TECHNISCHE
UNIVERSITÄT
WIEN
Vienna, Austria

DISSERTATION

A Graded Approach for Nuclear Security Management of Research Reactors

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines Doktors der technischen Wissenschaften unter der Leitung von

Ao. Prof. Dipl.-Ing. Dr. techn. Helmuth Böck

Atominstitut, Technische Universität Wien

und

Dipl.-Ing. Dr.techn. Johannes Sterba

TRIGA Center Atominstitut, Technische Universität Wien

eingereicht an der Technische Universität Wien
Fakultät für Physik

von

M.Sc. Vasily Kovtunov

Matrikelnummer: 01528518

Date: 25.11.2024

Abstract

The research described in this thesis provides a detailed methodology to develop a Research Reactor Nuclear Security Management (RR-NSM) graded approach. The RR-NSM graded approach determines the effort and resources needed for establishing the Physical Protection System (PPS) for research reactors. The methodology takes into consideration specifics of research reactors, tailored to a research reactor's purposes.

The fundamental principle of the RR-NSM graded approach is in line with recommendations of the International Atomic Energy Agency (IAEA) and considers threat evaluation, attractiveness of assets based on their properties and potential consequences associated with a malicious act at a research reactor [1]. The RR-NSM graded approach will serve as an effective tool assisting the decisions makers on the course of development or review of PPS and security strategies for a research reactor.

The overall attractiveness of assets at a research reactor is calculated considering two factors: consequences of a malicious act involving an asset and the attractiveness determined by the asset's properties. The level of an asset's attractiveness is then determined as very low, low, moderate, high, or very high.

Furthermore, the RR-NSM graded approach describes two methods to evaluate the PPS effectiveness for any potential malicious act scenario. These two approaches for PPS effectiveness evaluation are: one for outsiders and one for insiders. In addition, a combined approach can be used in case of a collusion of an outsider and an insider scenario. The level of PPS effectiveness for an asset is then determined as very low, low, moderate, high, or very high.

The developed RR-NSM graded approach was applied in three differed case studies for which four different scenarios of malicious acts were developed. Due to the confidentiality of real security related information on existing nuclear facilities, the hypothetical facility - the Shapash Nuclear Research Institute developed by the IAEA, was used. One case study describes a scenario of outsiders in collusion with an insider and three other scenarios for insiders. For the purpose of this research the layout of Shapash Nuclear Research Institute was modified to create a hypothetical radioisotope production facility. This allowed to create a realistic scenario involving other radioactive material.

The case studies allowed to demonstrate the application of the RR-NSM graded approach and demonstrated how to:

- Evaluate attractiveness of assets at a research reactor facility.
- Evaluate effectiveness of PPS in described scenarios.
- Evaluate the balance between established PPS arrangements effectiveness and attractiveness of assets.
- List potential improvements in PPS based on the evaluated balance.

This research demonstrates the strengths of the RR-NSM graded approach in assessing PPS, particularly its ability to tailor security measures to the specific attractiveness of assets and potential threat scenarios. However, challenges such as the complexity of the analysis and the need for strict confidentiality protocols are identified as potential limitations. The results emphasize the importance of integrating and developing user-friendly software tools to streamline the practical application of the methodology and suggest that future work should focus on expanding the accessibility of the RR-NSM graded approach through enhanced training and the development of secure data management protocols.

Kurzfassung

In den letzten Dekaden sind die Anforderung der physischen Sicherung von Forschungsreaktoren parallel mit den Sicherungsanforderungen von Kernkraftwerken angestiegen. In der vorliegenden Arbeit wurden diese Anforderungen in Relation zu den Sicherungsmaßnahmen untersucht.

Ziel dieser Arbeit ist es ein Verfahren eines angepassten Sicherungsmanagement für Forschungsreaktoren (RR-NSM) zu entwickeln.. Der Ansatz des RR-NSM verringert den Aufwand und die Ressourcen, die für das physische Sicherungssystems (PPS) von Forschungsreaktoren erforderlich sind. Die Methodik berücksichtigt die Besonderheiten von Forschungsreaktoren und ist auf die spezifischen Zwecke eines Forschungsreaktors zugeschnitten.

Das grundlegende Prinzip der Anpassung des RR-NSM entspricht den Empfehlungen der Internationalen Atomenergiebehörde (IAEA) und berücksichtigt die Bedrohungsbewertung, die Attraktivität des Zielmaterials basierend auf ihren Eigenschaften und die potenziellen Folgen, die mit einem böswilligen Akt in einem Forschungsreaktor verbunden sind [1]. Der angepasste Ansatz des RR-NSM wird als effektives Instrument dienen, das die Entscheidungsträger bei der Entwicklung oder Überprüfung von PPS und Sicherheitsstrategien für einen Forschungsreaktor unterstützt.

Die Gesamtattraktivität eines Zielobjektes in einem Forschungsreaktor wird unter Berücksichtigung von zwei Faktoren berechnet: den Folgen eines böswilligen Akts, der ein Zielobjekt betrifft, und der Attraktivität, die durch die Eigenschaften des Zielobjektes bestimmt wird. Die Größe der Attraktivität eines Zielobjektes wird dann als sehr niedrig, niedrig, moderat, hoch oder sehr hoch bestimmt.

Das für Forschungsanlagen angepasste Nuclear Security Managementsystem (NSM) wurde in drei unterschiedlichen Fallstudien mit vier möglichen Abläufen von Sicherungsangriffen untersucht. Auf Grund der Vertraulichkeit der Sicherungsvorkehrungen bei realen Nuklearanlagen wurde eine von der IAEO hypothetische Nuklearanlage „SHAPASH“ für die vorliegenden Untersuchungen verwendet.

Eine der Fallstudien untersucht eine Aktion einer außenstehenden Gruppe in Kooperation mit einem Insider, die drei anderen Fallstudien behandeln Insider Aktionen. Für diese Fallstudien wurde die hypothetische Shapash Anlage modifiziert, um zusätzlich eine Anlage zur Radioisotopen-Produktion ebenfalls untersuchen zu können. Dadurch ist es möglich ein realistisches Szenario für radioaktive (medizinische) Strahlenquellen mit einzubeziehen. Diese Fallstudien erlauben es, mittels dem angepassten NSM folgende Sicherungsaspekte genauer zu untersuchen:

- Wie attraktiv sind Einrichtungen und Materialien eines Forschungsreaktors?
- Wie effektiv sind Sicherungseinrichtungen in den beschriebenen Fallstudien?
- Gegenüberstellung der Sicherungseinrichtungen zur Attraktivität der Materialien
- Vorschlag zur Verbesserung der Sicherungssysteme auf Grund der Ergebnisse der Fallstudien

Diese Forschung zeigt die Stärken des Ansatzes des RR-NSM bei der Bewertung von PPS auf, insbesondere seine Fähigkeit, Sicherungsmaßnahmen an die spezifische Attraktivität von Zielobjekten und potenziellen Bedrohungsszenarien anzupassen. Allerdings werden Herausforderungen wie die Komplexität der Analyse und die Notwendigkeit strikter Vertraulichkeitsprotokolle als potenzielle Einschränkungen identifiziert. Die Ergebnisse betonen die Bedeutung der Integration und Entwicklung benutzerfreundlicher Software-Tools, um die praktische Anwendung der Methodik zu vereinfachen. Es wird vorgeschlagen, dass zukünftige Arbeiten sich auf die Erweiterung der Zugänglichkeit des Ansatzes des RR-NSM durch verbesserte Schulungen und die Entwicklung sicherer Datenmanagement-Protokolle konzentrieren sollen.

Contents

Introduction

It has been almost 80 years since the first research reactor started its operation. Since then, about 820 research reactors were built in about 70 different countries. Many of those have been decommissioned, however there are currently 222 operational research reactors in more than 50 different countries in the world [2]. For 80 years, research reactors have been serving as neutron sources and for various other purposes.

A few research reactors are supervised and operated by universities and provide opportunities for practical training to students and external parties. For convenience, the location is often chosen nearby a university or even in a university campus. Due to the variety of activities a facility is accessed not only by staff and contractors but also by students, trainees, visitors, or temporary researchers from other universities. Research reactor staff during their ordinary work activities can access different parts and resources of a research reactor facility. Contractors need to perform maintenance activities at a research reactor facility and have access to specific tools. These arrangements dictated by the objectives of a research reactor might create vulnerabilities and pose a certain security risk for a facility.

In the past with the construction of a research reactor some countries were aiming to build a facility that would be efficient for planned purposes and sometimes with a limited budget available. The security of a research reactor was not the priority and was not balanced in the design. The focus in a design of a research reactor was to meet their specific objective [3]. However, the protection of data such as experiment results were considered of a high importance for a country and necessary security arrangements were implemented to protect the data but not all security vulnerabilities and malicious scenarios were taken into consideration in the design of a research reactor facility, especially those that appeared with evolvement of the technology.

Nuclear material, as listed in the Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, includes specific types of material that require stringent security. Additionally, other radioactive material, which refers to any radioactive material that is not classified as nuclear also demands attention due to the potential risks associated with its misuse [39]. Given these concerns, physical security is employed as a system to protect research reactor facilities and their nuclear and other radioactive materials from malicious acts that could lead to unacceptable consequences.

With increased threats from terrorists, the appearance of black markets for nuclear and other radioactive material, the international community started to pay more attention to the security of a research facility. Due to the historical reasons and multipurpose research reactor facilities the conventional physical security approach that is used for at Nuclear Power Plants is not fully suitable and has to be adopted to the specific aspects of a particular research reactor facility.

This research builds on identified opportunities for improvement and highlights areas where further investigation could enhance the development of effective nuclear security measures for research reactors.

Nuclear facilities, including research reactors, are governed by international guidance and national regulations regarding security arrangements. The responsibility for developing, applying, and integrating a graded approach into the regulatory framework lies with a country's relevant authorities. This research explores how the graded approach can be specifically adapted to the unique characteristics of research reactors. It aims to expand upon existing guidance and enhance understanding of the development and application of this approach. Ultimately, the goal is to assist countries in establishing efficient nuclear security arrangements at research reactors.

This research advances the methodology for attractiveness assessment by integrating and expanding upon existing approaches. The research introduces a comprehensive framework that combines physical properties and potential consequences to evaluate the attractiveness of a research reactor's assets, providing a more holistic and tailored assessment specifically designed for research reactors. Building on established graded approaches, it broadens the potential scope of application to include not only nuclear and other radioactive materials but also the effectiveness of PPS for critical assets such as digital data, research documentation, and equipment.

This research does not include a methodology for assessing the probability of a malicious act. Instead, it introduces a hypothetical threat with specific capabilities to commit such acts at a research reactor. The research introduces four distinct threat groups and their motivation and capabilities: an outsider, an insider among staff, an insider among subcontractors, and an insider among students, trainees, or visitors. Complete and relevant threat profiles for individual research reactors are to be developed at the national level.

This research develops an approach to determine whether the established Physical Protection Systems (PPS) are aligned with the attractiveness level of an asset at a research reactor. This is achieved by introducing a set of coefficients that define the overall attractiveness of an asset. Each coefficient corresponds to specific physical properties of the asset or potential consequences of unauthorized access. In total, seven different coefficients are used, and equations are applied to quantify the overall attractiveness. A matrix of asset attractiveness versus PPS effectiveness is introduced as part of this approach. The methodology is demonstrated through case studies involving a hypothetical facility. In these case studies, the research identifies gaps in PPS effectiveness and proposes potential options for enhancing the PPS based on the specific scenarios.

1 LITERATURE REVIEW

This chapter reviews the literature on key concepts related to the graded approach for nuclear security management. It specifically examines existing research on the attractiveness of Nuclear and Other Radioactive Materials and the application of graded approaches.

1.1 The Design Basis Threat in Nuclear Security

The Design Basis Threat (DBT) is a core tool for planning and implementing physical security at a research reactor facility. According to the International Atomic Energy Agency (IAEA) (2001) the DBT provides a comprehensive description of potential threats posed by both insider and outsider adversaries, detailing their objectives, capabilities, and strategies. The DBT guides the development of appropriate physical protection systems that are aligned with the assessed threats. [1]

In the IAEA's Nuclear Security Series No. 10-G (2021), the Design Basis Threat (DBT) is established through a national nuclear security threat assessment that identifies credible adversaries, including their motivations, intentions, and capabilities. The DBT is then used to develop security measures that protect facilities based on performance-based or prescriptive regulatory approaches. [4]

1.2 Graded Approach in Nuclear Security

The IAEA (2011) highlights that the graded approach for nuclear security management is designed to allocate security resources proportional to the potential risks posed by malicious acts involving nuclear or other radioactive materials [5]. The IAEA (2016) suggests using risk management as a strategy that employs a graded approach to determine the appropriate level and effectiveness of nuclear security measures. This approach aims to achieve a balance between the risks associated with the potential unauthorized removal or sabotage of nuclear or other radioactive materials and the costs involved in implementing these security measures, which may include financial and other resources. In addition, the IAEA (2011) highlights that an implementation of the graded approach for nuclear security needs to take into consideration the particular characteristics of research reactors. [3]

The IAEA guidance (2001) recommends applying a graded approach, considering threat, attractiveness of nuclear materials, and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear material or nuclear facilities [1]. It is recommended that the graded approach is based on categorization of the nuclear material. In the Table 4.1 the IAEA categorization of nuclear material is demonstrated.

Material	Form	Category I	Category II	Category IIIc
1. Plutonium	Unirradiated	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2.Uranium-235	Unirradiated **b** -Uranium enriched to 20% U-235 or more	5 kg or more	Less than 5 kg but more than 1 kg	
	-Uranium enriched to 10% U-235 but less than 20% 235 U			
	-Uranium enriched above natural but less than 10% 235 U			
3.Uranium-233	Unirradiated **b**	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated fuel			Depleted or natural uranium, thorium or low enriched fuel (less than 10% fissile content) **d,e**	

Table 4.1: IAEA categorization of nuclear material

a All plutonium except that with isotopic concentration exceeding 80% in 238Pu.

b Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h at 1 m unshielded.

c Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.

d Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.

e Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/h at 1 m unshielded.

The IAEA's guidance (2021) recommends applying a graded approach to the security of Other Radioactive Materials, taking into account the threat level, the attractiveness of the material for malicious acts, the Code of Conduct on the Safety and Security of Radioactive Sources, and the categorization of radioactive sources. [5]

1.3 Attractiveness Assessment of Nuclear and Other Radioactive Materials

Attractiveness assessment is a critical component in determining the appropriate security measures for nuclear and other radioactive materials. In this context, attractiveness refers to the desirability of nuclear materials to potential adversaries, based on factors such as their ease of use in malicious acts, such as developing an improvised nuclear device (IND), a radiological exposure device (RED), or a radiological dispersal device (RDD), as well as their financial value. The literature on attractiveness assessment is well-developed, with numerous studies offering methodologies for evaluating the attractiveness of different types of nuclear materials.

Research by B. B. Ebbinghaus (2013) focuses on applying a graded approach to assess the attractiveness of nuclear materials at research reactors. This approach is based on an examination of the physical properties of nuclear materials and defines these properties across the phases of Acquisition, Processing, and Utilization. [6]

The U.S. Nuclear Regulatory Commission employs an approach to assess the attractiveness of nuclear materials based on their categorization. This categorization considers a wide range of material characteristics, including type, quantity, chemical composition, physical form, isotopic content, concentration, and level of irradiation. [7]

The IAEA (2015) recommends a risk-informed approach. This approach requires a detailed analysis of the potential impacts of unauthorized acts involving nuclear or other radioactive materials. The consequences considered include public health risks, environmental damage, and economic disruption, along with societal and political ramifications. This thorough evaluation process is crucial for determining the appropriate security measures needed to effectively mitigate identified risks. [8]

The IAEA's guidance (2009) emphasizes the importance of tailoring security measures for radioactive sources, categorized under "Other Radioactive Materials," to the specific risks they pose. The effectiveness of these security arrangements is recommended to be proportional to the categorization of the radioactive sources. This graded approach ensures that higher-risk sources receive more robust protection, while lower-risk sources are secured appropriately, thereby optimizing resource allocation and enhancing overall security effectiveness. [9]

S. Rane and J. T. Harris (2020) developed the Potential Facility Risk Index (PFRI) to quantify radiological security risks in healthcare facilities, integrating threat, vulnerability, and consequence factors. Focused on incidents involving Radiological Dispersal Devices (RDDs) and radionuclides like Cs-137, Co-60, and Ir-192, the PFRI enables self-assessment of security risks. In the PFRI the attractiveness of materials is measured considering radionuclide activity, danger value, and physical form. This approach highlights which materials are more vulnerable to theft or sabotage, providing healthcare facilities with a tool for proactive radiological risk management. [10]

Research by J. L. Kot and J. T. Harris (2024) describes the attractiveness of materials as a key factor in estimating the probability of nuclear terrorism. The study quantifies the relative attractiveness of nuclear facilities and their materials by evaluating multiple criteria. These criteria include the amount of radioactive material, its accessibility, the potential impact on population, economic significance, and the symbolic value of the facility. The more attractive a facility or its materials are in these respects, the higher its likelihood of being targeted in a terrorist attack. [11]

1.4 Assessment of Physical Protection Effectiveness

The IAEA's TECDOC (2019) describes the Assessment of Physical Protection Effectiveness, a central component of nuclear security assessment methodology. This methodology aims to establish a standard risk-informed, performance-based framework for evaluating security measures at nuclear sites. It involves assessing the effectiveness of physical protection systems (PPS) through path analyses, scenario simulations, and performance testing, such as force-on-force exercises. Additionally, it includes calculations of the probability of detecting an adversary. [12]

2 RESEARCH REACTORS

2.1 Power range of research reactors

Technology of research reactors include a broad range of different reactor types. The thermal power varies from below 10 W to about 100 MW. [13]. Generally, research reactors can be divided on

- Low Power (<5MW) with the flux $< 10^{13} n\, cm^{-2} s^{-1}$,
- Medium power (5–20 MW) with the flux $10^{13} - 10^{14} n\, cm^{-2} s^{-1}$, and
- High Power (≥20 MW) with the flux $> 10^{14} n\, cm^{-2} s^{-1}$ [14]

2.2 Applications of research reactors

A research reactor can be used in a variety of applications. However, the power of a research reactor is a limiting factor for some objectives, for example, training can be conducted on a research reactor of any power, but production of medical isotopes would require a neutron flux of a certain magnitude.

The applications of research reactors can be divided in the following areas [15]:

- Education and training.

Research reactors are used for education and training of various groups such as students and researchers, operators, maintenance personnel or nuclear inspectors. Research reactors can be also opened for public tours and visits. In general, with the increase of reactor neutron flux the number of applications it can be used for also increases.

Other radioactive materials such as radioactive sources stored at a research reactor can also be used for training purposes.

- Radioisotope production.

Research reactors can produce radioisotopes for various areas such as nuclear medicine, industry or agriculture. The production implies that those radioisotopes may be stored at the facility before being transported to stakeholders outside of a facility.

Other areas where research reactors are used for:

- Geochronology.
- Transmutation effects.
- Neutron imaging.
- Material structure and dynamics studies.
- Positron sources.
- Neutron capture therapy.
- Testing of materials.
- Neutron activation analysis.
- Prompt gamma neutron activation analysis.

2.3 Designs of research reactors

General designs of research reactors can be divided into pool-type and tank-type reactors. [16]

A reactor in a pool is submerged under water. The submerged core can be enclosed or not within a tank. The depth of the submerged core ensures sufficient protection for staff and public from neutrons and other radiation.

Another design places a reactor in a pool in a vessel with a primary cooling circuit under pressure.

Core construction contains fuel assemblies, control rods and empty channels for experiments.

Water serves as moderator of neutrons and at the same time ensures cooling the reactor. There are research reactors that can also operate with heavy water as moderator and coolant. Less common, research reactors require no moderator due to the operation with fast neutrons, however fast neutron research reactors require highly enriched uranium as fuel (HEU). HEU is a UO2 fuel with enrichment higher than 20% of U-235 [39].

Due to a much smaller size of a research reactor in comparison to a nuclear power reactor, less sophisticated safety systems for research reactors are required. Control rods serve to regulate the power and shut down a reactor. On a low power research reactor in case of a Loss of Coolant Accident with depletion of all coolant the air convection would be enough to maintain cooling of fuel assemblies and ensure the integrity of all barriers.

2.4 Nuclear and Other Radioactive Materials at a research reactor facility

Nuclear Material at research reactors

Primarily, nuclear materials at a research facility serve as fuel, as fissile material to generate neutrons. Historically, the design of a research reactor core was chosen to be compact. To maintain a relatively small core while generating the necessary neutron flux, the fuel must be enriched with more than 20% U-235 by mass, classifying it as highly enriched uranium (HEU).However, thanks to international efforts, and in particularly the US program called Reduced Enrichment for Research and Test Reactors (RERTR) which was launched by the Department of Energy in 1978 [17], it was possible that more than half of research reactors that were operating with HEU now operate with Low Enriched Uranium (LEU) [16]. However, some research reactors cannot use LEU and still use HEU fuel containing up to ~90% U-235.

In addition to fuel in a core, Uranium in different forms can be stored at a research reactor facility, such as:

- A storage of fresh fuel in fuel assemblies prepared to be used.
- If a research reactor facility has a fuel fabrication facility at premises, then nuclear materials used in fuel production can be stored in a different form, for example in the form of UO_2 powder.
- HEU can be stored and used for testing purposes.

Accessible nuclear materials at a research reactor can be attractive for adversaries and can be used for a malicious act, such as construction and detonation of an Improvised Nuclear Device (IND). An IND incorporates nuclear materials intended to produce a nuclear-yield reaction. [34]

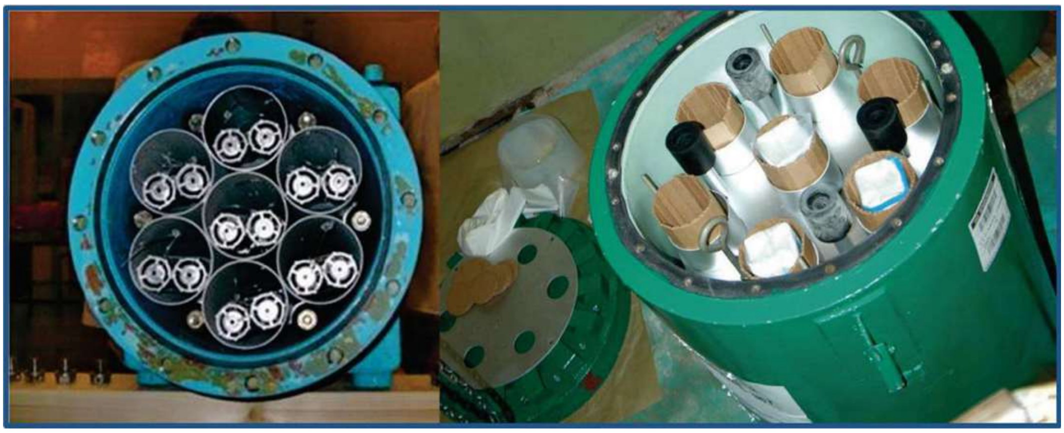


Figure 1.1. HEU fresh fuel storage in Vinca, Serbia, and in Swierk, Poland, at the Maria reactor. [18]

Other Radioactive Materials at research reactors

Depending on the application of a research reactor there can be various radioactive sources stored at a facility. Radioactive sources can be produced by irradiation using the neutron flux of a research reactor. For example, the radioisotope Molybdenum-99 is currently produced via a process that starts with a neutron irradiation of Uranium-235 contained in a plate covered by aluminium alloy. Produced sources then are dispatched to customers in batches by means of transportation. U-235 targets are stored at a research reactor facility. In addition, radioactive sources can be stored at a research reactor facility for training purposes or experiments. A radioactive waste storage building can be located at a facility as well.

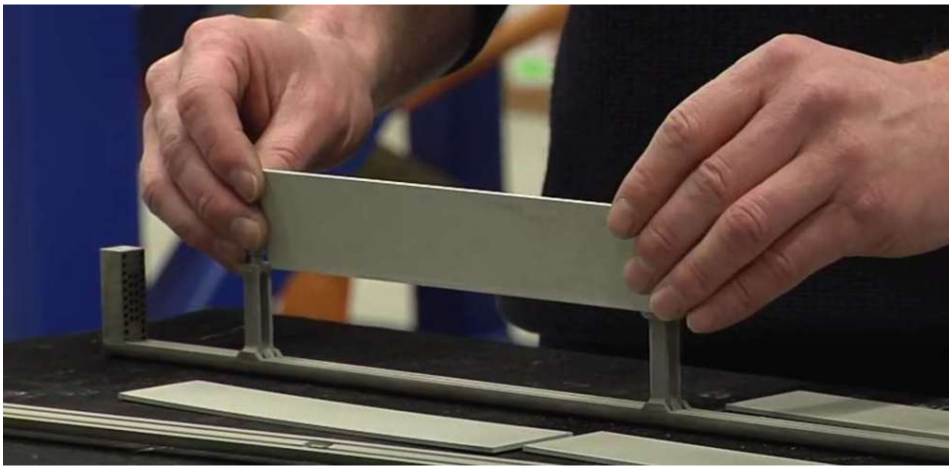


Figure 1.2. Plates of enriched Uranium-235 covered by aluminium alloy that serve as a target to produce Molybdenum-99. [19]

3 VULNERABILITIES OF RESEARCH REACTORS

As mentioned before, research reactors are designed and operated for various purposes. The design of a research reactor is influenced by its operation purpose. The specific designs a research reactor facility and its use might expose a research reactor to vulnerabilities. Vulnerabilities can be linked to easier access on premises, for example for students, visitors or temporary staff. In addition, vulnerabilities can arise from insufficient security procedures and a weak cybersecurity framework.

3.1 Vulnerabilities related to a purpose

In comparison to a nuclear power plant, a research reactor can be a used for a variety of purposes. For example, as a training and educational facility that can host students, visitors, operators, workers of external organizations, participants of mutual research and educational programmes. Research activities may allow unescorted frequent movement of people that are not staff of a research reactor. To effectively administrate security arrangements for the flow of different groups of people is challenging and creates a potential security risk for a facility.

Activities at a research reactor such as experiments, or production of radioisotopes often involve work with other radioactive materials. Research reactor staff and non-staff may be authorized to access and move at a facility with other radioactive materials. Sometimes movements of radioactive materials might not be well defined in a security protocol or not well monitored. This might create a vulnerability for a potential unauthorized removal of other radioactive materials, for example a radioactive source. [3]

3.2 Vulnerabilities related to characteristics and design

Nuclear power plants operate with fuel with a lower enrichment (3-5%) than that usually used at a research reactor (up to about 90%). Nuclear power plants have a much bigger core and hence larger and heavier fuel assemblies in comparison to a research rector’s fuel assemblies. A research reactor operates with a dense and compact core that comprises fuel assemblies of about 1,5 meters. A smaller size of a fuel assembly is likely to be more attractive for adversaries as it is easier in transportation.

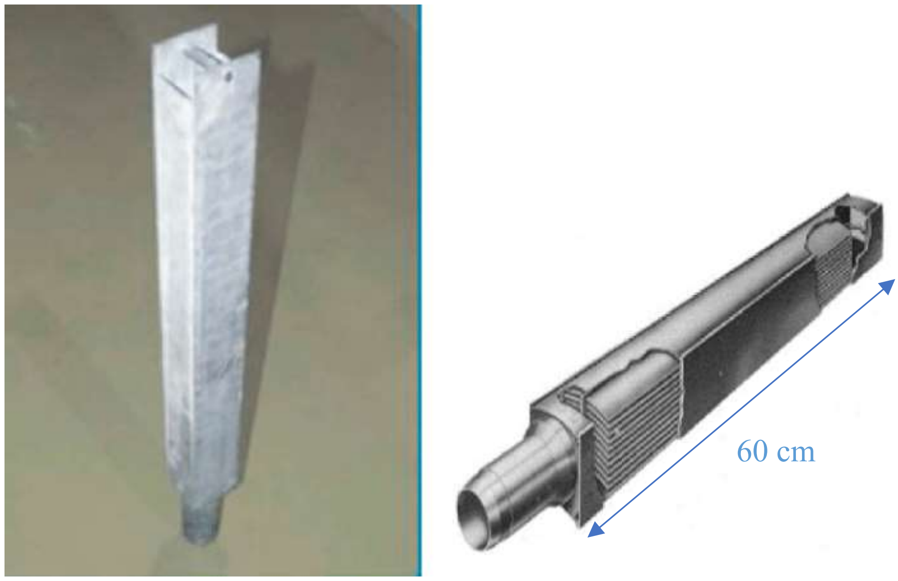


Figure 2.1. Compact research reactor MTR type fuel [20]

For malicious purposes not only fresh fuel can be attractive, but also a spent fuel assembly. Spent fuel from a power plant is most likely to be highly radioactive and difficult to handle and can incapacitate an adversary during an attempt of unauthorized removal. An adversary can be any individual performing or attempting to perform a malicious act [39]. Research reactors may not operate continuously and some spent fuel from a research reactor might not be immediately incapacitating for an adversary. [21]

Nuclear materials and other radioactive materials stored at a research reactor may be a more attractive targets than those at a nuclear power plant due to smaller dimensions that allow easier transportation of materials. In comparison with a Pressurized Water Reactor (PWR) assembly which is around 4 meters [22] a length of Fuel Element Plate MTR is around 60 cm [23] . In addition, chemical composition of nuclear materials in research reactor fuel might make it possible to avoid any chemical reprocessing due to high enrichment. Materials might be obtained easier due to potential weakness in established security measures than at a nuclear power plant. [3]

3.3 Vulnerabilities related to aging of a research reactor

The majority of research reactors are in operation for more than 30 years. The design of a research reactor at construction times might have led to weak security infrastructure and moreover with years the existing security infrastructure might have degraded or does not use up to date security equipment. This might decrease the effectiveness of the Physical Protection System on some old research reactors. [3]

3.4 Vulnerabilities related to equipment and tools that are used at research reactors

To support activities at a research reactor, a variety of experimental equipment is available and accessible for use. For example, tools that allow to remove fuel assemblies from a core, equipment that is used to transport nuclear material and other radioactive materials, tools for shielding. The availability of those tools and possibility of misuse without being detected creates a certain vulnerability at a research reactor [3].

