Evaluating the effectiveness of security systems regime of a hypothetical radiological facility using a risk calculation

M N S Ansah\textsuperscript{1}, B P Stepanov\textsuperscript{1}, P A Amoah\textsuperscript{1} and E B Agyekum\textsuperscript{2}

\textsuperscript{1} National Research Tomsk Polytechnic University, 30, Lenin Avenue, 634050, Tomsk, Russia
\textsuperscript{2} Ural Federal University named after the first President of Russia Boris Yeltsin, 19, Mira Street, 620002, Ekaterinburg, Russia

E-mail: michaelansah67@gmail.com

Abstract. This paper presents how security effectiveness can be measured by considering the cost involved in providing security for a radiological center and measures to improve security through risk analysis. The expansion of nuclear technologies and the possible use of nuclear and radioactive materials continues to grow. This increase comes with potential risk of radioactive materials being used for the wrong reasons; thus it is important to provide physical protection of nuclear related facilities to counter these threats and use atomic energy for peaceful purposes. The effectiveness of the security systems put in place at the facility can be assessed by making analysis of the risks associated to the facility.

1. Introduction
The significance of physical protection to humans and the environment as a whole cannot be overlooked since it affects every aspect of life including socio-economic structure of a state and organizations [1]. Physical protection systems are established to prevent, deter and or mitigate loss of treasured assets such as property or life [2]. In the presence of such threats, people have learned to develop measures to safeguard themselves and their properties over time [1]. Physical Protection System (PPS) integrates people, measures, and equipment to provide security for assets or nuclear-related facilities against theft, sabotage or other malicious attacks. The result of these malicious actions may be theft of radioactive material, sabotage at the radiological facility (fire, destruction, flooding, accident, etc.).

The International Atomic Energy Agency (IAEA) promotes the idea for all governments to take measures to ensure that effective national control systems operated within their jurisdictions in order to ensure the existence of effective national control systems for the protection of radioactive sources [3]. A security framework should employ the concept of defense in depth, so that many levels and methods of protection in terms of structural, technological, personnel and organizational need to be overcome by an enemy in order to realize his or her task. It is important for the PPS to perform detection, delay, and response functions in coordination in order for it to operate effectively. An automated system physical
defense system, which incorporates technical, software, and other means, as well as personnel, can be implemented to automate the processes of ensuring an object's security.

Hospitals use radioactive materials for treatment of their patients such as teletherapy and thus, in specially built devices, high-energy and high-activity sources are used to deliver radiation doses in a controlled way.

This paper presents a modeled hypothetical radiological facility and the possible paths that can be used by adversaries to sabotage the facility. The efficiency of the security systems at this facility is assessed by making the risk analysis associated with the facility.

2. Materials and methods
The configuration of the protection system for a radiological facility can be measured using the ratio of task accomplishment. If the ratio of the protection task accomplishment is high, the uncertainty related to the efficacy of the protection system is assumed to be lower. Cost considerations is made when performing risk calculation analysis and this cost interrelation helps in taking decisions [2].

The performance measure feature for the risk analysis is denoted as:

\[ Risk = P(A) \times [1 - P(E)] \times C \]  

where, \( P(A) \) is probability of attack, \( C \) is consequence measured in United States Dollars and \( P(E) \) is probability of system effectiveness.

\[ P(E) = P(I) \times P(N) \]  

\( P(I) \) is Probability of Interruption and \( P(N) \) is Probability of Neutralization.

2.1. The Protection Effectiveness of an Intrusion Path
The effectiveness of each unit of the protection system complex lies on the proper management or configuration of detection, delay, and response elements [4]. In this calculation, we adopt that each unit has three factors for the protection task: detection, delay and response. When protection task is entirely met, the ratio is 1 and the ratio equals to 0 when the protection task is entirely not achieved. For a specific task, the efficacy of protection of one unit \( j \) can be estimated as:

\[ U_j = \sum_{i=1}^{n} \omega_i \log \frac{1}{1 - R_i} \quad (j = 1, 2, ..., k; i = 1, 2, ..., n) \]  

where \( U_j \) is the effectiveness of protection of unit \( j \). \( R_i \) is the degree to which a protection task is accomplished for individual factors. \( (1 - R_i) \) is the degree of failure to perform the protection task for individual factors. It's worth noting that different variables in the security unit have different impacts on the efficiency of the protection provided. The weight of each factor is represented by \( \omega_i \) \( (i = 1, 2, ..., n) \). Because different factors have varied effects on the efficiency of a security system's protection, \( \omega_i \) is used to signify the effect weight of factor-\( i \) and can be represented as \( \sum_{i=1}^{n} \omega_i = 1 \) for this report. For an adversary to target or sabotage a facility, they consider different vulnerable paths and select the most vulnerable route selected by the adversary also have the lowest cost of intrusion. Defense effectiveness can be for a specific material present in the radiological facility can be determined as:

\[ E(\text{asset}) = \min [C(\text{Path1}), C(\text{Path2}), ..., C(\text{Pathn})] \]  

