The 15th International Congress of the International Radiation Protection Association
Development of a Radiological Safety and Security Risk Index: Pathway Analysis Example

Jason Harris[1]*, Emily Bragers[1]

[1]*School of Health Sciences, Purdue University, 550 Stadium Mall Drive, West Lafayette, Indiana 47907, USA*
*Corresponding author's e-mail: jtharris@purdue.edu

Abstract. Given the threat of radiological terrorism, it is imperative to assess if facilities, such as universities and medical centers, have the means to fully understand and evaluate the combined safety and security of their radioactive sources. This study aims to develop and demonstrate a methodology to compute a risk index for radiological facilities, based on the probability of occurrence of a Threat Event (TE) and its subsequent magnitude of incurred loss. This risk index provides a quantitative value for comparing risk and making decisions towards radiological safety and security improvements. The index employs inputs that include a set of threats, vulnerabilities, and consequences. These were used to construct a single composite number by weighing the threat scenario probabilities, relative attractiveness and characteristics of the radioactive material, multiple parameters elevating vulnerability of source security, and the consequence net loss. Probability density functions and event trees were then used to simulate scenarios to estimate the probability of successfully completing a malicious act. To demonstrate one aspect of this index, a higher education institution that uses a number of radioactive materials for research and teaching, was analyzed. Specifically, three facilities housing nuclear or radioactive sources at the university were compared: a research reactor facility, Co-60 irradiator, and radiopharmaceutical laboratory. Two proposed safety (equipment malfunction and human error accidents) and security (malicious attack of theft and sabotage) scenarios were simulated for each facility. The radiopharmaceutical laboratory sources yielded the highest probability of both successful sabotage and theft outcomes as well as probability of accident. The reactor facility yielded the highest consequences in the sabotage scenario. The contribution of the research is significant as it allows for a new tool in the field of coupled radiological source safety and security-one that is expected to introduce, analyze and numerically test a methodology that yields a facility level risk index.

KEYWORDS: radiological terrorism, radiological security, risk analysis, pathway analysis

1 INTRODUCTION

Following the events of September 11, terrorism and small independent non-state actors have become recognized as a greater threat. The shift of focus to non-state actors has resulted in the need to reassess potential targets and security incidents. Smaller, minimally defended targets have become more appealing to adversaries. Additionally, the potential of safety incidents to evolve into security scenarios, or for safety incidents to compound a security events to be compounded by causing additional safety incidents, creates the need to reevaluate how facilities are examined.

The IAEA depicts the topics of safety, security, and safeguards as overlapping concepts. While safeguards are largely the long-term responsibility of the state, safety and security are more near-term issues that are the responsibility of both facilities, local and national governments [1]. Focusing on the short-term facility obligations, safety and security are the focus when analyzing procedural and structural specifications of nuclear and radiological facilities.

Therein lies the need to integrate safety and security. Lower risk assets have significantly less security than nuclear facilities, which makes them more-vulnerable targets. The relative ease of acquiring radiological material and constructing a radiological dispersal device (RDD) using conventional explosives, increases the desirability of low-level facilities that previously were considered less of a target. Due to the ease of accessibility because of fewer boundary layers, the ease avoiding detection, the location of many of these facilities being in populated areas, and the portability of small sources, research reactor facilities are more attractive targets [2].

Established methods of estimating risk, including using probabilistic risk assessment to estimate safety risk proposed by the WASH-1400 report in 1975, and pathway analysis was used to generate the probability of effectiveness for an adversary attack, both using the probability of an event happening and the consequences of the event [3,4,5].

2 METHODOLOGY

The assets evaluated in this study were the PUR-1 research reactor, a cobalt irradiator, and the nuclear medicine laboratory at Purdue University [6]. Purdue University is a public university in West Lafayette, Indiana, USA. Each of these assets contained different radioactive materials, different locations and security, and different personnel. Due to the different nature of materials stored at each asset, the consequences of an incident at each of the assets would be different and of a different magnitude. For each asset groups, scenarios, pathways, response force times (where applicable) were determined. For each asset, four scenarios were analyzed. The two safety incidents analyzed were an equipment malfunction and a human error accident. The two security scenarios involved a malicious act of theft and a malicious act of sabotage. Pathway scenarios and their applications to security risk analysis are presented by Rane and Harris [7].

