is required by an adversary to remove or sabotage the radioactive source. Adversary awareness of delay barriers can also serve as a deterrent.
- ***Response*** encompasses the actions undertaken following detection to prevent an adversary from succeeding or to mitigate potentially severe consequences. These actions, typically performed by security or law enforcement personnel, and other State agencies, include interrupting and subduing an adversary while the attempted unauthorized removal or sabotage is in progress, preventing the adversary from using the radioactive source to cause harmful consequences,

recovering the radioactive source, or otherwise reducing the severity of the consequences. The prospect of successful response can also serve as a deterrent.

- ***Security management*** includes ensuring adequate resources (personnel and funding) for the security of sources. It also includes developing procedures, policies, records, and plans for the security of sources and for a more effective security culture, in general. This term also includes developing procedures for the proper handling of sensitive information and protecting it against unauthorized disclosure."

The recommended security level, as determined through the categorization of material, determines the respective security objectives as shown in Table 1.

TABLE 1. SECURITY LEVELS AND SECURITY OBJECTIVES

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 interrupt and prevent the unauthorized removal	Provide immediate initiation of response to interrupt the unauthorized removal	Implement appropriate action in the event of unauthorized 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 (see the Definitions)		
	Establish security event reporting system		

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

Further guidance can be found in Ref. [5].

5.1.4. Assessment for gamma knife

5.1.4.1. Detect

Security arrangements meet the first criteria of providing immediate detection of any unauthorized access to the secured area/source location. The area is equipped with passive infra-red (PIR)/microwave sensors, a balanced magnetic switch and closed circuit television (CCTV).

Security arrangements meet the second criteria of providing immediate detection of any attempted unauthorized removal of the source, including by an insider. There is an anti-tamper device located on the gamma knife that prevents access to the source.

Security arrangements meet the third criteria of providing assessment of detection. The area is under constant CCTV surveillance, although there is no information regarding the quality of the images provided or the area observed.

Security arrangements meet the fourth criteria of providing immediate communication to response personnel. There is a dedicated landline phone and all security staff members have two-way radios.

Security arrangements meet the fifth criteria of providing a means to detect loss through verification. The sources are under constant CCTV surveillance, as well as having tamper indicating devices and being in regular use.

5.1.4.2. Delay

Security arrangements meet the criteria of providing prescribed delay features for response personnel to interrupt the unauthorized removal. There are two barrier layers: (1) a door with security locks and a balanced magnetic switch and (2) the body of the gamma knife itself, which requires disassembly to access the sources.

5.1.4.3. Response

Security arrangements could be seen to meet the criteria of providing immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal, but quantification of actual response time against adversary operation time is not possible. Upon detection, two unarmed security personnel and one armed university police officer are instructed to respond to the alarm. If necessary, an additional armed police officer can respond. For events requiring further assistance, the 911 centre is contacted for additional support. Initial response time is estimated between 5 and 8 minutes, according to the case study document. No determination of the delay time associated with the physical protection system is provided.

5.1.4.4. Security management

Security arrangements meet the first criteria of providing access controls to the source location that effectively restrict access to authorized persons only. The shielding door is locked during out of hours and sensors are deactivated via personal identity number keypad.

Security arrangements do not meet the second criteria of ensuring trustworthiness of authorized individuals. While pre-employment background checks are conducted by an external company, the nature and depth are not proportional to the security level of the source, nor is the process periodically reviewed. There is no evidence that supervisors and managers ensure that personnel act responsibly and reliably. There is no information provided on a personnel security ‘aftercare’ programme.

Security arrangements are not defined with regards to the third criteria. The security of information is not detailed in the case study, though it is stated that knowledge about the gamma knife’s existence, and the isotope used, is common knowledge.

Security arrangements are not defined with regards to the fourth criteria. No detail of a security plan is given in this case study, but there is a reference to a security policies and procedures book. It is stated that during a period of increased threat (demonstration) the security measures were increased.

Security arrangements are not defined with regards to the fifth criteria. There is no information in this case study to suggest the existence of security contingency plans, but there is a reference to a security policies and procedures book. The UMC doubled security staff during a public protest.

Security arrangements are not defined with regards to the sixth criteria. Although there is allusion to reporting of incidents, no detail is given.

5.1.4.5. Prescriptive analysis assessment conclusions for the gamma knife

The security arrangements protecting the gamma knife are not adequate with regards to security management.

The gamma knife security may not be adequate with regards to response (difficult to quantify based on information available).

The UMC gamma knife security arrangements fail to meet the security management criteria due to a lack of proper vetting of staff, the lack of a formal security plan and a lack of associated details typically required to ensure appropriate response and reporting of incidents.

The prescriptive method employed does not provide an adequate assessment of the response criteria, as it is impossible to conclude if the 5–8 minutes estimated response is accurate or appropriate.

5.1.5. Assessment for blood bank irradiator

5.1.5.1. Detect

Security arrangements meet the first criteria of providing immediate detection of any unauthorized access to the secured area/source location. The area is equipped with PIR/microwave sensors, a balanced magnetic switch and CCTV.

Security arrangements meet the second criteria of providing immediate detection of any attempted unauthorized removal of the source, including by an insider. There is an anti-tamper device located on both blood irradiator devices that prevent access to the sources.

Security arrangements meet the third criteria of providing assessment of detection. The area is under constant CCTV surveillance.

Security arrangements meet the fourth criteria of providing immediate communication to response personnel. There is a dedicated landline phone and all security staff members have two-way radios.

Security arrangements meet the fifth criteria of providing a means to detect loss through verification. The sources are under constant CCTV surveillance, as well as having tamper indicating devices and being in use.

5.1.5.2. Delay

Security arrangements meet the criteria of providing delay sufficient for response personnel to interrupt the unauthorized removal. There are two barrier layers, though specifics depend upon access route. The first is either a door with security locks and a balanced magnetic switch, controlled by a video intercom and push switch system; or via a badge-swipe secured door. It is plausible that an adversary could access the blood bank via the window, but this is secured with a robust metal grid and would likely require specialist cutting tools or another method of bypassing the grid that would alert the guards. The second barrier is the bodies of the irradiators themselves; the sources are sealed within and require disassembly to access, though specifics as to the time required for disassembly are not specified.

5.1.5.3. Response

Security arrangements could be seen to meet the criteria of providing immediate response to an assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal, but quantification is challenging due to a lack of specific information. Upon detection, two unarmed security personnel and one armed university police officer are instructed to respond to the alarm. If necessary, an additional armed police officer can respond. For events requiring further assistance, the 911 centre is contacted for additional support. Initial response time is estimated between 5 and 8 minutes according to the case

study document. No determination of the delay time associated with the physical protection system is provided.

5.1.5.4. Security management

Security arrangements meet the first criteria of providing access controls to source location that effectively restrict access to authorized persons only. The video intercom and badge swipe systems are effective in allowing access to only authorized personnel.

Security arrangements do not meet the second criteria of ensuring trustworthiness of authorized individuals. While pre-employment background checks are conducted by an external company, the nature and depth are not proportional to the security level of the source, nor is the process periodically reviewed. There is no evidence that supervisors and managers ensure that personnel act responsibly and reliably. There is no information provided on a personnel security 'aftercare' programme.

Security arrangements are not defined with regards to the third criteria. The security of information is not detailed in the case study, though it is stated that knowledge about the blood bank irradiator's existence and the isotope used is common knowledge.

Security arrangements are not defined with regards to the fourth criteria. No detail of a security plan is given in this case study, but there is a reference to a security policies and procedures book. It is stated that during a period of increased threat (demonstration), the security measures were increased.

Security arrangements are not defined with regards to the fifth criteria. There is no information in this case study to suggest the existence of security contingency plans, but there is a reference to a security policies and procedures book. The UMC doubled security staff during a public protest.

Security arrangements are not defined with regards to the sixth criteria. While there is allusion to reporting of incidents, no detail is given.

5.1.5.5. Prescriptive analysis assessment conclusions for the blood bank irradiator

The security arrangements for the blood bank security are not adequate with regards to security management.

The blood bank security may not be adequate with regards to response (difficult to quantify based on information given).

The UMC blood bank security arrangements fail to meet the security management criteria due to a lack of proper vetting of staff, the lack of a formal security plan and a lack of associated details typically required to ensure appropriate response and reporting of incidents.

The prescriptive method employed does not provide an adequate assessment of the response criteria, as it is impossible to conclude if the 5–8 minutes estimated response is accurate or appropriate.

5.1.6. Assessment for the research irradiator

The research irradiator is a Category 2 source for this case study, subject to arrangements that meet Security Level B.

5.1.6.1. Detect

The security arrangements meet the first criteria of providing immediate detection of any unauthorized access to the secured area/source location. The area is equipped with PIR/microwave sensors, a balanced magnetic switch and CCTV.

Security arrangements meet the second criteria of providing detection of any attempted unauthorized removal of the source. There is an anti-tamper device located on the irradiator that prevents access to the source.

Security arrangements meet the third criteria of providing immediate assessment of detection. The area is under constant CCTV surveillance.

Security arrangements meet the fourth criteria of providing rapid, dependable communication to response personnel. All security staff members have two-way radios and CCTV operators have further access to communication devices.

Security arrangements meet the fifth criteria of providing a means to detect loss through verification. The source is under constant CCTV surveillance, as well as having an anti-tamper device.

5.1.6.2. Delay

Security arrangements meet the criteria of providing delay sufficient for response personnel to interrupt the unauthorized removal. There are two barrier layers: (1) a door fitted with security locks and balanced magnetic switch and (2) the body of the irradiator itself.

5.1.6.3. Response

Security arrangements could be seen to meet the criteria of providing immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal, though quantification is challenging. Upon detection, two unarmed security personnel and one armed university police officer are instructed to respond to the alarm. If necessary, an additional armed police officer can respond. For events requiring further assistance, the 911 centre is contacted for additional support. Initial response time is estimated between 5 and 8 minutes according to the case study document. No determination of the delay time associated with the physical protection system is provided.

5.1.6.4. Security management

Security arrangements meet the first criteria of providing access controls to source location that effectively restrict access to authorized persons only. There is a card reader with personal identity number keypad that disables the sensors in the corridor and irradiator room, allowing authorized persons to gain access. The sensors are active at all other times.

Security arrangements do not meet the second criteria of ensuring trustworthiness of authorized individuals. While pre-employment background checks are conducted by an external company, the nature and depth are not proportional to the security level of the source, nor is the process periodically reviewed. There is no evidence to suggest that supervisors and managers ensure that personnel act responsibly and reliably. There is no information provided on a personnel security 'aftercare' programme. Unsupervised access to the irradiator is only granted to staff once they are on an approved list; details of how an employee is deemed suitable to be on this list are unknown.

Security arrangements are not clear with regard to the third criteria. The security of information is not detailed in the case study, though it is stated that knowledge about the research irradiator's existence, and the isotope used, is common knowledge.

Security arrangements are not clear with regard to the fourth criteria. No detail of a security plan is given in this case study, but there is a reference to a security policies and procedures book. It is stated that during a period of increased threat (demonstration), the security measures were increased.

Security arrangements are not clear with regard to the fifth criteria. There is no information in this case study to suggest the existence of security contingency plans, but there is a reference to a security policies and procedures book. The UMC doubled security staff during a public protest.

Security arrangements are not clear with regard to the sixth criteria. While there is some allusion to reporting of incidents, no detail is given.

5.1.6.5. Prescriptive analysis assessment conclusions for the research irradiator

Irradiator security is not adequate with regards to security management.

Irradiator security may not be adequate with regards to response as it is difficult to quantify based on the information provided in the case study.

The UMC research irradiator security arrangements fail to meet the security management criteria due to a lack of proper vetting of staff, the lack of a formal security plan and a lack of associated details typically required to ensure appropriate response and reporting of incidents.

The prescriptive method employed does not provide an adequate assessment of the response criteria, as it is impossible to conclude if the 5–8 minutes estimated response is accurate of appropriate.

5.1.7. Conclusion for the prescriptive analysis assessment of UMC

According to the prescriptive requirements given in Ref. [5], the physical security of the UMC is, in general, adequate. There are concerns as to the sufficiency of the response criteria, but these need to be accurately quantified and confirmed by exercises. The most serious failing of the UMC is a consistent lack of security management; personnel security, information security (Principle L Ref. [7]), contingency planning (Principle K Ref. [7]) and poor security culture (Principle F Ref. [7]). The existing mechanisms are not suitable for purpose and it appears there are no mechanisms at all for several criteria. Extensive overhaul and re-evaluation is recommended to enhance performance in the security management area.

The guidance in Ref. [5] is comprehensive and highlights numerous issues that form the basis for a 'good' assessment to be undertaken, even in a hypothetical context. However, the prescriptive nature of using guidance in this way does create a degree of uncertainty in a number of areas. Accurately quantifying performance is extremely important in helping make the determination of whether security arrangements are suitable and adequate for purpose. The failings described above are typical of medical facilities, where culture and vetting are difficult to establish and/or maintain due to high staff turnover and the public nature of the facilities. This adds weight to the usefulness of Ref. [5] as a broad 'health check' type review.

There is potential variance in interpretation of some of the language used in Ref. [5]; for example, the phrase 'immediate detection' is not a universally specific phrase. The meaning and practical application in Country A could be that an adversary is detected with 10 seconds, but Country B could regard it as being within a minute. Furthermore, some may view that Ref. [5] may over-prescribe the security measures for a given source and meeting all the requirements would not be cost effective for the facility operator. This cost-effective analysis is difficult to determine using a prescriptive methodology as it provides no comparison between security options, nor does it consider additional detail or arrangements that may be relevant in forming a fuller understanding of applying a defence-in-depth or graded approach to the PPS. Levels of detail and specifics around the inventory of a facility are not covered; an irradiator that uses caesium chloride, in powder form, could be treated differently to one that uses a ceramic form of caesium, or a cobalt-60 (^{60}Co) source.

Additionally, prescriptive methods do not adequately take into account the DBT/threat statement (DBT/TS), and may not be reflective of the latest advice on adhering to regulatory requirements, or acknowledge the latest guidance on relevant best practice. By its very nature, a prescriptive methodology cannot account for, or clarify, every possible variable that bears relevance to source security.

The prescriptive methodology for this case study, based upon Ref. [5] provides relevant international guidance as to the levels of security expected for a given source across four important aspects: detection, delay, response, and security management. However, a security specialist is still necessary to provide advice to the operator on how to satisfy national and international guidance and/or state regulatory requirements. This specialist can also provide input on what constitutes an effective security system, which can somewhat degrade the value of the guidance.

In the absence of more specific national regulation, the checklist approach in Ref. [5] is certainly applicable to an initial assessment of the adequacy of the source security arrangements.

Performance could be improved by aligning the checklist approach with national regulation and supporting design, implementation and testing through national policing agencies.

5.2. QUALITATIVE ANALYSIS —PAKISTAN NUCLEAR REGULATORY AUTHORITY QUESTIONNAIRE[1]

5.2.1. Concept

The Pakistan Nuclear Regulatory Authority Questionnaire has developed a security assessment process which enables repeatable, reproducible evaluation of radiological facilities through use of a relatively simple audit-based approach. An electronic, software-based 'questionnaire format' is used, underpinned by a scoring or performance measure mechanism to provide a semi-quantitative tool. This enables a competent authority, regulator, or site operator to evaluate a facility and obtain an indication of the robustness with the associated security arrangements.

