International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 5, Sep- Oct 2021
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Upgrading the Physical Protection System (PPS) to Improve the Response to Radiological Emergencies Involving Malevolent Actions at the Komfo Anokye Radiotherapy Facility, Ghana

Eric C. D. K. Addison *, Richard Asamoah Opoku **, Simon Adu ***
*(*Physics Department,Kwame Nkrumah University of Science and Technology, Kumasi-Ghana*
Medical Physics Department, KomfoAnokyeTeaching Hospital, Kumasi-Ghana
Email: ektaddison@gmail.com)
** (*Physics Department, Kwame Nkrumah University of Science and Technology, Kumasi-Ghana*
Email:opokuasamoahrichard@gmail.com)
*** (Radiation Protection Department, *Nuclear Regulatory Authority, Accra-Ghana*
Email:adusimon2003@gmail.com)

----------**********----------

Abstract:

The evaluation of the probability of interruption, effectiveness and the risk of the security systems protecting the radioactive source at the radiotherapy facility in Komfo Anokye Teaching Hospital (KATH) was conducted using the Estimated Adversary Sequence Interruption (EASI) model and the Dai et al model based on information entropy. Through the probability of detection, measured delay and response force time values; the probability of interruption using the Estimated Adversary Sequence of Interruption (EASI) model for the physical protection systems was found to be 0.949999133 for path 1, 0.949999690 for path 2, 0.949997580 for path 3, 0.949997513 for path 4 and 0.949997079 for path 5 to the radioactive source. The effectiveness of each intrusion path using information entropy based on the Dai et al model for the radioactive source was 3.888494371 for path 1, 3.814602419 for path 2, 3.245619492 for path 3, 3.290665357 for path 4 and 3.400005255 for path 5. The associated risk for the physical protection systems was found to be 0.015577772. The physical protection systems were high enough with minimal risk for the radioactive source and the probabilities of interrupting an adversary before sabotaging the radioactive source were higher than the average range of 0.50 to 0.70 for physical protection systems. This paper will provide basic guidelines and counter measures in the evaluation of security systems to protect radioactive sources in radiotherapy centers and other medical facilities in Ghana.

Keywords **—Upgrading physical protection system, improving radiological response involving malevolent activities, Cobalt-60, Safety, Radiation Protection, Radiation Shielding, Komfo Anokye radiotherapy facility, Kumasi.**

----------**********----------

INTRODUCTION

Security of radioactive sources has turned into an issue of serious public concern after the devastating terrorist attacks all over world. Historical experience suggests that incidents relating to radioactive sources can cause difficult challenges since radioactive materials have the ability to produce widespread fear and dread if people with malicious intention gets their hands on it. Nuclear and radiological security threats or risks rise up from the creation of radiological dispersal devices or nuclear explosive devices through the acquisition (theft) of nuclear materials from nuclear and medical facilities or from the transport of radioactive materials [1]. The utilization of radioactive materials in nuclear explosive devices and radiological dispersal devices can pose potential threat to staff, the general public and the whole human race. Fortunately, nuclear attack is one of most challenging sorts of attacks for adversaries to achieve, however, a well-organized, efficient and determined adversary group with the right fissile materials will be able to manufacture and set off nuclear weapons which have the ability to terrorize the heart of many nations on this planet. The activities and declaration of terrorist groups tend to support this statement. According to the International Policy Institute for Counter-Terrorism in Israel, a message appeared on one of the websitesvisited by followers of al-Qaeda in December 2002, which warned: ”These coming days would show that Qa’idat al-Jihad has the capabilities with the help of Allah to turn the United States of America into a lake of deadly radiation” [2]. In view of this many nations regard nuclear security as a broad aspect of radiological safety since it helps deliver integrated physical protection to the general public from time to time [3]. Radiological and nuclear security orphysical protection incorporate not just anti-invasion, anti-theft, anti-destruction of the radioactive source yetin additionpersonalsafety, information security and communicationsecurity.Facilities utilizing radioactive sources, such as medical facilities, are typically less protected than other nuclear facilities. Such facilities typically have more restricted security, access control features, alarm stations as well as a restricted on-site guard force that are typically intended to protect the staff, visitors and the public; rather than for the specific purpose of protecting the radioactive material on the site. Adversary targets in such facilities are typically straightforward, usually involving the unauthorized removal or sabotage of a particular radioactive source, or machine housing sources. Physical harm to these facilities or interruption of their activities could inhibit a full effective response and intensify the consequence of a crisis situation. Regardless of whether these facilities are not the immediate focus of adversary attack, it could be altogether affected by secondary contamination involving radiological, biological or chemical agents. Exposures to such radioactive materials can pose radiological hazards to nuclear occupational workers and the general public and may have somatic and genetic effects. Due to the fact that radioactive sources are used all over the world, assuming a certain level of security is significant. To reach this goal nuclear and health physicist have to tackle the possible weakness and shortcomings of the security framework of nuclear and medical facilities to protect radioactive sources. The radiotherapy center provides the general public with important service of cancer treatment. This service provided by the facility makes it unreservedly open to all sorts of people with different intention (whether good or bad). This free access, be that as it may, makes it hard to recognize potential dangers and in turn forestall unauthorized entry into the facility.