Personnel from each asset were interviewed and spaces were toured. When confidentiality prevented the disclosure of information, estimates were made and noted accordingly. Groups were developed for each access based on access to the asset. Security elements and delay components were identified for each asset and scenario. Pathway analysis was performed for each asset and scenario using Garcia's EASI computer model with times from experimentation [4].

The Purdue University Police Department (PUPD) is responsible to respond to emergencies on campus. The West Lafayette Police Department can be contacted if additional forces are required. The Purdue Dispatch Center alerts the PUPD, and once the situation is investigated, a response is determined. In the event of a Level 1 emergency, defined as "a major disaster or imminent threat involving the entire campus and/or surrounding community", university is able to send alerts through the emergency warning notification system [8]. Based on the normal presence of 4 officers on duty during a day shift (not including leadership and administrative staff, for calculations the response force has 4 members and are equipped with automatic rifles) [9]. The Response Force time was estimated to be about 300 seconds, or 5 minutes, which is the approximate travel time from PUPD to the reactor building, allowing for time to verify the alarm and assemble personnel. Mean times of 30% standard deviation were used for actions/tasks ($T_{R)}$ when there was none available. In the event of a loss of radiological material or a radiological release, the office of Radiological and Environmental Management (REM) is part of the response team.

The Probability of Effectiveness (P_E) is determined by multiplying the Probability of Interruption (P_I) by the Probability of Neutralization (P_N):

$$P_E = P_I \cdot P_N \tag{1}$$

For neutralization, estimates were used to evaluate what force level would be necessary for the adversary to be neutralized versus success. For most scenarios, the adversary is a small force of 1 to 2 individuals armed with pistols, with the goal to remain undetected for as long as possible. The Response Force for a security incident on campus is the PUPD.

Consequences were described for scenarios, taking into consideration the activity/quantity of radioactive material that could theoretically be released to the public if it were successfully dispersed These are the worst-case scenarios and therefore the most conservative value for evaluating potential risk.

3 RESULTS

3.1 Research Reactor

The PUR-1 research reactor is a 10kW pool-type research reactor used for academic research and training. Items of interest (potential hazards/targets) include fuel (both in use, used, and surplus stored fuel assemblies), the reactor, and the subcritical pile.

3.1.1 Groups

Groups were identified for the reactor based on their level of security access. G1: All other individuals not included/covered in Group 2 or 3. Individuals must be granted access through each security feature and be supervised. G2s: Main Corridor Access (Proximity/ Limited Access): These individuals have access to the main corridor. Access can be given to anyone with a "need" and who can get a Trustworthy and Responsible (T&R) filed. These individuals may also be around an asset with supervision. This includes: Students with Access card, Maintenance, Cleaning, Subcontractors, Access Card: Limited to 24 students. Must have T&R on file. G2u: Un-Escorted Access: In addition to the same access as G2s, these individuals may also be granted permission to be around an asset while unsupervised, including operating the reactor. They cannot access the asset alone and must be given access by someone with Authorized Access. This group could be incorporated into G2s to form one group G2, but due to the semi-autonomous nature, this sub-group would have an improved advantage. Include: PUPD, REM (RSO, HP), Students training as reactor operator. G3: Authorized Access: These individuals have access to all assets. They require no supervision. Includes: Laboratory Director, Reactor Supervisor/Assistant Lab Director and, Electronics Technician

3.1.2 Scenario

3.1.2.1 Equipment Malfunction

If radiation detectors are not correctly detecting radiation levels, workers could potentially be working in radiation areas without knowing so, and without taking proper precautions to limit exposure (time, distance, shielding). Other possibilities include a fuel assembly dropped in a critical reactor from the start-up position, causing partial melting of a fuel assembly the control rod detector malfunctions and rods are withdrawn to the maximum position.[10]