The questionnaire consists of a series of questions relating to the adequacy of security arrangements with each question assigned a weighting. The questionnaire covers areas such as: detection, delay, response, contingency planning, security management, personnel security, information security and security culture.

The software outputs a percentage score based on the answers provided. The requirements for the different security levels (corresponding to material category as described in Ref. [5]) are factored into the assessment software. There are fifty-three (53) questions for Security Level A, fifty-one (51) for Security Level B and thirty-four (34) for Security Level C, corresponding to the diminishing requirements from the highest to the lower security levels.

This software approach was used to evaluate the hypothetical medical irradiator facility, for the purposes of comparing and demonstrating alternate methods of security assessment.

5.2.2. Results and analysis

The questionnaire was completed for each of the sources. The results are graded in accordance with Table 2.

TABLE 2. QUALITATIVE SCORING MECHANISM

Score	>90%	≤90% but >80%	≤80% but >70%	≤70% but >60%	≤60%
Results	Satisfactory	Minimally Acceptable	Needs Improvement	Unsatisfactory	Not Acceptable

The results from the assessment are:

- Gamma knife
  - 63.4% if the assessor deemed the delay insufficient;
  - 66.4% if it was sufficient.
- Blood bank irradiator
  - 58.4% if the assessor deemed the delay insufficient;
  - 61.4% if it was sufficient.
- Research irradiator
  - 65.9%;
  - Sufficient delay is not considered for Security Level B.

The performance of the security arrangements for the individual radioactive sources within the UMC is graded 'unsatisfactory', with the blood bank irradiator scoring 'not acceptable' if the assessor considers the delay to be insufficient.

---

[1] The International Atomic Energy Agency (IAEA) and the National Nuclear Laboratory (NNL) acknowledge and thank the Pakistan Nuclear Regulatory Authority (PNRA) for allowing the use of their questionnaire software in this case study.

5.2.3. Conclusion for the qualitative analysis assessment of UMC

The UMC's overall security arrangements are shown to be 'unsatisfactory' by the questionnaire, with only slight variation observed between the different sources.

While the scoring system provides a measure of facility assessment, the main issue with this qualitative method is that it does not provide any specific details on how effective the security arrangement components perform individually; there is no indication of whether delay is lacking, or whether security culture is poor. The only output is that the user has indication of the overall score for the facility. Additionally, the user would need to have a reasonable knowledge of security in order to answer some of the questions; particularly if delay is sufficient, which is usually a complicated question to answer even for a specialist.

This method does not take into account adversary capability, the defence-in-depth concept, graded approach, comparison of arrangements, cost effectiveness, DBT/TS, insider threat, relevant best practice and other details of the overall security arrangements. The weighting system is not visible to the user and quantifying the benefits of certain countermeasures is not as 'clear' as having a barrier such as a wall being worth specific percentage points. There is no clear interplay between the concept of having adequate detection and the subsequent adequate delay.

The qualitative method is mainly useful for self-assessment by operators and serves as an indication as to whether or not there is a need to be considering investing in improving security or employing specialist security analysts. Qualitative assessment cannot realistically be used as a standalone method except for providing an initial self-assessment.

5.3. SIMPLE PATHWAY ANALYSIS — SIMPLE PATHWAY SPREADSHEET

5.3.1. Concept

The simple pathway methodology analyses the time requirement of the possible routes (paths) an adversary could take to reach a given target and carry out a malicious act (sabotage or unauthorized removal) using an excel spreadsheet. If the time it takes an adversary to bypass all of the security arrangements is greater than the response time of security forces, then this provides an indication that the security arrangements are considered adequate. The methodology allows the failure of a security measure (detection, delay or response force procedures) to be considered and the impact that will have on the effectiveness of the PPS to be analyzed.

5.3.2. Methodology

It is first necessary to determine the target for the assessment and the purpose of the malicious act, unauthorized removal or sabotage of radioactive material. Then all the possible pathways available to an adversary are considered. This list of pathways is then simplified by removing indirect, inefficient or otherwise illogical paths. An option to reduce the assessment task is to combine similar paths into a single, or fewer, paths. This process is introduced in Section 5.3.3

The security arrangements that an adversary would encounter are considered and documented in the spreadsheet on a path-by-path basis. The possibility of detection at each point on the path is considered, including dependencies for detection and potential insider influence(s). A time delay is also assigned to each security feature with travel time between path points also accounted for.

For the purposes of this study, potential adversaries and security features (separated by type) in the UMC were assigned a 'class'. The different classes were then compared in a matrix, with each adversary class being considered against each security class to produce a delay time (see Appendix I.9.). Delay time was informed by expert knowledge, but can easily be changed to adhere to national standards. The matrix is shown in Table 3.

The total time taken for the path, factoring in if detection occurs at each point (when detection is possible), is calculated for each adversary type. This information is then used to determine the available time for response forces to reach denial points, including escape prevention points. Knowing the response time of the UMC security personnel to those denial points allows for an interpretation to be made on whether the PPS will be successful in preventative action for that particular path. Namely, if

an adversary can complete their malicious objective in a time less than the appropriate security response time, then the adversary will be deemed successful and the PPS as ineffective.

An initial denial is when security forces are able to prevent the adversary from bypassing the security measure that they are first detected at.

A final denial point is where the security forces have determined that an external malicious capability will not be allowed to proceed beyond under any circumstances, as they will not know if the attacker intends to commit an act of unauthorized removal or sabotage. It may be entry to a building, or a specific room or area of a building. To be able to prevent the adversary from bypassing the final security measure(s), this can entail the security personnel moving directly to the final denial point, regardless of where the adversary is first detected.

An escape denial point is when the security personnel are able to prevent the adversary from escaping the facility, either with the radioactive material or source (unauthorized removal prevention) or following an act of sabotage (such that the adversary can be held accountable in court for their actions).

5.3.3. Assessment for gamma knife

The case study threat definition (Section 4.4) is used to create the potential pathways to the target(s). For the gamma knife, twenty-one (21) possible paths exist and of these fifteen (15) are omitted due to inefficiency or are considered unrealistic. As the remaining 6 paths are similar and are able to be treated as such, this left one (1) pathway to analyze (Pathway A). Pathways were omitted for various reasons, most commonly because a pathway was long or otherwise indirect, or because it contained significantly more barriers than other paths.

The security arrangements on the remaining path were considered and implemented in the spreadsheet, with the entry linking to the time delay book within the spreadsheet. Then, a new row was entered for each possible point of detection. The spreadsheet was replicated and adjusted to suit each of the adversaries.

5.3.3.1. Pathway A

Considering an insider [Table 3], it is very unlikely that the UMC security personnel could respond in time to achieve an initial denial position but there is a reasonable chance they could achieve a final denial position – particularly if detection of the insider is made early. This is an inherent problem when dealing with insiders, as they tend to have at least some level of access to areas of the facility – thereby bypassing procedures for search, or simply circumventing physical protection or access control. Note that a final denial position can only be reached if the security personnel have knowledge of the intended target, which can be true from the secure area access detection point. This scenario leaves between 6 and 7 minutes for security to respond, whose average response time is around 6.5 minutes. Approximating from this, security would be able to provide denial of access approximately 50% of the time. Note that denial of access prevents any insider sabotage or unauthorized removal. Escape denial is slightly more likely to occur than denial of access, as the insider leaving the secure area will take approximately half a minute. Security has between 6.5 and 8.5 minutes to respond, which means that they would be able to provide escape denial in the majority of cases (estimated 80% prevention success). Note that providing escape denial will not prevent sabotage and consequently the adversary will achieve their objective if it is to sabotage.

Considering the activist team, it is again very unlikely the UMC security personnel could respond in time to achieve an initial denial position, especially if the activists are assisted by an insider. Achieving a final denial position is highly likely, even if the activists have insider assistance. Escape denial is also very likely – even if the security forces took the maximum expected response time of 8 minutes, they are still able to provide escape denial in around 80% of cases. If they respond with their average response time, they will always provide escape denial.

Considering the attack squad, the UMC personnel will never be able to provide initial denial. If the attack squad are detected at the first or second opportunity, there is a medium-low (~35%) chance the security personnel will be able to respond in time to provide final denial, but only if they are not assisted by an insider. Note that the usual caveat of the security forces having to have prior knowledge of the intended target applies, which is very unlikely in this case. Similarly, the security personnel are very unlikely to be able to provide escape denial.

5.3.4. Assessment for blood bank irradiator

For the blood bank irradiator, there are seven (7) viable pathways, with six (6) of those being similar. This leaves two pathways to consider, which are known as B and C. Note that for an exhaustive analysis, the 6 similar pathways would likely be broken down into 2 very similar, but different paths instead of the single path presented here. Pathways were logically omitted based on reasons similar to those for gamma knife pathways.

5.3.4.1. Pathway B

For an insider, UMC security personnel are unlikely to be able to provide initial denial in most cases. Providing final denial is much more likely and almost certain if the insider is detected early. Naturally, due to the nature of insiders, this is very unlikely as the insider would be authorized to be in those areas and even unusual behaviour is unlikely to prompt a response immediately. The chances for security personnel to respond in time to provide a final denial position are fairly good, but the likelihood of detecting or predicting the target early on is very low. The likelihood of preventing escape is medium-high; if the response force's response time is average, it is guaranteed to intercept the insider.

For an activist team, early detection would allow a final denial position to be guaranteed regardless of insider assistance being available. Generally, it is likely (approximately 80% - noting that security level A requires prevent) that security personnel would be able to provide final denial. This is not the case for initial denial, although if detection is made at the building boundary, there is a chance the security personnel can intercept if they respond in their fastest possible time (5 minutes). The security personnel are also very likely to be able to provide denial of escape. This applies to insider assisted and no insider assistance.

For an attack squad, under this scenario for the hypothetical medical irradiator facility, the indications of this assessment method are that the security forces are never able to provide initial denial. They are also very unlikely to be able to provide final denial, with the only chance being if they respond with a better than average time to a detection at the first point, with knowledge of the intended target. This scenario is in itself very unlikely. Escape denial is also very unlikely; the only chance being if the attack squad are detected at the first point of detection and they respond with their best possible response time of 5 minutes. This is regardless of insider assistance.

5.3.4.2. Pathway C

Considering an insider, there is little chance of providing an initial denial position, but a fairly good one of providing final denial, where an average or better response time will suffice. Escape denial is consequently very possible, where a response time of slightly worse than average will be sufficient.

Considering an activist team, initial denial is unlikely, especially with insider assistance. Final denial is likely, with a response time of worse than average being sufficient. The usual caveat of intended target identification applies. Escape denial is also very likely, with the necessary response time being 7.5 to 8 minutes; close to the maximum estimated response time of the security personnel.

For an attack squad, the security personnel have virtually no chance of being able to provide any form of denial, regardless of insider assistance or detection point. Note that in the best-case scenario, the security personnel have a maximum of three minutes to provide escape denial.

5.3.5. Assessment for research irradiator

For the research irradiator, there are twelve (12) available paths, of which paths five (5) through twelve (12) are similar, as are one (1) and two (2), and three (3) and four (4). These paths are labelled D, E and F respectively. For an exhaustive study, where a real facility was concerned, it is likely that every individual path would be considered.

5.3.5.1. Pathway D

For an insider, there is minimal chance for the UMC security personnel to achieve an initial denial position, with the only possible chance occurring at the source itself. Final denial is much more likely to occur. Only when detection is late and the response is below average will the security personnel fail

to provide final denial. The outcome is similar for escape denial, where only late detection and a very slow response will allow the insider to escape.

For an activist team, the security personnel have a very good chance of providing final denial and escape denial is almost certain. Initial denial is very unlikely, with the only possible point of initial denial being detection at the source housing and responding before the activists can penetrate the housing. Insider involvement significantly reduces the activist's operation time, but does not reduce it enough for the operation to likely be successful.

For an attack squad, the UMC security personnel have no chance of providing an initial Denial. They have a strong to reasonable chance of providing final denial if the attack squad are detected before they gain access to the basement. They have a small chance of providing final denial if the attack squad are detected before they gain access to the source area (research irradiator room) and virtually no chance if the attack squad is detected once inside the source area. The outcome for escape denial is very similar, where early detection provides a definite to very good chance to prevent escape, mid-operation detection offers a reasonable chance of prevention and late detection offers virtually no chance of preventing escape.

5.3.5.2. Pathway E

For an insider, the UMC security personnel have no chance to provide initial denial aside from at the source housing, where initial denial has a medium-low chance to occur. Final denial is certain for reasonably early detection, which itself is very unlikely. Later detection offers a medium chance for final denial. Escape denial is guaranteed for early detection (but itself very unlikely) and highly likely for later detection.

For an activist team, initial denial is impossible for all points but the source housing, where initial denial is fairly likely. Final denial is very likely even for late detection and virtually certain for early detection. Escape denial is almost certain, even for late detection. Insider assistance has very little influence in the effectiveness of the operation.

For an attack squad, the UMC security personnel have no chance of providing initial denial. Chances for final denial are reasonable if detection is made early on and non-existent for later detection. The outcome is similar for escape denial, where early detection facilitates a very good chance of denial and no chance of denial for late detections.

5.3.5.3. Pathway F

For an insider, the UMC security personnel have no chance of initial denial except for a medium-low chance at the source housing. Final denial is certain for early to mid-point detection and ranges from medium-low to medium-high likelihood for late detection. Escape denial is more likely than final denial, with escape prevention almost certain except for very late detections.

For an activist team, the UMC personnel have a very low chance to provide initial denial at the first point of detection, moderate chance to provide it at the source housing and no chance at the points in between. Final denial is certain for almost all points of detection, with detection at the source housing providing a very good chance of final denial. Escape denial is certain for all points of detection, with even detection at the source housing allowing 8 minutes for the security personnel to respond.

For an attack squad, the UMC personnel have no chance of providing initial denial. The likelihood of providing final denial is fairly good if detection is made early, very low for detection at mid-points and impossible for late detection. Escape denial is almost certain for early detection, medium-low for mid-point detection and non-existent for late detection.

5.3.6. Analysis

The threat matrix compiled from use of the pathway assessment method in Table 3 demonstrates the effectiveness of the UMC's security arrangements on a strictly numerical basis. While generally positive, it is important to consider the context mentioned in the previous sections.

The generally good performance in the escape denial category hides another issue: escape denial does not prevent acts of sabotage. While it is positive that the risk of unauthorized removal is generally very low, sabotage itself is a serious threat in terms of cost, resource availability and service operation

implications. Additionally, a successful sabotage operation may signal to other malicious groups that radioactive sources are not as secure as is understood.

The performance with regards to initial denial is very poor. This reflects the fact that the majority of the delay features within the UMC's security arrangements are inherent to the source housings.

The actual likelihood to provide final denial is lower than is presented in Table 3. As in the majority of cases, early detection of an adversary would not necessarily translate into a final denial position as the intended target of the adversary would not be clear. The same is true for escape denial.