3.5 Vulnerabilities related to a site location

Usually, the location of a nuclear power plant is not in an immediate proximity to a populated area. Research reactors though can be built in a city, for example near a university. In a scenario of an unauthorized removal of other radioactive materials they can be immediately used in a city against members of the public with malicious purposes. A city's traffic may delay the arrival of a response team.

4 THREATS TO RESEARCH REACTORS AND POTENTIAL MALICIOUS ACTS CONSEQUENCES

Threats to research reactors can be posed by adversaries that can be characterized as insiders, outsiders or insiders and outsiders that work in collusion. An insider is defined as an individual with authorized access to facilities, activities, sensitive information, or sensitive information assets who could commit or facilitate criminal or intentional unauthorized acts involving nuclear or other radioactive material, facilities, or activities that could adversely impact nuclear security. In contrast, an outsider is an adversary without such authorized access. [39]

Arrangements of a PPS against insiders at a research reactor pose the highest challenge due to authorized access for different groups of individuals involved in activities at a research reactor. Potential insiders can have access to different locations and tools that can be used for a malicious act.

To commit a malicious act, an adversary can use different tactics: deceit, force or stealth. Deceit tactic aims to defeat and overcome security systems being detected but not as an adversary, for example using a false staff badge. Force tactic aims to overcome security systems using force, this is an open attack on a facility which is almost certainly immediately detected, for example when a group of armed and skilled adversaries enters a facility. Stealth tactic aims to enter a facility and reach a target without being detected. Different combinations of tactics can be used for a malicious act, for example entering a facility without being detected but then change to using force. [24]

A research reactor can be targeted for the following purposes:

- Theft of nuclear material which can be used to:
  - Construct an improvised nuclear device (IND). "IND is a device incorporating radioactive materials designed to result in the formation of a nuclear-yield reaction." [39]
- Theft of any other radioactive materials, such as radioactive sources or spent fuel, which can be used to:
  - Construct a radiation exposure device (RED) (see fig 3.1 on the left). "RED is a device with radioactive material designed to intentionally expose members of the public to radiation". REDs emit radiation without dispersing radioactive substances, they can be installed and hidden in popular areas such as on a transport (e.g., a train or a bus) or a train station, music venues, restaurants, or sports arenas. [25]
  - Construct a radiological dispersal device (RDD) (see fig 3.1 on the right). "RDD is a device to spread radioactive material using conventional explosives or other means". RDDs have the capacity to disperse radioactive debris, potentially leading to contamination of nearby areas and an elevated risk of individuals developing radiation-related illnesses. Furthermore, RDDs can be used to trigger panic and fear in public spaces, potentially resulting in casualties. [25]

- Sabotage of equipment.
  - Sabotage can cause a disturbance in an operation of a research reactor or cause an accident with a radioactive release.

Figure 3.1. Radiological Exposure Device installed in a public transport (on the left) [26] and Radiological Dispersal Device (a "Dirty Bomb") (on the right). [27]

5 THE GRADED APPROACH FOR NUCLEAR SECURITY MANAGEMENT OF RESEARCH REACTORS (THE RR-NSM GRADED APPROACH).

5.1 Objective

The objective of this research develops a methodology of the RR-NSM graded approach based on the outlined recommendations of the IAEA. In addition, the objective is to demonstrate how the developed methodology can be applied to a research reactor using case studies.

The methodology elaborates on how to assess the attractiveness of a research reactor facility's assets. The assessed attractiveness of assets serves as input data to the RR-NSM graded approach. Based on attractiveness of assets the approach allows to identify or justify the level of Physical Protection Systems (PPS) effectiveness needed at a research reactor.

In addition, the methodology will allow to conduct self-assessments to assess if the effectiveness of Physical Protection Systems meets the necessary level of security needed based on the attractiveness of assets.

5.2 Scope

This methodology provides a description of hypothetical threats from adversaries of different groups: outsiders and insiders. The insiders are divided in groups: research reactor staff, students, visitors and subcontractors. The RR-NSM graded approach proposes conservative characteristics of hypothetical adversaries and lists their capabilities, motivation, tactics, and potentially used tools. Characteristics can be amended for a particular scenario of a malicious act based on available information. Methods on evaluation of threats by intelligence services is out of this work's scope.

The RR-NSM graded approach describes criteria that assist identifying the level of attractiveness of a research reactor asset based on two components:

1. Potential consequences of a malicious act involving a research reactor asset.

2. Physical properties of an asset.

Furthermore, it describes how to conduct a self-assessment of effectiveness of physical protection systems on a research reactor for outsider and insider in particular scenarios. The assessed effectiveness of the PPS is then compared to the attractiveness of assets.

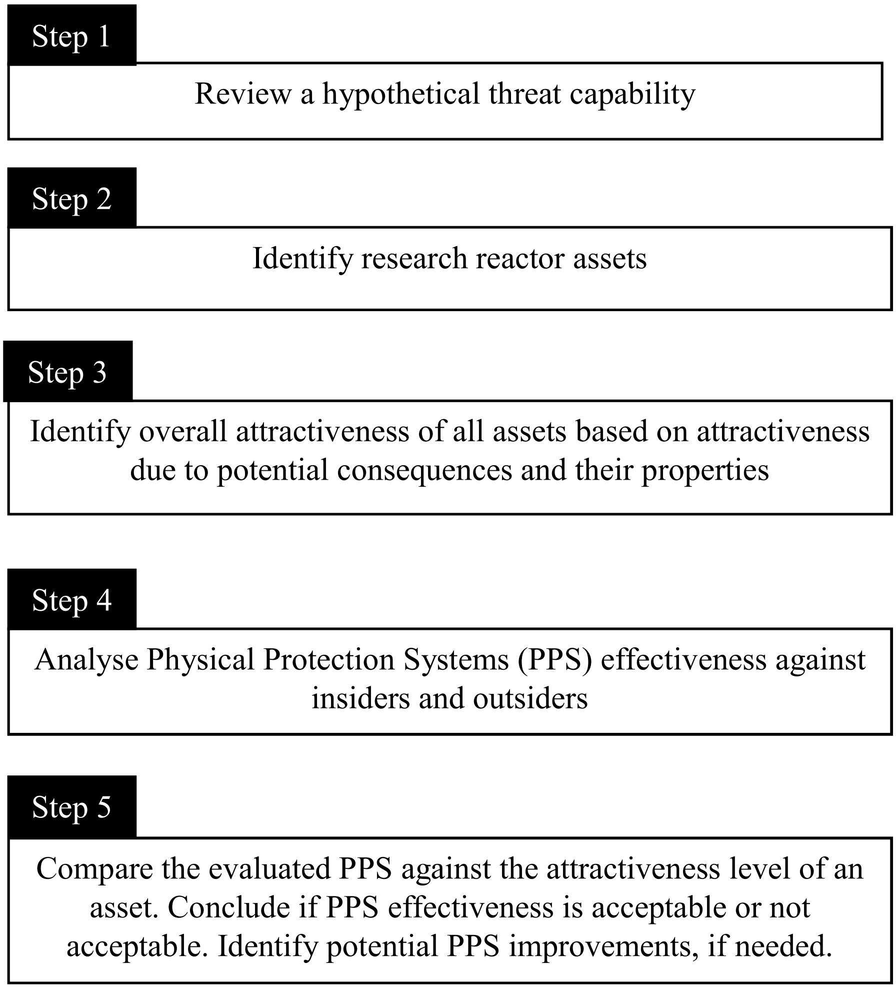
Finally, it will be tested with three case studies using three different scenarios of malicious acts.

For two of the case studies a hypothetical facility "The Shapash Nuclear Research Institute (SNRI)" developed by the IAEA will be used. For the third case study, for the purpose of this research, the hypothetical Shapash facility will be modified to an isotope production facility. The modified Shapash facility will allow analysing additional assets as potential targets.

Detailed assessment of an external response team effectiveness is out of the scope of this work. The RR-NSM graded approach has the following assumptions with regards to response team effectiveness:

- High probability of communication to Response Force.
- High probability of deployment to proper location.
- High probability of adversary neutralization or detention.
- High probability that capabilities of a response team overpower capabilities of adversary(ies).

5.3 Structure of the RR-NSM graded approach.



Step 1

Review a hypothetical threat capability

Step 2

Identify research reactor assets

Step 3

Identify overall attractiveness of all assets based on attractiveness due to potential consequences and their properties

Step 4

Analyse Physical Protection Systems (PPS) effectiveness against insiders and outsiders

Step 5

Compare the evaluated PPS against the attractiveness level of an asset. Conclude if PPS effectiveness is acceptable or not acceptable. Identify potential PPS improvements, if needed.

5.4 Step 1. Review a hypothetical threat for a research reactor.

Due to the broad range of a research reactors' objectives, its premises can be accessed by different groups of individuals including research reactor staff, students, subcontractors, external visitors and temporary staff. Different groups of individuals represent insiders and outsiders with different capabilities, knowledge, motivation and hence pose different threats. Each group is designated as a 'Threat Category' with a number from 1 to 4. In this research, the Threat Categories described are unique and were established specifically for this research, distinct from any existing threat categories.

The process to describe the threat groups includes developing conservative characteristics of hypothetical adversaries and lists their motivation, capabilities, possible tactics and potential tools. The considered capabilities of a threat can be amended for a particular scenario of malicious acts based on available information (e.g., from national intelligence service).

In addition, the hypothetical threat description can be updated based on any recent known malicious events or criminal groups activities in a country or in neighbouring countries. For example, if a nuclear facility gets attacked by adversaries, then neighbouring countries might consider changing the security posture at their nuclear facilities. Following an investigation of an attack on a nuclear facility (or other facility) neighbouring country might be able to share information related to the capabilities of adversaries though intelligence service liaisons. Based on received information, decision makers can update the description of a hypothetical threat and decide on introducing changes in a current nuclear security arrangement.

These activities related to describing and updating the threat groups may be done during a national nuclear security threat assessment in the framework of the Design Basis Threat development [1].

5.4.1 Threat Category I. An Outsider or a group of outsiders.

A description of a hypothetical threat from an outsider or a group of outsiders lists possible motivations, capabilities, potential targets, tactics that can be used and potential tools. The objective of the lists below is not to provide exhaustive information of all possible options but serve as a characteristic of a hypothetical outsider's profile. A conservative estimation of characteristics includes the following aspects:

1. **Presence and profile of outsider**

An outsider exists and can physically reach a facility. An outsider can be a local resident with a citizenship of the country where a research reactor is located or can be a foreign citizen. An outsider can have no registered police reports, can be not under observation or suspicion of police or intelligence services.

2. **Motivation of an outsider**

An outsider has a moderate motivation and intentions to commit a malicious act. Motivation can be dictated by financial gain objectives (e.g., selling stolen material or asking for a ransom), by ideological attitude (e.g., antinuclear activists) or by a personal reason with intention to cause causalities, panic, or property damage (e.g., a former worker whose attitude became hostile to a former employer). [24]

3. Capabilities of an outsider

An outsider has enough capabilities to attempt a malicious act and can operate in a group of outsiders.

Technical capabilities of outsiders:

- Capable to use tools or techniques (lockpicking) to breach all conventional barriers at a facility (fences, walls, reinforced concrete walls, any type of doors).
- Capable to use handheld weapons against guards and law enforcements.
- Capable to use methods of communication.
- Capable to organize a cyber-attack to compromise security systems (such as reduce the detection effectiveness at a facility, if technically possible).

Financial capabilities of outsiders:

- Potentially unlimited financial capabilities:
  - May purchase all necessary equipment.
  - May attempt to bribe staff or members of security.

Organizational capabilities of outsiders:

- Have a safe place that is unknown to police.
  - for meetings to plan a malicious act
  - for coordination on the course of a malicious act.

Tactical capabilities:

- Capable to apply different tactics:
  - Deceit – use technics to defeat a PPS by using false authorization and/or identification (e.g., use a stolen but valid identification documents, key cards, badges to enter a facility without being noticed).
  - Force - use technics to overpower physical barriers and security staff.
  - Stealth – use technics to overcome physical barriers but infiltrate the facility undetected.
  - Combined tactics – combination of tactics above. [24]

4. Outsiders can obtain and use the following tools

Weapons:

- Guns
- Assault rifles
- Hand grenades
- Knifes

Transport:

- Car
- Van
- Truck

Equipment tools:

- Lock picking tools
- Explosives
- Circular saw
- Ladder
- Sledgehammer
- Manual bolt cutters
- Roto hammer, drill
- Cutting torch and portable generator
- Other handheld tools that are available on the market.

5.4.2 Threat Category II. An insider.

Due to the broad range of objectives of a research reactor facility the premises can be accessed by different groups of people who have different access rights at a facility. A description of a hypothetical threat from an insider includes characteristics of three sub groups of potential insiders:

1) Research reactor staff, 2) Sub-contractor workers, 3) Students, trainees, or visitors.

Although there may be multiple insiders at a facility, the most probable threat is considered to come from a single insider. Capabilities of an insider from considered groups described below: [24]

5.4.2.1 An insider among the research reactor staff

An insider among research reactor staff represents a most powerful insider with possibility to move withing a facility. Traditionally a major part of a physical protection system is built to detect and delay an outsider, however an insider can overcome some physical barriers without detection. This category of an insider represents the highest potential threat to assets of a facility.

1. **Presence and background of an insider among research reactor staff**

An insider among research reactor staff might be present or might appear. An insider can be a local resident with a citizenship of the country where a research reactor is located or can be a foreign citizen. An insider can have no registered police reports, can be not under observation or suspicion of police or intelligence services. An insider has successfully passed security background checks during a recruitment process. An insider can have no indication of the following factors: degradation of his/her financial situation, consumption of drugs or alcohol, radicalization, connection with criminal structures, depression, psychological issues. An insider can be trusted by co-workers and security personnel.

2. **Motivation of an insider among research reactor staff**

An insider has the same motivation as an outsider. A research reactor staff may be radicalized during their work at a research reactor. A staff member may become frustrated with an employer or co-workers and become an insider.

3. Capabilities of an insider among research reactor staff

Knowledge:

- Value of assets.
- Location of assets, locations of tools, layout of a facility.
- Knowledge in radiation protection.
- Security arrangements on a facility.
- Schedule of activities (e.g., experiments, deliveries of materials, shipment of materials).
- Schedule of co-workers.
- Code combinations of doors, safes.
- PC passwords, passwords from an online library with digitally stored confidential documents.

Technical capabilities of an insider:

- Have access rights to areas with assets, do not need to be escorted.
- Capable to use tools available for staff.

Tools

- ID badges.
- Keys.
- Shield containers, dose rate meters.

Weapons:

- A gun
- A knife
- Available tools that can be used as a weapon (e.g., a hammer, scissors)

Tactical capabilities: [24]

- Can be passive (e.g., secretly provide information to outsiders and stay undetected)
- Can be active, but nonviolent (e.g., assist outsiders infiltrating a facility by eliminating physical barriers on their way and tamper with security systems to decrease an effectiveness of detection).
- Can be active and violent (e.g., participate in a violent attack along with outsiders or alone).

Transport:

- Car
- Van
- Truck

Access permissions

- Have permissions to access the protected area of an asset.

5.4.2.2 An insider among sub-contractor workers.

A research reactor facility may need to have sub-contractor workers to conduct certain activities on site. Sub-contractor workers are not part of research reactor staff but may conduct work involving assets or in the proximity of assets (e.g., refuelling of a research reactor). Sub-contractors can have access to tools available on site or tools belonging to a sub-contractor organization that they are authorized to bring to the facility.

1. Presence and background of an insider among sub-contractor workers

An insider among sub-contractor workers has the same background as an insider among research reactor staff.

2. Motivation of an insider among sub-contractor workers

An insider among sub-contractor worker has the same motivation as an insider among research reactor staff.

3. Capabilities of an insider among sub-contractor workers

Knowledge:

- Location of some assets, layout of a facility they have access to.
- Basic understanding of security arrangements based on visual observation.

Technical capabilities of an insider:

- Have access to protected areas, including areas with assets.
- Capable to operate large tools.

Tools

- ID badges of sub-contractor workers.
- Dose rate meters.
- Large tools (e.g., cranes for loading and unloading a research reactor, shipment containers).
- Repair tools (e.g. drills, hammers, ladders).

Weapons:

- A gun
- A knife
- Available tools that can be used as a weapon (e.g., a hammer, scissors)

Tactical capabilities: [24]

- Can be passive (e.g., secretly provide information to outsiders and stay undetected).
- Can be active, but nonviolent (e.g., assist outsiders infiltrating a facility by eliminating physical barriers on their way and damage security systems to decrease an effectiveness of detection, smuggle weapons on a site).
- Can be active and violent (e.g., participate in a violent attack along with outsiders or alone).

Transport:

- Car
- Van
- Truck

Access permissions

- Have permissions to access the protected area with an asset.
- Do not have permissions to access protected area.

5.4.3 Threat Category IV. An insider among students, trainees or visitors.

A number of research reactor facilities are affiliated with universities and may be visited by students to attend lectures, practical classes or conduct experiments. Staff from another establishment may be trained using equipment, instruments, nuclear material, other radioactive materials available on premises. In addition, visitors may be authorized to enter a research facility in an organized group for a short time.

1. Presence and background of an insider among students, trainees or visitors

An insider among students, trainees or visitors has the same background as an insider among research reactor staff, however they have no security background checks since they were not recruited. An insider from this group can have no visible indication of malicious intentions against a research reactor facility. An insider can be trusted by his/her classmates and professors from a research reactor staff.

2. Motivation of an insider among students, trainees or visitors

An insider among students, trainees or visitors has the same motivation as an outsider. A student may be frustrated with a professor affiliated with a research reactor facility.

3. Capabilities of an insider among students, trainees or visitors

Knowledge:

- Low or no knowledge regarding of a location of some assets and layout of a restricted area.
- Basic understanding of security arrangements based on visual observation.

Technical capabilities of an insider:

- Have no individual access rights to restricted areas with assets (only under supervision).
- Not capable to operate large tools.

Tools

- Authorized to use tools for training and experimental purposes.
- Not authorized to use large tools (e.g., cranes for loading and unloading a research reactor, shipment containers).
- Not authorized to use repair tools (e.g., drills, hammers, ladders).

Weapons:

- A gun
- A knife
- Available tools that can be used as a weapon (e.g., a hammer, scissors)

Tactical capabilities: [24]

- May be passive (e.g., secretly provide information to outsiders and stay undetected).
- May be active, but nonviolent (e.g., assist outsiders infiltrating a facility by eliminating physical barriers on their way and damage security systems to decrease an effectiveness of detection).
- May be active and violent (e.g., participate in a violent attack along with outsiders or alone).

Transport:

- Car.
- Van.
- Truck.

Access permissions

- Do not have permissions to access protected area or limited permissions to access the protected area (only under supervision).

5.5 Step 2. Identify a research reactor's assets (potential targets)

Assets of a research reactor are objects or equipment that are crucial for a research reactor's objectives and activities. Decision makers have to take into consideration that the same asset can be targeted for theft or for sabotage that can lead to different consequences. This thesis suggests an approach on how to identify research reactor assets based on services provided by a research reactor.

Services that are fulfilled by a research reactor are conducted based on established procedures and arrangements at a facility (see Fig. 5.1). In order to run processes at a facility research reactor staff use resources, those resources can be characterised as research reactor assets.

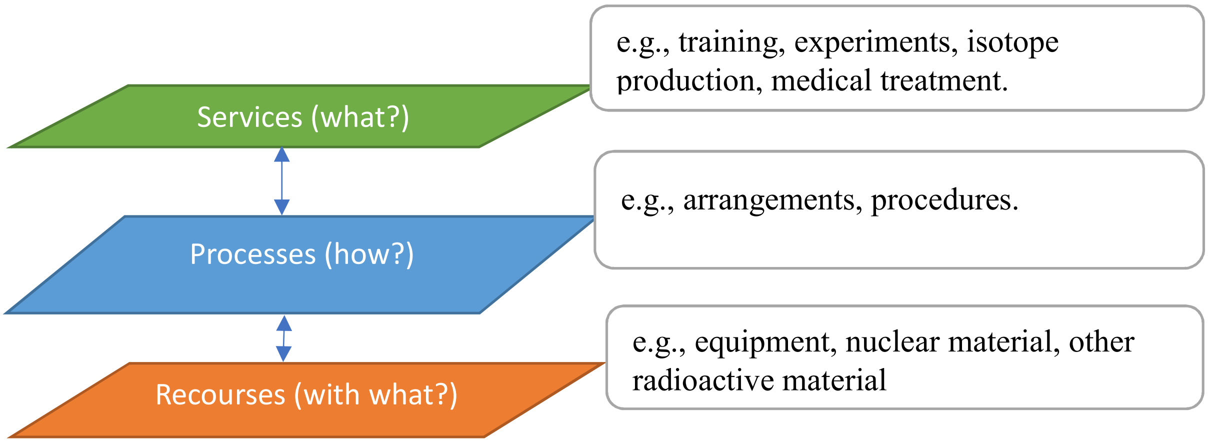

e.g., training, experiments, isotope production, medical treatment.
Services (what?)
e.g., arrangements, procedures.
Processes (how?)
e.g., equipment, nuclear material, other radioactive material
Recourses (with what?)

Fig. 5.1 Identification of assets based on services provided by a research reactor facility.

It is suggested to use a generic research reactor list of assets presented in Table 5.1 below as a starting point for identification of assets. Depending on a research reactor's activities (services) other assets may be identified and added to the list. Non-relevant assets can be removed from the generic list.

No	Asset of a research reactor	Theft target	Sabotage target
1	Nuclear Materials	yes	yes
2	Other Radioactive Materials	yes	yes
3	Information stored in digital or hard copies	yes	yes
4	Radioisotope production equipment		yes
5	Irradiation equipment, test items etc.		yes
6	Medical treatment equipment		yes
7	Equipment in laboratories, hot cells		yes

Table 5.1: Generic research reactor assets

5.6 Step 3. Identify overall attractiveness of assets.

Once the assets of a research reactor are identified, the next step of the RR-NSM graded approach is to evaluate the attractiveness of these assets. The RR-NSM graded approach provides a methodology to estimate the attractiveness of assets at a research reactor with consideration of two factors:

i) Consequences of a malicious act involving an asset.

ii) The asset's physical properties that can directly influence its attractiveness.

A detailed evaluation of attractiveness based on consequences and physical properties is presented below.

5.6.1 Attractiveness of research reactor assets based on potential consequences.

The attractiveness of research reactor assets based on potential consequences is characterized by three key aspects: health effects, financial impact, and the impact on the mission or reputation of the research reactor. To quantify the attractiveness in terms of these potential consequences, a set of coefficients is used. These coefficients serve to distinguish different properties of the asset that influence the severity of consequences. Each coefficient is associated with specific criteria, which reflect the potential outcomes of a malicious act. The values corresponding to these coefficients are later used in equations to quantify the overall attractiveness of the material.

The three aspects that characterize the potential consequences of a malicious act involving an asset are:

i) Health effects or radiological contamination, represented by coefficient HL

Health effects refer to potential harm to individuals working or studying at the research reactor, as well as to the public offsite. Radiological contamination that leads to health impacts is also considered. The criteria for determining health effects and contamination are based on the IAEA guide Categorization of Radioactive Sources [29].

ii) Financial impact, represented by coefficient F

Financial impact refers to the potential monetary losses for the organization operating the research reactor. The approach introduces generic criteria for assessing financial impact, but these criteria can be adapted according to the specific needs of the organization.

iii) Impact on mission and reputation, represented by coefficient M

This aspect evaluates the potential harm to the research reactor's mission, the operating organization, affiliated institutions (e.g., a university), or the broader nuclear industry in the country [8]. Like for the Financial impact, the RR-NSM approach suggests generic criteria for assessing the impact on mission and reputation, which can be modified as needed.

The attractiveness of an asset based on consequences is evaluated by examining the potential outcomes in these three areas. Each area is represented by a corresponding coefficient, and the criteria for each are described in detail below. These coefficients, once assigned, will be used in the subsequent equations to determine the overall attractiveness of the asset in the context of potential consequences.

5.6.1.1 Health Effects or/and radiological contamination

Consequences of a malicious act involving nuclear material or other radioactive material may cause an impact on public health or research reactor staff. In addition, it can lead to health impact of those who work or study on premises of a research reactor.

Consequences of a malicious act can lead to an exposure of an individual by a placed radioactive material at a public location (e.g. radioactive source) or if dispersed it may cause a radiological contamination on site or off site of a facility or be inhaled by an individual. Radiologically contaminated areas require remediation activities.

Health impacts due to exposure of a non-dispersed and/or dispersed material are divided in four levels: High (H), Moderate (M), Low (L) and Very Low (VL). Levels of impact on health or/and radiological contamination in line with the IAEA's guidance are described in Table 5.2.

Impact	Description
High (H)	- Contaminated area is more than 1 km² (Cat. I) - Permanent injury in more than a few minutes of exposure and fatal if exposure time is between a few minutes and an hour (Cat. I)
Moderate (M)	- Contaminated area is less than 1 km²; (Cat. II) - Permanent injury if exposure time is between a few minutes and an hour and fatal if exposure time is between hours to days (Cat. II)
Low (L)	- Contaminated area is a small fraction of 1 km² (Cat. III) - Permanent injury if exposure time is for some hours (Cat. III)
Very Low (VL)	- No significant contamination (Cat. IV-V) - Permanent injury is unlikely or impossible (Cat. IV-V)

Table 5.2: Impact levels on health due to exposure of non-dispersed or dispersed radioactive materials. [29]

5.6.1.2 Financial impact

A malicious act can lead to a financial impact on a research reactor facility. For example, due to a disruption of a research reactors services such as research activities, trainings, production of medical sources. In addition, depending on contracts with stakeholders a research reactor may be subjected to fees. In the RR-NSM graded approach, the financial impact is divided in four levels: High (H), Moderate (M), Low (L) and Very Low (VL) (see Table 5.3).

Impact	Description
High (H)	Extreme financial loss (more than 30% of annual funds)
Moderate (M)	High financial loss (10-30% of annual funds)
Low (L)	Significant financial loss (2-10% of annual funds)
Very Low (VL)	Negligible financial loss (less than 2% of annual funds)

Table 5.3: Financial impact levels

The proposed criteria for a financial loss can be amended by a research reactor facility, if needed.

5.6.1.3 Mission, Reputation

A malicious act can compromise a research reactor’s reputation and its mission commitments, for example a disruption of activities such as regular production of radioactive sources for medical activities. In addition, a malicious act can lead to a reputation damage of affiliated establishments (e.g. a university), reputation damage of a governmental regulator and a reputation of the nuclear industry and hence decrease of public support in nuclear in the country.

In this approach the impact on mission or reputation is divided in four levels: high, moderate, low and very low (see Table 5.4).

Impact	Description
High (H)	Complete breakdown of credibility, loss of stakeholders, loss of funding. Could cause grave damage to the organization. Could cause extensive or irreparable damage to the organizational interests.
Moderate (M)	Leading to reduced credibility and reduced funding. Could cause serious damage to the organization. Could weaken or impair the organizational' s interests. Serious impact to the course of action and outcome.
Low (L)	May lead to reduced credibility and reduced funding. Could be prejudicial to the organization. Could cause inconvenience or embracement to the organization. Impact is felt but not critical for the outcome.
Very Low (VL)	Not affected

Table 5.4: Impact levels of Mission and Reputation

5.6.1.4 Attractiveness of assets based on potential consequences as a result of a malicious act.

The attractiveness of assets based on potential consequences is assessed based on impacts on the three areas: Health, Financial and Reputation. Each asset that was identified (see chapter 5.5) should be included in the list for attractiveness assessment.

The same asset can be targeted for sabotage or theft. A scenario that leads to the most significant impact should be chosen for attractiveness assessment.

Table 5.5 represents a template to be used for analysing attractiveness by consequences. Values in the table 5.5 should be filled in based on levels of a potential impact as a result of a malicious act involving an asset. Values are obtained by using tables describing impact in specific areas (Tables 5.2, 5.3 and 5.4). A separate table for each asset should be created.

Asset	Impacted areas			Attractiveness by Consequences
	Health effect (HL)	Financial (F)	Mission, Reputation (M)	
Nuclear Materials				
Other Radioactive Materials				
Radioisotope production equipment				
Irradiation equipment, tested detectors etc.				
Medical treatment equipment				
Equipment in laboratories, hot cells				
Digitally stored data (e.g., on PCs, flesh drives, etc.)				
Information in hard copies				

Table 5.5: Generic table for analysing attractiveness by consequences

A malicious act impacting only one area may lead to unacceptable consequences. Thus, a level of the attractiveness by consequences is represented by the highest value of any impacted area for a particular asset. Values for different levels of attractiveness by consequences are presented in Table 5.6.