This free access to the facility joined with inadequate physical protection functions (detection, delay and response) to identify and stop potential threats makes the facility vulnerable to adversary attacks. Also, the effectiveness of the security systems protecting the Cobalt-60 source in the radiotherapy facility mainly depends on qualitative analysis of management science to find the risk of the radioactive source. Nevertheless, if the analytic system does not have a profound, complete perspective of the physical protection system then the risk assessment established on management science may lead to deviations [4, 5]. With a specific end goal to evaluate the security systems and its efficiency to avoid the above problems, there is the need for a viable and reliable physical protection system that can guard the radioactive source from adversary attack or sabotage. In spite of the fact that the radiotherapy facility inKATH has developed a security system to adequately protect its radioactive source yet it still experiences difficulties in dispensing enough resources to secure its radioactive material complex adequately. To help address these problems, this project seeks to evaluate and upgrade the current state of the physical protection systems in order to improve upon its response to adversary attack or radiological crises using the EstimatedAdversary Sequence Interruption (EASI) model and the Dai et al model based on information entropy.

I. METHODOLOGY

A. Description of the Radiotherapy Facility in Komfo Anokye Teaching Hospital (KATH)

The radiotherapy facility at the Komfo Anokye Teaching Hospital (KATH) is located in Kumasi, Ghana. The radiotherapy facility under the oncology directorate in KATH was established in 2004 with the aim of identifying and treating cancer cases. It is located beside the Komfo Anokye Out Patient Department building (Poly Clinic) and opposite the Kumasi Nursing and MidwiferyTraining College as shown in figure 1. The radiotherapy facility grounds are an open area with nearly direct vehicle access to the building on the front side. It operates with a shielded 2.5 cm diameter cirus Cobalt-60 teletherapy machine with minimum dose rate to water of 2.5 Gy/min at the depth of maximum dose at the isocentre

SAD in a 10 cm 10 cm field which rotates with full gantry from 00 to 3600. Cobalt-60 is a beta/gamma emitting radioisotope of Cobalt-59 with a half-life of 5.27 years. It undergoes beta decay to produce gamma radiation. The radiotherapy facility also provides low dose rate Cesium brachytherapy services for cervical cancer. The teletherapy machine has been operational for approximately 13 years; as of October, 2017; the activity of the Cobalt-60 source contained within has dropped from 12,000 Ci (444 TBq) to around activity of 2172 Ci (80 TBq) for the treatment of patients.

B. The Current State of the Security Systems at the Radiotherapy Facility

The external boundaries of the radiotherapy facility are fenced with a 1.5-meter mesh. There was no detection material in the external boundaries of the facility; however, there was a security guard who patrols along the front view of the facility where people use as access to the facility. All the five (5) entrances are connected to the facility and are sealed with a glass door which are opened and locked manually. There was no monitoring device to check the activities of people entering the facility. There are five (5) access paths to the teletherapy room; two of which are available to the staffs and patients from 08.00 am to 16.00 pm and is locked after that time. The other three (3) paths are locked all day and are not accessible to either the workers or the patients. The teletherapy room is sealed with three doors which are opened and locked manually. The first door is made up of wood which leads to the control room which is also sealed with a glass door and the second wooden door to the teletherapy room. The last door to the teletherapy room is made up of lead which blocks radiation from moving to other areas of the facility.