TABLE 3. SIMPLE PATHWAY DENIAL PROBABILITY MATRIX

Target	Pathway	Adversary	Initial denial likelihood	Final denial likelihood	Escape denial likelihood
Gamma knife	A	Insider	Very Low	Moderate	High
		Activist Team	Very Low	High	Very High
		Attack Squad	None	Very Low	Very Low
Blood bank irradiator	A	Insider	Low	High	High
		Activist Team	Very Low	High	High
		Attack Squad	None	Very Low	Very Low
	B	Insider	Low	Moderate	High
		Activist Team	Low	High	Very High
		Attack Squad	None	None	None
Research irradiator	A	Insider	Very Low	High	Very High
		Activist Team	Very Low	High	Very High
		Attack Squad	None	Moderate	Moderate
	B	Insider	Very Low	High	High
		Activist Team	Low	Very High	Very High
		Attack Squad	None	Low	Moderate
	C	Insider	Very Low	High	Very High
		Activist Team	Low	Very High	Very High
		Attack Squad	None	Very Low	Moderate

The insider adversaries also have unrestricted access to certain areas. While this is accounted for in the spreadsheet in terms of delay times, the effect on detection is not wholly accounted for. The most likely scenario is that an insider would be able to access the source housing before any serious concern was raised in the eyes of security personnel. This means that the necessary response time is actually equal to the time the insider needs to gain access to the source – which itself is fairly difficult to quantify. The actual time it takes to dismantle the source housing is largely dependent on the available tools and the skillset of the adversary. The actual skill level of the insider is difficult to predict, they could have witnessed a source replacement on the gamma knife, or may have had frequent access to the target source and have some level of familiarity with the internal structure of the machine. It is also possible that they have no expertise whatsoever. Actual access time could be as little as a few minutes.

Having identified the issues above, a level of realism can be applied through subject matter expert judgement, facilitated by the flexible nature of the simple pathway methodology which allows for qualitative adjustment to quantitative results.

An updated table (Table 4) demonstrates where the early detection and insider access issues are accounted for in a conservative manner. The final denial and escape denial likelihoods have been shifted down one stage for the activist team and attack squad and two stages for insiders. Additionally, the initial denial likelihood for the insider has been reduced to 'very low' in blood bank irradiator Pathway A to reflect the fact that detecting an insider prior to them accessing the source area is virtually impossible.

TABLE 4. SIMPLE PATHWAY REVISED DENIAL PROBABILITY MATRIX

Target	Pathway	Adversary	Initial denial likelihood	Final denial likelihood	Escape denial likelihood
Gamma knife	A	Insider	Very Low	Very Low	Low
		Activist Team	Very Low	Moderate	High
		Attack Squad	None	None	None
Blood bank irradiator	B	Insider	Very Low	Low	Low
		Activist Team	Very Low	Moderate	Moderate
		Attack Squad	None	None	None
	C	Insider	Very Low	Very Low	Low
		Activist Team	Low	Moderate	High
		Attack Squad	None	None	None
Research irradiator	D	Insider	Very Low	Low	Moderate
		Activist Team	Very Low	Moderate	High
		Attack Squad	None	Low	Low
	E	Insider	Very Low	Low	Low
		Activist Team	Low	High	High
		Attack Squad	None	Very Low	Low
	F	Insider	Very Low	Low	Moderate
		Activist Team	Low	High	High
		Attack Squad	None	None	Low

The alterations to the probability matrix allow a better view of the effectiveness of the UMC's security arrangements. It is evident that there is virtually no chance of initial denial for any adversary choosing any path – which is largely to be expected for a public facility such as the UMC. However, being a facility that is designed to encourage public access, it is not excusable to also allow easy access for malicious groups. A perimeter access control method can be adopted, where public entry can be managed through controlled channels. Controls of public access could be better controlled through a mechanism similar to the reception desk in the blood bank area, though this may prove too restrictive to emergency access.

Further, system performance for final denial is mixed. Activists generally perform the worst, with the attack squad performing best (as expected). Little difference is seen between paths, though the research irradiator seems to be the most secure source, most likely a result of the generally longer path length.

There is a low or less chance of final denial in around two thirds of cases.

The likelihood of escape denial is the highest of the three denial types. Notably there is a high chance of the activist team being intercepted prior to escape for all paths, except for the blood bank irradiator A. The attack squad are able to successfully steal both the gamma knife and blood bank irradiator sources with no possibility of interception and to steal the research irradiator source with only a low chance of being intercepted. Generally, an insider would also be able to successfully steal any of the sources, with a low chance of interception in all but two cases.

Internally, an improvement in security culture would likely serve to dissuade insider action and reduce the threat or possibility of coerced action.

5.3.7. Conclusion for simple pathway analysis assessment of UMC

The UMC's security arrangements generally perform very poorly when subjected to the simple pathway methodology. Most adversaries have a reasonable chance to successfully conduct an act of sabotage or unauthorized removal of any of the UMC's three sources with minimal resistance. An adversary with capabilities comparable to that of the attack squad is disconcerting, in that it has the ability to cause a high consequence event but fortunately it is very unlikely to occur. The most probable, and challenging, threat is that of an insider, who has the capability to bypass not only security measures, but also mitigate any suspicions of security personnel, are highlighted by the low interception chance. The UMC would need to comprehensively rethink its security arrangements to ensure security of their sources, though it will be difficult to maintain a balance of public accessibility and reliable security.

The simple pathway method's main strength is that it quantifies the delay of the security system and response time of the security personnel with respect to the operational time of the adversary. While this is only an estimate, national standards and exact measurements can be used to provide a reasonably accurate delay time. Response time of security personnel can be quantified exactly through timed exercises. Additionally, applying context to the numerical output of the simple pathway method allows a fairly in-depth analysis of the robustness of the security arrangements. Clearly, the method is highly dependent upon the quality of the data provided. The method gives a rough guide as to the amount of security required for a given source and consequently does provide a general cost effectiveness estimate.

Although the simple pathway methodology is not without issue, it is positive that it provides quantification on the delay and response categories but does not consider detect or security management categories. That is, it does not provide information on how likely it is that an adversary will be detected at each stage and consequently leaves uncertainty in the system when early detection facilitates adequate response and when late detection does not. The numerical outputs of the method are approximations and cannot be taken to be exact results, simply a useful estimation of system parameters. Other issues include a lack of DBT/TS integration, no comparison of security options, no defence-in-depth or graded approach consideration and no thought for relevant best practice. It does not provide context with regards to source category either.

An additional benefit of the simple pathway methodology is that it can be expanded upon to include things such as detection probability and barrier comparison (e.g. Class 3 versus Class 2 door). The simple pathway method also allows a security professional to provide guidance based on actual relevant figures; and therein lies the weakness of simple pathway, no context is provided – the focus is purely on numerical interplay between detect, delay and response. No consideration is given to the maintenance of the systems or any other security management practice. The results of the simple pathway assessment reflect the physical protection system operating from a mathematical perspective.

However, the pure numerical focus of the simple pathway method is also its strength. Such information allows for a security professional to make an informed decision in their assessment of a facility based upon auditable evidence. This further facilitates making qualitative adjustments to the quantitative results. A subject matter expert can use the quantitative information to inform their adjustments. Additionally, quantifying questions such as "how bad is it?" can be answered at the executive level, allowing for stronger buy-in by upper management, and support for a proportional response.

Pathway methodologies are extremely flexible in terms of the level of detail that can be achieved in the assessment. The intentionally designated 'simple' method demonstrated here is an entry-level example of pathway methodologies and is intended to provide a representative view of pathway methods as a whole.

5.4. MODELLING AND SIMULATION ANALYSIS

The case study used the ARES AVERT Version 7.1 security assessment software package and Google SketchUp 2014 for the model creation. Other security assessment software packages and model creation packages are available.

5.4.1. Concept (AVERT)

AVERT is a computer-based security vulnerability assessment package produced by ARES Corporation. It uses realistic three-dimensional (3D) models of sites and facilities, a database for the performance of a PPS and potential adversary capabilities, and Monte Carlo methods to create simulations to determine whether or not an adversary attack would succeed. It is also a powerful analysis tool, integrating security arrangements (including barriers and detectors), guards and adversary parameters that can be helpful in determining the overall performance of the PPS detection, delay and response arrangements.

5.4.2. Method (construction of model)

Prior to the creation of any computerized facility models, it was decided that omitting the basement level and the research irradiator allowed for model simplification and a significant reduction in the required preparation work. A 3D model of the UMC Facility was then created using Google SketchUp. The model was imported into AVERT and the AVERT Library Version 3.1[2] was loaded. Following testing of the 3D environment with a placeholder adversary and successful remedial actions, the barriers and detectors were added. A test guard team was added. Then, the interaction between the guards, adversaries and detectors were tested. The trial results were found to be sensible, but not entirely reflective of the UMC case study due to a select number of inaccuracies in the modelling setup. Work was undertaken to remedy those issues, which required the inclusion of fire escapes and also forcing a guard response time to between 5 to 8 minutes. Those amendments meant that those issues were mostly resolved. The remaining issue of fire escape functionality was considered as having only a very minor impact on the overall assessment findings.

5.4.3. Scenarios

The scenarios were modelled using the DBT/TS malicious capabilities and are detailed in Appendix I.8. Each Scenario featured four (4) attack plans (different adversary pathways) and one-hundred (100) runs of each plan (repeated simulations). See Tables 5 – 7.

[2] A generic performance library provided as part of software

5.4.4. Results

TABLE 5. FULL RESULTS FROM AVERT SIMULATIONS FOR EACH SCENARIO

Scenario	Adversary	Target	Objective	Plan 1		Plan 2		Plan 3		Plan 4	
				P(e)	%D	P(e)	%D	P(e)	%D	P(e)	%D
1	Insider	GK*	Unauthorized removal	100	6.0	100	8.5	100	9.0	100	7.5
2	Attack Squad	Either	Unauthorized removal	0	100.0	1	99.5	0	100.0	0	100.0
3	Insider	BBI*	Unauthorized removal	98	3.0	98	3.0	95	7.0	99	3.5
4	Insider	GK	Sabotage	52	74	57	50.5	53	55.0	59	70.5
5	Activists Team	GK	Unauthorized removal	99	9.5	99	28.5	99	14.5	97	12.5
6	Activists Team	BBI	Sabotage	100	3.5	100	1.0	100	3.5	100	2.5
7	Activists Team	BBI	Unauthorized removal	94	7.0	95	6.0	96	5.0	94	6.5
8	Attack Squad	BBI	Unauthorized removal	0	100.0	0	100.0	0	100.0	4	98.0
9	Attack Squad	GK	Unauthorized removal	7	96.5	7	96.5	13	93.5	9	95.5
10	Attack Squad	GK	Unauthorized removal	8	96.0	11	94.5	6	97.0	7	96.5

*: GK = gamma knife; BBI = blood bank irradiator

P(e) is the overall probability of effectiveness of the system and %D is the percent damage to the target.

TABLE 6. AVERAGE RESULT FOR UNAUTHORIZED REMOVAL/SABOTAGE FOR EACH SCENARIO

Scenario	Adversary	Target	Average adversary success rate (%)		Average adversary operation time (unauthorized removal)
			Sabotage	Unauthorized removal	
1	Insider	GK*	7.8	0	14m 55s
2	Attack Squad	Either (BBI* shown)	100	100	6m 0s
3	Insider	BBI	4	2	5m 5s
4	Insider	GK	63	45	13m 46s
5	Activists Team	GK	16	1	15m 44s
6	Activists Team	BBI	3	0	4m 55s
7	Activists Team	BBI	6	5	5m 52s
8	Attack Squad	BBI	100	99	8m 47s
9	Attack Squad	GK	96	91	14m 33s
10	Attack Squad	GK	96	92	6m 45s

*: GK = gamma knife; BBI = blood bank irradiator

TABLE 7. QUALITATIVE TABLE OF RESULTS FROM AVERT SIMULATIONS FOR UNAUTHORIZED REMOVAL/SABOTAGE

Target	Adversary	Sabotage prevention (or final denial likelihood)	Unauthorized removal prevention (or escape denial likelihood)
Gamma knife	Insider	High	High
	Activist Team	High	Very High
	Attack Squad	Very Low	Very Low
Blood bank irradiator	Insider	Very High	Very High
	Activist Team	Very High	Very High
	Attack Squad	None	None

5.4.4.1. Gamma knife

Scenarios 1, 4, 5, 9 and 10 target the gamma knife. As shown in Table 5, the gamma knife protection measures are not effective against the attack squad in Scenarios 9 and 10, but are effective in Scenarios 1 and 5 against the insider and activist team, respectively. However, the protection measures are less effective in Scenario 4, another insider scenario.

5.4.4.2. Blood bank irradiator

Scenarios 2, 3, 6, 7 and 8 target the blood bank irradiator. As shown in Table 5, the blood bank irradiator protection measures are not effective against the attack squad in Scenarios 2 and 8, but are effective in Scenarios 3, 6 and 7 against the insider and activist team.

5.4.4.3. Research irradiator

In order to simplify the model, the research irradiator was not included in the AVERT modelling. The results from the gamma knife and blood bank irradiator are representative of the method.

5.4.5. Analysis

The usage of AVERT allowed for accurate analysis of the PPS delay (including detection systems) and the response time of the guard force. It gave definitive answers in a variety of scenarios as to whether the detect, delay and response were sufficient, as well as allowing for an in-depth analysis of what was happening in each scenario. A limited selection of analysis is presented below.

The average operation times for Scenarios 3, 6 and 7 are low compared to the other scenarios (most notably Scenario 2, a ‘beyond DBT’ scenario). This was analysed further and was found to be a result of the system being highly effective; that is, the adversaries were interrupted and neutralized very quickly and AVERT regards this as the operation being complete. In these instances, the PPS can be regarded as being highly effective and learning can be extracted from the scenario runs as to why the system behaved in such a way.

When the adversaries were successful in stealing the target source in Scenario 3 (2% of the time), the average operation time for those successful runs was around 15 min 30 s. It took around 18 min 30 s for adversaries to reach the source (sabotage goal) in Scenario 6 and the average time for a successful unauthorized removal in Scenario 7 was 23 minutes. These figures are much more in line with what would be anticipated in comparison with operational times for the other scenarios. However, the length of the operation, versus the expected response time of the guard force, suggests a prolonged exchange of fire, or some other delay that extended the operation time of the adversaries. Such an anomaly can prompt further investigation.

5.4.6. Conclusion for modelling and simulation analysis

The ability to test individual scenarios (including detection performance, delay, pathway, adversary and guard force/security arrangement variations) is extremely useful to a subject matter expert interpreting the vulnerability of the facility. Not only are operational times output, but average operational times are given across hundreds or thousands of runs, enabling consideration to be given to where the variance within any one scenario comes from. AVERT provides pathway analysis through mathematical nodal network modelling and can find the optimal path in terms of time, least detection and least vulnerability to firepower (from the adversary perspective). Similarly, guard posting arrangements, patrol strategies and response strategies can also be tested. In these situations, modelling and simulation tools can provide great insights with benefit far beyond an overall score for the facility in question; the ability to identify vulnerabilities and generate new adversary attack routes that the facility may not be aware of is of great value. The speed at which data can be generated is useful, as is the ability to quickly alter physical, or human, protection elements, as well as test new adversary tactics, pathways and capabilities. Such a function allows a subject matter expert to do a pseudo-sensitivity analysis and evaluate the defence-in-depth of a facility. Such knowledge may also allow a subject matter expert to infer an understanding of how important a proper security culture (and broader security management) is to the function of the facility's PPS.