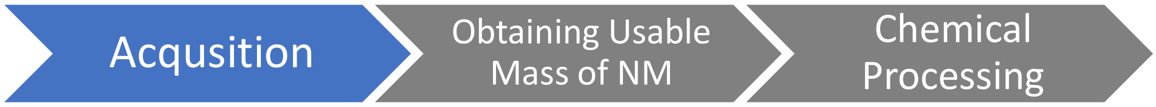
C1 - Overall attractiveness of an asset by consequences	
The highest from (HL, F or M)	
High (H)	1
Moderate (M)	0.75
Low (L)	0.5
Very Low (VL)	0.2

Table 5.6: Related values for different levels of attractiveness by consequences

5.6.2 Attractiveness of assets based on their properties.

5.6.2.1 Description of asset’s physical properties that influence attractiveness.

The second component that characterises attractiveness is dictated by the asset properties. In general, an adversary needs to overcome certain phases to complete a malicious act:



- Acquisition: to seize and transport an asset. Acquisition is applicable to both Other Radioactive Material and Nuclear Material. Acquisition is marked with a blue background above to highlight that it is applicable to both.

- Obtaining Usable Mass of Nuclear Material (NM): the Usable Mass represents quantity of NM that is sufficient to create an Improvised Nuclear Device. The International Atomic Energy Agency's (IAEA) Safeguards categorize this category of NM as “direct use material”. Direct use material - “Nuclear material that can be used for the manufacture of nuclear explosive devices without transmutation or further enrichment” [30].
For instance, if at a research reactor there is 125 kg of stored fresh nuclear fuel with 20% enrichment of U-235 it means that in total it contains 25 kg of U-235, the 25 kg of U-235 in HEU meets the threshold for constructing a nuclear device [30], in this case 125 kg of fresh nuclear fuel (containing 25 kg of U-235) is considered sufficient Usable Mass of Nuclear Material (NM). It is important to note that the total mass the adversary needs to acquire and then use is 125 kg of fresh fuel. However, separating U-235 from reactor fuel is a complex and technically challenging process, requiring sophisticated chemical and engineering techniques, which adds a significant barrier to the misuse of such material. These difficulties in separating uranium species are integral to the physical properties related to Chemical Processing and are discussed further in the subsequent sections.
In the RR-NSM approach the potential to obtain Usable Mass of NM for an Improvised Nuclear Device represents the highest level of attractiveness for an adversary.

It is important to highlight that the capabilities of the considered adversaries do not include processes such as transmutation and Uranium enrichment. Therefore, nuclear materials requiring further processing through methods like transmutation and enrichment (e.g., depleted, natural, and low-enriched uranium) are not considered in the stage of "Obtaining Usable Mass of NM".

- Chemical Processing: to conduct chemical processing activities with Nuclear Material before it can be used as a Nuclear Improvised Device (extracting pure fissile material like Pu-239 or U-233 using chemical processes). Chemical Processing is applicable to Nuclear Materials.

Each phase may represent certain challenges or obstacles for an adversary, depending on the material properties which can affect an asset's attractiveness [6].

For Other Radioactive Material the phase 'Acquisition' is the major part that influences the attractiveness based on properties. To commit a malicious act using Other Radioactive Material an adversary does not require any effort in 'Chemical Processing' and obtaining Usable Mass of NM is irrelevant. Using Other Radioactive Material in a malicious act might require some efforts involving handling it, but it doesn't require to consider a separate phase since the health risks are already taken into consideration in the 'Acquisition' phase.

Challenges during acquisition

Activities during this stage may include close contact with an asset during transportation. Any properties that can complicate an adversary's activities may reduce or even prevent an adversary from a malicious act. For example, an asset can be too bulky or heavy which can complicate carrying and transportation or vice versa can be small and easily transported in a bag or a pocket. An asset can have health effects on an adversary due to its radioactivity or toxicity. In the acquisition stage the properties of an asset that affect transportability and health effects during transportation are considered. In case of sabotage, transportability may play little role so only health effects would be considered.

Challenges during obtaining Usable Mass of Nuclear Material (NM)

There are two main challenges obtaining Usable Mass of NM:

- An adversary needs to obtain NM with appropriate properties [22]:
    - *Plutonium (for Pu containing less than 80% Pu-238)*
    - *U-233*
    - *U-235 in HEU (with U-235>=20%)*
- An adversary needs to obtain enough quantity of NM in order to be able to produce an Improvised Nuclear Device:
    - ***8 kg** plutonium (for Pu containing less than 80% Pu-238)*
    - ***8 kg** U-233*
    - ***25 kg** U-235 in HEU (with U-235>=20%). The total mass of NM will depend on the enrichment.*

If both criteria are met, the obtained NM is considered as Usable Mass of NM. If a facility stores NM with appropriate properties but only 10% of the quantity required to form a

Usable Mass of NM, that means that an adversary would need to obtain 90% more of the same NM which may require more effort and hence may decrease the attractiveness.

Challenges during chemical processing

Depending on the properties of NM (e.g., level of enrichment) acquired during the first stage, an outsider would also need to be able to extract fissile material and process it into a chemical and physical form that can be used for manufacturing an improvised nuclear device. This process requires access to advanced technologies, proficiency in chemistry and access to the necessary chemicals and equipment. In addition, knowledge in other domains is crucial, for example, such as explosives, electronics, nuclear physics, and engineering. Furthermore, the adversary would need to gain access to comprehensive design blueprints for nuclear weapon components and a fully assembled device. [31]

5.6.2.2 Grades of attractiveness based on asset's properties.

Grades of attractiveness represent how attractive an asset may be to an adversary (high, moderate, low, or very low). To quantify this, a coefficient is calculated based on the asset's physical properties, which directly corresponds to its attractiveness grade. These coefficients serve to distinguish different physical properties of the material, with each coefficient representing a specific characteristic that influences the overall attractiveness. These values are later used in an equation to quantify how attractive a material is to an adversary.

Four distinct physical properties of an asset are considered: *transportability, health effects during handling, chemical processing complexity and time (if applicable), and usable mass of nuclear material (if applicable).*

The potential adversary's effort is divided into three phases:

i) **Effort during Acquisition, which depends on:**

- Transportability of an asset, represented by coefficient P.
- Health effects on the adversary, represented by coefficient R.

ii) **Effort during obtaining Usable Mass of Nuclear Material, which depends on:**

- The required material mass, represented by coefficient M.

iii) **Effort during Chemical Processing, which depends on:**

- Processing time and complexity, represented by coefficient T.

Each effort is characterized by a specific description, corresponding to a coefficient. These are presented in the four tables below (5.7 - 5.10).

The physical properties related to chemical processing (time and complexity) and usable mass of Nuclear Material are applicable only for Nuclear Materials. In scenarios involving Other Radioactive Materials where no chemical processing is required, the corresponding coefficients should be omitted from the assessment.

A relevant value must be chosen after an assessment of properties that affect the transportability of an asset (see Table 5.7).

Transportability	Coeff. (P)	Comments
Can be transported by an individual	1	Consider if any available tools can be used to make the transportability easier
Requires a vehicle	0.75	
Requires a heavy truck	0.5	
Unlikely to be transported	0.2	

Table 5.7: Coeff. (P): Coefficient that define attractiveness based on properties affecting transportability during the acquisition stage.

A relevant value must be chosen after an assessment of properties contributing to the potential health effects due to radiation during an acquisition of an asset (see Table 5.8).

Health effects due to radiation dose rate	Coeff. (R)	Comments
Not fatal	1	
Permanent injury or fatal	0.75	after a short time of contact (minutes to hours) [29]
Promptly incapacitating	0.2	before the adversary can successfully steal the item

Table 5.8: Coeff. (R): Coefficient that define attractiveness based on properties contributing to the potential health effects.

A relevant value must be chosen after an assessment of the Usable Mass of NM that is needed to construct a nuclear explosive device (NED) (see Table 5.9).

A Usable Mass of NM requirement	Coeff. (M)	Comments
Sufficient material to build a NED (100% Usable Mass)	1	A single, or two, or multiple thefts of nuclear material must be performed
Twice the amount is needed (50% Usable Mass)	0.75	
Ten times the amount is needed (10% Usable Mass)	0.5	
More than ten times the amount is needed (less than 10% Usable Mass)	0.2	

Table 5.9: Coeff. (M): Coefficient that define attractiveness based on a Usable Mass requirement.

A relevant value must be chosen after an assessment of the properties that affect chemical processing time and complexity of an asset (see Table 5.10).

Chemical processing time and complexity	Coeff. (T)	Comments
No processing	1	Weapon Grade (>90% U-235) – no processing is required
Low processing	0.75	High Grade (20-90%)
Medium processing	0.5	Moderately Diluted (<20%)
High processing	0.2	Highly Diluted (<1%)

Table 5.10: Coeff. (T): Coefficient that define attractiveness based on minimum chemical processing effort.

Nuclear Material that must undergo Medium or High processing complexity (see Table 5.10) needs to be either enriched or irradiated and reprocessed before it can be used as a NED. The capability to irradiate or enrich NM falls outside the adversary's capabilities scope. However, the relatively low attractiveness of this type of NM is conservatively considered in the RR-NSM graded approach.

A combination of identified coefficients above represents the overall attractiveness of an asset by its physical properties.

Calculation of asset's attractiveness influenced by its properties.

To obtain a value for the overall attractiveness depending on properties an average value has to be calculated.

For Nuclear Material an average value is calculated by using all coefficients:

$$C2= (P+R+M+T)/4 \tag{5.1}$$

For other assets the attractiveness is assessed based on transportability (Coeff. P) and by health effect during an acquisition stage (Coeff. R).

$$C2= (P+R)/2 \tag{5.2}$$

Depending on the range of the calculated attractiveness value, a correspondent qualitative level of attractiveness is chosen. A qualitative level can be High, Moderate, Low or Very Low (see Table 5.11).

C2 - Overall attractiveness of an asset by properties	
The average from (P, R, M,T)	
High (H)	0.7 - 1
Moderate (M)	0.4 - 0.7
Low (L)	0.2 - 0.4
Very Low (VL)	<0.2

Table 5.11: Ranges of calculated value based on coefficients and correspondent qualitative levels of attractiveness.

The flowchart on the Figure 5.2 can be used in order to identify and record coefficient values based on the specified criteria, which can then be applied in equations (5.1) or (5.2).

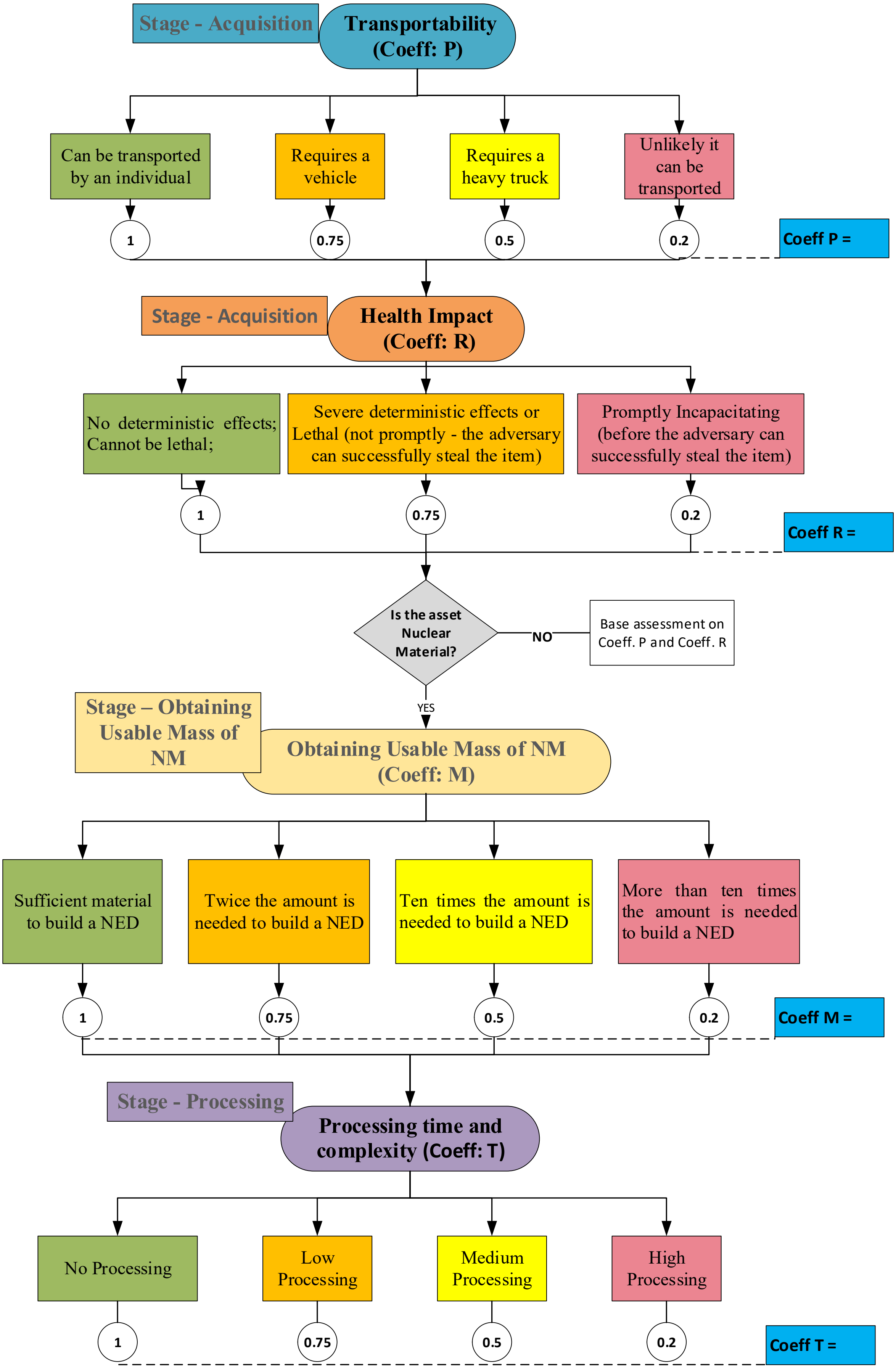

Stage - Acquisition
Transportability (Coeff: P)
Can be transported by an individual
Requires a vehicle
Requires a heavy truck
Unlikely it can be transported
1
0.75
0.5
0.2
Coeff P =
Stage - Acquisition
Health Impact (Coeff: R)
No deterministic effects; Cannot be lethal;
Severe deterministic effects or Lethal (not promptly - the adversary can successfully steal the item)
Promptly Incapacitating (before the adversary can successfully steal the item)
1
0.75
0.2
Coeff R =
Is the asset Nuclear Material?
NO
Base assessment on Coeff. P and Coeff. R
YES
Stage – Obtaining Usable Mass of NM
Obtaining Usable Mass of NM (Coeff: M)
Sufficient material to build a NED
Twice the amount is needed to build a NED
Ten times the amount is needed to build a NED
More than ten times the amount is needed to build a NED
1
0.75
0.5
0.2
Coeff M =
Stage - Processing
Processing time and complexity (Coeff: T)
No Processing
Low Processing
Medium Processing
High Processing
1
0.75
0.5
0.2
Coeff T =

Figure 5.2 Flowchart attractiveness coefficients identification based on criteria.

5.6.3 Identify overall attractiveness of each asset based on assessed consequences and properties of an asset.

To assess the overall attractiveness of an asset, an average value of both coefficients: C1 (attractiveness of assets based on potential consequences) and C2 (attractiveness of assets based on their properties) is calculated.

The overall attractiveness is calculated in the following way:

$$C = (C1+C2)/2 \tag{5.3}$$

The calculated value then falls in the specified range that defines the level of attractiveness of an asset (Very High, High, Moderate, Low or Very Low) (see Table 5.12).

Grade	Range
Very High (H)	0.9-1
High (H)	0.7 - 0.9
Moderate (M)	0.4 – 0.7
Low (L)	0.2 - 0.4
Very Low (VL)	<0.2

Table 5.12: Ranges that define overall attractiveness of an asset by its properties and consequences.

5.7 Step 4. Identify effectiveness of PPS for insider threats

5.7.1 Challenges for Nuclear Security arrangements set up at a research reactor facility against insiders.

There are known measures that can be applied at a research reactor facility to identify or prevent a malicious activity done by an insider [32]. Such as, for example:

- Provide security awareness for staff and contractors.
- Establish physical barriers on ways to assets.
- Prevent unauthorized access to assets.
- Establish control of tools available on site that can be used for malicious act.
- Establish design criteria: separation of tools and materials.
- Conduct pre-employment check for staff and contractors.
- Provide security of digitally stored information.
- Administrate Materials Accountancy System.
- Perform observation and Surveillance by security.
- Conduct activities to identify change in motivation of staff.
- Establish access system arrangements: Restrict access with weapons or tools.
- Establish access system arrangements: detect a theft.
- Establish cybersecurity: Detect unauthorized access to data and presence of malware.
- Establish a system that collects data for potential investigation.

The list above is not a comprehensive list of measures, but it provides an understanding that measures against an insider threat should comprise of a complex combination of different measures relying sometimes even less on effectiveness of physical barriers and more on specific arrangements. It is a challenge to implement an effective combination of measures that would prevent or significantly minimize the probability for insiders to commit a malicious act with negative consequences. The combination of measures against insiders becomes a part of the overall PPS set up at a research reactor.

5.7.2 Description of the RR-NSM graded approach

A significant effort put into the implementation of a number of measures against insiders does not automatically guarantee a high level of PPS effectiveness against insiders. It is important to identify and invest effort and resources in a specific combination of measures that would be effective to consider specifics of a research reactor facility and potential malicious scenarios.

To decide on the PPS arrangements against insiders the effectiveness should be measurable and be in correlation with the attractiveness level of assets.

The RR-NSM graded approach allows for the evaluation of PPS and helps justify the required efforts and resources for the PPS. In addition, it assists in selecting the most effective combination of nuclear security measures available on site.

The steps on how to evaluate PPS effectiveness are described below.

The effectiveness of PPS is evaluated analysing potential malicious act scenarios and detection probabilities. In each scenario a pathway of an adversary must be described. This description contains all obstacles and detection points encountered on the way from the first entry onto the facility's grounds to the final goal of the adversary (sabotage, theft etc.).

For an insider the RR-NSM graded approach analyses a combination of probabilities to detect an insider during a malicious act scenario. The combination of probabilities considers different components, such as the detection of an individual breaching a barrier or entering unauthorised zones, unauthorised use of internal and external tools, the probability to detect removed materials in abrupt and protracted malicious acts, and the probability to detect the act based on established procedures at a research reactor [12].

With regards to the response team(s) it is assumed:

- Response teams must always be able to overpower a detected insider from any of the considered groups.

A security response team(s) can be located onsite (e.g., research reactor security team) or offsite (e.g., police forces).

If the capabilities of security responders on site are enough to interrupt an insider than the response time to interrupt an insider can be immediate (for example, at the entrance gate) or it is equal to the time of the response team movement on site.

If a malicious scenario requires response from external security forces, the response arrival time should be considered in the PPS evaluation. For successful interruption of a malicious act a security response team time arrival should be enough to be able to engage with an insider.

Depending on a malicious scenario it might be necessary to identify a Critical Detection Point (CDP). A CDP is a point on a path before which an adversary has to be detected otherwise there is not enough time for a response team to interrupt a malicious act [24]. (see chapter 5.8.2 on how to identify a CDP)

In the approach described below it is assumed that an insider can be interrupted by a security force on site. In this case a Critical Detection Point (CDP) need not be considered.

The effectiveness of a PPS is characterized by the total probability to detect an insider along their path. The total probability is based on the combined detection probabilities of:

- **An adversary** on the path.
- **A stolen material** on the path.
- **External tools** (carry or use) on the path.
- **Internal tools** (carry or use) on the path.
- Additional components, if applicable:
  - Probability of Detection in case of a **protracted theft** of material.
  - Probability to successfully implement mitigation measures **after a malicious act** by an Insider.

Evaluating PPS elements' effectiveness on different phases of a path against an insider provides a clear picture of the distribution of effectiveness and efforts for the PPS along a path. For example, if at a facility all efforts in PPS arrangements are concentrated at an entrance gate to the facility it might expose a weakness of the PPS inside the facility and demonstrate low effectiveness for certain scenarios with insiders. The detailed analysis of all PPS elements along a path allows to identify the required balance of efforts towards the PPS needed at a research reactor facility. In addition, it allows to identify drawbacks and perform targeted improvements of a PPS at a facility. The improvement activities can be applied to equipment, people, or procedures at a research reactor.

5.7.3 Describe a malicious scenario to be used for assessment of PPS.

A malicious scenario involving asset(s) of a research reactor facility should be created. In the development of a malicious act scenario, assets of a research reactor serve as targets. A malicious act can target an asset for theft or sabotage. The scenario development steps are described below:

1. Choose an asset as a target of a malicious act.
2. Describe what the objective of a malicious act is.
   - Theft.
   - Sabotage.
3. Identify the attractiveness of the asset.
4. Describe an insider's motivation and capabilities for the scenario.

5. Based on the capabilities of an insider, identify the path of an insider and the sequence of actions to fulfil the malicious act.
6. Divide the pathway into sections, with each section representing a different obstacle that an adversary needs to overcome. For example, it can be a barrier to breach, or a distance between two barriers in a protected area.

When choosing a pathway, priority should be given to a path that takes advantage of vulnerabilities of PPS.

7. Analyse probabilities of detection on the pathway of an insider.

Other than the pathway of an outsider at a research reactor which can start with a breach of the first external barrier, the pathway of an insider might not be as clear due to their authorized access at the facility. Detection of an insider using their authorized access with malicious intention is a challenge. It can be argued that a path of an insider begins when an insider starts to perform activities with a malicious intent that can potentially be detected. However, to identify this exact point of time when an insider would begin malicious activities might be quite challenging. Due to this reason, the RR-NSM graded approach does not rely on identifying a starting point of the actual path of an insider with a malicious intention. It considers a full path of an insider starting from the first barrier (e.g., entrance gate) even if in some cases the detection probability is very low or almost impossible.

Hence if a pathway consists of barriers that can easily be overcome by an insider, they still need to be documented in the pathway of a scenario.

A scenario should take into consideration an insider's abilities to tamper with physical protection measures, such as amending databases, for example a database of accounted sources to hide a theft.

There can be more than one path to an asset at a research reactor. Each path should be assessed separately. The same path should be considered for all groups of insiders. Ideally all possible paths must be evaluated. Missing evaluation of a PPS on a potential path of an insider might leave a flaw in a security system.

In general, the path of an insider consists of barriers and distances that have to be covered, see Figure 5.3.

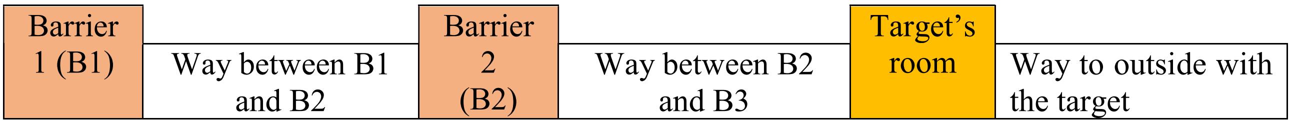


Figure 5.3 Overview of an insider's pathway

Due to the potential complexity of a path, it is more practical to develop a path in a table format. Each section of the insider's path should be described in a row. The first column indicates a barrier or an area, the second column contains a short description of the path's section and information on the section of the path, for example '*Entrance Door*', '*Corridor in the Protected Area*'. The third column describes activities an insider has to perform in accordance with a chosen scenario (see Table 5.12).

Barrier	Sections of the path	Activity description
Barrier 1 (B1)	A fence gate	Breach the fence gate
Outside protected area	Distance from the fence to a back entrance door (from B1 to B2)	Move from the fence to a back entrance door
Barrier 2 (B2)	The back entrance door B2	Breach the door
Inside protected area	Distance between the back entrance door to a target's room door	Move along the corridor in the Protected Area to the target's room door
Barrier 3 (B3)	Target's room door	Breach the target's room door
Barrier 4 (B4)	Target's room safe	Breach the safe
Inside protected area	Distance between the target's room door and a back entrance door	Remove the target and move back along the corridor to the back entrance door
Outside protected area	Distance between the back entrance door and the fence	Move from the back door entrance to the fence

Table 5.12: Representation of sections of a path and description of an activity an insider needs to do.

5.7.4 Five components that characterize the effectiveness of a PPS against an insider.

As mentioned above, it is a complicated task to measure the effectiveness of a PPS against an insider at a research reactor facility due to specifics of an insider threat, for example having access to the asset. The RR-NSM graded approach takes into consideration five different components that can lead to a detection of an insider. The effectiveness of a PPS against an insider is comprised of:

1. Effectiveness of onsite security forces.
2. Effectiveness of detection of a moving insider.
3. Effectiveness of detection of an unauthorized asset removal.
4. Effectiveness of an external tool detection.
5. Effectiveness of an internal tool detection.

The five components are described in more details below.

5.7.5 Assess effectiveness of onsite security forces response.

The effectiveness of onsite security forces response is the first of five components that are taken into consideration to assess the effectiveness of a PPS against insiders. There are two possible cases of a response to an insider threat: engage with an insider to detain them or call assistance of law enforcements.

If an insider has the intention to stay undetected and operate alone, they choose nonviolent tactics on-site and do not have the intention to use weapons. In this case the response of an onsite security team might well be sufficient. However, if an insider chooses a violent tactic and intends to use a weapon then in this case an on-site security staff might need to request assistance from offsite security forces. For example, in case when an insider uses a gun and security staff onsite are not authorised to use guns then they must request assistance from local law enforcement (e.g. police). The tactic of an insider depends on the chosen scenario of a malicious act.

If response of the onsite security team is sufficient:

The onsite security team response can be sufficient if their capabilities can overpower an insider (very high effectiveness of the onsite security team). For example, it can be in a scenario involving an insider who doesn't have intentions to engage in a violent resistance.

In this case there can be two possibilities (depending on a scenario):

1) An insider is detected and can be intercepted immediately. For example, at a main entrance/exit gate trying to smuggle in a weapon or smuggle out nuclear material.

The effectiveness of the onsite security team is very high, the response is considered immediate, hence the delay time is negligible. Since the delay time is negligible identification of Critical Detection Point (CDP) is irrelevant. Hence, it is not needed to:

- Evaluate delay time.
- To identify a response time of external security forces.
- To identify a CDP.

2) An insider is detected but cannot be interrupted immediately, even if onsite security team can overpower an insider. For example, breaching a final barrier – a door or a fence and running away. In this scenario it is necessary to detect an insider in advance to provide enough time for a security response team onsite. In this case Critical Detection Point (CDP) and delay times should be considered.

If for the chosen scenario and characterised insider, the response of the onsite team is NOT enough:

- It is needed to evaluate delay time (see 5.8.2).
- It is needed to assess the external response team arrival (see 5.8.2).
- It is needed to identify Critical Detection Point on the path and consider for evaluation only barriers before the CDP (see 5.8.2).

The value for effectiveness of onsite security forces response is not calculated and not included in a final calculation. However, it assists to decide if an external response team is required or not in a particular scenario and therefore indicates if a path must include CDP and if additional assessment of external response team effectiveness is required.

5.7.6 Analysing a detection effectiveness.

This sub-chapter describes an equation used to calculate detection effectiveness. It explains how individual probabilities are combined to assess overall detection effectiveness, explores the sources of these probabilities, and discusses the assumptions used in the calculation. Additionally, it addresses the level of uncertainty involved.

Detection can be performed by an instrument, such as a detector, or by a person, such as security staff.

Assessment can be carried out in two ways: by using equipment that transmits a video signal to a screen for detailed review, or by a person who evaluates the information directly within visual range.

The overall detection effectiveness (P_{eff}) depends on the probabilities associated with both:

P_d - Probability of detection at an analysed section of the path.

P_a - Probability of assessment at an analysed section of the path.

P_{eff} is derived from the multiplication of these probabilities: $P_d * P_a.$ In case there are multiple steps on the path that an adversary needs to overcome (e.g. breaching a barrier, moving in a protected area, breaching another barrier etc.) the P_{eff} is derived from a combination of several independent probabilities, each component probability ($P_{di} * P_{ai}$).

The equation to calculate the detection effectiveness across several stages on the path is the following [33]:

$$\boldsymbol{P_{eff} = 1 - \{\prod_{i=1}^{I}(1 - P_{d_i} * P_{a_i})\}} \tag{5.4}$$

The individual probabilities Pd and Pa might be estimated from past data, experiments, or simulations or an experienced with PPS equipment individuals, in all of which can have inherent variability or error.

The equation used to calculate the overall detection probability assumes that the probabilities of detection at each stage are independent. Each stage represents a component along a path, such as breaching a fence or a door, and the probability of detection for each component is based on the adversary’s likelihood of being detected at that stage. Given the nature of these stages, distinct physical and procedural barriers along the path, it is reasonable to assume that the probabilities are uncorrelated and independent, as the detection at one stage (e.g., breaching a fence) does not directly influence the detection at another stage (e.g., breaching a door). Therefore, for the purpose of this analysis, the assumption of independence holds, and introducing additional complexity or correlated probabilities is not necessary for this model.

It is important to mention the associated uncertainties. The quality of data used to derive the probabilities affects the overall uncertainty. For example, limited or biased data can lead to less reliable estimates. When multiple probabilities are multiplied together, the uncertainties in each probability can compound, leading to greater overall uncertainty in the final result.

This underscores the necessity of involving high-level specialists, including both PPS equipment technicians and experienced physical security professionals, to derive the most accurate probabilities.

