Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting
August 23-26 & August 30-September 1, 2021

DEVELOPMENT AND DEMONSTRATION OF A RESEARCH REACTOR NUCLEAR SECURITY RISK MODEL

Jason Harris[1], Emily Bragers[1], Emma Rekeweg[1], Destiny White[1]
[1]School of Health Sciences, Purdue University, 550 Stadium Mall Drive, West Lafayette, Indiana 47907, USA

ABSTRACT

Nuclear security of research reactors and associated facilities (RRAFs) faces unique challenges. Although RRAFs contain nuclear and radioactive materials of varying types and activities, they often possess weaker security measures compared to larger power plant facilities. Also, the variety in RRAF types and locations makes it difficult to meaningfully compare nuclear security risks. While work has been done to estimate RRAF risks, no broad model exists that takes into account threat, vulnerability, and consequences of malicious acts to these facilities. This study adapts the Potential Facility Risk Index (PFRI) to RRAFs. The PFRI is a quantitative risk-based methodology that facilities can employ to better understand facility risk. The use of quantitative values, instead of categorical qualitative ones, allows for generation of risk values that can then be used for comparison and (cost-benefit) decision making. The computation of the Potential Facility Risk Index (PFRI) is based on the triplet definition (threat, vulnerability, and consequences) of risk. The threat component of the PFRI is devised as a utility function weighing the threat group attributes and asset preference. The principles of probabilistic risk assessment and pathway analysis are implemented to account for different attack scenarios. Locational hazards and nuclear security culture are measured as a function of facility vulnerability. The consequences of loss of life and economic loss are computed, as a result of radioactive release from an attack. In order to demonstrate the functionality of the PFRI, two security scenarios, theft and sabotage, were analyzed for the Purdue University research reactor (PUR-1). The theft of reactor fuel assemblies and the destruction of the reactor with explosives were used to estimate the probability of success by the adversary. Parameters contributing to the facility risk were analyzed along with existing vulnerabilities. Consequence calculations incorporate population demographics, local economic measures, meteorological conditions, reactor properties, and radioactive material characteristics. The contribution of the research is significant because it is the next step towards development of a new tool in the field of RRAF nuclear security-one that is expected to introduce, analyze and numerically test a methodology that yields a facility level risk index.

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. While safety concerns may be less for research reactors compared to larger nuclear facilities, they may become more desirable targets to malicious actors due to reduced security measures. 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].

METHODOLOGY

Although current nuclear security risk models exist, none fully consider all aspects of specific facility threat, vulnerability, and consequences like the Potential Facility Risk Index (PFRI) developed by the author. The PFRI risk framework is strictly a facility-based approach, meaning the risk is unique to the facility, depending on the type of facility, location of the facility, asset type available at the facility, and human factors (such as culture) found at the facility [6, 7]. The PFRI index framework (Fig. 1.) gives a clear visualization of the multi-dimensional inputs of threat, vulnerability and consequences, hence being the premise of a quantitative evaluation of risk. The PFRI is mathematically represented as the exponential product of the maximum expected utility among the threat groups, the sum of the geographic vulnerability and cultural vulnerability, and the net consequences of loss of life and economic loss. Each input in the model is quantified and contributes to the overall PFRI (risk) score. The framework can be adapted for any facility, any location, and extended to include other parameters, such as human reliability. A C++ (MATLAB) graphical user interface (GUI) tool for the PFRI has been developed to incorporate all facility parameters. This GUI can be integrated into other programming languages (such as Python) for AI and machine learning applications.