Equation (5) can be used to calculate the risk value for a designed security system based on the risk concept of the security system suggested by Hicks:

\[ Risk = P(A) \times P(r) \times C \]  

(5)
where $P(A)$ is the probability of attack on a facility holding nuclear or radioactive material, which can be assessed by experts. $P(r)$ is the probability of successful attack. $P(r)$ describes the protection effectiveness of security system provided at the facility. The concept can be explained as follows: higher the protection effectiveness, the lower the possibility of successful attack $P(r)$. $C$ is considered consequence. The whole relation can be mathematically represented as:

$$E(\text{asset}) = \log \frac{1}{P(r)}$$  \hspace{1cm} (6)

Taking into account a facility with a number of safe properties (i.e., radioactive and nuclear materials), the risk of the security system provided can be determined as:

$$Risk = \sum_{i=1}^{n} \left[ P(A)_i \times \frac{1}{\exp[E(\text{asset}_i)]} \times C_i \right]$$  \hspace{1cm} (7)

where $E(\text{asset})$ is the protection effectiveness value of asset $i$, $P(A)_i$ is the probability of attack for asset $i$, it can be measured as the annual rate of occurrence of attack, $C_i$ is the value of the protection $\text{asset}_i$ [5].

3. Results
To explain the approach discussed above, a hypothetical radiological facility (hospital) is taken into account. It has a storage space where it stores used nuclear materials. The hospital houses X-ray and a blood irradiator, which serves as the asset of the facility and the target for the adversary. The source used by the blood irradiator in the radiological facility is $^{137}$Cs. The target for the adversary is to sabotage both equipment. For each asset or target, the adversary considers two paths and these is described in the diagram. To gain an access to the first target, the offender plans to enter the main entrance of facility A, move to the appropriate space, force security door C to be opened, and access secure radioactive sources (asset 1) or go through a second path by crossing fence B. The opponent intends to penetrate the premises, move to the room, force open security door C and access the secure radioactive sources (asset 1). For the second target or asset, similar path used for the first target was used to cause the sabotage. The following figure 1 illustrates the view of the facility and the adversary paths.

![Figure 1. Schematic diagram of radiological facility with adversary paths.](image-url)
For the purpose of this analysis, the factors have equal effect weight, \( \sum_{i=1}^{n} \alpha_i = 1 \). The effectiveness of each unit is calculated using equation (3) and presented in the table 1 below.

### Table 1. The effectiveness for each protection unit.

| Unit (U_j)       | Detection | Delay | Response | Effectiveness |
|------------------|-----------|-------|----------|---------------|
| Main Entrance A  | 0.6       | 0.70  | 0.90     | 0.6403        |
| Fence B          | 0.8       | 0.85  | 0.70     | 0.6819        |
| Security Door C  | 0.9       | 0.70  | 0.85     | 0.7823        |
| Security Door D  | 0.8       | 0.70  | 0.85     | 0.6819        |

The effectiveness of each intrusion path is determined as the summation of the individual effectiveness of units along a particular path and presented in Table 2.

### Table 2. The effectiveness for each intrusion path.

| Intrusion Path | Effectiveness |
|----------------|---------------|
| Path 1 for asset 1 | 1.4226        |
| Path 2 for asset 1 | 1.4642        |
| Path 1 for asset 2 | 1.3222        |
| Path 2 for asset 2 | 1.3638        |

Risk associated with the radiological object can be achieved by calculating for the effectiveness of the security measures established and it can be done using equation (4). For the purpose of this scenario, \( P(A) \) is assumed to be 0.65. The cost value \( (C_1) \) of the asset 1 is 100,000 dollars while the value \( (C_2) \) of the asset 2 is 100,000 dollars. From Equation (7), the risk associated with each target can be calculated as shown in Table 3.