In this research, the calculations were performed as an example, using selected probabilities that represent estimated values rather than actual detection or assessment probabilities. Since real values were not applicable, uncertainties were not accounted for, leading to some probabilities being reported with three significant digits (e.g., 97.2%), which suggests a high degree of precision. In reality, given the potential uncertainties, achieving such precision may be difficult. It is more realistic to report probabilities with one or two significant digits (e.g., 97% or 0.97). The results must be correlated with uncertainties to avoid overestimating confidence in the outcomes.

Equation Interpretation:

$\mathbf{1 - P_{d_i} * P_{a_i}}$ – this term represents the probability that a detection of an adversary does not occur in a particular stage *i* of a path.

$\boldsymbol{\prod_{i=1}^{I}(1 - P_{d_i} * P_{a_i})}$ – the result of the multiplied terms of all *I* stages gives the overall probability that a detection of an adversary does not occur along the whole path.

$\mathbf{1 -}$ – Subtracting the multiplied terms of all *I* stages from 1 gives the overall probability that a detection of an adversary occurs along the whole path.

5.7.7 Calculate effectiveness of detection of a moving insider.

The effectiveness of detection of a moving insider is a second component that contributes to assess the effectiveness of a PPS against insiders. This component relies on *a Probability of Detection* and *a Probability of Assessment* of a moving insider on an analysed section of the path (barrier or distance). The multiplication of those probabilities identifies the effectiveness of overall detection of a moving insider.

A detection can be performed during a barrier breach or during an unauthorized activity on a path, such as presence in a restricted area. For example, insiders from students and visitors can be detected in a restricted area when they are not accompanied by a research reactor staff member. However, effectiveness of detection of a moving insider from a research reactor staff group who has access to assets due to work activities can be zero.

To assess the effectiveness of detection of a moving insider, a qualitative probability is assessed for each pathway section of a considered scenario. The effectiveness of detection is a multiplication of probabilities: to *detect* and to *assess* at a chosen pathway section:

The column *Effectiveness of detection of a moving insider* is added in Table 5.13.

Path	**Activity description**	**Effectiveness of detection of a moving insider *(Peff.m)***
Path towards the target		
Through the back entrance door	Breach the door	*Pd.m1*Pa.m1*
From the back entrance door to a target's room door	Walk in the Protected Area	*Pd.m2*Pa.m2*
Through the target's room door	Breach the door	*Pd.m3*Pa.m3*
In the target's room safe	Breach a safe and remove an asset	*Pd.m4*Pa.m4*
Path back carrying the asset		
Through the target's room door	Walk through the door	*Pd.m5*Pa.m5*
From the target's room door and the back entrance door	Walk in the Protected Area	*Pd.m6*Pa.m6*
From the back entrance door to the fence gate	Walk outside of the Protected Area	*Pd.m7*Pa.m7*

Table 5.13: Path description with effectiveness of detection of a moving insider at each section of a path.

$P_{d.mi}$ – Probability of insider's detection at an analysed section of the path.

$P_{a.mi}$ – Probability of insider's assessment at an analysed section of the path.

$$P_{eff.m} = 1 - \{\prod_{i=1}^{I}(1 - P_{d.m_i} * P_{a.m_i})\} \qquad (5.5)$$

$P_{eff.m}$ – The effectiveness of detection of a moving insider on the full path. [12]

5.7.8 Calculate effectiveness of detection of an unauthorized asset removal.

The effectiveness of detection of an unauthorized asset removal is a third component that contributes to the assessment the PPS effectiveness against insiders. This component relies on a *Probability of Detection* and a *Probability of Assessment* of a carried (smuggled) asset on the path. For example, nuclear or other radioactive material can be targeted for a theft and carried (smuggled) outside of a research reactor premises. If the insider follows a usual daily work path, then the effectiveness to detect a moving insider is very low however the probability to detect a carried material can increase overall detection. Probabilities of detection and assessments are analysed on each section of a path.

The column *Effectiveness of detection of an unauthorized asset removal* is added in the Table 5.14.

Path	**Activity description**	**Effectiveness of detection of a moving insider (Peff.m)**	**Effectiveness of detection of an unauthorized asset removal (Peff.r)**
Path towards the target			
Through the back entrance door	Breach the door	*Pd.m1*Pa.m1*	
From the back entrance door to a target’s room door	Walk in the Protected Area	*Pd.m2*Pa.m2*	
Through the target’s room door	Breach the door	*Pd.m3*Pa.m3*	
In the target’s room safe	Breach a safe and remove an asset	*Pd.m4*Pa.m4*	
Path back from the target/with the target			
Through the target’s room door	Walk through the door	*Pd.m5*Pa.m5*	*Pd.r1*Pa.r1*
From the target’s room door and the back entrance door	Walk in the Protected Area	*Pd.m6*Pa.m6*	*Pd.r2*Pa.r2*
From the back entrance door to the fence gate	Walk outside of the Protected Area	*Pd.m7*Pa.m7*	*Pd.r3*Pa.r3*

Table 5.14: Path description with effectiveness of detection of a moving insider and unauthorized asset removal.

$$P_{eff.r} = 1 - \left\{\prod_{j=1}^{J}\left(1 - P_{d.r_j} * P_{a.r_j}\right)\right\} \tag{5.6}$$

where:

Pd.rj – Probability of detection of an unauthorized removed asset at an analysed section of the path.

Pa.rj – Probability of assessment of a detected unauthorized removed asset at an analysed section of the path.

Peff.r – The effectiveness of detection of an unauthorized removed asset being transported on the path.

The equation below combines two components that calculate the detection effectiveness on the path for:

- a moving insider.

- a transported asset.

$$Peff.m.r = 1-(1-Peff.m)*(1-Peff.r) = 1-\left\{\prod_{i=1}^{I}\left(1-P_{d.m_i}*P_{a.m_i}\right)*\prod_{j=1}^{J}\left(1-P_{d.r_j}*P_{a.m_j}\right)\right\} \quad (5.7)$$

Peff.m.r – The effectiveness of detection of a moving insider who carries a removed asset on the path.

5.7.9 Calculate effectiveness of an external tool detection.

The effectiveness of an external tool detection is a fourth component that contributes to assessment the PPS effectiveness against insiders. This component relies on a *Probability of Detection* and a *Probability of Assessment* of a carried (smuggled) tool from outside into a research reactor premises and being carried on along a path inside. An external tool is any object that is carried into premises of a research reactor and can be used with malicious intentions. The external tool can be used as a weapon, as a tool to breach barriers or use for a sabotage. Tools that are brought in by subcontractors and temporarily stored at a research reactor premises are considered as external tools.

For example, if an insider chooses a tactic to be active with a violent resistance to security forces or co-workers, they can try to smuggle a weapon on the premises, it can be a gun, a knife, a pepper spray or any other object that can be used as a weapon. If an insider has the intention to breach a barrier, they can try to smuggle a drill or a hummer. If an insider has the intention to do a sabotage by setting a fire, they can try to smuggle a bottle with inflammable liquid.

At the same time, use of external tools can be required at a research reactor for authorized activities, for example for a planned maintenance. The PPS arrangements should identify which type of external tools can be allowed at a facility and who is authorized to bring them in and carry them on premises.

Probabilities of detection and assessments are analysed on each section of a path.

Depending on the scenario a required external tool can be made of different material and have various dimensions. To assess the effectiveness of an external tool detection, three different methods of detection are assessed. The effectiveness of an external tool detection relies on three components: detection by a metal detector, detection by an explosives detector and visual detection [12].

- A tool containing metal parts can be detected visually and via metal detector.
- A tool containing explosives can be detected using an explosives detector.
- A tool that doesn't contain either metal parts nor explosives can be detected only visually.

Potentially, a visual detection of an external tool can also be done by non-security staff (e.g., a co-worker, a student, or a visitor). For example, an individual can notice that an insider is carrying a weapon. However, the communication of this detection might not be done in a timely manner and not to recipients that can trigger a response. This means that the probability of visual detection must be considered only if there are procedures established and an individual at premises is knowledgeable and trained on how to communicate a visual detection of a potential malicious use of an unauthorized external tool.

The column *Effectiveness to detect an external tool (Peff.ext_t)* is added in the Table 5.15.

Path	**Activity description**	**Effectiveness of detection of a moving insider (Peff.m)**	**Effectiveness of detection of an unauthorized asset removal (Peff.r)**	**Effectiveness to detect an external tool (Peff.ext_t)**
Path towards the target				
Through the back entrance door	Breach the door	*Pd.m1*Pa.m1*		*Peff.ext.tool1*
From the back entrance door to a target's room door	Walk in the Protected Area	*Pd.m2*Pa.m2*		*Peff.ext.tool2*
Through the target's room door	Breach the door	*Pd.m3*Pa.m3*		*Peff.ext.tool3*
In the target's room safe	Breach a safe and remove an asset	*Pd.m4*Pa.m4*		*Peff.ext.tool4*
Path back from the target/with the target				
Through the target's room door	Walk through the door	*Pd.m5*Pa.m5*	*Pd.r1*Pa.r1*	*Peff.ext.tool5*
From the target's room door and the back entrance door	Walk in the Protected Area	*Pd.m6*Pa.m6*	*Pd.r2*Pa.r2*	*Peff.ext.tool6*
From the back entrance door to the fence gate	Walk outside of the Protected Area	*Pd.m7*Pa.m7*	*Pd.r3*Pa.r3*	*Peff.ext.tool7*

Table 5.15: Path description with effectiveness of detection of a moving insider, unauthorized asset removal and an external tool.

$$Peff.ext\_t = 1 - \left\{\prod_{i=1}^{I}\left(1 - P_{d.srch_i} * P_{a.srch_i}\right) * \left(1 - P_{d.met_i} * P_{a.met_i}\right) * \left(1 - P_{d.exp_i} * P_{a.exp_i}\right)\right\} \tag{5.8}$$

where:

Pd.srch – Probability of an unauthorized external tool detection during a search.

Pa.srch – Probability of a correct assessment of an unauthorized external tool if detected.

Pd.met – Probability of an unauthorized external tool detection by a metal detector.

Pa.met – Probability of a correct assessment of an unauthorized external tool if detected by a metal detector.

Pd.exp – Probability of an explosive detection by an explosives detector.

Pa.exp – Probability of a correct assessment of an explosive if detected by an explosives detector.

The next equation combines three components that calculate the detection effectiveness on the path for:

- a moving insider detection (*Peff.m*).
- a transported removed asset (*Peff.r*).
- A transported and used external tool (Peff.ext_t).

$$Peff.m.r.ext\_t = 1 - (1 - Peff.m) * (1 - Peff.ext\_t) * (1 - Peff.r) = 1 - \left\{\prod_{i=1}^{I}\left(1 - P_{d.m_i} * P_{a.m_i}\right) * \left(1 - \left(1 - P_{d.srch_i} * P_{a.srch_i}\right) * \left(1 - P_{d.met_i} * P_{a.met_i}\right) * \left(1 - P_{d.exp_i} * P_{a.exp_i}\right)\right) * \prod_{j=1}^{J}\left(1 - Pd.r_j * Pa.r_j\right)\right\} \quad (5.9)$$

Peff.m.r.ext_t – The effectiveness of detection of a moving insider who carries a removed asset and has to use an external tool which had to be smuggled in.

Additional data to be considered.

If for an analysed malicious scenario an insider doesn’t need to use an external tool, then *Peff.ext_t* is not added into the equation.

5.7.10 Calculate effectiveness of an internal tool detection.

The effectiveness of an internal tool detection is a fifth component that contributes to assess the PPS effectiveness against insiders. This component relies on a *Probability of Detection* and a *Probability of Assessment* of an internal tool that is transported and used with a malicious intent at a research reactor premises. An internal tool is an object that is stored at a research reactor premises and is used for usual authorised tasks in accordance with established procedures. However, an internal tool can be used with a malicious intention, for example cranes to handle nuclear material, shielding containers, tools such as drills or hammers that are stored at a research reactor premises.

The column *Effectiveness to detect an internal tool (Peff.int_t)* is added in the Table 5.16.

Path	**Activity description**	**Effectiveness of detection of a moving insider (Peff.m)**	**Effectiveness of detection of an unauthorized asset removal (Peff.r)**	**Effectiveness to detect an external tool (Peff.ext_t)**	**Effectiveness to detect an internal tool (Peff.int_t)**
Path towards the target					
Through the back entrance door	Breach the door	*Pd.m1*Pa.m1*		*Peff.ext.tool1*	*Peff.int.tool1*
From the back entrance door to a target's room door	Walk in the Protected Area	*Pd.m2*Pa.m2*		*Peff.ext.tool2*	*Peff.int.tool2*
Through the target's room door	Breach the door	*Pd.m3*Pa.m3*		*Peff.ext.tool3*	*Peff.int.tool3*
In the target's room safe	Breach a safe and remove an asset	*Pd.m4*Pa.m4*		*Peff.ext.tool4*	*Peff.int.tool4*
Path back from the target/with the target					
Through the target's room door	Walk through the door	*Pd.m5*Pa.m5*	*Pd.r1*Pa.r1*	*Peff.ext.tool5*	*Peff.int.tool5*
From the target's room door and the back entrance door	Walk in the Protected Area	*Pd.m6*Pa.m6*	*Pd.r2*Pa.r2*	*Peff.ext.tool6*	*Peff.int.tool6*
From the back entrance door to the fence gate	Walk outside of the Protected Area	*Pd.m7*Pa.m7*	*Pd.r3*Pa.r3*	*Peff.ext.tool7*	*Peff.int.tool7*

Table 5.16: Path description with effectiveness of detection of a moving insider, unauthorized asset removal, an external tool and an internal tool.

$$Peff.int\_t = 1 - \left\{\prod_{i=1}^{I}\left(1 - P_{d.int\_t_i} * P_{a.int\_t_i}\right)\right\} \tag{5.10}$$

where:

Pd.int_t – Probability to detect an internal tool while being transported or used with a malicious intention.

Pa.int_t – Probability of a correct assessment of a detected internal tool.

The next equation combines four components that calculate detection effectiveness on the path (Peff.m.r.ext_t.int_t) for:

- a moving insider (*Peff.m*).
- a removed asset (*Peff.r*).
- an external tool (*Peff.ext_t*).
- an internal tool (*Peff.int_t*).

$$\begin{gathered} Peff.m.r.ext\_t.int\_t = 1 - (1 - Peff.m) * (1 - Peff.r) * (1 - Peff.ext\_t\,) * \\ (1 - Peff.int\_t) \;==\; 1 - \Big\{\prod_{i=1}^{I}(1 - P_{d.m_i} * P_{a.m_i}) * \Big(1 - (1 - P_{d.srch_i} * P_{a.sr\quad i}) * \\ (1 - P_{d.met_i} * P_{a.met_i}) * (1 - P_{d.exp_i} * P_{a.exp_i})\Big) * (1 - P_{eff.int\_t_i}) * \prod_{j=1}^{J}(1 - Pd.r_j * Pa.r_j)\Big\} \end{gathered} \tag{5.11}$$

5.7.11 Additional considerations for scenarios.

5.7.11.1 Digital data theft scenario.

In case of a digital data theft scenario, a probability to successfully detect and protect from the digital data theft must be considered. A digital data theft can be done by means of internal tools and external tools. A local PC at a research reactor can serve as an internal tool, for example, a data can be transferred via internet. An external tool can be, for example, a USB thumb drive that can also be used to download digital data, a camera can be used to take pictures of displayed digital data.

The probability of a successful detection should be added in the equation with other probabilities.

5.7.11.2 Protracted theft of material.

The RR-NSM graded approach allows flexibility in the assessment by offering the possibility to introduce additional components. For example, a component that estimates the effectiveness of a PPS in case of a protracted theft.

One of the major differences between insiders and outsiders is that an insider doesn't have constrains in time to perform a malicious act at a research reactor. Usually, outsiders aim for an abrupt malicious act such as, for example, theft of a material. An insider has the option to choose a tactic of protracted thefts. The protracted theft is "the repeated unauthorized removal of small quantities of nuclear material during several events". [39] An insider conducts a protracted theft of material even if material is stored in various locations. An insider might be able to bypass physical protection elements carrying a small quantity of material in one attempt. The quantity of material in one theft can be considered as not attractive, however in a sequence of thefts the overall quantity of material can become attractive and eventually reach a useful quantity. In addition to a protracted theft scenario, an insider has the option to perform a sequence of sabotage activities that could result in a sabotage with significant consequences. [32]

The effectiveness of PPS in the case of protracted theft depends on arrangements, such as:

1. Means to detect loss of material through verification.
2. Detection of falsification in a process of Nuclear Material Accounting and Control (NMAC).
3. Detection of substituted material with dummy samples.
    - Using electronic tamper detection equipment and/or continuous surveillance by operator personnel.
    - Using seals and tampers.

Probability of a successful detection should be added in the equation with other probabilities [34]. Description of PPS effectiveness levels is presented in the Table 5.17.

Range (Peff_protr)	Detection
Very High (VH) **0.9 - 1**	Is nearly guaranteed
High (H) **0.7 - 0.9**	Is likely to occur
Moderate (M) **0.4 - 0.7**	has an average chance of occurring
Low (L) **0.2 - 0.4**	system is functional but not likely to detect
Very low (VL) **< 0.2**	Little chance to detect. No system in place or very low reliability.

Table 5.17: Description of a PPS performance (effectiveness) within a specific range of successful detection probability.

5.8 Step 5. Compare the assessed PPS effectiveness against the attractiveness level of an asset.

Once the overall value of PPS effectiveness against an insider is obtained, it should then be compared to the attractiveness level of an asset. Table 5.18 is used to determine if the evaluated PPS effectiveness correspondent to an asset with a certain attractiveness.

Attractiveness	Effectiveness of PPS				
	VH (0.9 – 1)	H (0.7 - 0.9)	M (0.4 - 0.7)	L (0.2 - 0.4)	VL (< 0.2)
Very High (VH) **0.9 - 1**	1	2	3	4	5
High (H) **0.7 - 0.9**	0	1	2	3	4
Moderate (M) **0.4 - 0.7**	0	0	1	2	3
Low (L) **0.2 - 0.4**	0	0	0	1	2
Very low (VL) **< 0.2**	0	0	0	0	1

Table 5.18: Matrix of suggested relationship between levels of attractiveness and effectiveness of PPS.

0 - Very strong PPS effectiveness for a particular asset's attractiveness.

1- Strong PPS effectiveness. PPS effectiveness is well balanced with the attractiveness of an asset.

2 - Close to the required level of PPS effectiveness. Actions to increase PPS effectiveness should be considered. Medium risk – an insider's attempt can lead to an average chance of a successful malicious act occurrence.

3 - Poor PPS effectiveness for a particular attractiveness of an asset. Actions are required to increase PPS effectiveness or reduce asset attractiveness. High risk – an insider's attempt can lead to a high chance of a successful malicious act occurrence.

4, 5 - Very poor PPS effectiveness for a particular attractiveness of an asset. Immediate actions required. Very high risk – an insider's attempt can lead to a very high chance of a successful malicious act occurrence.

It is possible that decision makers can accept a certain risk and keep the PPS effectiveness disbalanced with attractiveness of asset. This can be accepted, for example, when consequences are not significant and mitigation measures after a malicious act are expected to be effective. In the next chapter it is described how mitigation measures can be assessed.

5.8.1 Assessing mitigation measures when PPS effectiveness is poor.

Generally, the confrontation of an insider with established PPS arrangements should result in the prevention and detection of a malicious act. However, it is extremely challenging to rule out the possibility of a malicious act and provide guaranteed interruption of an insider before a malicious act is committed. In some scenarios an insider can only be detained after a malicious act is done. For example, physical damage to assets, sabotage of processes at a research reactor, or digital theft of assets. In this case the fact of an occurred malicious act can be discovered without detecting an insider during a malicious act.
Depending on the attractiveness of an asset, decision makers can accept the risk of a malicious act and its consequences if mitigation actions such as identification of the insider, search and detain are possible and effective. The effectiveness of the mitigation actions dependents on arrangements and equipment at a facility and the probability to detect the missing asset or fact of a sabotage in a timely manner, and the probability to identify and detain the insider.

Assessment of the mitigation actions

The effectiveness of mitigation actions depends on the probability to detect a committed malicious act and the probability to identify the insider. A committed malicious act must be detected in a timely manner which ensures that data for the identification of an insider is still available. For example, if a malicious act is detected too late, it is possible that footage from CCTV cameras is not available anymore because it is stored for a limited period only.

<u>Probability to detect a committed malicious act in a timely manner.</u>

- Depends on established arrangements such as:
    - Material Accounting and Control program.
    - Communication of detected malicious act to local security or external law enforcement.

<u>Probability to timely identify an insider who committed the malicious act:</u>

- Depends on established arrangements and available equipment.

- Staff location tracking via access system data collection (scan the badge, fingerprint).
- Footage from CCTV cameras.
- Documented history of activities in sensitive areas.

The detection effectiveness is divided in the levels presented in Table 5.19.

Probability	Detection effectiveness
Very High (VH)	Is nearly guaranteed
High (H)	Is likely to occur
Moderate (M)	Has an average chance of occurring
Low (L)	System is functional but not likely to identify
Very low (VL)	Little chance to identify an insider after a malicious act is committed. No system in place or very low reliability.

Table 5.19: Description of mitigation actions performance (effectiveness).

To identify the overall effectiveness of mitigation actions, two probabilities must be assessed, and the lowest grade should be taken as a result to indicate the effectiveness of mitigation actions. Decision makers then identify if the effectiveness of mitigation actions is acceptable for the considered scenario. Table 5.20 can be used for mitigation actions assessment.

- If yes, then the effectiveness of the current mitigation actions should be maintained, and PPS improvement could be not urgently considered.
- If no, the effectiveness of mitigation actions or PPS must be improved.

Malicious act	Probabilities	
	Probability to timely detect a committed malicious act	**Probability to timely identify an insider who committed the malicious act**
Sabotage		
Theft		

Table 5.20: Table to be used during mitigation actions assessment.

The flow chart on the Figure 5.4 describes a flow of a decision making based on mitigation actions assessment.

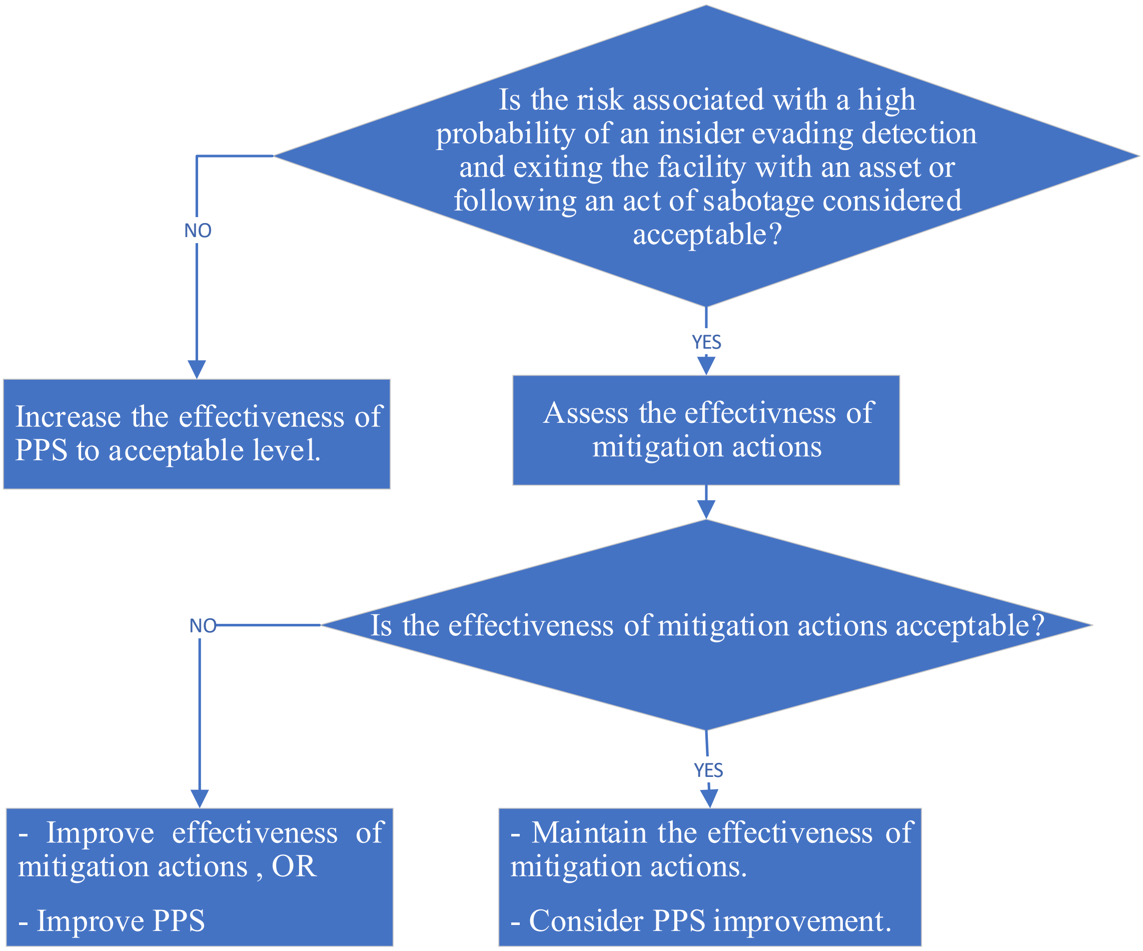

Is the risk associated with a high probability of an insider evading detection and exiting the facility with an asset or following an act of sabotage considered acceptable?
NO
YES
Increase the effectiveness of PPS to acceptable level.
Assess the effectivness of mitigation actions
Is the effectiveness of mitigation actions acceptable?
NO
YES
- Improve effectiveness of mitigation actions , OR
- Improve PPS
- Maintain the effectiveness of mitigation actions.
- Consider PPS improvement.

Figure 5.4: A decision making flowchart based on mitigation actions assessment.

5.8.2 Identify effectiveness of PPS for outsider(s) in collusion with an insider.

An outsider can attempt to commit a malicious act in collusion with an insider or without insider's help. An insider can assist an outsider in passing certain barriers, for example leaving a door unlocked or tamper with security systems which can decrease the probability of detection.

This chapter describes the approach that is taken to analyse the effectiveness of Physical Protection Systems against an outsider that can act in collusion with an insider or without. If in a scenario an outsider acts in collusion with an insider, then the overall effectiveness of the PPS should be assessed by combining the approach for an outsider and the approach for an insider (see 5.7).

Assessment of the PPS for outsiders is focused on the following aspects [24]:

- Probability of Detection of an outsider on a path.
- Probability of an Assessment of a detection on a path.
- Sufficient Delay provided by barriers for the response.

- Timely Response aimed to interrupt the adversary before a malicious act at a research reactor is done.

5.8.2.1 *Estimate performance measures of physical protection barriers.*

Physical Protection System effectiveness of barriers is characterized by the probability to correctly and timely detect an outsider.

The effectiveness of detection is comprised of two factors:

- Probability of Detection (Pd).
- Probability of Assessment (Pa).

Detection of an outsider can be performed by sensors, by security staff or by facility staff that can timely communicate to the security staff on site.

Assessment of a detection by security staff requires a person to understand if the activated alarm due to detection is valid or invalid. At a research reactor the probability of an irrelevant alarm is higher than at a Nuclear Power Plant, due to a different nature of operation, for example, visitors, students, researchers from other facilities might be not familiar with a facility and mistakenly trigger an alarm. It is important to arrange an adequate assessment of an alarm and include it in the estimation of the PPS performance.

Assessment can be done visually via CCTV cameras by security guards. The effectiveness of assessment via CCTV cameras can be characterized by equipment parameters such as: video quality, field of coverage, resolution, capture speed, regular maintenance [24]. Some assessment can be done visually by staff at a facility. The research reactor staff must be trained on security culture and understand the process on how to communicate the information to the security forces.

5.8.2.2 *Identification of the Critical Detection Point (CDP) on the path.*

When analysing a particular scenario, it is necessary to identify the Critical Detection Point (CDP). CDP is a point or place on a pathway, after which the adversary, if not detected, can accomplish a task and manage to escape, which means response forces would not have enough time to interrupt the adversary (see Figure 5.5). [24]

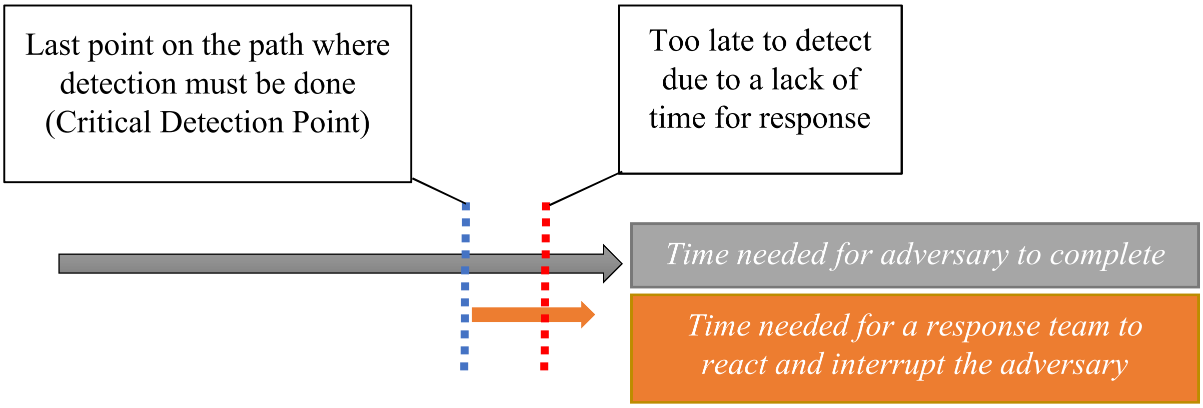

Last point on the path where detection must be done (Critical Detection Point)
Too late to detect due to a lack of time for response
Time needed for adversary to complete
Time needed for a response team to react and interrupt the adversary

Figure 5.5: Critical Detection Point (CDP) concept.