3.1.2.2 Human Error

A reactor operator cannot alter the reactor programming to perform anything dangerous because PLC would prevent the request from being completed. However, several operations involve human action. When installing new fuel assemblies to the reactor, the used fuel assemblies are moved to wet storage within the pool. This requires personnel to stand above the pool and use a long pole to pick up, move, and place the fuel assembly into its new position. This procedure is open to human error. The operator could fall into the pool during the movement of the fuel assembly into the storage position. The operator could also place the fuel assemblies into the wrong position, causing a prompt criticality.

3.1.2.3 Theft

Any surplus fuel in the facility would be enriched to ~19.75%, so it would not be as desirable for an RDD. Additionally, the storage location can change without notice, making it more difficult for an adversary to plan an operation. The fuel in the operating reactor could be hot from operation (depending on when the last shutdown occurred). Theft of material in the subcritical pile is possible. Used fuel is the most-desirable asset due to it containing Pu-239 and fission products that could be used for an RDD. The security elements for this asset are given in Table 1 [4]. Additional tools would be necessary to complete this task.

Table 1: Reactor Security Elements

Element/Area	Delay Component	Detection Component
Stairwell	Door Lock, Time Required to Walk	Door Sensor (Alarm), Security Cameras
Main corridor to Reactor Room	Locked door, Time Required to Walk	Door Sensor (alarm), Cameras, Personnel See
Reactor Room	Door Locked	Door Sensor (Alarm), Cameras
Reactor Pool	Under 5.18m of Water	Cameras

This theft scenario was chosen because it would require the fewest number of accomplices and would not require collusion with a G2 or G3 individual. As seen in Table 2, a G1 Adversary breaks in and steals fuel assemblies from the reactor pool. Using the minimum adversary task times (which would have been the most conservative), there was no Critical Detection Point (CDP), meaning that even if the adversary was detected at the very first detection point, they could still complete their tasks before the Response Force arrived. Using the maximum activity times, and with the response time at 300 seconds with a standard deviation of 90 seconds, there is a chance the response force would arrive in time to interrupt.

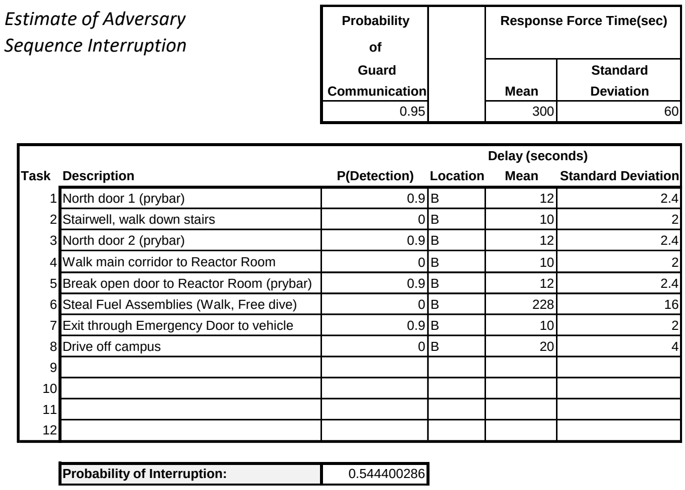
Table 2: Adversary Path for Reactor Fuel Theft

Path	Delay Time	Adversary Task Time Remaining	*P(D)*
North Door 1 (prybar)	12 sec	302 sec	0.9
Stairwell, Walk down stairs	10 sec	292 sec	0
North door 2 (prybar)	12 sec	280 sec	0.9
Walk main corridor to Reactor Room	10 sec	270 sec	0
Break open Door to Reactor Room (prybar)	12 sec	258 sec	0.9
Steal Fuel Assemblies (Walk, Free dive, Retrieve Fuel & Pack) (8 assemblies)	228 sec	30 sec	0
Exit through Emergency Door to Vehicle	10 sec	20 sec	0.9
Drive off Campus	20 sec	0 sec	0