However, AVERT provides analysis in terms of security management (and in fact assumes specified performance of both physical and human protection methods, as input by the subject matter expert, and relies heavily upon subject matter expert capability, resourcing and judgement. For this reason, AVERT, and similar modelling and simulation methods, are powerful tools in further assessing the interplay between detect, delay and response, but serve to supplement subject matter expertise, rather than replace it (in part or in its entirety) or provide comprehensive facility assessment in line with IAEA guidance.

Further, modelling and simulation tools do not include an ability to review cyber security at the facility, nor the impact that a cyber-attack may have on the PPS (blended attack concept).

5.5. TABLETOP EXERCISE

5.5.1. Process for using the tabletop evaluation method

The analysis approach for the manual evaluation method of a tabletop (TT) exercise is depicted using a common diagram (Fig. 6).

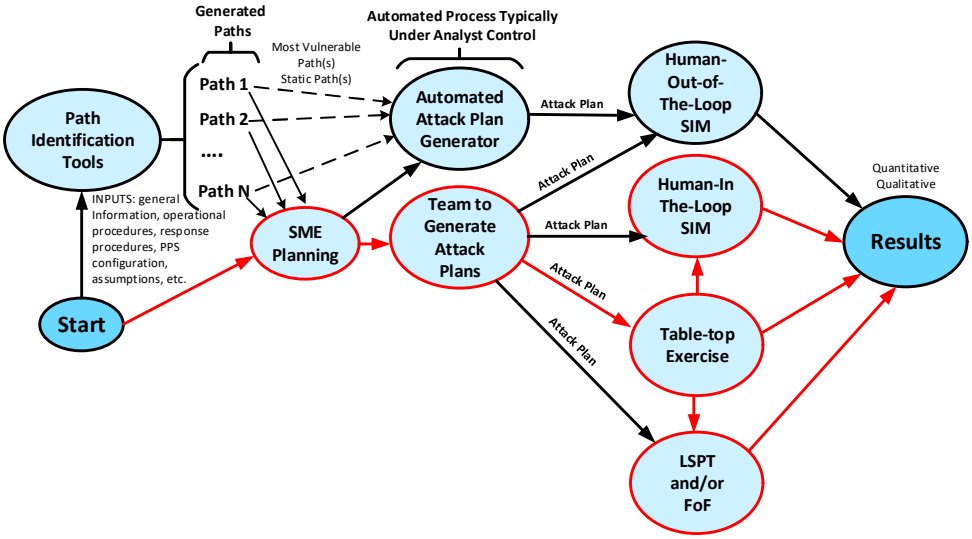


FIG. 6. Scenario analysis process overview for tabletops

The analysis process begins at the Start node. Prior to the planning process, general information is gathered about the facility or transport such as convoy configuration, route information, target configuration/packaging, etc. Based upon the provided information, a subject matter expert can create an adversary attack plan.

Table-top Purpose: To demonstrate how a manual analysis process can be applied to determine quantitative and/or qualitative information about the effectiveness of a physical protection system or security arrangements whether for a site, facility or transport activity.

Scope: The simulation can include secondary response forces as part of an overall contingency response to a security incident.

Objectives: To determine how effective the site, facility or transport operation is against relevant adversary scenario(s).

Adversary objectives: Unauthorized removal and/or sabotage of target material

The following highlight the termination conditions for the tabletop:

- Adversaries win if they complete their unauthorized removal of nuclear material or sabotage task or the response forces have been neutralized to the point there are no response forces that can engage the adversary on the rest of the scenario.
- Response forces win if adversary forces are degraded to the point that they cannot complete their task objective(s).

5.5.2. Tabletop model and implementation

A TT exercise is an analysis methodology intended to generate discussion of various issues regarding a particular facility or transport configuration. TT exercises have many benefits. They can be used to enhance general awareness of all parties responsible for the protection of assets or response to events. TT exercises are used to validate security plans and procedures, tactical response plans, rehearse planned changes or upgrades, and assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to, and recovery from a defined security incident. TT exercises are an excellent tool to facilitate nuclear security system or programme understanding. This method identifies strengths as well as identifying areas for improvement.

During a TT exercise, stakeholders are encouraged to discuss issues in depth and collaboratively examine areas of concern in order to solve problems. The effectiveness of a TT exercise is derived from the energetic involvement of participants and their assessment of recommended revisions to current policies, procedures, and plans.

TT exercises can range from basic to complex depending on the goal of the simulation and the desired accuracy in the outcomes. In a basic TT exercise, the goals are typically higher level in nature to discover obvious issues or to promote common understanding of the processes and plans to all stakeholders. Participants apply their knowledge and skills to a list of issues identified by stakeholders, site/transport management, and agency or national oversight organizations. The issues are systematically presented by a facilitator where the problems are discussed as a group who then simulate current methods for protection to determine if the issue(s) are factual and where the group could introduce change to improve the system. Using the table-top tool, the group 'upgrades' the system from the baseline then carries out additional simulations to evaluate the upgraded systems' response. The results and upgrades are documented for more analysis as needed. Basic TT exercise s can range from four hours (baseline) to 16 hours (or more) for a single scenario depending on how well the group works together and how many simulations are needed to meet the groups' goals.

In a more advanced TT exercise, the level of detail in the characterization process as well as the documentation requirements and validation of results process are more disciplined and precise. From an evaluation perspective there are literally unlimited ways to evaluate the nuclear security programme and its people's knowledge. Often the more advanced TT exercises are needed for the results to yield high confidence that the outcomes of the analysis are accurate. In many cases, individual actions of the protective system would need to be validated as accurate before the simulation can proceed to the next step. These more complex versions can utilize a very accurate and detailed 3D scaled model. The 3D models help confirm player actions, movements, and response timelines. Before the simulation begins,

it is common that the facilitator confirms the physical locations of response forces and the time required to respond to a specific event from those locations. Response times are confirmed either by the site's test data or by asking the 'real' players to perform an activity and collecting data on their actions.

Additionally, play can become more complex by introducing in-scenario cues. In these cases, play advances as players receive pre-scripted messages that may be in the form of statements of communications from the central alarm station or that events are happening on the site that those leading the response have to consider. An example is communication received of an explosion in the vicinity of a building of concern. These cues can be additional information to carry out the scenario or they may be intended to be distractions for the response to measure their knowledge and training of a tactical plan. A facilitator usually introduces cues one at a time in the form of a written message, simulated telephone call, videotape, or other means. Players discuss the issues raised by each cue, referencing established authorities, plans, and procedures for guidance. Player decisions are incorporated as the scenario continues to unfold. Player reactions to the cues are recorded and later graded for appropriateness or correctness.

During a TT exercise, all participants are encouraged to contribute to the discussion and be reminded that they are making decisions in a 'no-fault' environment. Effective TT exercise facilitation is critical to keeping participants focused on the exercise objectives and associated capability targets.

A transportation security TT exercise provides the operator or regulator with a tool to assess and evaluate the effectiveness of personnel, physical protection equipment, inter-agency planning and response coordination and overall radioactive material transport security policies and procedures.

Aside from the TT exercise methods, there are several other tabletop tools available. Each have their value in evaluating a nuclear security programme including:

- Vulnerability to Intrusion System Analysis (VISA)
- Criticality, accessibility, recuperability, vulnerability, effect and recognizability (CARVER).

All table-top methods rely heavily on the expert judgement of the subject matter expert(s) and the integrity of all persons involved so that the analysis conducted is based on the facts of the actual facility/transport system or on the defined parameters of a proposed upgrade. The facilitator is ultimately responsible for ensuring the best possible learning outcome.

5.5.3. Scenario – adversary and response teams

The adversary team consists of three (3) armed adversaries: A1, A2 and A3. The response team consists of two (2) armed guards: P1 and P2 and three (3) non-armed guards: G1, G2 and G3. G3 remains posted in the hospital security centre (HSC).

5.5.4. Results – radioactive material unauthorized removal

Unauthorized removal of radioactive material was considered as the primary objective for the three-person adversary team. To facilitate a successful mission, the adversary team has selected to conduct their unauthorized removal of radioactive material mission in the early morning hours (approximately 0200 hours) when facility staff were anticipated to be absent and the only opportunity for detection would occur via casual observation of video cameras, or other fixed detection systems that may be known or unknown to the adversaries. Using the shortest path to the room in which the gamma knife is located, the adversary team enters the research wing of the university hospital through the automatic glass doors on the northwest side of the building. The team proceeds down the hallway into the university hospital and breach an emergency exit door providing access near the gamma knife room. The team breach this emergency exit door (120 second delay) and then disable the cameras in the gamma knife room. Two team members begin the task to remove the radioactive source material from the gamma knife (600 second task time) while the third member stands in the hallway to provide cover for the task team. Once the task is complete (750 seconds into the attack), the team begins exiting the university hospital using the same path used during their initial entry. At 770 seconds into their mission, the adversary team successfully accomplishes their mission and removes the target material from the facility. Figure 7 depicts the events of this scenario.

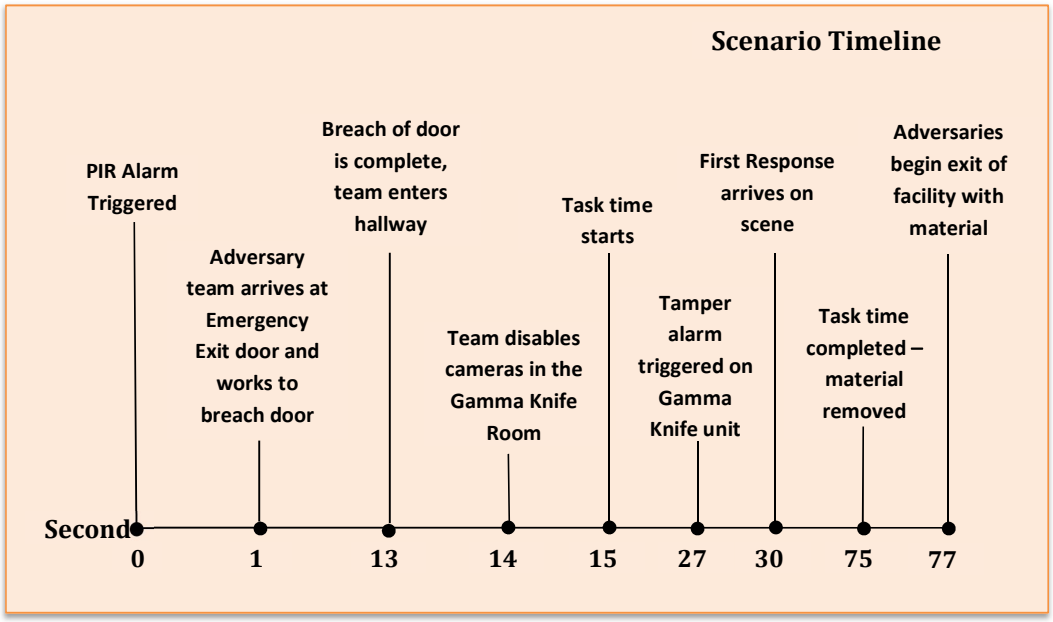


FIG. 7. Tabletop timeline for unauthorized removal of radioactive material scenario

Table 8 details the step-by-step events for each predefined measure of time for the scenario previously described.

TABLE 8. TABLE-TOP RESULTS – UNAUTHORIZED REMOVAL OF RADIOACTIVE MATERIAL SCENARIO

Blue	Time Hack (sec.)	Total Time (sec.)	Red	Blue KIA	Red KIA
HSC receives PIR alarm. Response initiated.	10	10	A2 Disables hallway camera.		
P1, G1 and G2 300 second delay to response points and P2 has a 480 delay.			A1 moves to door starts breach (120 Seconds).		
HSC receives multiple alarms from the Gamma Knife room.	120	130	A3 provides security at the entrance to the corridor leading to the Gamma Knife room.		
HSC sees two individuals entering the room.			A1 and A2 breach the Gamma Knife room door.		
HSC loses pictures from both interior Gamma Knife room cameras.	10	140	A1 and A2 disable cameras in Gamma Knife room.		
P1, G1 and G2 still responding.	10	150	A1 and A2 on task. (Task is 600 seconds; completed @ 750 seconds).		
HSC receives tamper alarm from the Gamma Knife.	120	270	A1 and A2 on task.		
P1, G1 arrive at the NW lobby entrance.	30	300			
G2 arrives at the SW stair well near the blood bank.					
P1 and G1 move tactically to the hallway to the double doors at the NIR and set up security.	100	400			
G2 provides rear security at the T intersection near the research wing and the EW hallway leading to the double doors.					
P1 moves inside of the double doors to a position 10 meters from the emergency exit door.	30	430			
G1 remains behind the double doors.					
P2 arrives at the hallway near the NSE.	60	490	Adversary task time complete and have material.		
	10	750	Adversary task time complete and have material.		
HSC receives PIR alarm in hallway outside of the Gamma Knife room.	10	760	Adversaries start exit from facility.		
P1 engages A3 with handgun 10m results A3 KIA.	10	770	Adversaries enter the hallway from the emergency exit.		A3
P1 engages A2 with handgun 10m results A2 KIA.			A2 engages P1 with handgun 10m results P1 KIA.	P1	A2
G1 and G2 take cover near stairwell entrance observe and report only.			A1 engages P2 with handgun 10m results P2 KIA.	P2	
			A1 up and moving to the NW lobby door and exits facility.		
Tabletop End State at 770 seconds as no other armed response available					

5.5.5. Conclusion for tabletop exercise

In this single iteration, the adversary forces were successful in achieving their objective.

TT exercise s can be as complex or as simple as required to identify the strengths or potential weaknesses of security arrangements. TT exercises can be also be used to evaluate complete systems, or elements of the system. They can be used to evaluate potential enhancements for security systems, against extreme adversaries, to determine if those enhancements are potentially effective.

A TT exercise requires security and operational specialists to participate in their roles, so that it is realistic, representation of arrangements and 'all' important interactions are assessed. This can make a TT exercise expensive to undertake, and requires diligent planning to appropriately challenge the participants and 'stress' the security arrangements.

A TT exercise does not easily allow multiple runs of the exercise to be undertaken due to time requirements, but it can allow portions of the exercise to be revisited to improve learning. The interaction of the armed malicious and response forces, can if not adequately considered, create potentially unrealistic outcomes if the response force is always neutralized in the first 'contact'.

The TT exercise is an effective method to evaluate the wider PPS, as it involves both the physical and technical components, and the response and procedures aspects.

6. OVERALL ASSESSMENT OF SECURITY ASSESSMENT METHODS

Following assessment of the facility by the different assessment methods, and using the method to derive a performance effectiveness value for the prescriptive method, it is possible to undertake a comparison and begin to understand the merits of the different approaches. The basis for these scores is found in Section 5.

The prescriptive score was estimated at 62.5% for all three radioactive sources, and the qualitative score was 63.4/66.4% for the gamma knife, 58.4/61.4% for the blood bank irradiator and 65.9% for the research irradiator. If, when performing the assessment, it was assumed that the delay provided by the existing systems was not sufficient, the average score for qualitative reduced to 62.6%.

The overall system effectiveness for each scenario and path was averaged for each method, giving results of 49% from AVERT and 52% from the simple pathway method, as shown in Table 9.