If in a scenario the level of adversaries' capabilities allows a confrontation with security forces on site with a high probability of neutralization, then the response time is faster than the response of an external team and the CDP can be placed on a path accordingly. Security forces on site do not need to exceed capabilities of an adversaries if the external response team is capable to arrive on time and provide the efficient response, however the response time can be longer in this case.

5.8.2.3 Calculate detection effectiveness of the barriers before CDP.

On each section of the path, the Probability of Detection **(Pd)** and the Probability of Assessment **(Pa)** needs to be assessed. In Table 5.21 below the effectiveness of Pd and Pa are graded as Low (L), Moderate (M), High (H) or Very High (VH) [34].

***Pd* -** Probability of detection (or Probability of Sensing)

***Pa* -** Probability of a correct assessment providing that the detection occurred.

Table 5.21 probabilities of detection and assessment are described for each Effectiveness Grade (value).

Effectiveness Grade	Value	Probability of Detection (Pd)	Probability of Assessment (Pa)
Very High (VH)	0.9	Detection is **nearly guaranteed.** At least two different detection methods are in place and function.	Assessment **very likely to happen**, either by reliable technical means or by personnel in a timely manner.
High (H)	0.75	Detection occurs **almost always.** May be some doubt about the reliability of some element of the system.	Assessment **likely to occur**, but **not as effectively.**
Moderate (M)	0.5	**Often.** Detection has an **average chance of occurring**, systems are in place and functional, but reliability may be questionable.	Assessment **may occur but may be delayed** to the point where it affects response.
Low (L)	0.25	**Occasionally.** Detection system is functional but not likely to detect. Systems are not reliable. Methods available to bypass or defeat system.	Assessment **may not occur.** System has high susceptibility to deceit or defeat.
Very low (VL)	0.1	Detection **almost never or never.** Very little or no chance of detection. No system in place or very low reliability.	Assessment will **very likely not** occur.

Table 5.21: Effectiveness grades probabilities of detection and assessment [34]

5.8.2.4 *Estimate the delay time for an outsider.*

The delay time on a pathway is assessed based on the capabilities of an outsider, barrier characteristics and extent of assistance from an insider (if a collusion type scenario is considered). All pathways leading to an asset or assets that could be chosen by an adversary have to be analysed. In addition, if a barrier's characteristics alters depending on the day of the week or daytime then the same pathway should be analysed more than once taken into consideration barrier characteristics in different times. For example, a main entrance door can be open during work hours but can be closed during non-working hours.

The time that an adversary takes to move forward along a section of a pathway (e.g. breach a barrier or move along the way between barriers) is the delay time of a particular section of a pathway. Estimating delay times of all sections of the pathway results in the total delay time on the pathway.

The grades listed in the Table 5.22 is used to estimate the possible delays:

Level of delay	**Time of a barrier's delay**
Low (L)	< 3 min (2 min as average)
Moderate (M)	3-10 min (5 min as average)
High (H):	> 10 min

Table 5.22: Levels of a barrier delay time used in the approach.

5.8.2.5 *Estimate the response team effectiveness.*

The effectiveness of a response team consists of two factors:

- Probability of Neutralization
- Response team arrival time

Probability of Neutralization

Conservative characteristics of the hypothetical outsider's threat in a country may be obtained during an assessment of national nuclear security threat in the framework of Design Basis Threat development [1]. Based on the DBT responsible organizations must ensure that a high probability of a successful confrontation is guaranteed. The assumption, in the RR-NSM graded approach, is that the response team is in the majority, armed, well trained for a force-to-force confrontation, has better equipment and tools than the hypothetical outsiders. In this approach the assumption is taken that the probability of neutralization is very high.

Response team arrival time

The Response team arrival time depends on the location of a research reactor facility and the location of the response teams. The response team arrival time includes time spent at a facility until the moment of engagement with the adversary. Receiving correct information on the location of adversaries at a facility can reduce the response time. The response time can be assessed by conducting exercises, by analysing historical events or simulations using software. In this approach the response time is divided in:

- Fast: < 3 min
- Moderate (M): 3-10 min
- Slow (H): > 10 min

5.8.2.6 *Estimate the assessed PPS effectiveness.*

The approach to estimate the effectiveness of the PPS for a particular scenario and an asset is described in 5.7.

5.8.2.7 *Analyse potential paths to identified targets.*

There are multiple ways an outsider adversary may use to enter a facility and get to an asset, including obtaining help from an insider. The most vulnerable paths are usually the most protected. To apply the approach comprehensively, it is required to do the assessment of the PPS for several potential paths that lead to identified targets (assets). In addition, estimations must be done taking into consideration different security regimes. For example, working hours and non-working hours when security resources on site might be reduced. However, it is challenging to address every single potential scenario. A list of credible scenarios should be considered for an analysis. The number of scenarios and different pathways will depend on the risk appetite or risk tolerance of decision makers. In any case the risk tolerance chosen must be in line with requirements of local regulators.

5.8.2.8 *Adapt identified Physical Protection System performance to high likelihood of attack due to a high motivation.*

By default, the RR-NSM graded approach describes hypothetical adversary's motivation as moderate. There can be cases when an operator is provided with information regarding increased motivation of an adversary to perform an attack on a facility. In this case the operator may consider adapting to a high likelihood of attack and increase the PPS performance. It is important to reassess the adversary's capabilities that might also become more sophisticated with the increase of likelihood. The PPS effectiveness performance should be elevated one level in comparison to the previous model. For example, if an attractiveness of a material is **Low** than the correspondent level of PPS effectiveness performance should be **Moderate.** Alternatively, attractiveness of assets can be decreased. If it is estimated that the high likelihood of an attack is temporary it can be decided to relocate transportable assets from a research reactor to a more protected facility. If a research reactor is used to produce radionuclides, then it can be decided to temporary stop the production of radionuclides if it is not possible to adapt the PPS in a timely manner.

6 CASE STUDIES

Case studies were used to demonstrate the developed RR-NSM graded approach. For the case studies, two hypothetical nuclear facilities were used:

The first hypothetical facility is the Shapash Nuclear Research Institute (SNRI) – developed by the National Laboratory Los Alamos, USA and further improved by the IAEA. The Shapash facility is a research reactor with a fuel fabrication facility in its protected area. Transport and storage of nuclear materials for fuel fabrication takes place on an ongoing basis.

For the purpose of research in this thesis, a second hypothetical facility was created. It is a modified Shapash Nuclear Research Institute (SNRI). Modifications included changes in the layout and composition of buildings on site. In the modified layout the Fuel Production facility is removed, and a Radioisotope Production Facility (Radioisotope Production building) is added. Several Security Systems were eliminated (see 6.4 for detailed description).

For both facilities, the attractiveness of all identified assets is calculated.

6.1 The Shapash Nuclear Research Institute (SNRI).

6.1.1 Description of the Shapash facility.

Shapash Nuclear Research Institute (SNRI) (see Figures 6.1 and 6.2) is a hypothetical nuclear research facility. Besides various research programmes the Shapash facility also produces nuclear fuel for its research reactor. For this purpose, on the premises, inside the protected area of the Shapash facility there is a fuel fabrication facility. Materials for fuel fabrication are stored in a separate building located inside the protected area - Oxide Storage Bunker. The research reactor at SNRI operates using uranium oxide fuel. In addition, SNRI performs research on various types of nuclear materials (Uranium with various enrichment) [34].

6.1.1.1 Description of the layout.

The layout of the facility can be divided in two main areas: the Administrative Area (AA) and the Protected Area (PA) (see the layout on the Figure 6.1 and 6.2).

The AA is surrounded by a fence. The main entrance to the facility is through the AA, the gate is unlocked during working hours and locked during off working hours. The research reactor staff can still access the facility during off working hours with a staff badge. The Shapash facility is patrolled by 24-hour guards on foot.

The main Shapash facility buildings are located in the PA perimeter. There are the Research Reactor Building, the Fuel Fabrication Building, Shipping and Receiving Building, the Oxide Storage Bunker, X-ray Facility for fuel assembly quality control.

Entering the PA, staff has to pass through an Access Control Building (5 on the layout) that also hosts the Central Alarm Station and Special Response Team.

Offices for staff working in the PA are mainly located in the Technical Area Administrative Annex 1 (17 on the layout) and the Research Reactor Building (25 on the layout).

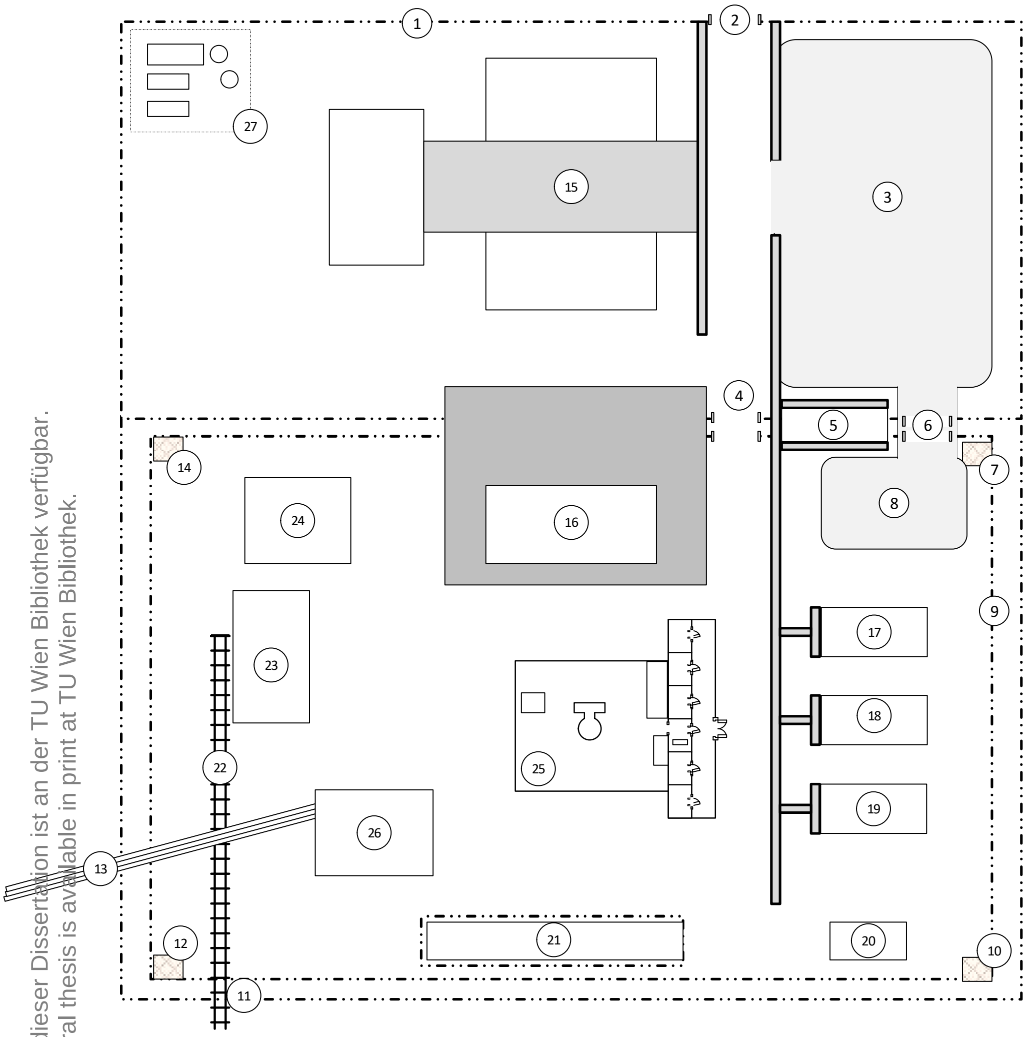


Figure 6.1 Layout of the Shapash facility

1. Site Perimeter fence
2. Site Entrance
3. Parking Area
4. Tech Area Commercial Vehicle Access Control Point (ACP)
5. Access Control Building (ACB), Central Alarm Station (SAS), Special Response Team (SRT) Alert Facility (Vital Area)
6. VIP Gate
7. NE Guard Tower
8. VIP Parking
9. Tech Area Inner Perimeter Fence
10. SE Guard Tower
11. Rail Gate
12. SW Guard Tower
13. Commercial Power Lines
14. NW Guard Tower
15. External Administrative Campus
16. Tech Area Cafeteria
17. Tech Area Admin Annex I
18. Analytical Laboratory
19. Waste Measurement Facility
20. Oxide Storage Bunker (Vital Area)
21. Scrap Yard
22. Rail Spur
23. Shipping and Receiving Facility
24. X-ray Facility (Inner Area)
25. Research Reactor Building and Offices (Vital Area)
26. Fresh Fuel Fabrication Building (Vital Area)
27. Radioactive Waste Site

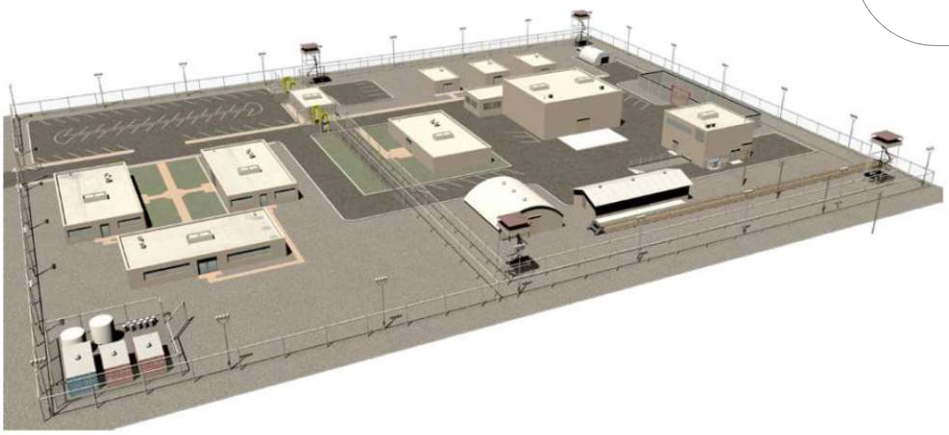


Figure 6.2 3D view of the Shapash facility [34]

6.1.2 Assets of the Shapash facility.

6.1.2.1 Nuclear Materials

At the Shapash facility Uranium is stored in different forms and used for various purposes. In Table 6.1 identified nuclear materials are listed and considered as assets of the Shapash facility.

Facility Area	Location	Material Form	Material Amount (% enrichment)	Total Isotope Amounts
Research Reactor	Reactor	UO_2HEU Fuel Assemblies (240 in reactor)	686.4 kg U (36%)	247.2 kg U-235
	Fresh Fuel Vault	UO_2 HEU Fresh Fuel Pins (80 assemblies in storage)	228.9 kg U (36%)	82.4 kg U-235
	Fuel Pool Irradiated fuel	UO_2 HEU irradiated fuel Pins (100 in pool)	28.6 kg U (36%)	10.3 kg U-235
	R091 Product Vault	HEU metal	23 kg U (95%)	22 kg U-235
X-ray Facility		Fresh Fuel Pins	8.6 kg U (36%)	3.1 kg U-235
		HEU metal	5.2 kg U (95%)	5 kg U-235
Oxide Storage Bunker		UO_2 HEU	250 kg U (36%)	90 kg U-235
Fuel Fabrication Building	Oxide Vault	UO_2	94.5 kg U (36%)	34 kg U-235
	Pin Vault	UO_2	69.5 kg U (36%)	25 kg U-235
	Pellet Vault	UO_2	69.5 kg U (36%)	25 kg U-235
Waste Storage Site	Tanks	Liquid Mixture (2 tanks, 1,000 liters)	Trace Amounts of U (3%)	trace

Table 6.1: The inventory of Nuclear Material at the Shapash facility.

6.1.3 Attractiveness of Shapash facility assets related to potential consequences of a malicious act.

Coefficients representing the severity of an impact caused by a malicious act are listed in the Table 6.2.

Potential Impacts	Description	Coefficient
High (H)	Unacceptable impact	1
Moderate (M)	Undesirable impact	0.75
Low (L)	Tolerable impact	0.5
Very Low (VL)	Acceptable impact	0.2

Table 6.2 Coefficients of an impact severity due to a malicious act.

Table 6.3 lists assets of the Shapash facility and coefficients characterising severity of consequences related to 'Health', to 'Financial' and to 'Reputation' areas. Coefficients are chosen based on the criteria described in chapter 5.6.1. The attractiveness of an asset related to potential consequences equals the highest value of the coefficient in any of three areas for a single asset.

Facility Area	Location	Consequences for public and staff	Consequences for organization		Attractiveness by consequences	Impacts
		Health	Financial	Reputation		
Research Reactor	UO$_2$ HEU Fuel Assemblies (240 in reactor)	1	1	1	**1**	**H**
	UO$_2$ HEU Fresh Fuel Pins (80 assemblies in storage)	0.2	1	0.75	**1**	**H**
	UO$_2$ HEU irradiated fuel Pins (100 in pool)	1	0.5	0.75	**0.75**	**M**
	HEU metal	0.2	0.75	0.75	**0.75**	**M**
X-ray Facility	Fresh Fuel Pins	0.2	0.2	0.5	**0.5**	**L**
	HEU metal	0.2	0.2	0.5	**0.5**	**L**
Oxide Storage Bunker	UO$_2$ HEU	0.2	1	1	**1**	**H**
Fuel Fabrication Building	Oxide Vault UO$_2$	0.2	0.5	1	**1**	**H**
	Pin Vault UO$_2$	0.2	0.5	1	**1**	**H**
	Pellet Vault UO$_2$	0.2	0.5	1	**1**	**H**
Waste Storage Site	Liquid Mixture (2 tanks, 1,000 litres)	1	0.5	0.75	**1**	**H**

Table 6.3 Nuclear Materials at the Shapash facility and their evaluated attractiveness by consequences.

6.1.3.1 Attractiveness of Shapash facility assets related to its properties.

Table 6.4 lists assets of the Shapash facility and coefficients characterising properties related to 'Transportability', to 'Health impact', to 'Processing time and complexity' and to 'Obtaining Usable Mass' areas. Coefficients are chosen based on the criteria described in chapter 5.6.2. The attractiveness of an asset related to its properties equals an average value of coefficients in four areas for a single asset.

Facility Area	**Material Form**	**Process of acquisition and obtaining Usable Mass of Nuclear Material**				**Attractiveness by property**
		Transportability	**Health impact** (during acquisition)	**Processing time and complexity**	**Obtaining Usable Mass**	
Research Reactor	UO_2 HEU Fuel Assemblies (240 in reactor)	0.2	0.2	0.2	1	0.40
	UO_2 HEU Fresh Fuel Pins (80 assemblies in storage)	0.5	1	0.5	1	0.75
	UO_2 HEU irradiated fuel Pins (100 in pool)	1	0.2	0.2	0.5	0.48
	HEU metal	1	1	0.75	0.5	0.81
X-ray Facility	Fresh Fuel Pins	1	1	0.75	0.2	0.74
	HEU metal	1	1	0.75	0.2	0.74
Oxide Storage Bunker	UO_2 HEU	0.75	1	0.75	1	0.88
Fuel Fabrication Building	Oxide Vault UO_2	0.75	1	0.75	0.75	0.81
	Pin Vault UO_2	0.75	1	0.75	0.75	0.81
	Pellet Vault UO_2	0.75	1	0.2	0.75	0.68
Waste Storage Site	Liquid Mixture (2 tanks, 1,000 liters)	0.2	0.2	0.2	0.2	0.20

Table 6.4 Nuclear Materials at the Shapash facility and their evaluated attractiveness by properties.

6.1.3.2 Overall attractiveness of each asset at the Shapash facility.

The overall value of an asset's attractiveness equals an average value of attractiveness related to potential consequences and attractiveness related to asset's properties (see Table 6.5). The final attractiveness grade is chosen based on the corresponding range that is described in the chapter 5.6.3.

Facility Area	Material Form	Attractiveness by consequences	Attractiveness by property	Total Attractiveness value	Attractiveness grade
Research Reactor	UO_2 HEU Fuel Assemblies (240 in reactor)	1	0.40	**0.7**	**High**
	UO_2 HEU Fresh Fuel Pins (80 assemblies in storage)	0.75	0.75	**0.75**	**High**
	UO_2 HEU irradiated fuel Pins (100 in pool)	0.75	0.48	**0.61**	**Moderate**
	HEU metal	0.75	0.81	**0.78**	**High**
X-ray Facility	Fresh Fuel Pins	0.5	0.74	**0.62**	**Moderate**
	HEU metal	0.5	0.74	**0.62**	**Moderate**
Oxide Storage Bunker	UO_2 HEU	1	0.88	**0.94**	**Very High**
Fuel Fabrication Building	Oxide Vault UO_2	1	0.81	**0.9**	**Very High**
	Pin Vault UO_2	1	0.81	**0.9**	**Very High**
	Pellet Vault UO_2	1	0.68	**0.84**	**High**
Waste Storage Site	Liquid Mixture (2 tanks, 1,000 liters)	1	0.20	**0.6**	**Moderate**

Table 6.5 Overall attractiveness of Nuclear Materials at the Shapash facility.

6.2 Case study 1: Application of the RR-NSM graded approach at the Shapash research facility for a scenario of a malicious act by an outsider in collusion with an insider.

6.2.1 Description of the hypothetical scenario.

Target: Uranium oxide powder (UO_2) enriched up to 36% stored in the Oxide Vault of the Fuel Fabrication facility (building). Target is 80 kg of UO_2 enriched up to 36%, which contains about 29 kg of U-235.

Threat: 4 adversaries are outsiders, and 1 adversary is an insider.

Actions of insider: leave the door to the Fuel Fabrication facility unlocked. The unlocked door represents one barrier less to be breached by outsiders. Insider's action decreases the delay time and probability to be detected by guards since outsiders need to spend less time in the area observed by guards.

Actions of outsiders: breach external barriers, move to the Fuel Fabrication facility unspotted by guards, breach barriers in the building, remove the oxide material and leave in the same way.

Tools that outsiders use:

- Manual bolt cutters.
- Lock picking tools.
- Roto hammer, drill, sledgehammer.
- Cutting torch and portable generator.
- 4 Guns.

Tactics: As discreet as possible but violent response is possible.

Time of attempt: Attempt is planned at 3 a.m. on Saturday.

Path to the fuel Fabrication facility (see Figure 6.3)**:**

- Breach the perimeter fences.
- Move to the Fuel Fabrication facility.

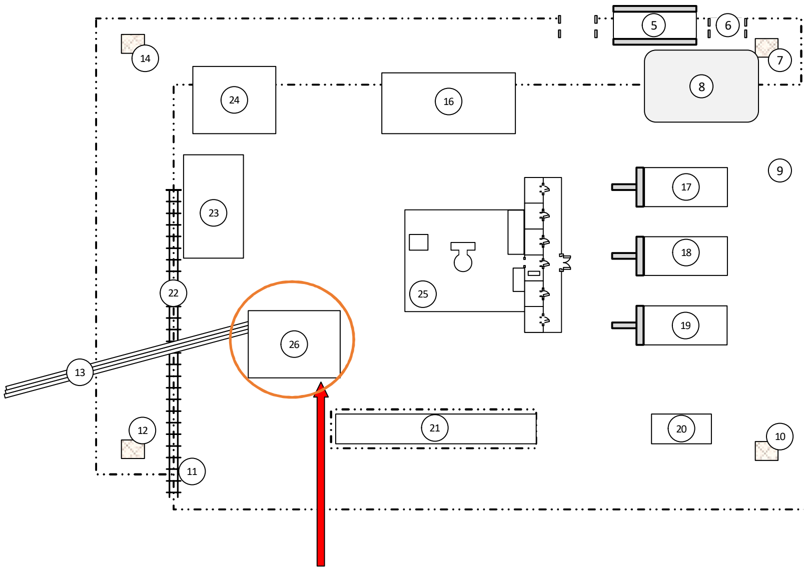


Figure 6.3 Path of outsiders to the Fuel Fabrication facility

5. Access Control Building (ACB)
6. VIP Gate
7. NE Guard Tower
8. VIP Parking
9. Tech Area Inner Perimeter Fence
10. SE Guard Tower
11. Rail Gate
12. SW Guard Tower
13. Commercial Power Lines
14. NW Guard Tower
15. External Administrative Campus
16. Tech Area Cafeteria
17. Tech Area Admin Annex I
18. Analytical Laboratory
19. Waste Measurement Facility
20. Oxide Storage Bunker
21. Scrap Yard
22. Rail Spur
23. Shipping and Receiving Facility
24. X-ray Facility
25. Research Reactor Building and Offices
26. **Fresh Fuel Fabrication Building**

Path inside the Fuel Fabrication facility (see Figure 6.4)**:**

- Enter the Fuel Fabrication facility.
- Breach one internal door in the Fuel Fabrication facility.
- Breach the 20 cm thick concrete wall to the vault.
- Unpack the sealed containers and distribute 80 kg of UO_2 with 36% U-235 from the Oxide Storage Bunker between 4 people.
- Leave all used tools at the scene and leave the facility using the same way back.

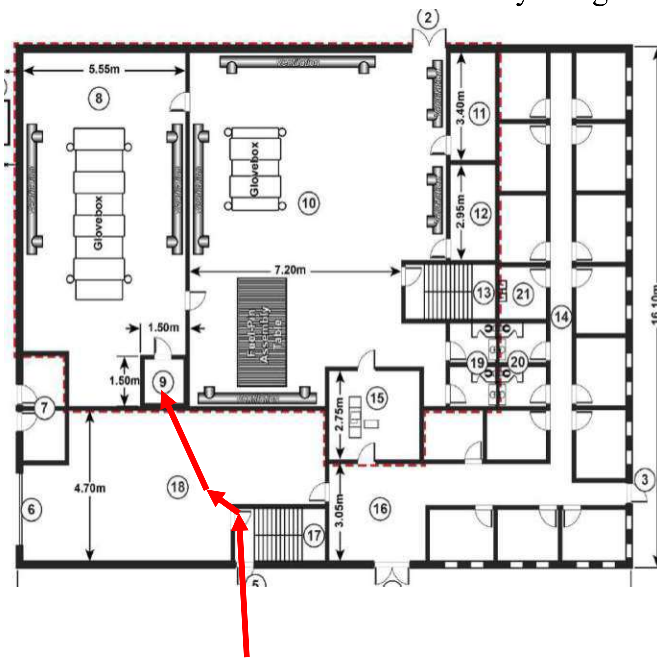


Figure 6.4 Path of outsiders inside the Fuel Fabrication facility

6.2.2 Calculate delay time on the analysed path.

Every barrier has its delay time (or a range of delay times), the delay time depends on a breaching method and tools outsiders use [35]. In every section of the path adversaries need to fulfil a task - to breach a barrier with a particular property using certain breaching method and tools. Table 6.6 shows the cumulative delay time is calculated by analysing delay time of each section on the path. The identified cumulative delay time is 12 min 50 sec.

Task description	Barrier properties	Barrier breaching method	Delay time (min)	Cumulative delay time (min)
Breach the fence	two 2.5-m-high chain-link fences with an alarmed isolation zone between the two fences.	Manual bolt cutters	0.2	0.2
Move towards the door to the Fuel Fabrication Facility	no barrier	no barrier	0.5	0.7
Breach the door to Fuel fabrication facility	Standard industrial pedestrian door, 1.6-mm metal.	no barrier (door is unlocked)	0.05	0.75
Move towards the internal door	no barrier	no barrier	0.1	0.85
Breach the internal door	Standard industrial pedestrian door, 1.6-mm metal.	Lock picking tools	0.1	0.95
Move towards the wall of the Oxide Vault	no barrier	no barrier	0.1	1.05
Breach the wall to Oxide storage	Concrete – 20 cm Thick, Reinforced	Rotary hammer drill, sledgehammer, cutting torch portable generator	7	8.05
Open containers and collect the 80 kg of UO_2 with 36% U-235	Each container is secured with several nuts that can be unscrewed using conventional key	Unscrew nuts and distribute the material in backpacks of adversaries	4	12.05
Move back towards the internal door	no barrier	no barrier	0.1	12.15
Move back towards the external door of the Fuel fabrication facility	no barrier	no barrier	0.1	12.25
Move back towards the fence	no barrier	no barrier	0.5	12.75
Move through the fence	no barrier	no barrier	0.1	12.85

Table 6.6 Estimated barriers delay time.

6.2.3 Identify Critical Detection Point (CDP) on the path.

Based on the Shapash facility documentation the Response Team can reach the Fuel Fabrication Building in 2 minutes [34]. One minute is added to cover the time for communication among the response team, assessment of the threat. The CDP on the path is a location and a point of time during the malicious act attempt when adversaries need to be interrupted. In Table 6.7 the CDP on the path is identified by taking 3 minutes from the cumulative delay time. It was identified that the adversaries must be detected at the latest at about 10 min after the malicious act attempt starts, this is after 2 minutes of the breach of the wall to Oxide storage using rotary hammer drill, sledgehammer, cutting torch and portable generator.