### Table 3. Values for calculating the risk of each asset.

| Parameter      | Target 1 | Target 2 |
|----------------|----------|----------|
| \( E(\text{asset}_i) \) | 1.4226   | 1.3222   |
| \( P(\text{A}_i) \)    | 0.65     | 0.65     |
| \( C_i \)              | 100,000  | 100,000  |
| \( \text{Risk}_i \)    | 1.7\times10^4 | 1.8\times10^4 |

3.1 Improvement strategies for protection

By using certain techniques, attempts are made to efficiently reduce the risk of radiological facility protection systems. Four tactics were employed herewith the first being, increase the detection factor of the entrance to 0.7. The second is to make improvement on the response factor of the fence B to 0.8. Thirdly, increase the Security Door C delay factor to 0.75. Finally, increase the Security Door D delay factor to 0.8. Table 4 presents the measured effectiveness of the protection units following the improvement tactics applied.

### Table 4. The effectiveness for each protection unit after the improvement strategies.

| Unit (U_j)       | Detection | Delay | Response | Effectiveness |
|------------------|-----------|-------|----------|---------------|
| Main Entrance A  | 0.7       | 0.70  | 0.90     | 0.6819        |
| Fence B          | 0.8       | 0.85  | 0.80     | 0.7406        |
The effectiveness of each intrusion path after the improvement strategies have been applied is determined as the summation of the individual effectiveness of units along a particular path and presented in Table 5.

Table 5. The effectiveness for each intrusion path after the applied tactics.

| Intrusion Path       | Effectiveness |
|----------------------|---------------|
| Path 1 for asset 1   | 1.4906        |
| Path 2 for asset 1   | 1.5493        |
| Path 1 for asset 2   | 1.4225        |
| Path 2 for asset 2   | 1.4812        |

Assuming that the cost of the methods used is 1000 dollars for each target, we use the previous equations to measure the efficacy and risk of the target. Both assets are likely to have the same \( P(A) = 0.65 \) for a potential attack on the facility. With the gathered parameters as shown in the Table 6 below, new values for risk associated with the assets of the radiological facility can be calculated.

Table 6. Values for calculating the risk of each asset after the applied tactics.

| Parameter | Target 1 | Target 2 |
|-----------|----------|----------|
| \( E(\text{asset}_i) \) | 1.4906 | 1.4225 |
| \( P(A)_i \) | 0.65 | 0.65 |
| \( C_i \) | 101,000 | 101,000 |
| Risk \( i \) | \( 1.6 \times 10^4 \) | \( 1.7 \times 10^4 \) |

The risk associated with the entire radiological facility before and after the improving the security systems is represented by a graph in figure 2 below.

Figure 2. Graphical representation on the risk associated with the radiological facility calculation.
4. Conclusion
The designing and implementation of Physical Protection system helps to identify areas of vulnerability that can be remedied and practices that can be improved during the risk and threat assessment exercise. The total risk of the facility’s security system before improvement tactics concerning the two targets was calculated as $3.5 \times 10^4$. With respect to the two targets, the overall risk of the facility protection system after the improvements was estimated as $3.3 \times 10^4$. The risk associated with the radiological facility was decreased by $2.0 \times 10^3$ following the tactics applied. The reduction of the risk value associated with the radiological facility is 5.7%, which indicates that the reliability of the protection mechanism given for the hypothetical radiological facility has been enhanced. When this analysis is properly applied to a radiological facility, it may help in making vital decision when securing a radiological facility.

Acknowledgment
The authors express gratitude to Nuclear Fuel Cycle Department of Tomsk Polytechnic University, Russia for providing support to this paper.

References
[1] Omotoso O and Aderinto A A 2012 Assessing the performance of corporate private security organizations in crime prevention in Lagos State, Nigeria Journal of Physical Security 6 1 73-90
[2] Graves G H 2006 Analytical foundations of physical security system assessment Texas A&M University 1-80
[3] International Atomic Energy Agency 1998 The safety of radiation sources and the security of radioactive materials IAEA General Conference Resolutions 42 Res. 12
[4] Davies S J and Minion R R 2008 Security supervision: theory and practice of asset protection Butterworth-Heinemann ed 3 579
[5] Dai J, Hu R, Chen J and Cai Q 2012 Benefit-cost analysis of security systems for multiple protected assets based on information entropy 14 571-580