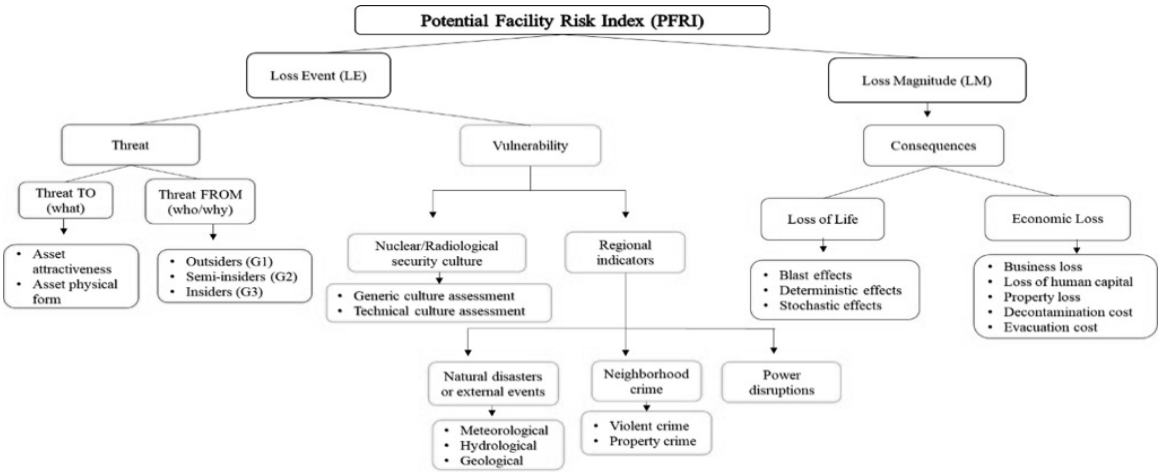

Figure 1. Potential Facility Risk Index (PFRI) framework

To demonstrate the PFRI, three assets were evaluated at Purdue University: the PUR-1 research reactor, a cobalt irradiator, and the nuclear medicine laboratory [8]. 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]. However, due to space and time, only the PUR-1 scenarios will be discussed in this paper

Personnel 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 [9]. 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) [10]. 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.

RESULTS

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.

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.

1.2 Scenario

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.[11]

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.

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. 2, the Probability of Interruption (P_I) was determined to be 0.544 [4].

Estimate of Adversary Sequence Interruption

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

Task	Description	P(Detection)	Location	Delay (seconds) 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

Figure 2: EASI Computer Model for Theft of Fuel Assemblies

The probability of neutralization (P_N) is shown in Fig. 3 [12]. 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.

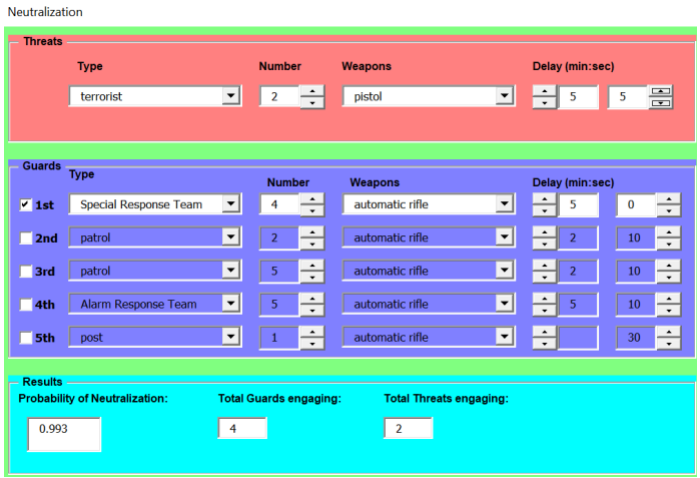

Figure 3: Probability of Neutralization software

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.

DISCUSSION

For the majority of scenarios and simulations performed, 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.

CONCLUSIONS

In order to direct resources appropriately for safety and security of radiological academic assets, the risk 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 the research reactor asset 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. 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.

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] Rane, Shraddha V. "Quantitative Model of a Facility -Level Radiological Security Risk Index" (thesis, Purdue University Graduate School, 2020), https://doi.org/10.25394/PGS.12730247.v1.

[7] Rane, Shraddha V & Harris, Jason T. "Development of a Potential Facility Risk Index for Radiological Security," *Risk Analysis*, November 17, 2020, risa.13625, https://doi.org/10.1111/risa.13625.

[8] 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].

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

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

[11] 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].