Task description	Delay time (min)	Cumulative delay time (min)	CDP based on response Force Time (-2min)
Breach the fence	0.2	0.2	Detection at any point of this part of the path will provide enough time for the response team for successful response
Move towards the door to the Fuel Fabrication Facility	0.5	0.7	
Breach the door to Fuel fabrication facility	0.1	0.75	
Move towards the internal door	0.1	0.85	
Breach the internal door	0.1	0.95	
Move towards the wall of the Oxide Vault	0.1	1.05	
Breach the wall to Oxide storage	7	8.05	Critical Detection Point is 2 minutes after the breaching this barrier starts
Open containers and collect the 80 kg of UO_2 with 36% U-235	4	12.05	Detection at any point of this part of the path will not provide enough time for the response team for successful response
Move back towards the internal door	0.1	12.15	
Move back towards the external door of the Fuel fabrication facility	0.1	12.25	
Move back towards the fence	0.5	12.75	
Move through the fence	0.1	12.85	

Table 6.7 Estimated Critical Detection Point (CPD).

6.2.4 Assess the effectiveness of cumulative effectiveness of PPS on the path until the CPD

The coefficients of Pd and Pa are chosen based on knowledge of detection instruments and instruments that allow to conduct assessment, and internal procedures. This usually should include estimations provided by specialists. In Table 6.8 estimated effectiveness of PPS on the path until the CPD is described. Effectiveness grades probabilities of detection and assessment are provided in the table 5.21.

Task description	Description of PPS [34]	Probability of detection (Pd)	Pd	Probability of assessment (Pa)	Pa	Peff
Breach the fence	Guard towers at each corner of the perimeter Alarmed isolation zone between the two fences	**High (H)** Detection occurs almost always. May be some doubt about the reliability of some element of the system.	0.75	**Moderate (M)** Assessment may occur but may be delayed to the point where it affects response.	0.5	0.875
Move towards the door to the Fuel Fabrication Facility	Guard towers at each corner of the perimeter	**Very low (VL)** Detection almost never or never. Very little or no chance of detection.	0.1	**Low (L)** Assessment may not occur. System has high susceptibility to deceit or defeat.	0.25	0.325
Breach the door to Fuel fabrication facility	There are no alarms in the offices or sensors on the office doors	**Very low (VL)** Detection almost never or never. Very little or no chance of detection.	0.1	**Low (L)** Assessment may not occur. System has high susceptibility to deceit or defeat.	0.25	0.325
Move towards the internal door	No sensors, no cameras	No Detection	0	No Assessment	0	0
Breach the internal door	There are no alarms in the offices or sensors on the office doors	No Detection	0	No Assessment	0	0
Move towards the wall of the Oxide Vault	No interior sensores, no cameras	No Detection	0	No Assessment	0	0
Breach the wall to Oxide Storage	Routine patrol can hear	**Moderate (M)** Often. Detection has an average chance of occurring, systems are in place and functional, but reliability may be questionable.	0.5	**Very low (VL)** Assessment will very likely not occur.	0.1	0.55

Table 6.8 Estimated effectiveness of PPS on the path until the CPD.

6.2.5 Conclusion on the PPS effectiveness.

The effectiveness of the PPS for the scenario of 80 kg UO_2 theft from the fuel fabrication facility by 4 adversaries in collusion with an insider is calculated by equation:

$$Peff.r = 1 - \left\{\prod_{j=1}^{J}(1 - Pd * Pa)\right\} = 1\text{-}(1\text{-}0.85)*(1\text{-}0.325)*(1\text{-}0.325)*(1\text{-}0.55) = \mathbf{97\%}$$

In Table 6.9 the summary of calculated results of the attractiveness and PPS effectiveness are presented.

Asset	**Location**	**Attractiveness of the asset**	**Effectiveness of PPS on the analysed path**
80 kg of UO_2 (36%)	Fuel Fabrication Building (Oxide Vault)	**90%***	**97%**

Table 6.9 Estimated attractiveness and PPS effectiveness for the Case Study 1 scenario

**80 kg of UO_2 (36%) is of the same attractiveness as 94 kg of UO_2 (36%).*

The effectiveness of PPS is higher than the assessed attractiveness of the asset which means that the effectiveness of the PPS corresponds to the attractiveness of the asset for the chosen scenario. Other scenarios of UO_2 theft from the fuel fabrication facility should be considered to get a more comprehensive picture of the PPS effectiveness.

The result is demonstrated in Table 6.10 with the purple dot and is identified as **1**- Strong level of PPS effectiveness which means that the PPS effectiveness is well balanced with the attractiveness of an asset.

Attractiveness	**Effectiveness of PPS**				
	VH (0.9 – 1)	H (0.7 - 0.9)	M (0.4 - 0.7)	L (0.2 - 0.4)	VL (< 0.2)
Very High (VH) 0.9 - 1	1 ●	2	3	4	5
High (H) 0.7 - 0.9	0	1	2	3	4
Moderate (M) 0.4 - 0.7	0	0	1	2	3
Low (L) 0.2 - 0.4	0	0	0	1	2
Very low (VL) < 0.2	0	0	0	0	1

Table 6.10 Calculated value displayed on the matrix of Asset's Attractiveness vs PPS effectiveness.

It is important to note that the main contributor to the PPS effectiveness in this scenario is the detection at the fence. If, for some reason, detection on the fence fails then the overall PPS effectiveness would be poor. It could be considered to add redundancy in the overall PPS arrangements to reduce a strong dependency on one PPS element.Case Study 2: Application of the RR-NSM graded approach at the Shapash for a scenario of a malicious act by an insider.

6.2.6 Description of the hypothetical scenario

Target: 4 kg of uranium oxide powder (UO_2) with 36% U enrichment. The UO_2 is stored in a container.

The entire container weighs around 50 kg. The shipping container and the overpack weighs 35 kg, the packing material weighs 6 kg, the material container weighs 5 kg, and the UO_2 material from one container weighs 4 kg.

Threat: The insider is a staff from the Material Balance Area group that verifies delivered nuclear materials.

Nuclear material delivery process description:
Four containers with uranium oxide powder (UO_2) with 36% U enrichment are delivered via rail at the Shipping and Receiving Facility.

All containers with delivered uranium oxide powder are transferred to the Oxide Storage Bunker the same day they are received. However, the containers are left in the shipping and receiving facility for two to three hours. This is done for the purpose of verification and completing necessary paperwork before transferring to the Oxide Storage Bunker. Two staff members from the Material Balance Area group verify weights, serial numbers, seals, and isotopic measurements. The nuclear material is never left unattended and in addition, the security patrol checks the area and material every 30 minutes.

Actions of an insider:
During the registration of the new UO_2 powder delivery, while the procedure of isotopic measurements the Material Balance Area group staff hides 4 kg in their bag and returns to the container an empty material container and closes all lids and puts a seal on the container. Then they complete all paperwork as usual. After the verification procedure the containers are being escorted to the Oxide Storage Bunker. The insider goes in their office in the Tech Area Admin Annex I and leaves the facility through the conventional exit at the end of the working day, they leave by car through the main site gate.

Tools that the insider uses:
A bag to put and hide the uranium oxide powder (UO_2).

Tactics: Evade detection on any path section, not violent and no weapons to be used.

Time of attempt: Attempt is planned during working hours.

Path of the insider shown on the layout.

The path of the insider is shown on the Figure 6.5. The insider removes the UO_2 during the verification processes in the Shipping and Receiving Facility (number 23). The insider seals an empty container and transports it to the Oxide Storage Bunker (number 20). The insider stays in their office at the Tech Area Admin Annex I with the stolen UO_2 material (number 17). The insider leaves at the end of the working day through the Access Control Building (number 5) and then through the main site gate (number 2) by their car.

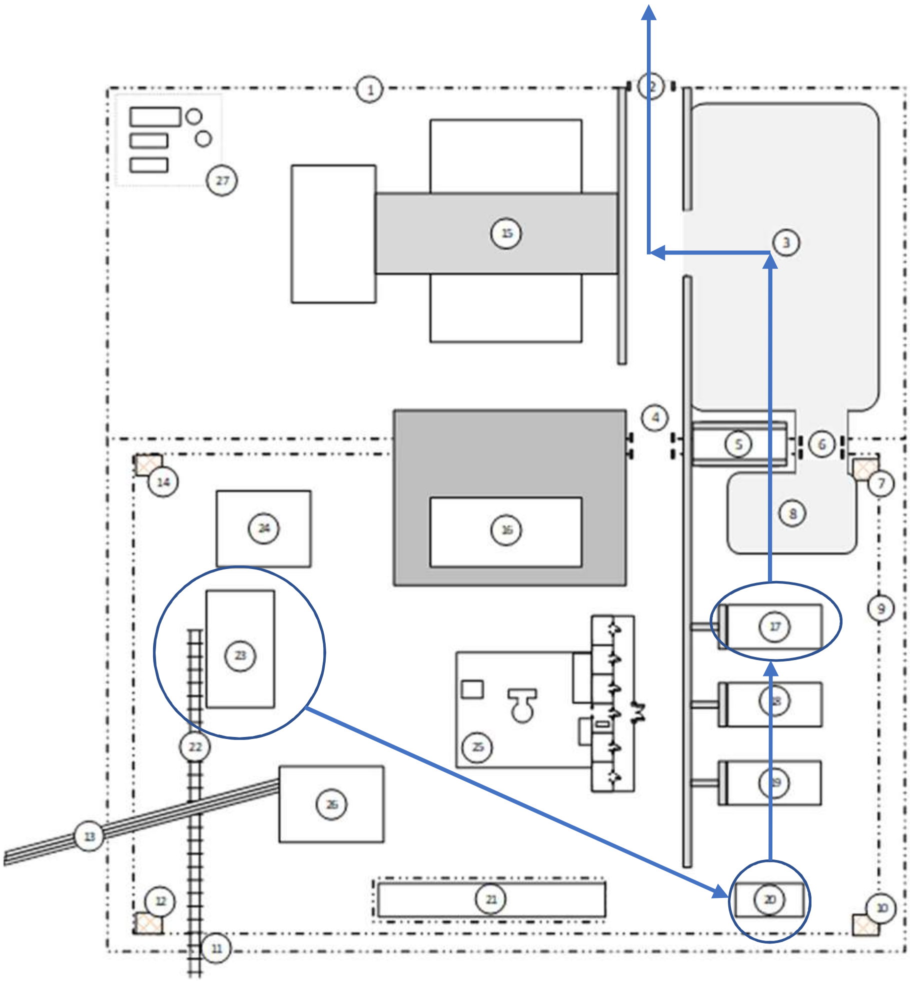


Figure 6.5 Path of the insider at the facility

5. Access Control Building (ACB)
17. Tech Area Admin Annex I
20. Oxide Storage Bunker (Vital Area)
23. Shipping and Receiving Facility

6.2.7 Identify Total Attractiveness of the asset.

The calculated attractiveness of assets in the Shapash facility described in the chapter 6.1.26.1.3 included assessment of all UO_2 stored in the Oxide Storage Bunker. In total, this is 250 kg UO_2 (36%) which corresponds to 90 kg U-235. In the chosen scenario the insider attempts to steal only part of the stored UO_2. Hence, the attractiveness of the nuclear material should be calculated specifically for 4 kg of UO_2 (36%). In Table 6.11 the attractiveness by consequences due to the theft of 4 kg of UO_2 (36%) is identified (C1). In Table 6.12 the identified impact level is demonstrated.

Facility Area	Location	Health	Financial	Reputation	Attractiveness by Consequences (C1)
Shipping and Receiving Facility	Shipping and Receiving Facility	0.2	0.2	0.5	**0.5**
Comments					
		Consequences for offside and onside are very low. The material cannot produce a significant contamination and permanent injury is unlikely or impossible.	Financial implications are very low. The cost of the stolen material is less than 2% of annual funds. Temporary missing material will not cause disruption in operation	Reputation of the facility can be damaged and may lead to reduced credibility and reduced funding. However, the impact is not critical for the operation of the Shapash facility.	**The highest value is chosen.**

Table 6.11 Attractiveness by consequences of Nuclear Material at the Shapash facility (UO_2 (36%)).

C1 = Maximum of (0.2; 0.2; 0.5) = 0.5 – The attractiveness by consequences is assessed as **Low (L)** which can be classified as "tolerable impact"

Potential Impacts	Description	Coefficient (C1)
High (H)	Unacceptable impact	1
Moderate (M)	Undesirable impact	0.75
Low (L)	Tolerable impact	0.5
Very Low (VL)	Acceptable impact	0.2

Table 6.12 A level of a potential impact based on consequences of a malicious act.

In Table 6.13 the attractiveness of 4 kg of UO_2 (36%) by properties of the material is identified (C2). In Table 6.14 the identified impact level is demonstrated.

Facility Area	Material Form	Process of acquisition and Obtaining Usable Mass				Attr. by property (C2)
		Transportability (P)	Health impact (R)	Processing time and complexity (T)	Obtaining Usable Mass (M)	
Shipping and Receiving Facility	UO_2 HEU (36%)	1	1	0.75	0.2	**0.74**
Comments						
		4 kg of uranium oxide powder can be easily transported by an individual. The powder form is beneficial for hiding the material.	No health impact for an individual who knows how to handle the UO_2 material.	The material is HEU with 36% U enrichment. Low reprocessing might be required.	4 kg of UO_2 with 36% U enrichment contains about 1.5 kg of U-235. More than 10 times of this amount is needed to build a nuclear improvise device.	**Average value is calculated.**

Table 6.13 Attractiveness by properties of Nuclear Material at the Shapash facility (UO_2 (36%)).

C2= (P+R+T+M)/4 = (1+1+0.75+0.2)/4 = **0.74** – The attractiveness by properties is assessed as **High (H)**

C2 - Attractiveness of an asset by properties	
0.7 - 1	High (H)
0.4 - 0.7	Moderate (M)
0.2 - 0.4	Low (L)
<0.2	Very Low (VL)

Table 6.14 A level of a potential impact based on properties of the material (UO_2 (36%)).

Total attractiveness is calculated as an average value of attractiveness based on potential consequences and attractiveness by properties of an asset. In Table 6.15 the total attractiveness grade of the material (UO_2 (36%)) is presented. In Table 6.16 the identified total impact is demonstrated.

C = (C1+C2)/2 = (0.5*0.74)/2 = **0.62 -** The total attractiveness falls in the range 0.4-0.7 and is correspondent to a **Moderate (M)** level of attractiveness**.**

Facility Area	Material Form	Attractiveness by consequences	Attractiveness by property	Total Attractiveness value	Attractiveness grade
Shipping and Receiving Facility	4 kg UO_2 powder (36% U enriched)	0.5	0.74	**0.62**	**62% = Moderate**

Table 6.15 Total attractiveness grade of the material (UO_2 (36%))

C = (C1+C2)/2	
Very High (H)	0.9-1
High (H)	0.7 - 0.9
Moderate (M)	0.4 – 0.7
Low (L)	0.2 - 0.4
Very Low (VL)	<0.2

Table 6.16 A total level of a potential impact based on properties of the material (UO_2 (36%)) and on consequences of a malicious act

6.2.8 Effectiveness to detect an insider using four detection criteria.

The effectiveness of the PPS is analysed by four aspects to detect an insider on the path: a moving individual (insider), a removed material that is being carried, a presence of an external tool, presence and unauthorized use of an internal tool. In Table 6.17 the inputs of probabilities of detection (Pd) and probabilities of assessment (Pa) on every path section for the considered scenario are demonstrated. The effectiveness to detect an individual (insider) who is a staff member during his/her movement at the Shapash facility in this scenario equals zero since it is a usual work path, hence the columns are grayed out in Table 6.17.

Effectiveness to detect an external or internal tool during unauthorized use or carrying is not applicable since the adversary follows usual procedures, hence the columns are grayed out in Table 6.17.

Table 6.17 Estimated values representing effectiveness of PPS on the path using four detection criteria.

Path	Task description	Effectiveness to detect							
		An individual		A stolen material		An external tool		An internal tool	
		Pd	Pa	Pd	Pa	Pd	Pa	Pd	Pa
In the Shipping and Receiving Facility building	Hide 4 kg of UO_2 powder material in a bag under clothes while the procedure of isotopic measurements.	0	0	0,5	0,75	N/A	N/A	N/A	N/A
In the Shipping and Receiving Facility building	Return to the container an empty material container and close with bolts all lids with tamper indicating device.	0	0	0,5	0,75	N/A	N/A	N/A	N/A
From Shipping and Receiving Facility to Oxide Storage building	Holding the material. Escort containers to the Oxide Storage Bunker.	0	0	0	0,75	N/A	N/A	N/A	N/A
Go to the Tech Area	Hide Material in the office of the Tech Area and wait until the end of the working hours.	0	0	0	0,75	N/A	N/A	N/A	N/A
Exit through the Access Control Building	Go through the Radiation Detector Gate	0	0	0,1	0,75	N/A	N/A	N/A	N/A
Exit through the main gates	Drive the car through the site entrance gates	0	0	0	0	N/A	N/A	N/A	N/A

In this scenario there is no need to identify a Critical Detection Point (CDP) on the path since the insider is leaving through the Access Control Building (ACB) and the on-site guards' capabilities are sufficient to detain the insider if successfully detected.

6.2.8.1 Cumulative effectiveness of PPS on the path.

Since the effectiveness to detect an individual (insider) and effectiveness to detect an external or internal tool are considered zero only the column related to carrying stolen material is considered in Table 6.18.

In Table 6.18 estimated cumulative effectiveness of PPS to detect stolen material on the path is presented.

Path	Task description	A stolen material		Total Effectiveness	Comments
		Pd	Pa		
In the Shipping and Receiving Facility building	Hide 4 kg of UO_2 powder material in a bag under clothes while the procedure of isotopic measurements. Return to the container an empty material container and close with bolts all lids with tamper indicating device.	0,5	0,75	**0.375**	Probability of visual detection due to procedures: 1) Two staff members conduct the isotopic measurements. 2) Security patrol every 30 minutes.
From Shipping and Receiving Facility to Oxide Storage building	Holding the material. Escort containers to the Oxide Storage Bunker.	0	0,75	**0**	There is no detection mechanism on this stage but if a material could be detected by another staff, then there is a high probability of correct assessment (material is recognized)
Go to the Tech Area	Hide Material in the office of the Tech Area and wait until the end of the working hours.	0	0,75	**0**	There is no detection mechanism on this stage but if a material could be detected by another staff, then there is a high probability of correct assessment (material is recognized)
Exit through the Access Control Building	Pass through the radiation detection gates	0,1	0,75	**0.075**	Probability to detect a very low radioactivity of UO_2 is low, but if detected then there is a high probability that it would be assessed correctly.
Exit through the main gates of the facility	Drive the car through the site entrance gates	0	0	**0**	There is no detection mechanism on this stage

Table 6.18 Estimated effectiveness of PPS on the path with comments.

The effectiveness of the PPS for the scenario of 4 kg UO_2 theft from the fuel fabrication facility by an insider is calculated by equation:

$$Peff.r = 1 - \left\{\prod_{j=1}^{J}(1 - Pd * Pa)\right\} = 1\text{-}((1\text{-}0{,}375)*(1\text{-}0{,}075)) = 0{,}42 = \mathbf{42\%}$$

6.2.8.2 Conclusion on the PPS effectiveness for a chosen scenario.

In Table 6.19 the summary of calculated results of the attractiveness and PPS effectiveness are presented. Both attractiveness of the asset and effectiveness of an insider detection for the chosen scenario are characterised as Moderate.

Asset	Attractiveness of the asset	Effectiveness of PPS on the analysed path
4 kg of **UO_2** powder (36% U enriched)	**62% - Moderate**	**42% - Moderate**

Table 6.19 Estimated attractiveness and PPS effectiveness for the Case Study 2 scenario

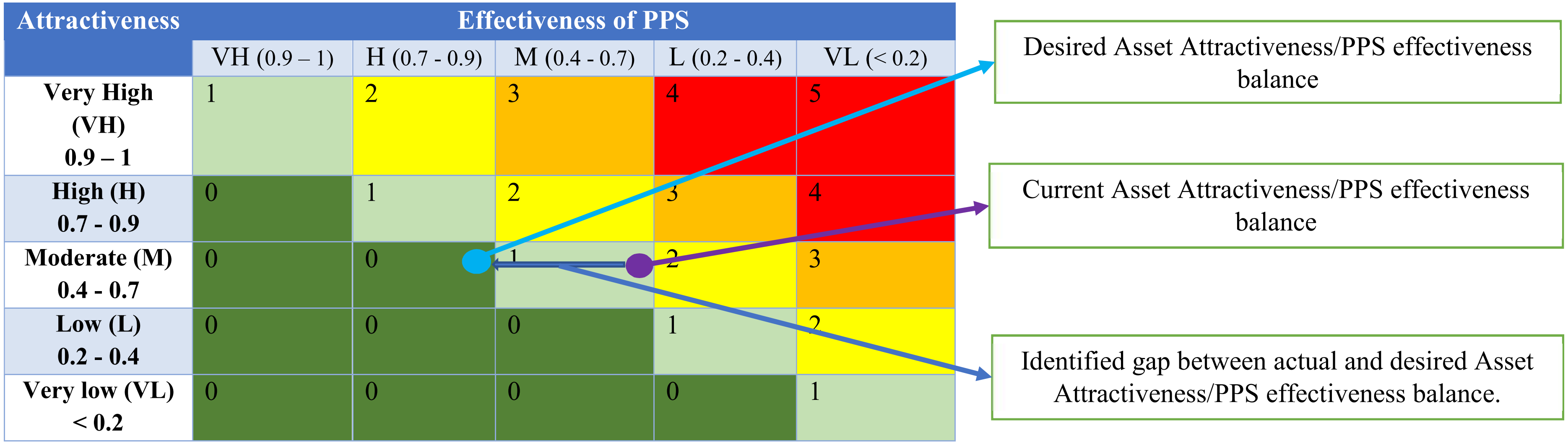
The calculated level of effectiveness of the PPS for the chosen scenario is 62%, it is 20% lower than calculated level of attractiveness which is 42%. Having obtained such results decision makers have to discuss several options and can conclude on accepting or not accepting the risk:

- *Accepting the risk:* the balance between asset attractiveness and PPS effectiveness is appropriate, no additional modifications or improvements are required.

OR

- *Not accepting the risk:* even if the asset attractiveness and PPS effectiveness are both characterized as “Moderate” there is an inappropriate disbalance, additional modifications or improvements are required. Modifications can be done to:
    - Decrease attractiveness level of the asset.
    - OR/And improve PPS effectiveness.

In Table 6.20 the result is demonstrated by the purple dot. The result is identified as **1**- Strong PPS effectiveness, the result is on the border with the category 2 (close to the required level of PPS effectiveness but improvements should be considered). Potential desired balance between asset attractiveness and PPS effectiveness is demonstrated on the matrix in Table 6.20 with the blue dot. Between the purple and the blue dot there is a gap that can be addressed by improving PPS effectiveness. The blue dot placement and the amount of effort required to improve PPS (represented in the length of the gap) should be identified by relevant decision-makers.



Attractiveness	**Effectiveness of PPS**				
	VH (0.9 – 1)	H (0.7 - 0.9)	M (0.4 - 0.7)	L (0.2 - 0.4)	VL (< 0.2)
Very High (VH) 0.9 – 1	1	2	3	4	5
High (H) 0.7 - 0.9	0	1	2	3	4
Moderate (M) 0.4 - 0.7	0	0	1	2	3
Low (L) 0.2 - 0.4	0	0	0	1	2
Very low (VL) < 0.2	0	0	0	0	1

Desired Asset Attractiveness/PPS effectiveness balance

Current Asset Attractiveness/PPS effectiveness balance

Identified gap between actual and desired Asset Attractiveness/PPS effectiveness balance.

Table 6.20 Calculated value displayed on the matrix of asset's Attractiveness vs PPS effectiveness and identified gap.

Other scenarios of UO_2 powder theft should be considered in order to get more comprehensive picture of the PPS effectiveness.

Potential options that can be considered to improve the PPS for the chosen scenario:

1. Improve procedure during of isotopic measurements conducted by two staff.
    - Check of the material before sealing the container by another staff (or by staff and security).
2. Improve detection in the Access Control Building.
    - Staff should exit through metal detector gates and not only through a gamma detector gate.

6.3 Case Study 3.1: Application of the RR-NSM graded approach at the radioisotope production facility for a scenario of a malicious act by an insider.

Since the Shapash facility operates only with nuclear material and not with Other Radioactive material, for the purpose of this research the Shapash facility was modified to a radioisotope production facility[1]. The modification is done to allow using a different type of asset (Other radioactive material) in the case study 3.1 and 3.2. The layouts are shown on Figures 6.6, 6.7 and 6.8. The Radioisotope production facility does not produce any fuel, hence there is no Fuel Production building. The Fuel Production building was replaced with the Radioisotope production building. All introduced changes in the Shapash facility:

- A Radioisotope Production building was placed instead of the Fuel Production building (marked with a green circle on the Figure 6.6).
- Storage for HEU U-235 targets was placed in the research reactor building's restricted area. For irradiation by neutrons and further isotope production purposes.
- No Oxide Storage Bunker – removed because it was only relevant to fuel production.
- No X-Ray Facility – removed because it was only relevant to fuel production.
- No Scrap Yard – removed because it was only relevant to fuel production.

Changes in the Security arrangements:

- No entrance/exit control at the isotope production facility.
- No second line of fence.
- No guarding towers in the corners of the Protected Area.

[1] Description of the radioisotope production facility does not belong to any official publication, it is based on the Shapash layout and created only to support research in this thesis.

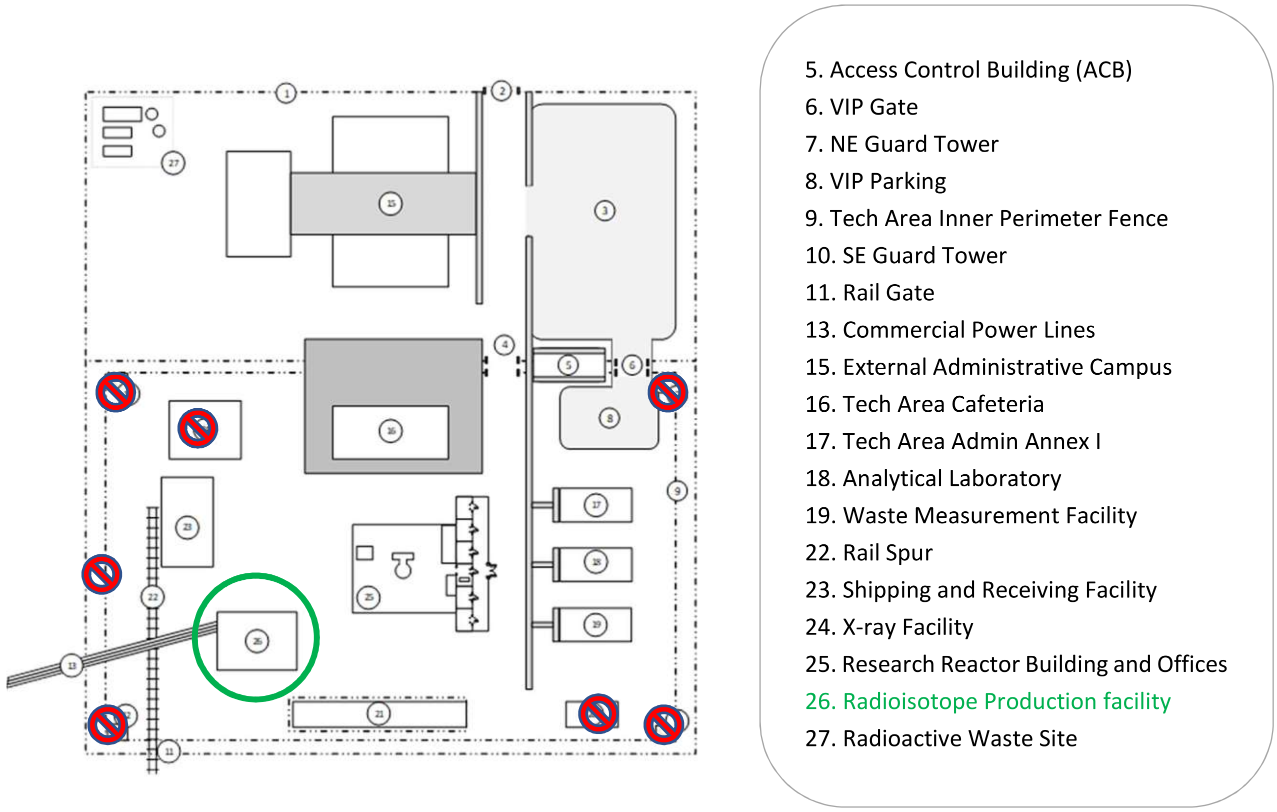

5. Access Control Building (ACB)
6. VIP Gate
7. NE Guard Tower
8. VIP Parking
9. Tech Area Inner Perimeter Fence
10. SE Guard Tower
11. Rail Gate
13. Commercial Power Lines
15. External Administrative Campus
16. Tech Area Cafeteria
17. Tech Area Admin Annex I
18. Analytical Laboratory
19. Waste Measurement Facility
22. Rail Spur
23. Shipping and Receiving Facility
24. X-ray Facility
25. Research Reactor Building and Offices
26. Radioisotope Production facility
27. Radioactive Waste Site

Figure 6.6 Introduced changes in the layout of Shapash facility to create the radioisotope production facility

6.3.1.1 Layouts of the radioisotope production facility.

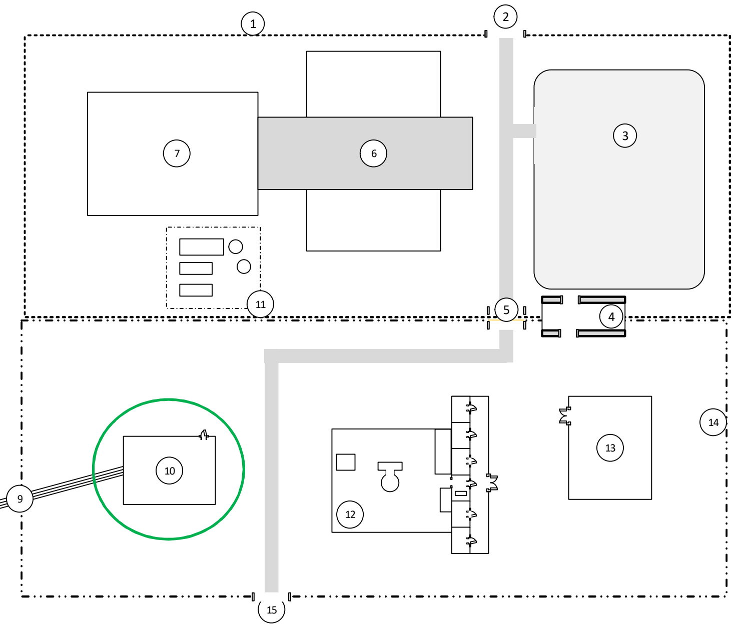
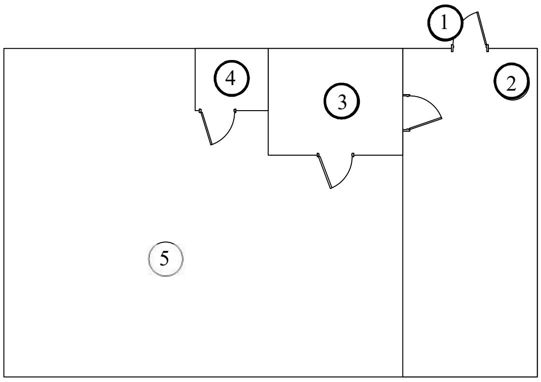


Figure 6.7 The layout of the radioisotope production facility.