The probability of Detection (*P(D)*) for the door alarms was estimated from Garcia [5]. The *P(D)* for cameras in the stairwell is low because "based on the scientific evidence demonstrating that this approach starts to degrade after 30 min and is not reliable after 1h" [4]. There is no dedicated force using cameras to detect intruders. The cameras are for assessment (after another detection device alerts security) and verification (not a false alarm), and therefore are unlikely to contribute to the chance of detecting an intruder.

The Critical Detection Point (CDP) for this example is when the adversary is walking down the first flight of stairs because 300 seconds (the Response Force Time, T_{RFT}) puts the last opportunity for detection with the chance of Interruption at that time (The Minimum Adversary Task Time Remaining that is Greater than Response Force Time, T_{RFT}). The Response Force time is estimated to be about 300 seconds, or 5 minutes, which is the approximate travel time from PUPD to the reactor building, allowing for time to verify the alarm and assemble. Using the EASI Computer Model for Theft seen in Fig. 1, the Probability of Interruption (P_I) was determined to be 0.544 [4].

Figure 1: EASI Computer Model for Theft of Fuel Assemblies



Estimate of Adversary Sequence Interruption

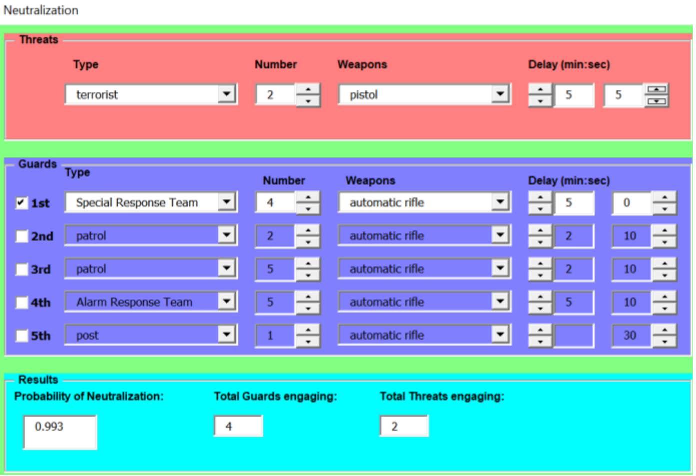
Probability of Guard Communication		Response Force Time(sec)	
		Mean	Standard Deviation
0.95		300	60

				Delay (seconds)	
Task	Description	P(Detection)	Location	Mean	Standard Deviation
1	North door 1 (prybar)	0.9	B	12	2.4
2	Stairwell, walk down stairs	0	B	10	2
3	North door 2 (prybar)	0.9	B	12	2.4
4	Walk main corridor to Reactor Room	0	B	10	2
5	Break open door to Reactor Room (prybar)	0.9	B	12	2.4
6	Steal Fuel Assemblies (Walk, Free dive)	0	B	228	16
7	Exit through Emergency Door to vehicle	0.9	B	10	2
8	Drive off campus	0	B	20	4
9					
10					
11					
12					

Probability of Interruption:	0.544400286

The probability of neutralization (P_N) is shown in Fig. 2 [11]. The adversary is a small force of 2 individuals armed with pistols. The Response Force for a reactor security incident is the PUPD. Based on the normal presence of 4 officers on duty during a day shift, the response force has 4 members and are equipped with automatic rifles. The delay time was calculated based on the time it would take the adversary to complete their tasks after they are first detected, which was 325 seconds. This yields a 0.993 P_N. The probability of effectiveness (P_E) of the adversary = 0.540.