TABLE 9. SUMMARY OF OVERALL SECURITY SYSTEM EFFECTIVENESS AS DETERMINED BY FOUR ASSESSMENT METHODS

Method	Prescriptive	Qualitative	Quantitative	Modelling and simulation	TT exercise
Result (%)	62.5	62.6	52.1	49.2	ADV WIN

The results indicate a reasonable correlation and consistency between the four methods, although more detailed analysis identifies some interesting observations, most notable is the apparent performance 'grouping' of the prescriptive and qualitative methods, at ~62%; and the quantitative and modelling and simulation methods, at ~50%. There appears to be a step-change in overall effectiveness value when moving from the judgement-based, qualitative approaches, to the more complex numerical methods. Note that for the TT exercise, the adversary team was successful in the one iteration undertaken, though it was apparent that the outcome could plausibly be different.

There is disparity between them (some 12%) but this can be attributed to inherent differences between the methods. It is believed that the introduction of data and a systematic approach in both the pathway and in the modelling and simulation methods reduces subjectivity in the analysis and consequently leads to increased confidence in the outcome. This trade-off, of reduced overall performance against increased confidence in the result, is one of many identified through this study, which is explored further in the subsequent discussion. In particular, the individual methods provide different types of insights and may not be suitable for 'standalone' use.

6.1. ASSESSMENT METHOD EVALUATION

In order to explore some of the differences and trade-offs between the different approaches, a suite of assessment method factors (requirements) were identified and evaluated, as shown in Table 1.

TABLE 10. COLOUR MATRIX OF EACH METHOD AGAINST SEVERAL METRICS

Method	Prescriptive	Qualitative	TT exercise	Quantitative	Modelling and Simulation
Cost	Low – few hours to complete assessment.	Low – few hours to complete assessment.	Moderate – requires set-up and resourcing to run effectively. Actual run costs incurred low – preparation more significant.	Moderate – requires proficient use of spreadsheet to set-up relational tables, macros, etc. Performance data required for security features.	High – high initial licence cost; high-spec computing capability, performance data required. Days to create model and undertake analysis.
Data	Largely based upon judgement and experience of assessor.	Largely based upon judgement and experience of assessor.	Requires detail of facility layout, and understanding of guard and PPS arrangements, but only to a qualitative extent. Judgement and experience of exercise team required.	Data dependent approach, but extent is limited. Consequently, approximations can be used.	Data dependent approach. Requires considerable data, and verification to be useable. Standard libraries contain significant volume of data, but will require review of adequacy and alignment/adaptation to suit specific State or sector norms.
Complexity	Easy to apply evaluation using the existing Nuclear Security Series No.11 document and familiarization with the facility.	Easy to apply evaluation using the structured evaluation questions and familiarization with the facility.	Conceptually simple. Effectiveness relies upon the expertise of the exercise team. Requires clearly defined red team and blue team roles and responsibilities – as well as an 'independent' referee.	Conceptually simple, step-wise logic of activities and timings to achieve objective. Semi-automating via a spreadsheet approach requires strong capability in use of spreadsheets. Multiple data elements and inter-relational tables.	Very complex model, but easy user-interface. High level of user defined/user-modified data in the performance library to ensure accuracy. Relatively advanced computing skills necessary to build model of facility and introduce security features appropriately. Significant amount of data output generated.
Time	Few hours (approx. 3 for this study)	Few hours (approx. 5 for this study)	Preparation – several hours (approx. 8). Execution – several hours (approx. 2).	Approx. 24 hours for this study including population of performance data, etc.	Approx. 140 hours for first use, similar size model to take 40-50 hours thereafter depending upon level of detail required.
Skill and Knowledge Required	Easy to use for non-security specialist.	Easy to use for non-security specialist.	Dependent upon expertise and knowledge of the exercise team. Actions of adversary/guard force dependent on individual 'pilots'.	Requires proficiency with spreadsheets, and in-depth security assessment expertise.	In-depth security expertise, suited to multi-disciplinary teams, although can be performed by an individual with the correct skills. Additional expertise in model building required.
Reproducibility	Prescriptive, structured plain English assessment, although dependent upon quality of assessment/ reporting.	Simple question elements are reproducible enough, but subjective ranking questions introduce a lot of variability in interpretation.	Base scenario easily reproducible, but variance in individual choices as scenario unfolds and influence of P_h/P_k and other 'by chance' events can cause significantly different outcomes.	Data may introduce variance. Different users may analyse paths differently or choose different paths entirely. Methodology is very structured.	Complex model with variability in level of fidelity added. However, scenarios run/repeated within the same model environment (Facility) have excellent reproducibility of results. Edits to library, and input files (scenarios, threats, etc.) require appropriate quality assurance.
Transparency/ Auditability	Prescriptive, structured approach that allows for review of assessment but may involve judgement.	Structured questions, with capture of response provides enhanced transparency to overall performance and auditability but no real justification.	Preparatory and implementation stages are structured. Variance in execution due to individual influence, but this is recorded. Actions can be challenged/ explained.	Pathway analysis allows investigation of the parameters included and the assessment made.	Significant amount of data underpinning analysis. Full capture of the interactions and results within the model to incredible levels of detail. Possibility to lose/hide errors in the complexity. Requires significant effort to check input data and assumptions but detail is there to be investigated.

TABLE 10. COLOUR MATRIX OF EACH METHOD AGAINST SEVERAL METRICS (CONT.)

Method	Prescriptive	Qualitative	TT exercise	Quantitative	Modelling and Simulation
Robustness	Relatively simple evaluation of the facility at a basic level.	Relatively simple evaluation, although the structured evaluation format drives some structure to the assessment.	Logical and step-wise, but essentially a qualitative evaluation of how a scenario might play out. Many repetitions are needed to gain a balanced insight into facility performance. Adds 'human element'.	Logical, step-wise evaluation of the pathway, coupled with performance based assessment of time to traverse chosen/assessed route.	Comprehensive evaluation of all routes to/from objective, coupled with performance based assessment of all attributes within model. Monte Carlo analysis provides integrated sensitivity, and multiple permutations.
Flexibility	Prescriptive guidance that is material specific.	Much more flexibility in terms of facility and assessment of security countermeasures .	Preparation and implementation stages are structured, but the scenario being tested can be highly varied.	Highly flexible as method can be altered significantly depending on purpose. Incurs cost and time increases.	Model can be as simple or as complex as necessary to meet objectives of assessment. Performance parameters in library databases fully editable.
Functionality	Limited to its specific purpose.	Applicable to various facilities but still limited in terms of function.	Broad functionality, but any iteration and testing incurs significant time costs. Methodology can be altered, but requires further expertise.	Broader functionality but still limited to the strict methodology. Methodology can be expanded to perform additional functions.	Flexible tool enabling the user to evaluate and explore different configurations and options. Reporting, review and playback facilities enable intimate insight to the facility and security arrangements.
Risk-based	Prescriptive only. Some element of risk, dependent upon judgement of acceptability/adequacy by assessor.	Some element of risk dependent upon judgement of acceptability/adequacy by assessor.	Provides a qualitative insight into a particular scenario, but can be used to explore nuances of that scenario. Can be repeated to provide broader risk-assessment.	Provides quantitative analysis of each pathway assessed. Method can be expanded to include risk-based assessment.	Provides quantitative analysis of system effectiveness, allows user to determine acceptability of risk for different scenarios/threats and configure security system accordingly.
Confidence	Low – judgement based assessment approach.	Low – judgement based assessment approach.	Confidence in the scenario chosen is high, but performance in a particular scenario does not provide insight into other scenarios.	Good – systematic analysis of pathways.	High – comprehensive Monte Carlo evaluation of the facility with additional capability to test different security arrangements.
Overall Effectiveness	Provides quick and easy assessment for simple, low risk facilities.	Adaptation of prescriptive approach to provide some measure of performance and areas to focus enhancements.	Provides reasonable insight into a specific scenario subject to appropriate expertise. Can be further expanded to provide broader certainty.	Provides a transparent analysis of each pathway assessed to determine security arrangements.	Comprehensive analysis of the integrated security system via a Monte Carlo simulation. Enables easy reconfiguration and evaluation of options and cost-benefit analysis. Supports risk-based decision making.

(Courtesy of J. Edwards and J. Scott, National Nuclear Laboratory, United Kingdom)

6.2. EVALUATION AND GENERAL TRENDS

In order to simplify the analysis and comparison of how well the different methods achieved the requirements, the requirements were condensed into three broader topics: (1) resource — cost, knowledge, time and data, (2) quality — confidence, robustness, risk-based and functionality, (3) applicability — complexity, transparency/auditability, flexibility and reproducibility.

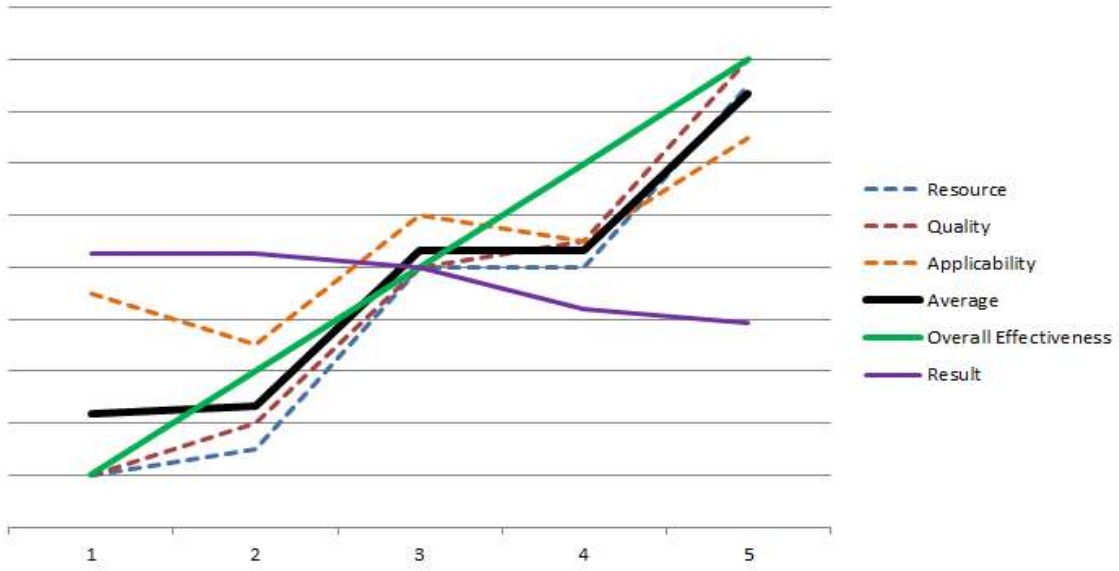
Each method was given a score against each requirement corresponding with the colour matrix where;

- Red = very poor;
- Light red = poor;
- Amber = moderate;

- Light green = good;
- Dark green = very good.

The scores for the requirements in each topic were summed and then averaged. An additional measure was constructed, an average of performance between resource, quality and applicability.

These were then plotted and compared to both overall effectiveness (as scored in Table 10) and the actual results given by the methods (see Table 9). The graph is presented in Fig. 8.



(Courtesy of J. Edwards and J. Scott, National Nuclear Laboratory, United Kingdom)

FIG. 8. Comparative graph of topics and results[3]

As a general rule, an increasing resource requirement translates into an increase in quality and applicability. This correlates well with overall effectiveness and the actual results if it is true that the quantitative and modelling and simulation method produce more accurate results.

For a facility using radioactive material, the presented methods appear to give realistic results that are all in the region of what would be considered a correct answer. It is arguable that the quantitative and modelling and simulation methods are more accurate in delay and response quantification but do not consider areas outside this such as information security and security management. The simpler methods tend to focus more on these contextual aspects of security, but in doing so provide valuable information that is otherwise missed by the quantitative and modelling and simulation methods.

In keeping with the above, it becomes apparent that one size does not fit all for security assessment – each method has its own niche and applicability that depends upon the user, the facility in question and the purpose of the assessment. Further points are discussed below.

When considering the prescriptive and qualitative methods, a fail on any one point is a direct fail of the facility. With modelling and simulation, and to an extent with quantitative methods, a fail on any one point may actually be compensated by a more sufficient part of the system. For example, susceptibility in delay mechanisms may be compensated with a strong response force presence. In modelling and simulation, this would be reflected by an adversary reaching a goal, but being defeated by the guard force. This would result in the same overall system effectiveness as if the delay mechanisms had been sufficient. Similar insights can be gained from TT exercises, provided an appropriate scenario is being tested. This insight helps to generate an understanding of defence-in-depth.

[3] Note that the TT exercise 'Result' was nominally designated '3' as the true result of '0' was non-representative in this analysis.

However, it is therefore important to engage in sensitivity studies when using modelling and simulation, table-top or quantitative methods to determine the critical components of the system. It may be that security professionals could learn from safety practice in this regard. A well-balanced security system would ideally not have any absolutely critical components, and a degree of flexibility through a combination of complementary defence-in-depth measures that allow the PPS to function optimally even when some part of the PPS may fail (through malicious intentions or otherwise).

The modelling and simulation method may well be considered too in-depth for an irradiator facility such as the UMC, but this still translates into a realistic representation of the strength and weaknesses of the method in comparison to the other methods. It is noted that a similar study on a nuclear facility may be beneficial in this context.

The inclusion of a tabletop study, which generally aligned with the results of the other methods, has allowed for comparison of prescriptive, performance and exercise based methods. Further validation would only be possible by inclusion of a force-on-force exercise. Indeed, force-on-force and tabletop exercises are generally utilized in conjunction[4], though typically focus on a particular scenario or type of scenario. Multiple runs are prohibitively expensive.

Exercise-based methods have the same drawbacks as the quantitative-based methods, and do not include security management or information security impacts (though these can be built into a scenario, they are not inherently a part of the evaluation). Most importantly, exercise based methods are extremely expensive, very complex to organize, run and evaluate. Exercise-based methods do offer a degree of flexibility for testing against more complex threat scenarios, such as insiders.

The suite of methods analyzed in this case study complement one another through their ability to draw out different aspects of facility security. It may be that the NUSAM project finds that using a combination of methods for any given application is the most appropriate route forward.

Actual usage of the above methods will be influenced by the operator's intention; whether the underlying security plan simply adheres to basic regulatory standards (and hence meets minimum requirements) or whether it strives for best practice will determine which method(s) are most suitable in any given case.

6.3. CASE STUDY CONCLUSION

This case study, part of the IAEA Coordinated Research Project on Nuclear Security Assessment Methodologies, aimed to evaluate the accuracy of several security assessment methods and their suitability for purpose. The five methods investigated were found to be in good agreement with one another and were, in turn, in agreement with what was anticipated. To that end, the methods are regarded as comparable but it is noted that each method has definite strengths and weaknesses that give each a niche in which to fit. Prescriptive methods are auditable, reproducible and cost effective to undertake, but offer little in the way of quantification or risk-based assessment. The qualitative method used offered a further degree of flexibility and functionality in exchange for reproducibility and auditability. The quantitative method used incurred a higher cost and required more security expertise, but associated confidence, robustness and overall effectiveness were all improved. The modelling and simulation method incurred significant cost, complexity and time requirements in exchange for the greatest level of confidence and a true risk-based, flexible and functional solution to security assessment. The tabletop exercise offered a level of realistic insight, but had similar drawbacks as the quantitative and modelling and simulation methods in that no evaluation of security management or information security was possible. No one solution can be regarded as the outright best, each method is appropriate for specific situations and offers insight into different aspects of security.