1. Site Perimeter fence
2. Site Entrance
3. Parking Area
4. Access Control Building (ACB), Central Alarm Station (SAS), Special Response Team (SRT) Alert Facility (Vital Area)
5. Tech Area Commercial Vehicle Access Control Point (ACP)
6. Tech Area Cafeteria
7. External Administrative Campus
8. Electrical Power distribution building
9. Commercial Power Lines
10. Radioisotope Production Building
11. Radioactive Waste Site
12. Research Reactor Building, Labs for experiments and a storage for HEU U-235 targets
13. Offices and Analytical Laboratory
14. Tech Area Perimeter Fence
15. Tech area vehicle gate and emergency



1. Main Entrance
2. Non-Restricted Area
3. Changing room
4. Products Vault
5. Isotopes Production Area

Figure 6.8 Radioisotope Production building layout.

6.3.2 Description of the Radioisotope Production building.

The facility produces two radionuclides: Mo-99 and Cs-137.

Production of the **Mo-99** source at the facility:

- The Mo-99 radioisotope is produced for medical purposes and dispatched immediately after production and is not stored at the facility.
- The produced radioisotopes are packed and shipped to nuclear medical centres for their use.
- The activity of one produced Mo-99 source is 8.0 Ci = 0.3 TBq.
- Category: Cat II source [29]

Production of the **Cs-137** source at the facility:

- Cs-137 is produced to be used as a Brachytherapy source.
- Cs-137 is produced as a sealed source (see Figure 6.9).
- After production the Cs-137 sources are stored at the facility before dispatching. The dispatching of sources takes place twice a month.
- The activity of the source is 8.0 Ci = 0.3 TBq.
- Category: Cat II source [29]
- Cs-137 sources are produced on request.
- Storage location is the Product Vault in the Radioisotope Production building. Currently there are 10 sources stored in the product vault at the radioisotopes production facility waiting to be dispatched.

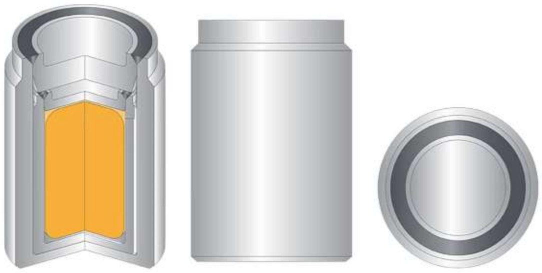


Figure 6.9 Cs-137 sealed source [36].

6.3.3 Description of the scenario

Target: one sealed Cs-137 source from the product vault at the radioisotope production building.

Threat: One insider from the Operations support staff. The insider has access to sealed sources only while performing paperwork and sources packaging before transport to external clients.

Actions of the insider and the path:

1. 5 days before the shipping day of the sealed sources bring a dummy of a sealed source and hide it in an office.

2. 3 days before shipping day of the sealed sources bring the transport container for a sealed source from outside into facility and hide it in an office.

3. On the shipping day, during the procedure of verification and packaging of ten Cs-137 sealed sources substitute one of them with a dummy (fake one that looks like real but just a metal – for a final visual inspection by the second staff).

4. Hide one sealed source in the radioisotope production building but outside of the storage vault (can be accessed by the insider unnoticed, see a layout of the building in Figure 6.10).

5. After sending the vehicle off with sealed sources the insider goes to the office and takes hidden transport container.

6. The delivery vehicle needs to drive a minimum of 3 hours before the first delivered source verification. The insider does not wait until the end of the working hours and leaves work simulating flu symptoms.

7. The insider goes to the Radioisotope Production building and puts the sealed source in his shielded container.

8. The insider goes immediately to the exit through the Access Control Building carrying the Cs-137 source (Cat II) in a shielded container in his backpack.

9. The insider leaves by car.

Insider's path in the Radioisotope Production building.

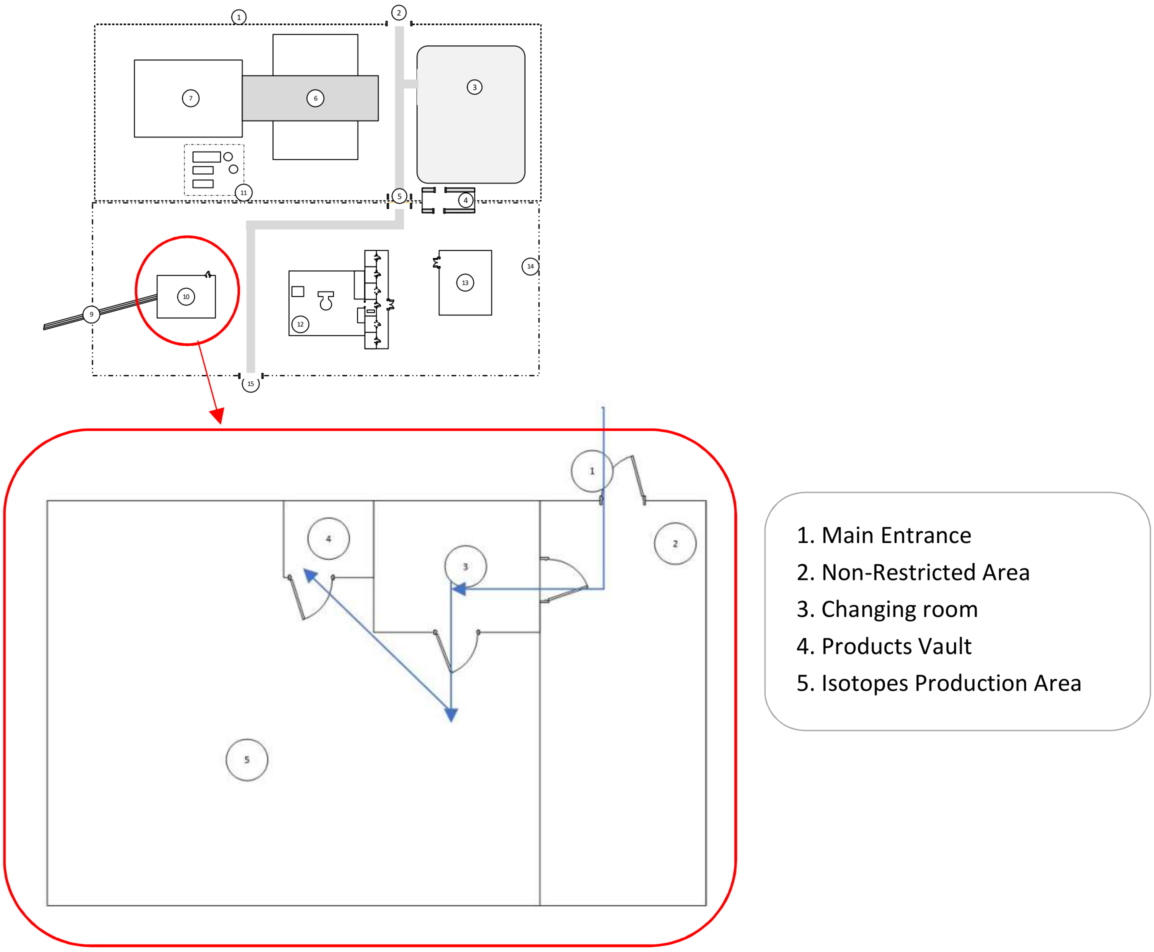


Figure 6.10 Insider's path in the Radioisotope Production building (with the same way out).

Tools that the insider uses:

- A dummy Cs-137 source
- A shielded portable container for transportation of radioactive sources (see Figure 6.11) [37].
  - Weight is 10 kg.
  - Lead thickness (walls, cover and bottom) is 2.5 cm.

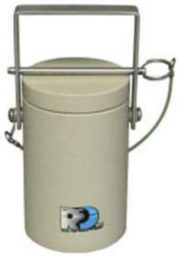


Figure 6.11 Shielded portable container for transportation of radioactive sources.

Tactics: Evade detection on any path section, not violent and no weapons to be used.

Time of attempt: Attempt is planned during working hours.

6.3.4 Total attractiveness of the asset

In Table 6.21 the attractiveness by consequences due to the theft of Cs-137 – Cat II source is identified (C1). In Table 6.22 the identified impact level is demonstrated.

Location	Material Form	Health	Financial	Reputation	Attractiveness by Consequences (C1)
Isotope Production building, Product Vault	Cs-137, sealed source (Cat II)	0,75	0,2	0,5	**0,75**
Comments					
		Health related consequences for offsite and onsite are moderate. Cs-137 due to its properties can be used as a dispersive device (RDD), however contaminated area would not be more than 1 km². Cs-137 can be used as an exposure device (RED) and cause a permanent injury if exposure time is between a few minutes and an hour and lethal if exposure time is between hours to days.	Financial implications are very low. The cost of the stolen material is less than 2% of annual funds. The missing material can cause an insignificant delay of a delivery to a customer.	Reputation of the facility can be damaged and may lead to reduced credibility.	**The highest value is chosen.**

Table 6.21 Attractiveness by consequences of Other Radioactive Material (Cs-137 – Cat II).

C1 = Maximum of (0.75; 0.2; 0.5) = 0.75 – The attractiveness by consequences is assessed as **Moderate (M)** which can be classified as "undesirable impact".

Potential Impacts	Description	Coefficient
High (H)	Unacceptable impact	1
Moderate (M)	Undesirable impact	0.75
Low (L)	Tolerable impact	0.5
Very Low (VL)	Acceptable impact	0.2

Table 6.22 A level of a potential impact based on consequences of a malicious act.

In Table 6.23 the attractiveness of a Cs-137 sealed source (Cat II) by properties of the material is identified (C2). In Table 6.24 the identified impact level is demonstrated.

Facility Area	**Material Form**	**Process of acquisition of Other Radioactive Material**				**Attr. by property (C2)**
		Transportability (P)	**Health impact (R)**	**Processing time and complexity (T)**	**Obtaining Usable Mass (M)**	
Isotope Production building	Cs-137, sealed source (Cat II)	1	0,75	N/A	N/A	**0,87**
		Comments				
		One sealed source has small size and can be easily transported by an insider.	Handling Cs-137 Cat II source can cause a permanent injury to an insider.	Not applicable for radioactive sources.	Not applicable for radioactive sources.	**Average value is calculated.**

Table 6.23 Attractiveness by consequences of Other Radioactive Material (Cs-137 – Cat II).

C2= (P+R+T+M)/4 = (0.75+1)/2 = **0.87** – The attractiveness by properties is assessed as **High (H)**

C2 - Attractiveness of an asset by properties	
0.7 - 1	High (H)
0.4 - 0.7	Moderate (M)
0.2 - 0.4	Low (L)
<0.2	Very Low (VL)

Table 6.24 A level of a potential impact based on properties.

6.3.4.1 Identify Total Attractiveness of the asset (C).

Total Attractiveness is calculated as an average value of attractiveness based on potential consequences and attractiveness by properties of an asset (see Table 6.25). In Table 6.26 the identified total level of potential impact is demonstrated.

C = (C1+C2)/2 = (0.75*0.87)/2 = **0.81 -** The total attractiveness falls in the range 0.7-0.9 and is correspondent to a **High (H)** level of attractiveness**.**

Facility Area	Material Form	Attractiveness by consequences	Attractiveness by property	Total Attractiveness value	Attractiveness grade
Isotope Production building	Cs-137, sealed source (Cat II)	0.75	0.87	**0.81**	**81% = High (H)**

Table 6.25 Total attractiveness grade of the material.

C = (C1+C2)/2	
Very High (H)	0.9-1
High (H)	0.7 - 0.9
Moderate (M)	0.4 – 0.7
Low (L)	0.2 - 0.4
Very Low (VL)	<0.2

Table 6.26 A total level of a potential impact.

6.3.5 Effectiveness to detect an insider using four detection criteria.

The effectiveness of the PPS is analysed by four aspects to detect an insider on the path: a moving individual (insider), a removed material that is being carried, a presence of an external tool, presence and unauthorized use of an internal tool. Table 6.27 demonstrates inputs of probabilities of detection (Pd) and probabilities of assessment (Pa) for every path section for the considered scenario.

In this scenario there is no need to identify a Critical Detection Point (CDP) on the path since the insider is leaving through the Access Control Building (ACB) and the on-site guards' capabilities are sufficient to detain the insider if successfully detected.

6.3.5.1 PPS effectiveness during preparation to the theft of Cs-137 source.

In the preparation phase an insider smuggles external tools onto the facility such as a source dummy that looks like an actual Cs-137 source and a shielding container to be used for transportation of the source. The dummy source is brought on site five days before the theft and the shielded container brought on site three days before the theft.

Path	Task description	Effectiveness to detect								Total Effectiveness
		An individual		A stolen material		An external tool		An internal tool		
		Pd	Pa	Pd	Pa	Pd	Pa	Pd	Pa	
From outside enter the protected area with an external tool Nr 1	Day -5. From outside go through entrance gates with a metallic cylinder that looks like a sealed source.	0	0	0	0	0.9	0.1	0	0	0.09
Enter the offices building	Day -5. Hide a metallic cylinder that looks like a sealed source in an office.	0	0	0	0	0	0	0	0	0
From outside enter the protected area with an external tool Nr 2	Day -3. From outside go through entrance gates with a shielded container that can be used to transport a sealed source.	0	0	0	0	0.9	0.1	0	0	0.09
Enter the offices building	Day -3. Hide a shielded container that can be used to transport a sealed source in an office.	0	0	0	0	0	0	0	0	0

Table 6.27 Values (Pd and Pa) to estimate effectiveness of PPS during preparation activities to the theft of Cs-137 source using four detection criteria.

Comments: Both metallic objects can be detected by the metal detector. Both tools are not known as unauthorized tools to the guards. In addition, the insider is characterized as an individual with high social skills. Hence during the assessment by guards the tools likely will not be recognized as unauthorized external tools. Total effectiveness to detect external tools in this scenario is very low. However, it adds 17% probability to detect one of two objects (external tools). It can be calculated by the equation: 1-((1-0,09)*(1-0,09)) = 0,17 = **17%.**

Table 6.28 demonstrates values of Pa and Pd during the day of theft.

Path	Task description (all on the Day 0)	Effectiveness to detect							
		An individual		A stolen material		An external tool		An internal tool	
		Pd	Pa	Pd	Pa	Pd	Pa	Pd	Pa
From the office building to the radioisotope production building	Enter the radioisotope production building carrying the dummy of the sealed source.	0	0	0	0	0	0	0	0
At the radioisotope production building, in the storage vault	During the procedure of verification and packaging of ten Cs-137 sealed sources substitute one of them with a dummy.	0	0	0.1	0.9	0.1	0.5	0	0
At the radioisotope production building	Hide one sealed source at the radioisotope production facility outside of the storage vault so it can be collected later by the insider unnoticed.	0	0	0.1	0.9	0	0	0	0
From office building to the radioisotope production building	Enter the radioisotope production facility carrying a shielded container that can be used to transport a sealed source.	0	0	0	0	0	0	0	0
At the radioisotope production facility	Collect the sealed source and put it in the shielded container.	0	0	0	0	0	0	0	0
From the radioisotope production facility through the Access Control Building	From the radioisotope production building go through the Access Control Building carrying Cs-137 source in the shielded container in his backpack.	0	0	0.75	0.9	0	0	0	0
Leave the facility	Drive the car through the site entrance gates.	0	0	0	0	0	0	0	0

Table 6.28 Values (Pd and Pa) to estimate effectiveness of PPS on the path using four detection criteria on the day of theft.

Table 6.29 demonstrates PPS effectiveness during the theft of the Cs-137 sealed source.

6.3.5.2 Cumulative effectiveness of PPS on the path.

Task description (all on the Day 0)	A stolen material		An external tool		**Total Effectiveness**	**Comments**
	Pd	Pa	Pd	Pa		
Enter the radioisotope production building carrying the dummy of the sealed source.	0	0	0	0	**0**	There is no detection mechanism at this stage.
During the procedure of verification and packaging of ten Cs-137 sealed sources substitute one of them with a dummy.	0.1	0.9	0.1	0.5	**0.13**	1) There is a low probability that theft of a sealed source is visually detected by another staff. 2) There is a low probability that the use of external tool is visually detected by another staff.
Hide one sealed source at the radioisotope production building but outside of the storage vault so it can be collected by the insider unnoticed.	0	0	0	0	**0**	There is a low probability that an insider is visually detected during hiding the material at the radioisotope production facility. But conservatively the probability is 0 due to no detection mechanism.
Enter the radioisotope production building carrying a shielded container that can be used to transport a sealed source.	0	0	0	0	**0**	There is no detection mechanism at this stage.
Collect the sealed source and put it in the shielded container	0	0	0	0	**0**	There is no detection mechanism at this stage.
From the radioisotope production building go through the Access Control Building carrying Cs-137 source in the shielded container	0.75	0.9	0	0	**0.675**	There is a high probability that the Radiation Detector Gate can detect the Cs-137 source in a portable shielded container (2.5 cm wall thickness) and successfully assessed by the security guards *(see Figure 6.12 for details on calculation of the estimated dose rate).*
Drive the car through the site entrance gates	0	0	0	0	**0**	

Table 6.29 Estimated cumulative (total) effectiveness of PPS on the path.

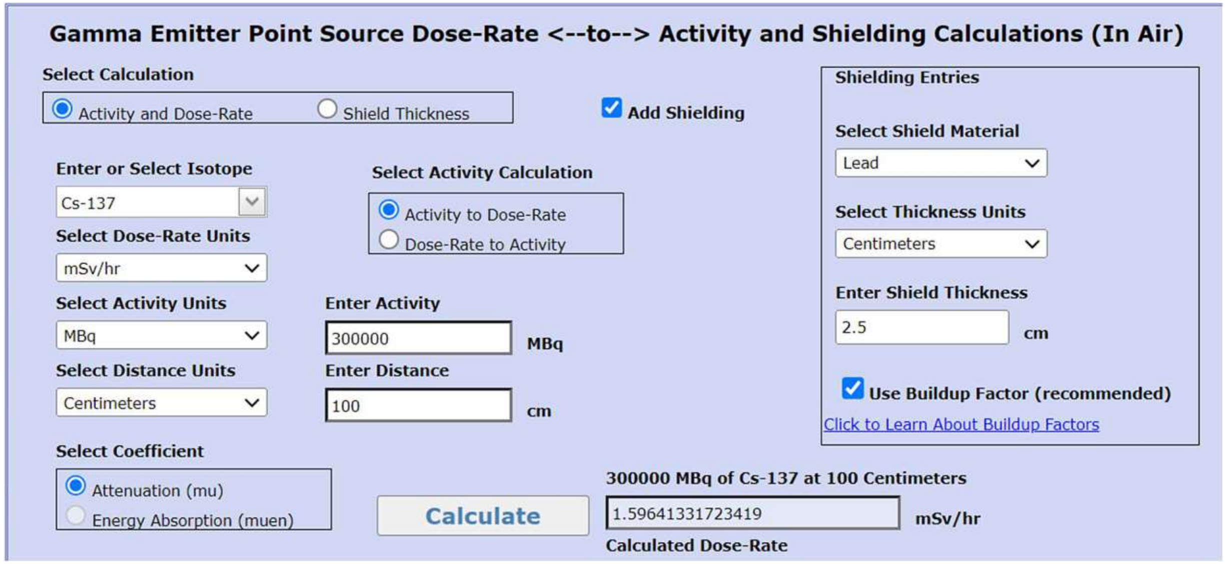
The effectiveness of the PPS for the scenario of Cs-137 theft from the fuel fabrication building by an insider is calculated by equation:

$Peff.r = 1 - \left\{\prod_{j=1}^{J}(1 - Pd * Pa)\right\}$= 1-(1-0,17)*(1-0,13)*(1-0,675)) = 0,76 = **76%**

6.3.5.3 Calculation of a dose-rate registered by the gate detector while carrying a shielded container with Cs-137 source.

To calculate the Dose-Rate, the software 'Rad Pro Calculator' was used [38]. As input Cs-137 with an activity of 0.3 TBq was used, distance was conservatively chosen as 100 cm and lead was added as shielding material with 2.5 cm thickness.

The result of calculation (see Figure 6.12) was around 1.6 mSv/h which in some places can be ten thousand times more than a natural background dose-rate. The probability that a gate detector can alarm guards of a high dose-rate registered at a gate depends on duration of time that the source is present in the detectable zone. This means that if an insider runs through the gate, it might decrease the probability. However, for the current scenario the probability is high since the assumption is that the guards are knowledgeable and do not allow staff to run by the detectors.



Gamma Emitter Point Source Dose-Rate <--to--> Activity and Shielding Calculations (In Air)

Select Calculation
● Activity and Dose-Rate ○ Shield Thickness

☑ Add Shielding

Enter or Select Isotope: Cs-137
Select Dose-Rate Units: mSv/hr
Select Activity Units: MBq
Select Distance Units: Centimeters

Select Activity Calculation
● Activity to Dose-Rate
○ Dose-Rate to Activity

Enter Activity: 300000 MBq
Enter Distance: 100 cm

Shielding Entries
Select Shield Material: Lead
Select Thickness Units: Centimeters
Enter Shield Thickness: 2.5 cm
☑ Use Buildup Factor (recommended)
Click to Learn About Buildup Factors

Select Coefficient
● Attenuation (mu)
○ Energy Absorption (muen)

300000 MBq of Cs-137 at 100 Centimeters
1.59641331723419 mSv/hr
Calculated Dose-Rate

Figure 6.12 Calculation results in the Rad Pro Calculator software.

6.3.6 Conclusion on the PPS effectiveness for a chosen scenario.

Both attractiveness of the asset and effectiveness of an insider detection for the chosen scenario are characterised as High. Attractiveness of the asset is 5% higher than effectiveness of the PPS (see Table 6.30).

Asset	Attractiveness of the asset	Effectiveness of PPS on the analysed path
One Cs-137 sealed source (Cat II)	**81% - High**	**76% - High**

Table 6.30 Estimated attractiveness and PPS effectiveness for the Case Study 3.1 scenario.

The result is demonstrated on the Table 6.31 with the purple dot. The result is identified as **1**- Strong PPS effectiveness. PPS effectiveness is well balanced with the attractiveness of an asset.

Attractiveness	Effectiveness of PPS				
	VH (0.9 – 1)	H (0.7 - 0.9)	M (0.4 - 0.7)	L (0.2 - 0.4)	VL (< 0.2)
Very High (VH) 0.9 – 1	1	2	3	4	5
High (H) 0.7 - 0.9	0	1 ●	2	3	4
Moderate (M) 0.4 - 0.7	0	0	1	2	3
Low (L) 0.2 - 0.4	0	0	0	1	2
Very low (VL) < 0.2	0	0	0	0	1

Table 6.31 Calculated value displayed on the matrix of asset's Attractiveness vs PPS effectiveness and identified gap.

Having obtained such results, decision makers have to discuss several ways forward and can conclude that:

- The balance between asset attractiveness and PPS effectiveness is appropriate, no additional modifications or improvements are required.

OR

- Even if the asset attractiveness and PPS effectiveness are both characterized as "High" there is an inappropriate disbalance, additional modifications or improvements are required.

It is important to consider other malicious scenarios with the same asset to get a more comprehensive picture of the PPS effectiveness. The next case study represents the same threat to the same asset (unauthorized removal of a Cs-137 source by an insider) but using a different scenario.

6.4 Case Study 3.2: Adaptation of the scenario 3.1 to evade the radiation detector gate at the main entrance gate.

6.4.1 Description of the hypothetical scenario.

Target: one sealed Cs-137 source from the product vault at the radioisotope production building.

Threat: One insider from the Operations support Staff who performs paperwork, sources packaging, and deals with transportation the source at the facility's site.

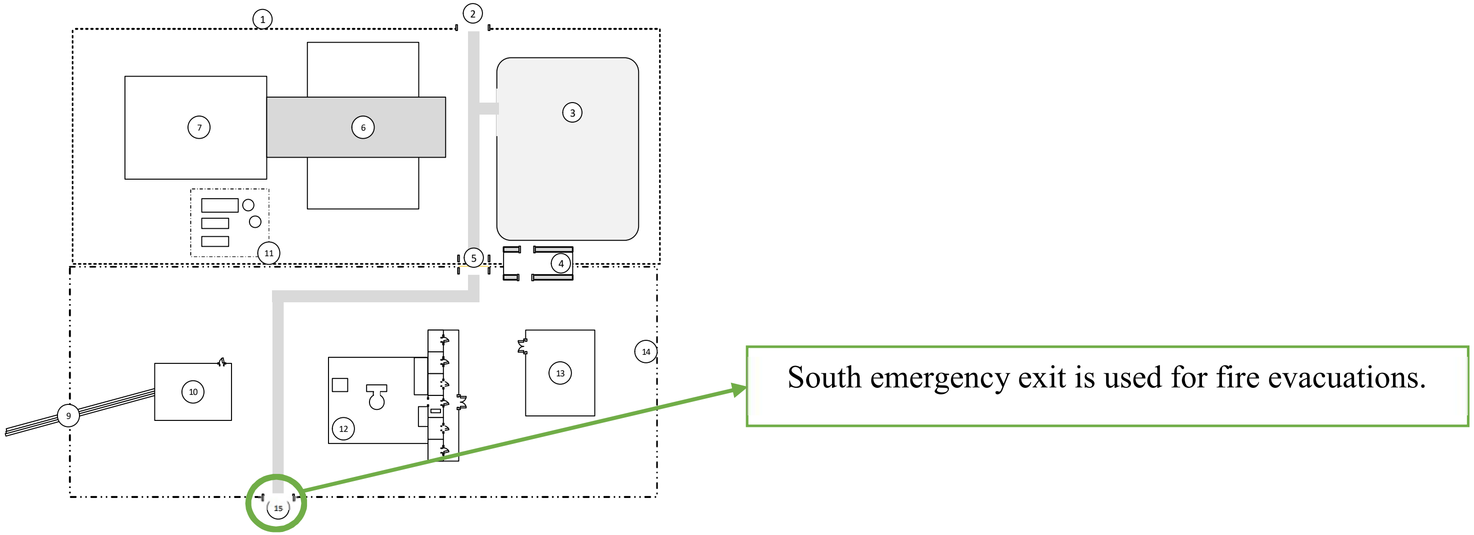
Tools that the insider uses:
A shielded container for transportation.
A dummy source to be used for replacement with a real radioactive source.

Tactics: Evade detection on any path section, not violent and no weapons to be used.

Time of attempt: Attempt is planned during working hours.

Actions of an insider and the path:
The main difference in the current hypothetical scenario to the previous scenario (scenario 3.1) is that instead of trying to smuggle out the Cs-137 source through the Access Control Building which is equipped with a gamma detector the insider causes a fire which initiates staff evacuation via the south emergency exit. The insider knows that the south emergency exit is not equipped with a radiation detector capability and there are no procedures for security staff to hold a portable radiation detector during a fire evacuation.

1. 5 days before the shipping day of the sealed sources bring a dummy of a sealed source and hide in an office.
2. 3 days before shipping day of the sealed sources bring the transport container for a sealed source from outside into facility and hide in an office.
3. 2 days before the shipping day bring 2 litres of inflammable liquid in a plastic bottle and hide it.
4. 1 day before the shipping day bring 2 litres more of inflammable liquid in a plastic bottle and hide it.
5. On the shipping day, during the procedure of verification and packaging of ten Cs-137 sealed sources substitute one of them with a dummy (fake one that looks like real but just a metal – for a final visual inspection by the second staff).
6. Hide 1 sealed source the radioisotope production building but outside of the storage vault (can be accessed by the insider unnoticed).
7. After sending the vehicle off with sealed sources and 1 fake one the insider goes to the office and takes hidden transport container.
8. Using 4 litres of inflammable liquid, starts a fire in the office building.
9. Enter the radioisotope production building carrying a shielded container that can be used to transport a sealed source.
10. Collect the sealed source and put it in the shielded container and a regular backpack.
11. From the radioisotope production building go through the south emergency exit according to the fire evacuation plan with all other staff (see Figure 6.13).