Figure 2: Probability of Neutralization software



Neutralization

Threats

Type	Number	Weapons	Delay (min:sec)	
terrorist	2	pistol	5	5

Guards

	Type	Number	Weapons	Delay (min:sec)	
☑ 1st	Special Response Team	4	automatic rifle	5	0
□ 2nd	patrol	2	automatic rifle	2	10
□ 3rd	patrol	5	automatic rifle	2	10
□ 4th	Alarm Response Team	5	automatic rifle	5	10
□ 5th	post	1	automatic rifle		30

Results

Probability of Neutralization:	Total Guards engaging:	Total Threats engaging:
0.993	4	2

3.1.2.4 Sabotage

Sabotage of the reactor would yield little damage because there is very little fuel (10kW), but if an attack were ideologically motivated, destruction of the reactor or computer operating system would effectively stop it from operating. Protections are in place that prevent a change in reactor operations if it violates programming in the PLC (Programmable Licensed Controller) (which has hard[physical] key access), so this is an unlikely scenario. Also, there is no external access to the reactor operation computer (Wi-Fi/internet/etc.). However, physical destruction is possible and reasonably achievable.

In this scenario, a G1 adversary gains access to the Reactor Room via a tour during the day. The security elements for this scenario are the same as those listed in Table 1. Attendees are normally escorted to a classroom off of the main corridor where they receive a brief lesson about the reactor. They are then instructed to leave jackets and bags in the classroom room before walking to the reactor room for the tour. At this point the adversary uses a bomb vest to damage the reactor. It is important to note, the P(D) doesn't have a value in this scenario because none of the detection devices observed in the facility would be designed to detect something wrong. The adversary is being escorted by someone with access (G3), and therefore there are no sensors to alarm. The only detection possible would be if someone physically observed the adversary "acting" suspicious or anxious, and there is no way to plausibly estimate the probability of this occurring. There is no value for *P(D)* because there are no devices to detect something wrong. As a result, the Response Force would not be deployed to stop the adversary, so a P_I and P_N (or P_E) cannot be calculated.

3.2 Cobalt Irradiator

In this restricted area there is a Cobalt Irradiator and a Cesium Check Source. Co-60 and Cs-137 sources are in the range of terabecquerel (TBq) activities. The cobalt irradiator is sealed, and a collar is in place to protect users when inserting material to be irradiated. There is no access to the source within. There are multiple detection devices to prevent unauthorized access to the restricted area.

3.2.1 Groups

Groups were identified based on their level of security access. There are really only 2 groups, those with authorized unescorted access, and those without. For irradiator spaces: G1: All other individuals not included/covered in Group 2 or 3. Individuals only have Main Corridor Access. G2: Supervised Access: These individuals may also be granted permission to be around an asset while supervised. This group would have an improved access advantage from G1. These include students receiving training during a laboratory. G3: Authorized Unescorted Access: These individuals have access to all assets. They require no supervision. Access is granted in compliance with 10CFR37 [12] so each individual must be deemed trusted and reliable by a reviewing official and have completed security training. Include: REM (RSO and HPs, and PUPD. Access can be given to anyone with a “need” and who meets the requirements to get a T&R (Trustworthy and Responsible).

3.2.2 Scenario

3.2.2.1 Equipment Malfunction

While using the irradiator, the sample drop column apparatus jams and cannot lower into the irradiator. A collar exists to limit exposure to the user, but in order to repair it, a Health Physicist from REM would need to fix it (and be in proximity to do so). This would place the worker in a position to receive an unnecessary dose of radiation.

3.2.2.2 Human Error

When performing maintenance or repairing the irradiator, particularly the sample loading device, a worker could position themselves, when safety shielding is removed to allow for work, that could allow them to receive a higher radiation dose. Alternatively, when using the calibration source, an operator could stand in a position that would increase their radiation dose or the operator could fail to turn on detector/change batteries in the room when using the calibration source, resulting in them receiving an unknown radiation dose.