It may be that a combined method could be developed, where Member States with developing security assessment capability may wish to combine the prescriptive approach Ref. [5] with a modified simple pathway method to develop a baseline assessment of a given facility. For Member States with more advanced security assessment capabilities, an in-depth and repeatable software-based questionnaire may be appropriate for evaluating security management and culture, and the use of an advanced pathway

[4] See, for example, the NRC Frequently Asked Questions page on Force-on-Force exercises; https://www.nrc.gov/security/faq-force-on-force.html

method may be suitable for less complex facilities, and a modelling and simulation approach may be most appropriate to more complex facilities (such as power plants and bulk handling facilities).

7. CONCLUSIONS

Performance-based, risk-informed approaches have been developed and used to assess security effectiveness at facilities with the highest potential radiological consequences. There have been some efforts to similarly assess security of a Category I shipment of nuclear material. In the past several years, the methodologies developed for facilities with Category I nuclear materials have been adapted for nuclear power plants. Generally, the security arrangements at facilities with lower potential radiological consequences have not been as thoroughly or extensively assessed. These facilities have been secured more on the determination that a set of prescriptive requirements were in place and functioning. This approach does not confirm that there is adequate security as designed, nor whether the failure of an element or component of the security system will be appropriately replaced with the proposed or implemented compensatory measures.

The NUSAM CRP held its first meeting in April 2013. Security experts from more than a dozen countries agreed to meet the challenge of developing a performance-based, risk-informed approach for assessing security effectiveness at a broad range of sites, facilities and activities: Category I nuclear facility, nuclear power plants, low-enriched uranium fuel fabrication, reprocessing, radioactive materials use, spent fuel storage facilities, and nuclear and radioactive material in transit.

After three years, the NUSAM CRP has developed and validated a methodological framework. It has identified the necessary data required to perform such an analysis, how to collect the data, and how to use it to assess security effectiveness at a range of facilities and activities. It has identified a variety of tools that can be used to implement NUSAM. Those tools range from semi-quantitative tools that assess security at facilities with predominantly prescriptive requirements to complex computerized modelling and simulation tools that address those sites that have performance or outcome-based requirements. Techniques such as TT exercises and limited and full-scale performance tests, are equally adequate to be used for facilities with either type of security requirement.

In order to test the methodology and the associated tools, the project undertook three hypothetical case studies: a nuclear power plant which was developed from example facilities used in IAEA training activities; a Category 1 radioactive source in transit and a medical irradiator facility. Each case study used the NUSAM methodology to assess the effectiveness of the security arrangements using at least one of the assessment tools or methods. TT exercises were undertaken on each case study. Semi-quantitative approaches were used in one or more. Computerized modelling and simulation tools were used in two of them. In addition, the nuclear power plant case study was provided to three vendors, who modelled the facility and performed their security assessments; demonstrating how different modelling techniques may produce non-identical results, but are generally consistent in their overall outcomes.

The project team also performed TT exercises using two different approaches. A traditional approach of having all participants in the same physical location was used for the material transport and nuclear power plant. However, the TT exercise for the irradiator facility was performed despite having the participants in four locations on two continents.

The NUSAM project has successfully developed a methodology that can be appropriately used across a wide range of nuclear material and other radioactive materials facilities. This enables security managers at most nuclear and radioactive material facilities and activities to perform performance-based, risk-informed security assessments to determine the adequacy of security arrangements and the likely effectiveness of any proposed compensatory measures.

A methodology is only of value if it can be used easily by a practitioner. If the NUSAM project had only focused on developing a strategic methodology as provided in this report, the overall value of the project would be marginal to the stakeholders in nuclear security. It could be limited to being a good research project for presentation at technical and specialist conferences, but not much more.

The NUSAM project tested the methodology against hypothetical facilities based on realistic situations in order to determine, amongst a great many other things, whether it could easily be used by a practitioner. The fully documented case studies for a wide range of facilities and activities will be of

value, providing insight to the approach, method and considerations necessary to undertake an assessment for training, specialist skills development and implementation guidance. These case studies validated the use of tools and methods and the overall NUSAM methodology.

The NUSAM CRP can be considered a success as it met the project objectives and has provided a validated approach for the assessment of security arrangements at a variety of sites, facilities and activities.

8. RECOMMENDATIONS

Using the NUSAM methodology (See Fig. 2) of planning, collecting information, conducting the assessment and creating an overall assessment of security is an effective approach to security assessment. The variety of methods available, from simple checklists to more complex modelling and simulation and TT exercise, all have value for a facility such as the UMC. All assessment techniques used in this case study have value for this type of facility. The quantitative methodology is probably the optimum technique for a facility of this form, balancing resource, quality and applicability (Fig. 8); but all techniques considered provide value. The exact selection of methodology will be determined by many factors, including the facility, the threat and the experience and knowledge of the personnel performing the assessment.

As the techniques get more complex, the additional data produced allows a more extensive assessment to be undertaken, and provides more insight as to where enhancements are likely to be required. Some approaches, such as modelling and simulation, allow multiple runs to be undertaken as well as easily implemented changes to the physical, technical and response arrangements. This enables optimization and also consideration of cost-benefit analysis for modifications or enhancements. Modelling and simulation also allows the malicious capability to be adapted, either through enhanced or degraded capability, or to change the attack approach (e.g. by splitting the group into multiple sub-units) to learn more about the effectiveness of the PPS to account for development of the malicious capability. Therefore, modelling and simulation can provide some assurance towards future-proofing the solution. Despite the beneficial aspects, each method does not comprehensively cover all relevant aspects of security. It is therefore the recommendation of this case study that these security assessment methods be considered as individual tools to be used in conjunction with one another to provide complete assessment of all relevant aspects of security.

Appendix I

UNIVERSITY MEDICAL CENTRE - HYPOTHETICAL FACILITY INFORMATION

I.1. GAMMA KNIFE DESCRIPTION

Since 1998, the UMC has operated a gamma knife facility to treat several types of neurological and structural disorders of the brain. The gamma knife is located in the neurological surgery centre (NSC) in the southeast corner of the 1st floor of the hospital. It has 201 double encapsulated stationary ^{60}Co pencils (approximately 1.12 Terabecquerel (TBq) each with a total of 227 TBq measured on 05 December 2012) that are located in a hemispherical central shield body. The 201 ^{60}Co pencils are to be replaced every 5 to 8 years.

The ^{60}Co pencils are enclosed within a hemispherical shield body that weighs approximately 20 tons. The pencils can be removed if the shield body is disassembled. There is a shield door at the front of the machine that opens while the machine is in operation. The patient is slid in on the table automatically when the machine is put into operation, and the shield doors rise to allow patient exposure. The ^{60}Co pencils cannot be physically removed from the unit through this path.

The gamma knife surgery room itself has no windows and only one entrance (metal shielding sliding door). Two of the 45 cm thick concrete radiation-shielding walls in the gamma knife facility form part of the outer building wall (the roof over the gamma knife is 20 cm concrete). The surgery room door is kept closed and locked except during patient transport for treatment. Safety interlocks on the doors are solely for radiation protection purposes and operate in conjunction with the gamma knife unit. If the door is inadvertently opened during operation of the unit, the unit's table and patient will be immediately withdrawn and the source shield doors will automatically close. In addition, an alarm will sound in the immediate area and an emergency light will flash to indicate a problem.

The unit is operated from a control computer located immediately outside the surgery room. There are two viewing cameras in the surgery room. One camera close to the machine monitors the patient and the unit during operation, the second one is a security camera connected to the HSC. A patient is never left unattended while the machine is in operation.

Resourcing of the ^{60}Co pencils in the gamma knife is conducted entirely by the manufacturer. The process is done within the facility by two technicians using an automated reload machine. The reload procedure happens on site and takes about 2.5 hours (including calibration and verifying the new activity levels after re-sourcing). The reload process requires disassembly of the hemispherical shield body into two halves and movement of the back half, which weighs approximately 10 tons. An automated robot is mated to the front half of the hemisphere and removes the old pencils and replenishes them with new pencils. The tools (which are not that specialized) required to disassemble the unit are not kept in the NSC. No additional security measures are put in place during a resourcing.

I.1.1. Physical protection measures

I.1.1.1. Detection, assessment, and access control systems

A drawing of the floor plan of the gamma knife room and security equipment is shown in Fig. I.1.

There are dual (PIR and microwave) sensors located within the surgery room and in front of the room sliding door to detect unauthorized access to the corridor leading to the gamma knife room outside of NSC working hours. The sliding door is equipped with standard and security locks and a balanced magnetic switch (door wing position sensors) to detect door opening. All above-mentioned detectors are disarmed during operational hours. Activation and deactivation of the intrusion detection system is made by the keypad located in the corridor outside the room.

There is a tamper indicating device installed on the machine shell to signal opening of the enclosure leading to the ^{60}Co pencils. The tamper indicating device is armed (in operation) at all times.

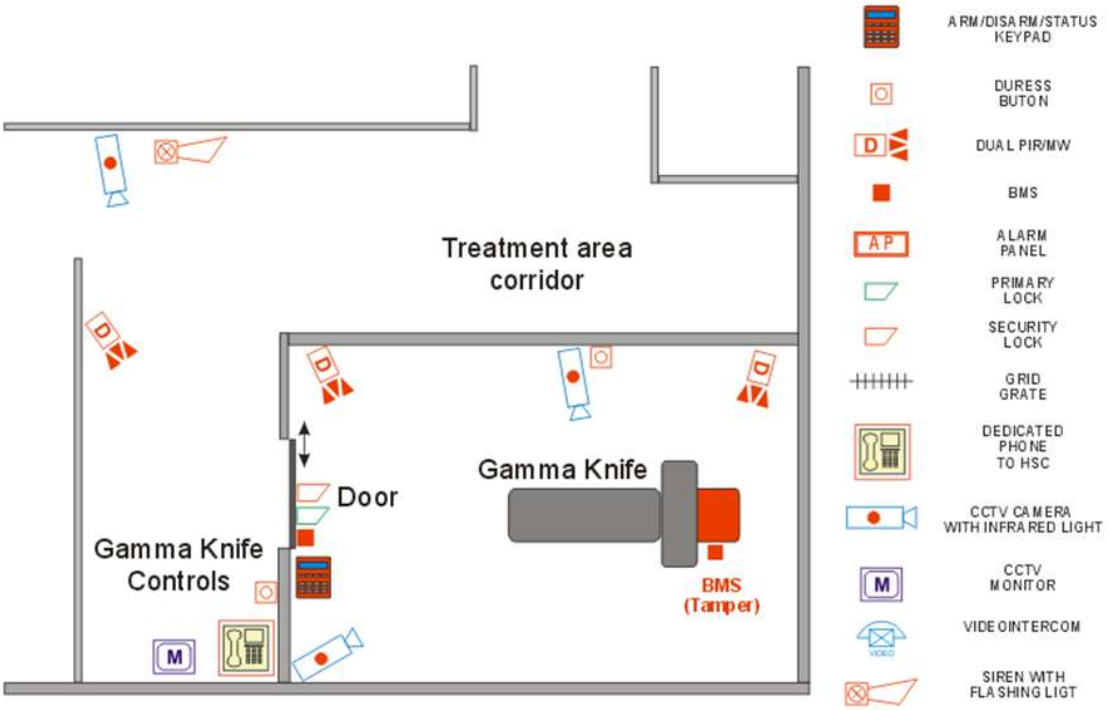


FIG. I.1. Gamma knife security equipment layout

Security equipment located around the gamma knife surgery room is connected to the HSC at the front desk near the ER entrance which is supervised by the university police. In case of alarm, assessment is made via security CCTV camera in the corner of the surgery room and a CCTV camera located in the corridor that is focused on the room sliding door (on Fig. I.1, one camera is used to monitor patients and not as a security camera). Personnel can use a duress button in case of emergency, which is in operation at all times. The local alarm in the gamma knife area is a siren with flashing light located in the treatment area corridor.

Detection capability during operational hours is performed by personnel that are generally in the vicinity and may have the opportunity to detect an unknown person or intruder and alert the police.

There is an alarm on the gamma knife room door when the room is in use. However, the alarm is a local alarm and only for safety purposes. Hospital security patrols the corridors of the research wing on a random basis and checks doors to ensure that they are locked after hours. All checks are done from the main corridor only, since hospital security does not enter or patrol inside the NSC.

The NSC is occupied from 0900 to 1900 hours, Monday through Friday. During these operational hours, the area is active with many people at all times, and most of the sensors are not activated. According to operating personnel, the traffic is significantly less during off hours since the NSC is located in the outpatient area of the hospital (which closes at 1900 hours) and next to the research wing (which closes at 1800 hours). Access to the NSC is controlled by lock and key. Housekeeping, two nurse supervisors, and two physicians have keys to the NSC.

I.1.1.2. Delay systems

There are two ways to enter the NSC. The main entrance off the out-patient area corridor is a set of large solid wood doors (WD1). The doors lead to a second large, solid wood door in the lobby with a glass viewing pane. Both sets of doors are normally locked when the facility is shut down for the night. From this entrance, there is a distance of about 25 metres to the surgery room where the unit/sources are located.

The second entrance to the NSC is directly from the hospital corridor through a wood emergency exit door, which is always locked from the outside (there is a crash bar on the inside). The door is supposed to be used only for emergency egress from the facility, but some employees exit through this door instead of the lobby door. Sometimes employees will enter through this door if they happen to notice another employee opening it from the inside. The gamma knife is 15 metres from this entrance.

There are no specialized delay/barrier systems installed in or around the NSC. The majority of delay will come from the time required for breaking through the metal sliding door leading to the gamma knife room and disassembly of the machine to reach the sources. Since the unit is too heavy to be moved, the only unauthorized removal potential is through disassembly of the unit and removal of the pencils. Disassembly of the unit consists of removal of several hexagonal bolts located around the shield body. It is estimated that the disassembly of the unit will provide some significant delay since this is the only way to access the sources.

I.2. BLOOD BANK IRRADIATOR DESCRIPTION

The UMC operates a blood bank with two blood irradiators. Each weighs approximately one ton and contains a single source of about 33 TBq of caesium-137 (^{137}Cs). The source (caesium chloride powder pressed into pellets) is doubly encapsulated in stainless steel capsules with fusion welded end caps. Each source is sealed inside the machine and has never been replaced.

The key required to operate the irradiator is located in the open cabinet directly underneath the machine. The sample chamber will not open without the key. The sample chamber rotates clockwise to allow access for loading the samples. The ^{137}Cs source cannot be accessed through the sample chamber area.

The blood bank operates 24 hours per day, 364 days per year (closed on Christmas Day) with the following staffing:

- Day Shift: 12 – 18 personnel
- Swing Shift: 6 personnel
- Night Shift: 3 personnel

I.2.1. Physical protection measures

A drawing of the floor plan of the blood bank area and security equipment is shown in Fig. I.2.

I.2.1.1. Detection, assessment, and access control systems

There are two entrances into the blood bank: a normal (through the secretary desk) and a controlled entrance door equipped with badge (card) reader. Since hospital staff need to access the blood bank at all hours, the normal entrance is locked by simple electrical latch lock. That lock and door balanced magnetic switch are controlled from the secretary desk based on video intercom request. The secretary desk is permanently staffed even on holidays (holidays are staffed at the swing shift level or below) except for Christmas. The second controlled entrance leads directly into the irradiator area and is always locked. Access through this door is controlled by a card reader that operates an electronic strike-and-disarm balanced magnetic switch, detecting opening of the door. Both doors have crash bars.