South emergency exit is used for fire evacuations.

Figure 6.13 Layout of the radioisotope Production facility showing the south emergency exit.

6.4.2 Effectiveness to detect an insider using four detection criteria.

In this scenario there is no need to identify a Critical Detection Point (CDP) on the path since the insider is leaving through the Access Control Building (ACB) and the on-site guards' capabilities are sufficient to detain the insider if successfully detected.

6.4.2.1 PPS effectiveness during preparation to the theft of Cs-137 source.

Same as in the scenario 3.1 (see 6.3.5) the probability to detect one of two objects (external tools: dummy source and/or a shielded container) and recognize (assess) that these are objects to be used on site with malicious intent equals **17%** (see Table 6.32).

Path	Task description	Effectiveness to detect								Total Effective ness
		An individual		A stolen material		An external tool		An internal tool		
		Pd	Pa	Pd	Pa	Pd	Pa	Pd	Pa	
From outside enter the protected area with an external tool Nr 1	Day -5. From outside go through entrance gates with a metallic cylinder that looks like a sealed source.	0	0	0	0	0.9	0.1	0	0	0.09
Enter the offices building	Day -5. Hide a metallic cylinder that looks like a sealed source in an office.	0	0	0	0	0	0	0	0	0
From outside enter the protected area with an external tool Nr 2	Day -3. From outside go through entrance gates with a with a shielded container that can be used to transport a sealed source.	0	0	0	0	0.9	0.1	0	0	0.09
Enter the offices building	Day -3. Hide a shielded container that can be used to transport a sealed source in an office.	0	0	0	0	0	0	0	0	0
From outside enter the protected area with an external tool Nr 3	Day -2. Bring 2 litres of inflammable liquid in a plastic bottle	0	0	0	0	0	0	0	0	0
Enter the offices building	Day -2. Hide the 2 L bottle.	0	0	0	0	0	0	0	0	0
From outside enter the protected area with an external tool Nr 3	Day -1. Bring 2 litres of inflammable liquid in a plastic bottle	0	0	0	0	0	0	0	0	0
Enter the offices building	Day -1. Hide the 2 L bottle.	0	0	0	0	0	0	0	0	0

Table 6.32 Estimated values characterising effectiveness of PPS during preparation activities to the theft of Cs-137 source using four detection criteria.

6.4.2.2 PPS effectiveness during the theft of the Cs-137 sealed source.

Table 6.33 demonstrates values for Pd and Pa during the theft of Cs-137 source. Table 6.34 provides comments on the chosen Pd and Pa.

Path	**Task description (all on the Day 0)**	**Effectiveness to detect**							
		An individual		A stolen material		An external tool		An internal tool	
		Pd	Pa	Pd	Pa	Pd	Pa	Pd	Pa
From Office building to the radioisotope production building	Enter the radioisotope production building carrying the dummy of the sealed source.	0	0	0	0	0	0	0	0
At the radioisotope production building	During the procedure of verification and packaging of ten Cs-137 sealed sources substitute one of them with a dummy.	0	0	0.1	0.9	0.1	0.5	0	0
At the radioisotope production building	Hide one sealed source at the radioisotope production facility but outside of the storage vault so it can be collected by the insider unnoticed.	0	0	0	0	0	0	0	0
From Office building to the radioisotope production building	Using 4 litres of inflammable liquid start the fire in the offices building.	0	0	0	0	0	0	0	0
At the radioisotope production facility	Enter the radioisotope production building carrying a shielded container that can be used to transport a sealed source.	0	0	0	0	0	0	0	0
From the radioisotope production facility through the Access Control Building	Collect the sealed source and put it in the shielded container	0	0	0	0	0	0	0	0
Leave the facility	From the radioisotope production building go through the south emergency exit according to the fire evacuation plan	0	0	0	0	0	0	0	0

Table 6.33 Estimated values characterising effectiveness of PPS during the theft of Cs-137 source using four detection criteria.

Task description (all on the Day 0)					Comments
	A stolen material		An external tool		
	Pd	Pa	Pd	Pa	
Enter the radioisotope production building carrying the dummy of the sealed source.	0	0	0	0	There is no detection mechanism at this stage.
During the procedure of verification and packaging of ten Cs-137 sealed sources substitute one of them with a dummy.	0.1	0.9	0.1	0.5	1) There is a low probability that theft of a sealed source is visually detected by another staff. 2) There is a low probability that the use of external tool is visually detected by another staff.
Hide one sealed source at the radioisotope production facility but outside of the storage vault so it can be collected by the insider unnoticed.	0	0	0	0	There is a low probability that an insider is visually detected during hiding the material at the radioisotope production building. The probability is 0 due to no detection mechanism.
Enter the radioisotope production building carrying a shielded container that can be used to transport a sealed source.	0	0	0	0	There is no detection mechanism at this stage.
Using 4 litres of inflammable liquid start the fire in the offices building	0	0	0	0	The fire is detected by smoke detectors but there is no detection mechanism of an actual individual causing deliberate fire.
Collect the sealed source and put it in the shielded container	0	0	0	0	There is no detection mechanism at this stage.
From the radioisotope production building go through the south emergency exit according to the fire evacuation plan	0	0	0	0	There is no radiation detector gate. There is no procedure for a security guard to monitor staff with a portable dose rate detector during a fire alarm evacuation.

Table 6.34 Estimated values characterising effectiveness of PPS during the preparation activities and during an actual theft of Cs-137 source using four detection criteria.

6.4.3 Conclusion on the PPS effectiveness for a chosen scenario.

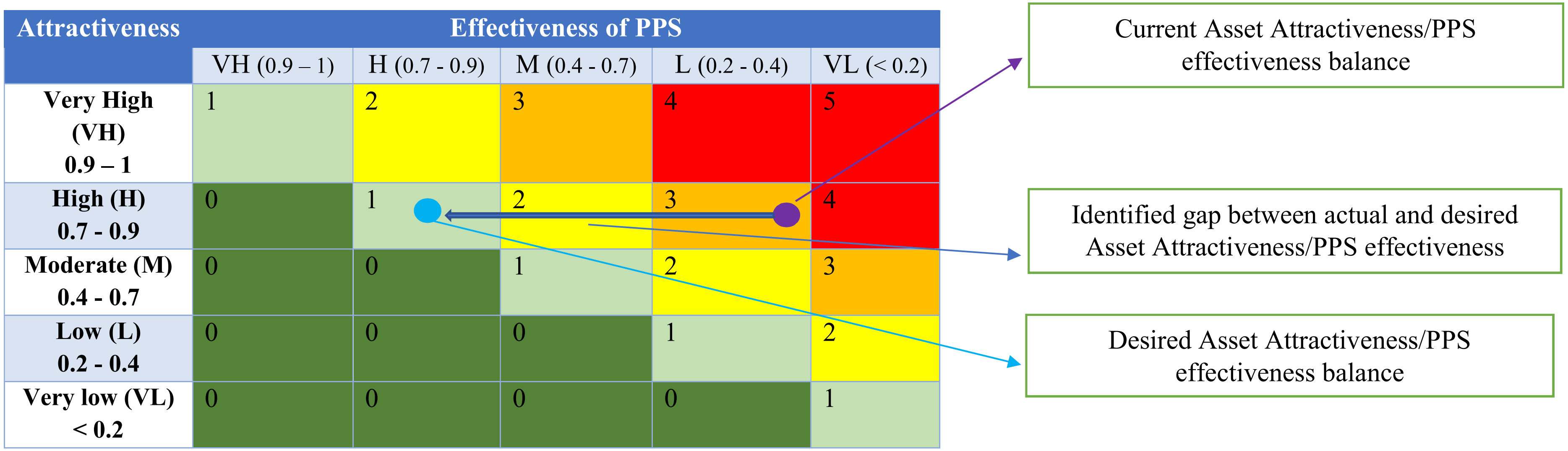
The effectiveness of the PPS for the scenario of Cs-137 theft from the fuel fabrication facility by an insider is calculated by equation: $Peff.r = 1 - \left\{\prod_{j=1}^{J}(1 - Pd * Pa)\right\}$= 1-(1-0,17)*(1-0,1*0,9)*(1-0,1*0,5)) = 0,28 = **28%**

PPS effectiveness is identified as *Low* and attractiveness of the asset is *High.* This shows that effectiveness of PPS to detect an insider in this particular scenario does not correspond to the high level of the asset attractiveness (see Table 6.35).

Asset	Attractiveness of the asset	Effectiveness of PPS on the analysed path
One Cs-137 sealed source (Cat II)	**81% - High**	**28% - Low**

Table 6.35 Estimated attractiveness and PPS effectiveness for the Case Study 3.2 scenario.

The result presented in the Table 6.36 shows poor PPS effectiveness for a particular attractiveness of an asset. Actions are required to increase PPS effectiveness or reduce asset attractiveness. High risk – an insider's attempt to use the demonstrated scenario can lead to a high chance of a successful malicious act occurrence.



Attractiveness	**Effectiveness of PPS**				
	VH (0.9 – 1)	H (0.7 - 0.9)	M (0.4 - 0.7)	L (0.2 - 0.4)	VL (< 0.2)
Very High (VH) 0.9 – 1	1	2	3	4	5
High (H) 0.7 - 0.9	0	1 ●	2	3 ●	4
Moderate (M) 0.4 - 0.7	0	0	1	2	3
Low (L) 0.2 - 0.4	0	0	0	1	2
Very low (VL) < 0.2	0	0	0	0	1

Current Asset Attractiveness/PPS effectiveness balance

Identified gap between actual and desired Asset Attractiveness/PPS effectiveness

Desired Asset Attractiveness/PPS effectiveness balance

Table 6.36 Calculated value displayed on the matrix of asset's Attractiveness vs PPS effectiveness and identified gap.

Identified gap can be addressed by improving PPS effectiveness[2].

Potential options that can be considered to improve the PPS for the chosen scenario:

- Improve procedure during evacuation at the south evacuation gate.
  - ▶ Install a fixed radiation detector at the south emergency exit.
  - ▶ Equip security officer(s) with a portable detector and train on its use.

[2] The description of gap analysis process is not in the scope of this research.

7 CONCLUSIONS

7.1 Summary and contribution to establishing balanced physical security arrangements at a research reactor.

This thesis described and demonstrated the development and application of the RR-NSM graded approach providing case studies as examples of the practical application to the Nuclear Security Management at research reactor facilities. The RR-NSM graded approach offers several contributions to establishing balanced physical security arrangements at a research reactor facility:

7.1.1 Assists in Evaluating balance of PPS effectiveness and Asset Attractiveness:

- The RR-NSM graded approach helps in developing a comprehensive nuclear security strategy by evaluating the balance of Physical Protection System (PPS) arrangements and the attractiveness of assets during both the planning and operational stages, as well as for decommissioned facilities. It also would help to reassess needed PPS effectiveness after decrease of assets' attractiveness.

7.1.2 Facilitates Justification of Security Expenditures:

- By identifying necessary security arrangements, the RR-NSM approach aids in justifying nuclear security expenditures that are needed at a research reactor.

7.1.3 Assessing Asset Attractiveness:

- The approach assesses asset attractiveness by analysing the combination of consequences of potential malicious acts and the properties of assets.

7.1.4 Assessment of PPS Effectiveness:

- Describes methods to perform assessment of PPS effectiveness for any potential malicious act scenario.

- The approach can be used in the assessment of PPS effectiveness against an insider. The equation is comprised of four components that cover detection and assessment on different activities that insider can perform with a malicious intention.

- The approach can be used for scenarios involving an outsider or insider in collusion with an outsider.

7.1.5 Risk Assessment for a research reactor assets:

- The RR-NSM approach enables risk assessment by considering asset attractiveness and hypothetical threats describing adversary's capabilities and motivation, ultimately providing a comprehensive understanding of PPS effectiveness.

7.1.6 Identification of Weaknesses and Critical PPS Elements:

Once the RR-NSM graded approach is applied, one obtains a full picture of PPS effectiveness for a particular malicious scenario, this allows to:

- Identify weaknesses or vulnerabilities in a research reactor facility's PPS arrangement, in turn, assists to identify elements for targeted improvements. The improvements can be made to equipment, people or procedures at a research reactor facility.
- Identify a crucial element of PPS that provides the most protection on a path. This can indicate that this crucial element of PPS has to be properly maintained and tested. It can also suggest introducing redundancy in PPS arrangement to evade one point failure at a path in case an insider or outsider breaches the crucial element of PPS.

7.2 Challenges and limitations for the RR-NSM graded approach.

The application of the RR-NSM graded approach to Nuclear Security Management at Research Reactor facilities provides a robust framework for assessing Physical Protection Systems (PPS). However, several challenges and limitations must be considered to understand the constraints of this methodology.

7.2.1 Complexity and Resource Requirements

Implementing the RR-NSM graded approach is a resource-intensive process. It demands considerable time, specialized knowledge, and collaboration among multidisciplinary teams, including security specialists, technical experts, and software analysts. The complexity of the approach, while ensuring thorough analysis, may make it impractical for facilities with limited resources or personnel.

7.2.2 High Number of Scenarios to Analyse

The RR-NSM graded approach requires the analysis of multiple malicious scenarios, considering various threats (outsiders, insiders, and their collusion), different assets, and multiple adversaries' paths. This extensive approach is essential for a comprehensive evaluation but can become overwhelming, potentially leading to analysis paralysis, where the total volume of data makes decision-making difficult.

7.2.3 Specialization and Software Needs

Accurate assessment of PPS effectiveness often requires the involvement of technical specialists in installing, maintaining and testing physical protection equipment, analytical software, modelling techniques and physical and cyber security specialists. These requirements can be barriers to adoption, particularly in facilities lacking access to such resources or the ability to train personnel in their use.

7.2.4 Confidentiality Concerns

The RR-NSM graded approach involves handling sensitive and confidential information, which may restrict the number of staff who can participate in the analysis. This limitation can create bottlenecks in the assessment process, particularly if key personnel are unavailable or overburdened.

7.3 Critical Evaluation.

This chapter provides a critical evaluation of the RR-NSM graded approach, assessing its strengths, weaknesses, and the implications of its use in Nuclear Security Management at research reactor facilities. By examining the approach in detail, this section aims to highlight areas for improvement and offer insights into how the methodology can be refined.

7.3.1 Evaluation of Complexity and Resource Requirements

Strengths:

The comprehensive nature of the RR-NSM graded approach is one of its key strengths, as it allows for a detailed assessment of PPS across various stages of a research reactor's lifecycle. A broad range of expertise can enhance the reliability and depth of the analysis, ultimately leading to the establishment of a robust and effective PPS that is appropriately tailored to the facility's assets attractiveness, avoiding over- or under-setup.

Weaknesses:

However, this complexity can be a double-edged sword. The significant time and resources required to implement the approach may make it inaccessible to smaller or less well-funded facilities. Additionally, the need for specialized knowledge can limit its use, reducing its broader applicability.

Implications:

These limitations suggest that while the RR-NSM graded approach is highly effective in well-resourced environments, its complexity may deter its adoption in smaller facilities. Future work should explore ways to simplify the methodology without sacrificing its analytical power.

7.3.2 Evaluation of Scenario Analysis

Strengths:

The RR-NSM graded approach's thorough scenario analysis ensures that all potential threats are considered, providing a robust framework for identifying vulnerabilities. This exhaustive consideration is crucial for ensuring that no possible attack vector is overlooked.

Weaknesses:

The drawback of this thoroughness is the high number of scenarios that must be analysed, which can be overwhelming and resource intensive. This may lead to difficulties in prioritizing which scenarios to address first and how many actual scenarios need to be considered.

Implications:

Given the vast number of possible scenarios, facilities must make strategic decisions about which scenarios to prioritize. Threat environment, resources need to be carefully assessed to determine how many scenarios should be analysed and which ones warrant the most attention. This prioritization is vital for effectively allocating resources and ensuring that the most significant risks are addressed and at the same time meeting all needed regulations.

7.3.3 Evaluation of Specialisation and Software Needs

Strengths:

The use of advanced analytical software and the involvement of technical specialists enhance the precision and reliability of the RR-NSM graded approach. These tools and expertise would allow sophisticated modelling of PPS effectiveness, which is crucial for accurate assessments.

Weaknesses:

The reliance on specialized personnel and software is a significant limitation, particularly for facilities that may not have access to such resources. This dependence can also increase the cost and time required to conduct assessments, further limiting the approach's applicability.

Implications:

The implementation of the RR-NSM graded approach faces significant challenges related to the complexity and resource demands of the methodology. The integration of user-friendly software tools is crucial for addressing these challenges. While existing tools can assist in analysing potential adversaries' paths, the approach could benefit from the development of additional tools designed to simplify and streamline the process. Combining these existing and new tools can enhance the efficiency and accessibility of the approach.

7.3.4 Evaluation of Confidentiality Concerns

Strengths:

The emphasis on confidentiality within the RR-NSM graded approach underscores the importance of protecting sensitive and critical information related to physical security from unauthorized access. While the specifics of data security management are beyond the scope of this research, it is strongly recognized that robust data security measures must be in place to ensure the effectiveness and reliability of the RR-NSM graded approach.

Weaknesses:

However, the need to handle sensitive information with high confidentiality creates weaknesses. The restriction on data access limits the number of staff who can participate in the analysis, leading to potential bottlenecks in the assessment process. This limitation can be aggravated if key personnel are unavailable or overburdened, causing delays and affecting the overall efficiency of the analysis. Additionally, the strict confidentiality protocols can deter collaboration and information sharing, reducing the ability to leverage a diverse range of expertise and potentially compromising the depth of the analysis.

Implications:

The implications of these confidentiality concerns are notable. The restricted access to sensitive data can slow down the assessment process and place stress on a limited number of qualified personnel. To address these issues, it is crucial to apply secure and flexible data access protocols that facilitate efficient collaboration without compromising confidentiality.

Implementing such solutions could ensure that the application of the RR-NSM graded approach remains both secure and practical for widespread application.

7.4 Future Work

Building on the critical evaluation provided above, several ways for future research and development can be identified to improve the RR-NSM graded approach and its application in Nuclear Security Management.

7.4.1 Development of Advanced Analytical Tools

To further address the challenges identified, future work should focus on both developing and integrating user-friendly software tools and training programs. The tools will allow research reactor facilities to be better equipped to implement the RR-NSM graded approach effectively. This will not only improve the practical application of the methodology but also make it accessible to a broader range of facilities. Additionally, enhancing training programs will help build a larger pool of personnel capable of applying the approach, ultimately supporting more effective and widespread use of the RR-NSM graded approach.

7.4.2 Exploration of Dynamic Threat Scenarios

Additional research should explore the application of the RR-NSM approach to dynamic and evolving threat scenarios, particularly those involving cyber threats. As these threats become more prevalent, adapting the methodology to address them will be crucial for maintaining its relevance and effectiveness.

7.4.3 Standardization and Best Practices

Developing standardized procedures and best practices for implementing the RR-NSM approach across different facilities would help ensure consistency and reliability in its application. This standardization could also facilitate the sharing of knowledge and resources between facilities, further enhancing the approach’s utility. For example, this might involve creating a repository of procedures that can be tailored to various reactor types.

7.4.4 Broadening the Scope of Application

Potentially, the RR-NSM approach could be extended to other types of critical infrastructure beyond research reactors. Investigating its applicability to broader contexts could significantly enhance its utility and impact, potentially leading to improved security measures across various sectors.

8 BIBLIOGRAPHY

[1] 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, Vienna: IAEA, 2001.

[2] International Atomic Energy Agency, "Research Reactor Database (RRDB)," IAEA, [Online]. Available: https://nucleus.iaea.org/RRDB/RR/ReactorSearch.aspx. [Accessed: 23 09 2024].

[3] Nuclear Security Management for Research Reactors and Related Facilities, IAEA-TDL-004, Vienna: IAEA, 2016.

[4] International Atomic Energy Agency, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No.10-G, Vienna: IAEA, 2021.

[5] International Atomic Energy Agency, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No.14, Vienna: IAEA, 2011.

[6] Ebbinghaus, B. B., Bathke, C. G., Dalton, D. S., and Murphy, J. P., "The Application of Material Attractiveness in a Graded Approach to Nuclear Materials Security", LLNL-CONF-640708, Paper presented at Global'13: International Nuclear Fuel Cycle Conference, Salt Lake City UT, 2013.

[7] United States Nuclear Regulatory Commission, Rulemaking for Enhanced Security of Special Nuclear Material, US NRC Regulatory Basis Document, RIN number: 3150-AJ41
NRC Docket ID: NRC-2014-0118, 2015.

[8] International Atomic Energy Agency, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 24-G, Vienna: IAEA, 2015.

[9] International Atomic Energy Agency, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, Vienna: IAEA, 2009.

[10] Harris, J. T., Rane, S., “Quantification of a Facility Radiological Security Risk Index With a Graphical User Interface Tool” Health Physics, 122(5):632–644, 2022.

[11] Kot, J. L., Harris, J. T., “Risk Assessment for Nuclear Terrorism Probability and Its Application on a Hypothetical Nuclear Facility,” Health Physics, DOI: 10.1097/HP.0000000000001842, 2024.

[12] International Atomic Energy Agency, Nuclear Security Assessment Methodologies for Regulated Facilities, TECDOC-1868, Vienna: IAEA, 2019.

[13] International Atomic Energy Agency, Research Reactors for the Development of Materials and Fuels for Innovative Nuclear Energy Systems, IAEA Nuclear Energy Series No. NP-T-5.8, Vienna: IAEA, 2017.

[14] International Atomic Energy Agency, Applications of Research Reactors, IAEA Nuclear Energy Series, No. NP-T-5.3, Vienna: IAEA, 1999.

[15] International Atomic Energy Agency, Applications of Research Reactors, IAEA Nuclear Energy Series, No. NP-T-5.3, Vienna: IAEA, 2014.

[16] International Atomic Energy Agency, Research Reactors: Purpose and Future, Vienna: IAEA, [Online]. Available: https://www.iaea.org/sites/default/files/18/05/research-reactors-purpose-and-future.pdf. 2016. [Accessed: 23 09 2024]

[17] Civiak, R. L., Closing the Gaps: Securing High Enriched Uranium in the Former Soviet Union and Eastern Europe, Report for the Federation of American Scientists, Washington DC: Federation of American Scientists, [Online].
Available: https://carnegieendowment.org/files/Closing_the_Gaps.pdf. 2002. [Accessed: 23.09.2024]

[18] Pan, P., Boyer, B. and Murphy, C., Safeguards by Design (SBD): Safeguards Guidance for Research Reactors and Critical Assemblies, LA-UR-12-26349, Next Generation Safeguards Initiative, Safeguards-By-Design Facility Guidance Series NGSI-SBD-003, Washington, D.C.: United States Department of Energy, National Nuclear Security Administration, [Online].
Available: https://www.energy.gov/sites/default/files/2017/10/f37/2013-10-22%25203%5B1%5D.pdf. 2012. [Accessed: 23 09 2024]

[19] Technical University of Munich (TUMuenchen), Manufacturing Molybdenum-99 for medicine at TUM's Research Neutron Source, The Research Neutron Source Heinz Maier-Leibnitz of the Technical University of Munich, [Online]. Available: https://www.youtube.com/watch?v=rcTBlq-53wI. [Accessed: 23 09 2024]

[20] Ratiko, R., Wisnubroto, D.S., Nasruddin, N., Mahlia, T.M.I. "Current and future strategies for spent nuclear fuel management in Indonesia," Energy Strategy Reviews, 100575, Volume 32, ISSN 2211-467X, no. 100575, 2020.

[21] Bunn, G., Braun, C., and Steinhausler, F., "Nuclear terrorism potential: Research reactors vs power reactors?," OMZ: Osterreichische Militarische Zeitschrift (Austrian Military Periodical), pp. 9-14, Stanford: Center for International Security and Cooperation, [Online]. https://cisac.fsi.stanford.edu/publications/nuclear_terrorism_potential__research_reactors_vs_power_reactors. 2003. [Accessed: 01 09 2023]

[22] Oettingen, M., Centar, J., "Comparative analysis between measured and calculated concentrations of major actinides using destructive assay data from Ohi-2 PWR," Nukleonika, vol. 60, no. 10.1515/nuka-2015-0102, 2015.

[23] Ramadhan, A. I., Suwono1, A., Umar E., and Tandian, N. P., "Preliminary Study for Design Core of Nuclear Research Reactor of TRIGA Bandung Using Fuel Element Plate MTR," Engineering Journal, Volume 21, DOI:10.4186/ej.2017.21.3.173, no. 3, 2017.

[24] Garcia, M. L., The Design and Evaluation of Physical Protection Systems, 2nd Edition, Burlington MA: Butterworth-Heinemann, 2007.

[25] Menon, S., Vagish, K., “Weaponizing Radioactive Medical Waste - The Looming Threat,” International Journal of Nuclear Security, Vol. 5: No. 1, Article 4., https://doi.org/10.7290/ijns050104, https://trace.tennessee.edu/ijns/vol5/iss1/4, 2019.

[26] US Department of Health and Human Services, Centres for Disease Control and Prevention, “Radiological Exposure Device,” [Online]. Available: https://www.cdc.gov/nceh/radiation/emergencies/pdf/Infographic_Radiological_Exposure_Device.pdf. [Accessed 26 05 2022].

[27] US Department of Health and Human Services, Centres for Disease Control and Prevention, “Dirty Bomb or Radiological Dispersal Device,” [Online]. Available: https://www.cdc.gov/nceh/radiation/emergencies/pdf/Infographic_Radiological_Dispersal_Device.pdf. [Accessed 26 05 2022].

[28] Adams Jr., A., “The Application of a Graded Approach in the Regulation of Research Reactors and Test Reactors at the U.S. Nuclear Regulatory Commission”, Paper presented at the International Conference on Research Reactors: Safe Management and Effective Utilization, IAEA Research Reactors Conference, Vienna: IAEA, [Online]. Available: https://conferences.iaea.org/event/75/contributions/10756/attachments/5230/6383/IAEA_Graded_Approach_paper_A_Adams.pdf. 2015. [Accessed 23 09 2024].

[29] International Atomic Energy Agency, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9 General Safety Guides Safety Guides, Vienna: IAEA, 2005.

[30] IAEA, IAEA Safeguards Glossary, Vienna: IAEA, 2022.

[31] Iftikhar, A., and M., Sadiq, “The Perils of Non-State Actors in Pakistan: Assessing the Risks of Nuclear Safety and Security,” International Journal of Nuclear Security, Vols. Vol. 8: No. 1, Article 5., 2023.

[32] International Atomic Energy Agency, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, Vienna: IAEA, 2008.

[33] Bertsekas, D.P., Tsitsiklis, J.N., Introduction to Probability, Massachusetts Institute of Technology, Cambridge: M.I.T, 2000.

[34] International Atomic Energy Agency, Hypothetical Facility Data Book The Shapash Nuclear Research Institute (SNRI), Vienna: IAEA, 2015.

[35] Garcia, M. L., Vulnerability Assessment of Physical Protection Systems, 1st Edition, Burlington MA: Butterworth-Heinemann, 2005.

[36] QSA Global Inc., Cesium-137 (Cs-137) Industrial Gamma Sources, [Online]. Available: https://www.qsa-global.com/industrial-cs-137-gamma-sources. [Accessed: 04. 08 .2022].

[37] Radiation Products Design, Inc., Lead Carrying Case 1 Inch Pb, Cavity 1.5 Inch Dia. X 4 Inch Deep, [Online]. Available: https://www.rpdinc.com/lead-carrying-case-1-inch-pb-cavity-15-inch-dia-x-4-inch-deep-8778.html. [Accessed: 23 09 2024].

[38] Rad Pro Calculator, [Online]. Available: http://www.radprocalculator.com/.
[Accessed 23 09 2024].

[39] International Atomic Energy Agency, Nuclear Security Series Glossary, Version 1.3, Vienna: IAEA, 2015.

9 PUBLICATIONS AND ACADEMIC ACTIVITY

Publications (related to the present thesis work):

Kovtunov V., Böck H., Sterba J. H., *A graded approach for nuclear security arrangement at a research reactor,* Proceedings of Research Reactor Fuel Management Conference (RRFM), 2021, Helsinki, Finland; 24-29 September; © 2016 European Nuclear Society, Brussels, Belgium; ISBN: 978-92-95064-36-2

Conferences (during the present thesis work):

- Oral presentation at Research Reactor Fuel Management Conference (RRFM), 2021, Helsinki, Finland, 24-29 September.

- Poster presentation at International Conference on Research Reactors: Safe Management and Effective Utilization, IAEA Headquarters, Vienna, Austria, 16–20 November 2015.

- Poster presentation at International Conference on Physical Protection of Nuclear Material and Nuclear Facilities IAEA Headquarters, Vienna, Austria, 13–17 November 2017.

10 ACKNOWLEDGEMENTS

I would like to express my gratitude to Prof. Helmuth Böck, whose expertise and continuous encouragement have been instrumental in my academic pursuits. His guidance, support, and valuable suggestions have significantly contributed to my gradual achievements during this work. I am honoured to have had the opportunity to learn from him during my Ph.D. journey.

I extend my deepest gratitude to Dr. Johannes Sterba, whose invaluable guidance and support have been very helpful in shaping my Ph.D. journey. I appreciative the time and effort he invested in guiding me, offering invaluable feedback which enhanced the quality of my work. I am truly fortunate to have had the privilege of doing this work under his supervision.

Special thanks to my wife, Jessica, who was a constant source of support and encouragement during this work.