3.2.2.3 Theft

In this scenario, a G1 adversary would need to gain assistance from a G3 individual (or insider) to gain access and steal the cobalt source. The adversary would need to overcome multiple detection devices to access the restricted area, including cameras, locks, pin-pad entry, and would be delayed by the physical act of penetrating the shielding to access the cobalt sources. Cutting through the shielding would require cutting ~25.4 cm of lead shielding. To cut through 25.4 cm of mild steel (at a rate of 2.3 seconds/cm for each 1cm thickness), would result in a cut rate of 58.4 seconds/cm using an oxygen acetylene cutting torch [5]. If the source cage inside is ~20 cm in height and ~20 cm in diameter, it would take over an hour. The time required to remove the source from the heavily shielded irradiator would be too great to achieve before Response Forces arrived if the adversary was detected by the several detection components in place. The adversary could then use the source in an RDD to harm the public.

Using the EASI Computer Model [4], the probability of interruption (P_I) was determined to be 0.855. The probability of neutralization (P_N) was 0.993 [11], with the adversary using a small force of 2 individuals armed with pistols, and a response force has 4 members equipped with automatic rifles. The probability of effectiveness (P_E) of the adversary= 0.849.

3.2.2.4 Sabotage

An adversary could potentially damage the irradiator and breach the source shielding with the use of a bomb. An adversary would need to penetrate the security features in order to access the irradiator. It would take ~340 seconds to set up a 500lb explosive [5] [13]. Pathway analysis was used to analyze the adversary path to detonate a conventional bomb to destroy the irradiator. Based on the location of the facility room underground, and the thickness of the walls, it is unlikely that contamination would spread any great distance. However, the facility is under a medical building and its destruction would require a great amount of decontamination were it successful.

Using the EASI Computer Model [4], the probability of interruption (P_I) was determined to be 0.784 for sabotage of the cobalt irradiator. The probability of neutralization (P_N) was 0.993 [11], with the adversary using a small force of 2 individuals armed with pistols, a delay time of 5 minutes and 55 seconds, and a response force has 4 members equipped with automatic rifles. The probability of effectiveness (P_E) of the adversary = 0.779.

3.3 Nuclear Medicine Laboratory

Students use the Nuclear Medicine Laboratory for class and lab work. These spaces include a classroom, a large laboratory, and a small laboratory space used primarily for storage. The laboratory and classroom are also shared with health science classes. The small storage lab is locked, and material is stored within, and only pharmacy has access. The generators are stored within. Additionally, another computer-driven molybdenum generator is locked at all times except when extracting material. All the rooms are used for student training.

Sources include Molybdenum-99m Technicium-99m generator 10Ci liquid (molybdenum), which decays in ~1month, and is routinely kept for ~2 years to allow it to decay before disposal. The Technetium generated decays in ~60 hours. There are also sealed sources (in the range of µCi's) used as check sources. Procedural controls in the Nuclear Medicine Laboratory ensure materials are not accessible except when in-use by students during class.

Official inventories are performed by REM annually on sealed sources. An unofficial inventory is performed with each use when materials are put away in the storage lab after class by the professor in charge. If materials were missing, this would be reported to REM. The computer-driven molybdenum generator with a tungsten source is surveyed before opening the shielded door to prevent unintended exposure in the event the filter cracks.

3.3.1 Groups

Groups were identified for the Nuclear Medicine Laboratory based on their level of security access. G1: All other individuals not included/covered in Group 2 or 3. Individuals must be granted access through each security feature and be supervised. Students and non-students can access the building and the hallway exterior to the Nuclear Medicine Laboratory and could access the room when class is in session. G2:Includes PUPD, REM (RSO, HP), The building manager has keys to all the rooms. Cleaning crews access the classroom for regular cleaning. Cleaning of the lab is limited to once a year by cleaning crews. Students and the instructor clean the room themselves, and trash is held for 2 weeks to ensure any accidental contamination has decayed. Other Health Sciences instructors have access to the laboratory and classroom. G3: Authorized Access: These individuals have access to the laboratory rooms, the locked storage lab, and the generator. They require no supervision. Include: Professors, professional pharmacy students (per the radioactive materials license).