Workers are badged and know each other well. Workers are supposed to challenge anyone they do not recognize that is in the lab area without an escort and call security (only employees are allowed past the secretary's desk in the blood bank). Since multiple personnel are in the area at any time, the chances of detecting suspicious behaviour or an intruder and alerting security are highest during the day and lowest during the late shift.

There is a robust grid on the window located in the main room.

There is one dual (PIR and microwave) sensor located within the irradiator room to detect unauthorized movement out of the blood bank during working hours. An electric strike on the door leading to the secretary desk is controlled by a push button at the secretary desk and requires basic video intercom identification of personnel requesting passage through the door.

There is a tamper indicating device installed on both irradiator shells to signal opening of the enclosure leading to the source. This tamper indicating device is armed (in operation) at all times.

Security equipment installed in the blood bank area is connected to the HSC at the front desk near the ER entrance and is supervised by the university police.

Assessment of alarms can be made via security CCTV cameras located in the secretary room, in the main room and in the blood irradiator room.

Personnel can use duress buttons in case of emergency. These devices are in operation at all times.

There is a local siren with flashing light located in the main area and is activated in case of alarm in the blood bank area.

Hospital security patrols the corridors of the research wing on a random basis and checks doors to ensure that they are locked after hours. All checks are done from the main corridor only, since hospital security does not enter or patrol inside the blood bank area.

I.2.1.2. Delay systems

Other than the doors, there are no significant barriers in the blood bank area. The majority of the delay to unauthorized removal will come from the irradiator itself. It is likely that this device would be too heavy to steal intact. A well-prepared adversary would be able to remove the sources from the devices. The task time for accomplishing this will depend on several factors, including the tool set used and opportunities for practicing before the event. The closest door out of the facility is about 12 metres away from the irradiators.

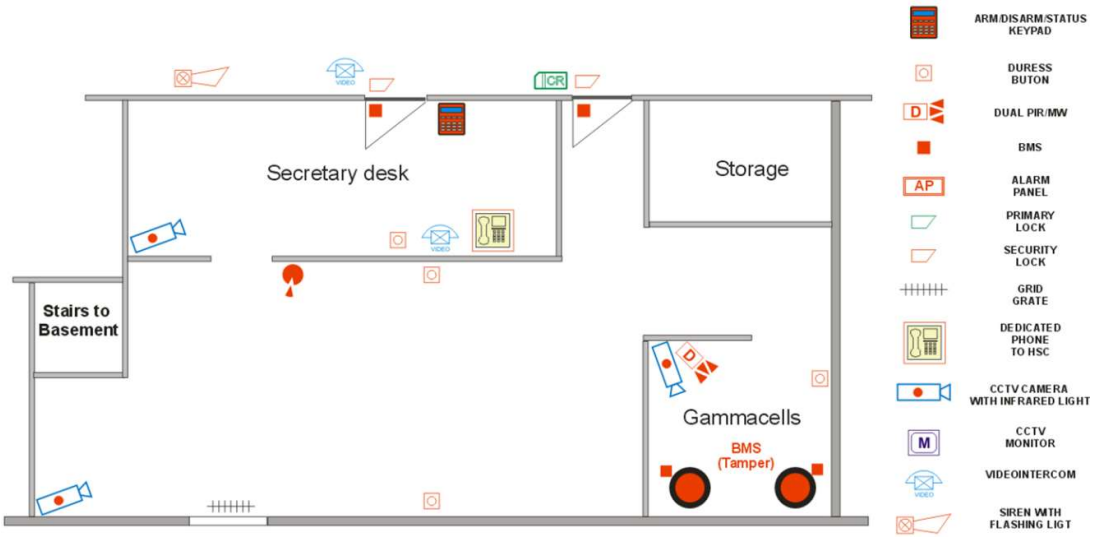


Fig. I.2. Blood bank irradiator security arrangements

I.3. MEDICAL RESEARCH IRRADIATOR DESCRIPTION

The UMC utilizes another irradiator, located in the basement of the research wing, to expose cells, tissues, animals, and other biological samples to a controlled dose of ionizing radiation. The irradiator unit is a pneumatic drive system. The machine is very large and cannot be moved through the existing doorway; it weighs approximately 3 tons. The unit contains two ^{137}Cs sealed sources (originally totaling 111 TBq) located in the rear of the machine. On average, the irradiator room is used once per week for about 3 hours.

The research irradiator unit has been in place for approximately 10 years, during this time the activity of the ^{137}Cs sources contained within the irradiator have dropped from 3000 Curie (~111 TBq) to around 2386 Curie (~88 TBq), as shown in Eq. (I.1).

The activity level of the source places it within Category 2 and is therefore subject to Security Level B.

$$Activity = 3000 \times (0.5)^{10/30.17} = 2386\ curie \quad (I.1)$$

Figure I.3 shows the floor plan of the basement and the location of the irradiator.

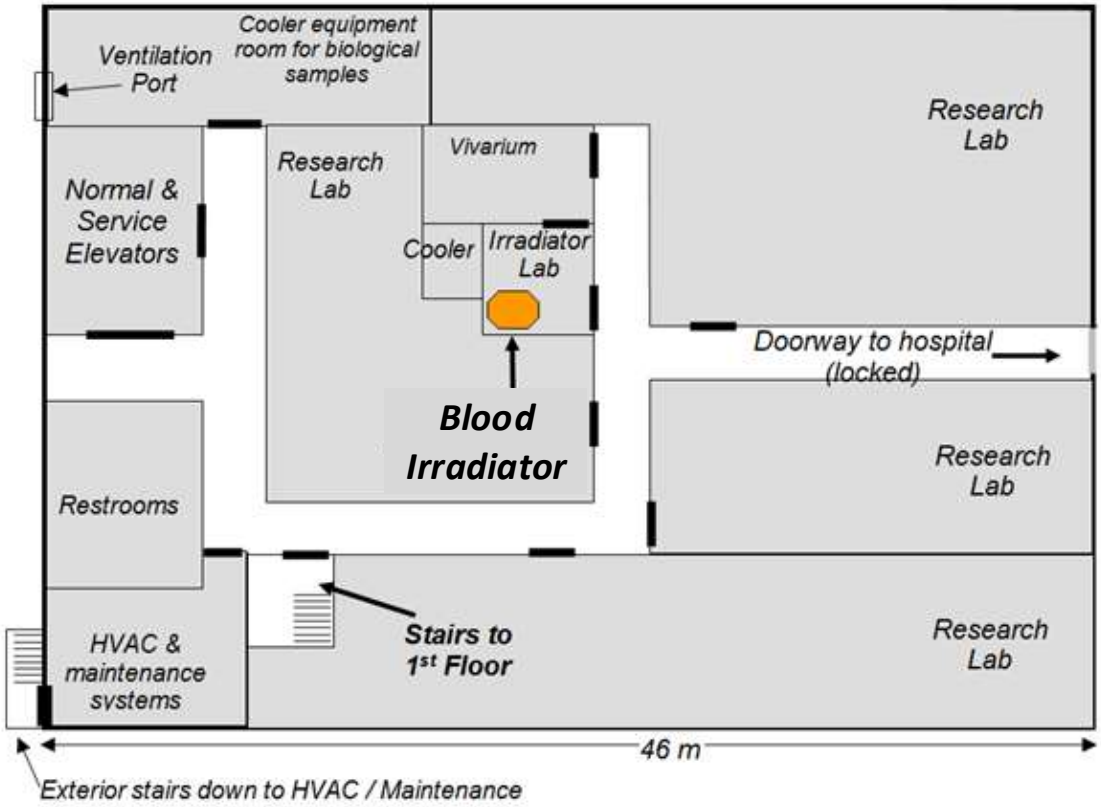


Fig. I.3. UMC basement layout

The irradiator is adjacent to a vivarium containing research animals (insects and small rodents), and a cooler containing biological samples and agents. Normal entrance to the basement is from the first floor, down the stairs or the elevator. The door at the bottom of the stairwell is locked by security at 1900 hours and is opened again at 0600 hours. All lab supervisors have keys to this door so they can access the labs and work at night if necessary.

The elevator is set to operate only during normal hours (0600 to 1900 hours daily). After normal hours, the stairs are the only access to the basement. The service elevator operates at all times, but only with the elevator key. It is seldom used, and generally only by housekeeping or maintenance staff.

The irradiator and vivarium rooms are always locked when not in use.

All users of the irradiator would need to be on the approved users list before they can operate the irradiator unescorted.

I.3.1. Physical protection measures

A drawing of the floor plan of research area and security equipment is shown in Fig. I.4.

I.3.1.1. Detection, assessment, and access control systems

There is a dual (PIR and microwave) sensor located within the irradiator room to detect unauthorized movement in the room. Doors leading from the corridor to the irradiator and vivarium rooms are equipped with security locks and balanced magnetic switches (door wing position sensors) to detect door opening.

There is tamper indicating device installed on the machine shell to detect opening of the enclosure leading to ^{137}Cs sources. This tamper indicating device is armed (in operation) at all times. All other detectors are armed or disarmed by card reader with personal identity number in front of the irradiator room door. The reader indicates the status of the detecting system (armed/disarmed) in the irradiator room.

Security devices are connected to the HSC at the front desk near the ER entrance and is supervised by university police.

Alarms assessment can be made by the security CCTV camera in the corner of the irradiator room and a CCTV camera located in the corridor covering both doors leading to the irradiator and vivarium rooms.

Personnel can use duress buttons in case of emergency. These devices are in operation at all times.

In case of alarm, a local siren with flashing light located in the corridor is activated.

I.3.1.2. Delay systems

There are no specialized delay/barrier systems installed in or around the irradiator. Both doors leading to the irradiator and vivarium rooms are constructed of industrial 2 mm thick sheet metal. The majority of delay will come from the time needed for break through one of the doors and breaking into the irradiator to reach the sources. The task time for accomplishing this will depend on the tool set used to remove the sources from the machine and on the skills and experience of the adversaries.

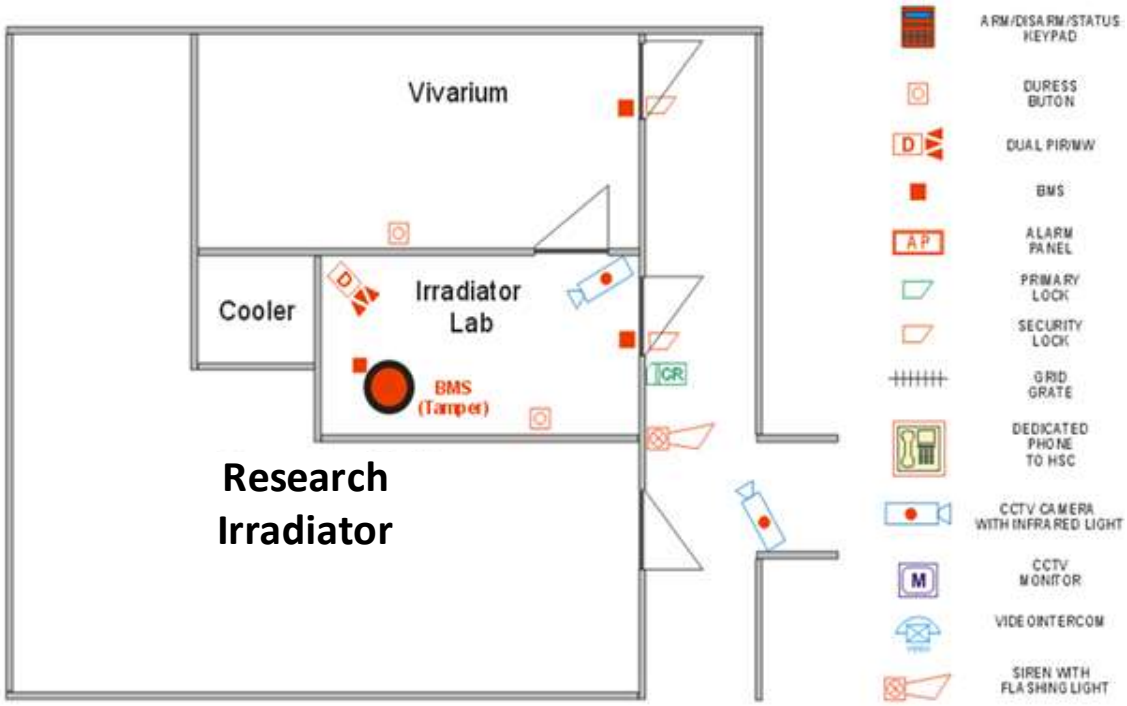


FIG. I.4. Research irradiator security arrangements

I.4. UMC FACILITY - ADDITIONAL DETAILS

As the purpose of the study is to compare assessment methodologies, a comprehensive and definitive answer as to the adequacy of security arrangements is not required. However, the context, scenario, assumptions and chosen values (for delay etc.) would need to be representative of a real application for the study to have meaning. The scenario and other considerations are presented below.

I.4.1. Facility Background

The UMC located in the Republic of Lagassi contains three sources, each of which could be the target of sabotage or unauthorized removal. Two of the sources are Category 1 and require measures to the standard of Security Level A. The remaining source is Category 2 and requires Level B measures. The

Category 2 source would normally be treated as Category 1 due to its nature, but that recommendation is ignored in this study for representative purposes.

I.4.2. Facility security arrangements

The UMC has four guards and two university police officers on duty at all times, excluding holidays. The guards and police are assumed to be in good health, including perfect sight and hearing, with training relevant to their roles as dictated by Lagassi. The security staff are well disciplined and are reasonably alert (factoring in fatigue during shift etc.). All security staff members are equipped with two-way radios, handcuffs and batons. The police are also armed with pistols.

Two guards and one policeman are on roving patrol around the main corridors of the UMC (separately). The remaining two guards man the HSC, located at the front desk of the ER entrance. The other policeman is on guard in the ER. Due to the roving nature of the patrols, the location of the patrols can never be guaranteed at any specific time.

All of the security measures in the UMC are well-maintained and working as intended at the time of the attack.

I.4.3. Facility staffing

Although the UMC operates at all times, several areas are closed or restricted after hours. The following areas are open at all times: blood bank, Service elevator, main and ER entrances. From 0600 until 1900 hours: basement (stairs), elevators and the outpatient area. The research wing is open from 0600 to 1800 hours. The NSC is open from 0900 until 1900 hours on weekdays. Staff members are required to wear identification badges at all times and persons without a badge are challenged by guards, though no formal identification checks take place. Visitors (un-badged persons) entering the UMC after 1900 hours are to acquire a visitor's pass from the front desk.

The blood bank is staffed at all times, with 12–18 staff on the day shift (1000 – 1800 hours), 6 on the swing shift (0600 – 1000 hours and 1800 – 2200 hours) and 3 on the night shift (2200 – 0600 hours). The reception desk is also staffed at all times.

Staff recognize each other and are supposed to challenge anyone they do not recognize, but the culture of the UMC is fairly relaxed and this cannot be counted on. Staff members may not offer resistance against armed adversaries, but will attempt to trigger duress alarms if possible.

The research lab in the basement is staffed 0900 – 1700 hours weekdays. Staff have a chance to detect adversaries navigating the basement corridors, but would be easily subdued and are unlikely to report the intrusion.

I.5. SOURCE CATEGORIZATION

The UMC facility source categorization criteria is shown in Fig. I.5.