3.3.2 Scenario

3.3.2.1 Equipment Malfunction

The shielded filter of the computer-driven generator could crack, causing a spill. The door is normally surveyed before opening in order to detect high radiation levels. High radiation levels are an indication this has occurred.

3.3.2.2 Human Error

The shielded filter of the computer-driven generator could crack, causing a spill. The door is normally shielded before opening to detect high radiation levels which would indicate this has occurred. If a student forgot to perform this survey, they could expose themselves to high levels of radiation.

3.3.2.3 Theft

An adversary could break into the lab storage room and steal the Molybdenum-Technetium generators (better if after new shipment because activity will be higher) or pry open the computer-driven generator. The generator could be stolen if it was unbolted from its stand, but it weighs >100lbs. The Tungsten vial radioactive source could be removed by disassembling the generator. This would require hand tools. The entire generator could be stolen and used as an RED by removing the shielding or door. The tungsten source would be the most desirable target because it has the greatest amount of activity and a long enough half-life to be dangerous for a longer period of time.

A G1 adversary breaks in to steal material during non-class hours. There is no detection component for entering the building or the hallway. However, building doors may be locked during holidays. It is not unusual for students or staff to being in the building late at night. The laboratory does not contain detection equipment. Detection would require detection by a passerby who knew the intruder didn't belong. Delay components include the lock on the door, the lock on the generator door, and the time to disassemble the unit to access the source. An estimation of 5 minutes was made for disassembling the generator based on the source placement in the adversary path analysis; however, due to there being no detection components, the adversary would hypothetically have as much time as they needed without affecting their outcome. There is no *P(D)* for breaking open the lab door because it would only be detected if there was a passerby.

The CDP for this example is while walking through the lab (time remaining 345 seconds). Because of the Response Force Time of 300 seconds that puts the last opportunity for detection, along with any chance of interruption, at that time at the point when the adversary breaks open the laboratory door. Realistically, there is little to no chance of detection during this scenario. The adversary would have to be seen by a passerby, in a rarely used hall, during non-work hours. With a negligible probability of detection because there are no devices to detect something wrong, the probability of interruption becomes 0, the response force would not be deployed to stop the adversary, the probability of effectiveness would effectively be one.

3.3.2.4 Sabotage

A disgruntled student or staff member could remove door or shielding from the computer-driven generator. This would create a radiation emitting device (RED) by removing the shielding. Once this was done, it would not be detected until the next time the equipment was used because the door is surveyed before opening. The laboratory does not have detection devices in place to alert staff if unauthorized individuals access the space.

Adversary task times were approximated based on how the laboratory staff described the ease of completing the task. The *P(D)* doesn't have a value because there are no devices to detect something wrong. As a result, the Response Force would not be deployed to stop the adversary, so a P_I and P_N (or P_E) cannot be calculated.

4 DISCUSSION

For the majority of scenarios, the Critical Detection Point (CDP) yielded a delay time that was less than the Response Force Time, as a result, the adversary would not be neutralized before they could complete their tasks. However, due to the low level of activity and half-lives, the consequences would be drastically lower than other more-desirable targets. These lower risk assets have significantly less security than nuclear facilities, making them more-vulnerable targets; however, due to the limited consequences that could be achieved with the low levels of activity, the risk remains low for each of these assets.

The highest consequences would be observed following the theft of used fuel. The loss of used fuel would be the most dangerous of scenarios. The presence of fission products would make the subsequent radiological release dangerous to nearby public and require the shutting down of local businesses and operations in the area during the resulting extensive clean-up. An accidental exposure to radiation fields would vary depending on the event, but it would likely only affect 1-2 personnel, and due to the small amount of fuel and the shielding provided by the pool, would remain relatively low. Sabotage would result in significant damage to the building, a significant loss of life depending on the building occupancy at that time, and contamination of the surrounding area which would interrupt the operations of the university and nearby businesses.