Category	Source[a]	A/D[b]
1	Radioisotope thermoelectric generators (RTGs) Irradiators Teletherapy sources Fixed multi-beam teletherapy (gamma knife) sources	A/D > 1000
2	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	1000 > A/D > 10
3	Fixed industrial gauges that incorporate high activity sources[c] Well logging gauges	10 > A/D > 1
4	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	1 > A/D > 0.01
5	Low dose rate brachytherapy eye plaques and permanent implant sources X ray fluorescence (XRF) devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	0.01 > A/D and A > exempt[d]

[a] Factors other than A/D alone have been taken into consideration in assigning the sources to a category (see Ref. [3], Annex I).

[b] This column can be used to determine the category of a source purely on the basis of A/D. This may be appropriate, for example, if the facilities and activities are not known or are not listed, if sources have a short half-life and/or are unsealed, or if sources are aggregated (see Ref. [3], paragraph 3.5).

[c] Examples are given in Ref. [3], Annex I.

[d] Exempt quantities are given in Schedule I of Ref. [5].

FIG I.5. Categorization table taken from Ref [5]

I.6. THREAT STATEMENT

Three possible adversary types are considered: a lone insider, a team of two activists and a three-member attack squad. Attacks are possible during day and night and different tactics may be used (e.g. overt/covert). The adversaries are all in good health, including perfect sight and hearing.

The activist team are equipped with basic manual tools and have some limited criminal trespass ability and may use force if opportune or necessary. They are also familiar with basic radioactive material handling. They have a vehicle available for escape.

The attack squad are equipped with an appropriate array of power tools and are well-trained in the use of such tools as well as criminal trespass. They are armed with pistols, willing to use force to achieve their goals and are familiar with handling radioactive material. They have a vehicle available for escape.

The insider may be from any discipline within the UMC. That is, he or she could be a physician, a guard, a researcher, intern, janitor or other maintenance staff or any other employee or contractor with access to the facility. The insider will have access to equipment appropriate to his or her role (e.g. a physician or researcher will have a pass card and personal identity number with access rights to relevant areas of the UMC, maintenance staff will have a set of keys and be able to use the service elevator etc.). The insider may have also purposely concealed a basic tool or tools on his or her person to facilitate goal completion. A maintenance person would be able to carry a toolbox into most areas of the facility

without raising suspicion.

If an insider is assisting another adversary type, he or she will provide access and concealment where possible, will not engage in any violent activity, and will be unwilling to engage in a direct conflict. He or she will attempt to reduce the chances of discovery post event. The insider is assumed to be acting on malicious intent (own desire) or under duress – monetary or violent.

I.7. ASSUMPTIONS

- It is assumed that the adversaries have knowledge of the layout of the UMC and plan an attack path accordingly, bringing the appropriate tools for the chosen path of attack.
- Adversaries enter the facility at the same point and stay in a group for the duration of the attack.
- The path chosen will be logical (e.g. non circular) and as direct as possible.
- The attack squad will also commandeer a vehicle if they deem it necessary (i.e. to ram a wall or escape).
- It is also assumed that adversaries will not use any distraction tactics, or attempt to neutralize guards as part of the attack plan.
- While the activists will not openly engage in conflict, they will attempt to subdue guards if presented with an opportunity to do so.
- The insider assisting the adversary is assumed to be the one that is most effective at assisting them on the chosen path (i.e. worst case scenario) unless otherwise stated.
- The adversaries do not have the capability to remove a source without first dismantling the housing.
- The guards cannot know the intended target of the adversaries unless/until they are detected in the source area around a given target.
- The guards cannot know whether the adversaries intend to sabotage or steal the target.
- Adversaries will attempt to escape the facility the same way as they entered.
- All adversaries have at least some knowledge of how to dismantle each of the source housings. The time it takes each is reduced by skill and available tools.
- It is assumed the attack does not take place on a holiday.

- The balanced magnetic switch is assumed to always be effective and trigger an alarm.
- In the event of detection being possible, the detection is assumed to occur immediately if successful.
- Staff in the blood bank will most likely detect an intruder, but may not be able to trigger an alarm.
- Staff will not necessarily challenge an unrecognized person.
- All doors are locked unless otherwise stated.
- Guards will seek to verify an alarm by an initial response that takes 5–8 minutes. This can be succeeded by a ‘true’ response.
- Detection by CCTV will trigger a ‘true’ response if necessary as CCTV viewing provides verification (e.g. armed attack squad detected).

I.8. SCENARIOS

The scenarios intended for use within AVERT are detailed below. They take the format as follows:

- Scenario X
  - Adversary;
  - Time/circumstance;
  - Target (unauthorized removal/sabotage);
  - Staff levels;
  - Path choice;
  - Tools, equipment and weapons;
  - Insider (if adversary is not insider);
  - Additional notes.

The following are the scenarios used in this case study:

- Scenario 1
  - Lone insider (maintenance technician);
  - Day;
  - Gamma knife (unauthorized removal);
  - Two staff in the source area;
  - Least detection;
  - Keys and access pass. Toolbox containing basic tools. Unarmed.
  - Note – individual would be able to gain access to the source area without raising suspicion.
- Scenario 2[5]
  - Lone insider (physician);
  - Day;
  - Gamma knife (sabotage);
  - Two staff in the source area;
  - Least detection;
  - Access pass and PIN. Concealed tool (spanner, screwdriver). Unarmed.
    - Note – individual would be able to gain access to the gamma knife without raising suspicion. Alarm would only be raised via CCTV or balanced magnetic switch on the device.
- Scenario 3
  - Lone insider (maintenance technician);
  - Night;
  - Gamma knife (unauthorized removal);
  - No staff in the source area;
  - Least detection;
  - Keys and access pass. Toolbox containing basic tools. Unarmed.
  - Note – individual would be able to gain access to the source area without raising suspicion.

[5] Scenario 2 was originally envisioned in this format, but was altered to be a "beyond DBT" scenario in the AVERT assessment. The scenario was as Scenario 8, but the attack squad had power tools, assault rifles and were able to choose their target.

- Scenario 4
  - Lone insider (physician);
  - Night;
  - Gamma knife (sabotage);
  - No staff in the source area;
  - Least detection;
  - Access pass and PIN. Concealed tool (spanner, screwdriver). Unarmed.
    - Note – individual would be able to gain access to the Gamma Knife without raising suspicion. Alarm would only be raised by CCTV or anti-tamper balanced magnetic switch on device.
- Scenario 5
  - Activists (2);
  - Night;
  - Gamma knife (unauthorized removal);
  - No staff in the source area;
  - Least detection;
  - Basic Tools. Unarmed.
- Scenario 6
  - Activists (2);
  - Night;
  - Blood bank (sabotage);
  - 3 staff in the source area;
  - Least detection;
  - Basic Tools. Unarmed.
- Scenario 7
  - Activists (2);
  - Night;
  - Blood bank (unauthorized removal);
  - Three staff in the source area;
  - Least detection;
  - Basic Tools. Unarmed.
  - Insider assistance: physician – provided access pass and PIN, fools staff in area into believing the activists are contractor maintenance staff working in blood bank area.
- Scenario 8
  - Attack squad (3);
  - Night;
  - Blood bank (unauthorized removal);
  - Three staff in the source area;
  - Least detection;
  - Power tools. Armed with pistols.
  - Note - Staff are incapacitated before alarm can be raised.

- Scenario 9
  - Attack squad (3);
  - Night;
  - Gamma knife (unauthorized removal);
  - No staff in the source area;
  - Least detection;
  - Power tools. Armed with pistols.
- Scenario 10
  - Attack squad (3);
  - Night;
  - Gamma knife (unauthorized removal);
  - No staff in the source area;
  - Least detection;
  - Power tools. Armed with pistols.
  - Insider assistance: Maintenance – provides access to facility and VA.

More scenarios may be considered in each individual analysis, dependent on if more information is required to ascertain the effectiveness of a given methodology.

I.9. SECURITY AND ADVERSARY CLASSIFICATIONS

To properly evaluate the methodologies, the effectiveness of the UMC's security arrangements were put into context via a classification system that ranks each type of defence. Each rank has an associated time delay, used for both the spreadsheet and simulation analyses. See Fig. I.6.

A defence can be ranked from 1 to 4, with rank 4 offering the most protection. Rank 1 offers moderate resistance to basic types of attack. Rank 2 offers moderate resistance against moderate (but non-specialist) attack and substantial resistance against basic attack. Rank 3 offers moderate resistance against specialist attacks and substantial resistance to moderate non-specialist attack. Rank 4 offers substantial resistance against a range of powerful and specialist attacks. Defences that offer no protection, such as a normal window, will be unclassified.

For the purposes of this study, the security measures are classified as follows:

- External Windows – unclassified
- External Doors – Rank 2
- Vent Access Panel – Rank 1
- Roll-up doors – Rank 2
- Window Grid – Rank 2*
- External Walls – Rank 1
- Standard Internal Door – unclassified
- Internal Door with Security Locks – unclassified
- Sliding Door – Rank 2
- Internal Walls – Rank 1
- Source Housings – Rank 2

The adversary capabilities are ranked in a similar way, with rank 4 being the most effective attack. Rank 1 assumes the adversary has little knowledge of physical barriers and a limited range of easily available

tools. Rank 2 assumes the adversary has a limited knowledge of physical barriers and a range of non-specialist tools and portable instruments. Rank 3 assumes the adversary to have good knowledge of physical barriers and a comprehensive range of non-specialist tools and equipment. Rank 4 assumes the adversary to have professional knowledge of physical barriers and the ability to plan and execute an attack efficiently.

For the purposes of this study, the adversaries are classified as follows:

- Insider – Rank 1
- Activists – Rank 2
- Attack Squad – Rank 4

Note that the classification of insiders only applies to barriers for which they would not normally have access. All times in the tables below are considered hypothetical.

Time Delay Rank Matrix (time in minutes)
WINDOWS

Adversary Rank				
R1	NA	8		NA
R2	NA	3		NA
R3				
R4	NA	0.5		NA
Defence Rank >	R1	R2	R3	R4

- External windows - Unclassified
- Window grid - Rank 2*

Window grid can be removed via tow rope

Unclassified gives zero resistance to attack
Unclassified: 0

Time Delay Rank Matrix (time in minutes)
DOORS

Adversary Rank				
R1	5	8		NA
R2	2	5		NA
R3				
R4	0.2	2		NA
Defence Rank >	R1	R2	R3	R4

- Standard internal door - Unclassified
- Internal Door with security locks - Unclassified
- External Doors - Rank 2
- Roll-up doors - Rank 2
- Sliding door - Rank 2*
- Vent access panel - Rank 1

Sliding door is designed for safety, not security (i.e. shielding)

Time Delay Rank Matrix (time in minutes)
WALLS

Adversary Rank				
R1	8	NA		NA
R2	2	NA		NA
R3				
R4	0.2	NA		NA
Defence Rank >	R1	R2	R3	R4

- External walls - Rank 1
- Internal walls - Rank 1

Time Delay Rank Matrix (time in minutes)
HOUSINGS

Adversary Rank				
R1	NA	6	*	NA
R2	NA	7		NA
R3				
R4	NA	2		NA
Defence Rank >	R1	R2	R3	R4

- Source housings - Rank 2

* Assume insider has knowledge and familiarity with housing

FIG. I.6 Time delay rank matrix

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Coordinated Research Project, J02004, Final Report - Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2019)

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Coordinated Research Project, J02004, Nuclear Power Plant Case Study for the Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2019)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Coordinated Research Project, J02004, Transport of Radioactive Material Case Study for the Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2019)

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).

[6] Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, IAEA, Vienna (2004).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Coordinated Research Project, J02004, Final Report - Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2018)

ABBREVIATIONS

3D	Three dimensional
BBI	Blood bank irradiator
CCTV	Closed-circuit television
CRP	Coordinated research project
DBT	Design basis threat
GK	Gamma knife
H	High
HSC	Hospital security centre
IAEA	International Atomic Energy Agency
LINAC	Linear accelerator
NSC	Neurological surgery centre
NUSAM	Nuclear security assessment methodologies
PIR	Passive infrared
PPS	Physical protection system
PRT	PPS response team
SA	Security assessment
TA	Threat assessment
TBq	Terabecquerel
TS	Threat statement
TT	Tabletop
UMC	University Medical Centre

LIST OF PARTICIPANTS

Alam, B	Bangladesh Atomic Energy Commission, Bangladesh
Brüecher, W.	GRS, Germany
Chetaine, A.	University of Mohammad V Rabat, Morocco
Edwards, J.	National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland
Garrett, A.	International Atomic Energy Agency
Greenhalgh, D.	Oak Ridge National Laboratory, United States of America
Hall, C.	Expert, United States of America
Hill, S.	Sandia National Laboratories, United States of America
Hogan, T.	Sandia National Laboratories, United States of America
Hwang, M.	Korea Atomic Energy Research Institute, Republic of Korea
Iwuala, E.	Nigerian Nuclear Regulatory Authority, Nigeria
Izmaylov, A.	State Co. Scientific Production Union “Eleron”, Russian Federation
Jang, S.	International Atomic Energy Agency
Jung, W.	Korea Atomic Energy Research Institute, Republic of Korea,
Kawata, N.	Japan Atomic Energy Agency, Japan
Kibria, F.	Bangladesh Atomic Energy Commission, Bangladesh
Leach, J.	Sandia National Laboratories, United States of America
Lee, J.	Korea Institute of Nuclear Nonproliferation and Control, Republic of Korea,
Legoux, P.	World Institute for Nuclear Security
Lindahl, P.	OKG AB, Sweden
Little, R.	Quintessa Ltd., United Kingdom
Mahmood, R.	Pakistan Nuclear Regulatory Agency, Pakistan
Malach, J.	EBIS, Czech Republic
Malachova, T.	EBIS, Czech Republic
Mahdi, A.	Iraqi National Monitoring Authority
Malik, S.	National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland
Martin, K.	Oak Ridge National Laboratory, United States of America
Naoko, N.	Japan Atomic Energy Agency, Japan
Norichika, T.	Japan Atomic Energy Agency, Japan
Reynolds, J.	National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland
Rivers, J.	Nuclear Regulatory Commission, United States of America
Rodger, R.	National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland
Scott, J.	National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland
Sergovantsev, P.	State Co. Scientific Production Union “Eleron”, Russian Federation
Shaheen, H.	Egyptian Nuclear and Radiological Regulatory Authority, Egypt
Shakoor, A.	Pakistan Nuclear Regulatory Agency, Pakistan
Shridhar, A.	Bhabha Atomic Research Centre, India
Shull, D.	International Atomic Energy Agency
Snell, M.	Sandia National Laboratories, United States of America
Stangebye, J.	SKB, Sweden
Stefanka, Z.	Hungarian Atomic Energy Authority, Hungary
Terao, N.	Japan Atomic Energy Agency, Japan
Vaclav, J.	UJD SR, Slovakia
Yamaguchi, T	Japan Atomic Energy Agency, Japan
Zielman, B	URENCO Nederland B.V., Netherlands

Consultants Meeting

Vienna, Austria: 6–8 March 2013, 3–4 February 2014, 17–21 March 2014, 2–3 September 2014, 13–17 October 2014, 16–20 March 2015, 13–17 April 2015, 10–14 August 2015, 27 June–1 July 2016

Preston, United Kingdom: 9-13 February 2015

Albuquerque, New Mexico, United States of America: 2-6 November 2015

Daejeon, Republic of Korea: 14-18 March 2016