The probability of effectively committing a theft increase; however, the destruction of the irradiator with a bomb would result in moderate consequences due to the damage to building & equipment. The release of the radioactive cobalt source would be significant if it could be distributed, but due to the location of the irradiator below ground level, a conventional bomb used for sabotage would not allow for maximum distribution. In the event of a malfunction or human error, exposure of personnel could be very high, but the training received by personnel would make them conscious of the radiation field.

While the Nuclear Medicine laboratory was the most likely of the three assets to successfully be stolen, a release of material from the nuclear medicine laboratory would result in the lowest consequences due to the low level of activity used in the laboratory. The Molybdenum-99m-Technicium-99m generators which initially contain 10Ci, decay in ~1month and the Technetium generated decays in ~60 hours. In the event of the loss of tungsten source, low to moderate consequences could be expected if it was used in an RED due to its ~6-month half-life. Low to moderate consequences could be expected from an accident or sabotage due to the exposure personnel would receive by standing near an unshielded source. because the generators are on the far side of the lab away from working areas, personnel would spend little time near the radiation field.

5 CONCLUSIONS

In order to direct resources appropriately for safety and security of radiological academic assets, the risk those assets pose needs to be evaluated in an objective and mathematically supported manner. Using pathway analysis to evaluate security scenarios, and with a qualitative analysis of consequences, this manuscript attempted to assess three assets at Purdue University. The theft of used fuel from the reactor would yield the greatest consequences but had the lowest probability of being successfully carried out. While the nuclear medicine laboratory was the most likely of the three assets to successfully be stolen, a release of material from the nuclear medicine laboratory would result in the lowest consequences due to the low level of activity used in the laboratory. Going forward, we will need to evaluate the Probability of Adversary attack during period of time (P_A) and a more specific Consequence Value (C), and to develop a means of calculating total risk which would include safety and security risk and applying it to a facility risk index.

6 REFERENCES

[1] Antonio Cippollaro and G. Lomonaco, "Contributing to the nuclear 3S's via a methodology aiming at enhancing the synergies between nuclear security and safety," *Progress in Nuclear Energy,* vol. 86, pp. 31-39, 2016.

[2] A. Sfetsos and e. al, "Quantifying potential target attractiveness in research reactors and associated facilities," in *ICONS International Conference on Nuclear Security,* Vienna, 2020.

[3] R. Bartel, "WASH-1400 The Reactor Safety Study: The Introduction of Risk Assessment to Regulation of Nuclear Reactors," 2016.

[4] M. L. Garcia, The Design and Evaluation of Physical Protection Systems, 2nd ed., Butterworth-Heinemann, 2008.

[5] M. L. Garcia, Vulnerability Assessment of Physical Protection Systems, Butterworth-Heinemann, 2006.

[6] Purdue University Nuclear Engineering, "PUR-1, Purdue's Nuclear Reactor," [Online]. Available: https://engineering.purdue.edu/NE/research/facilities/reactor/index_html. [Accessed 31 10 2020].

[7] S. Rane and J. Harris, "Development of a Potential Facility Risk Index for Radiological Security," *Risk Analysis,* no. in press, 2020.

[8] "Annual Security and Fire Safety Report 2019," West Lafayette Campus, 2019.

[9] "Staff Directory," 7 10 2020. [Online]. Available: https://www.purdue.edu/ehps/police/about/directory.html. [Accessed 18 11 2020].

[10] J. Jenkins and E. Merritt, "Safety Analysis Report for the Conversion of the Purdue University Research Reactor from HEU to LEU Fuel," 2006.

[11] Lawrence Livermore National Laboratory, "Joint Conflict and Tactical Simulation," Livermore.

[12] U. NRC, "Part 37-Physical Protection of Category 1 and Category 2 Quantities of Radiological Material," 23 9 2020. [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part037/index.html. [Accessed 29 10 2020].

[13] Department of Homeland Security, "IED Attack: Improvised Explosives.," Depatment of Homeland Security, [Online]. Available: https://www.dhs.gov/sites/default/files/publications/prep_ied_fact_sheet.pdf. [Accessed 1 12 2020].