There was only one monitoring camera in the facility and was found in the teletherapy room; which is monitored by technicians in the control room during treatment. The functions of the physical protection system (PPS) at the Oncology center is dependent solely on the early response of the physical protection system unit at KATH; in case of any sabotage or theft of the radioactive source, the alarm in the teletherapy room triggers to alert the security guards for assistance through the security unit which is at 150 m away from the radiotherapy facility. In view of this, upgrading the physical protection system will help cover the three physical protection functions in the form of detection, delay and response so as to help increase the fast responds to malevolent activities on the radioactive source in the facility.

C. Scenario Description of the Current State of the Physical Protection System (PPS) at the Radiotherapy Facility

The facility has five (5) entrances that are; the main entrance, the south entrance, the southwest entrance, the west entrance and the north entrance. The main entrance and the south entrance are used by the staffs and the patients and are locked after working hours (08.00 am to 16.00 pm) from Monday to Friday. The southwest entrance, the west entrance and the north entrance are emergency paths for staffs and are locked 24 hours. There is only one asset in the radiotherapy facility of which path 1 (from the main entrance) and path 2 (from the south entrance) are similar, as are path 3 (from southwest entrance), path 4 (from west entrance) and Path 5 (North entrance). Considering the current status of the PPS and the two general broad intrusion paths for the adversary to sabotage the target; In order to minimize detection, the adversary (one person or a team) will attack the KATH radiotherapy facility during non-operational hours. The adversary intends to climb the radiotherapy facility fence line and traverse to the main radiotherapy building. Using hand tools, the adversary will breach the outer chain-link mesh fence to the building. Once the fence is cut, the adversary will immediately move to the door of the radiotherapy building (main door, south door, southwest door, west door and the North door) without any detection by cameras or sensors.

The adversary may force open the door using mechanical tools or an explosive charge and then enters the building. Inside the facility, the adversary may move to the door to the patient waiting area and subsequently to the door to the control room or straight to the door to the control room through either the main/south door or the southwest/west/north door respectively; once again with no cameras or sensors to detect the presence of the adversary. The adversary will then breach the door and move toward the 1st door to the target (teletherapy machine) and next to the 2nd to the target without any detection (cameras or sensors). The adversary will finally enter the teletherapy room and sabotage the target (teletherapy machine). The teletherapy room however, has a CCTV surveillance which monitors the activities of patients and for timely detection of unauthorized actions such as tampering or interference with the radioactive source. Figure 1 below represents the detailed layout of the radiotherapy facility and its current security systems. The adversary may be an insider, an insider assisting an outsider or an outsider. An insider adversary is a person with authorized access to the radiotherapy facility or the radioactive source who could attempt sabotage or unauthorized removal of the radioactive source or aid an external adversary to do so.

Scenario Conditions

- General Scenario Description: Adversary intends to attack the radiotherapy facility with the objective of sabotaging the radioactive source through stealth strategies or quick surprise attack to gain access to the radiotherapy facility.
- Design Basis Threat: Adversary will be armed with automatic weapons, hand tools, mechanical tools and explosive breaching charges.
- Adversary Assumptions: Adversary will attack on foot. Further, adversary will use information gained from a passive insider, the information concern technical level details

about sabotage of the control room and in turn the teletherapy machine.

- Response Force Assumptions: The response forces may use weapons only in self-protection or if ordered from the commander. Only response force team may engage with the adversary. Guards may shoot in self-protection only.
- Attack Conditions: Both opened (operational) and closed condition (non-operational); clear weather conditions.

D. Risk Assessment of the Radioactive Source

The risks were evaluated on the hypothesis that the radioactive source (teletherapy machine) is not managed securely or kept safely and a critical accident, harm or robbery could prompt the release of radioactive material into the environment if the shield protecting the teletherapy unit is removed [6]. In the event that a radioactive source is uncontrolled and unshielded due to malevolent act oraccident, people will get exposed to radiation above international permissible levels which are dangerous to the health of the people. In view of this, IAEA established a new classification method for radioactive sources to keep them under control with respect to their corresponding radiological hazards. This classification method depends on the ability of radioactive sources to produce deterministic effects (effects which do not appear until a threshold value is surpassed) and the seriousness of the effect becomes high with increased dose beyond the threshold value [7]. The risk factor was estimated through the following equation:

$$D_f = \frac{A}{D} \qquad (1)$$

where Df is the risk factor, A is the activity (TBq) of each radionuclide in a nuclear facility which could be lost in case of emergency or event and D is constant for isotopes. Df ranges from < 0.01 to > 1000.0 and is found in appendix 8 of [7].

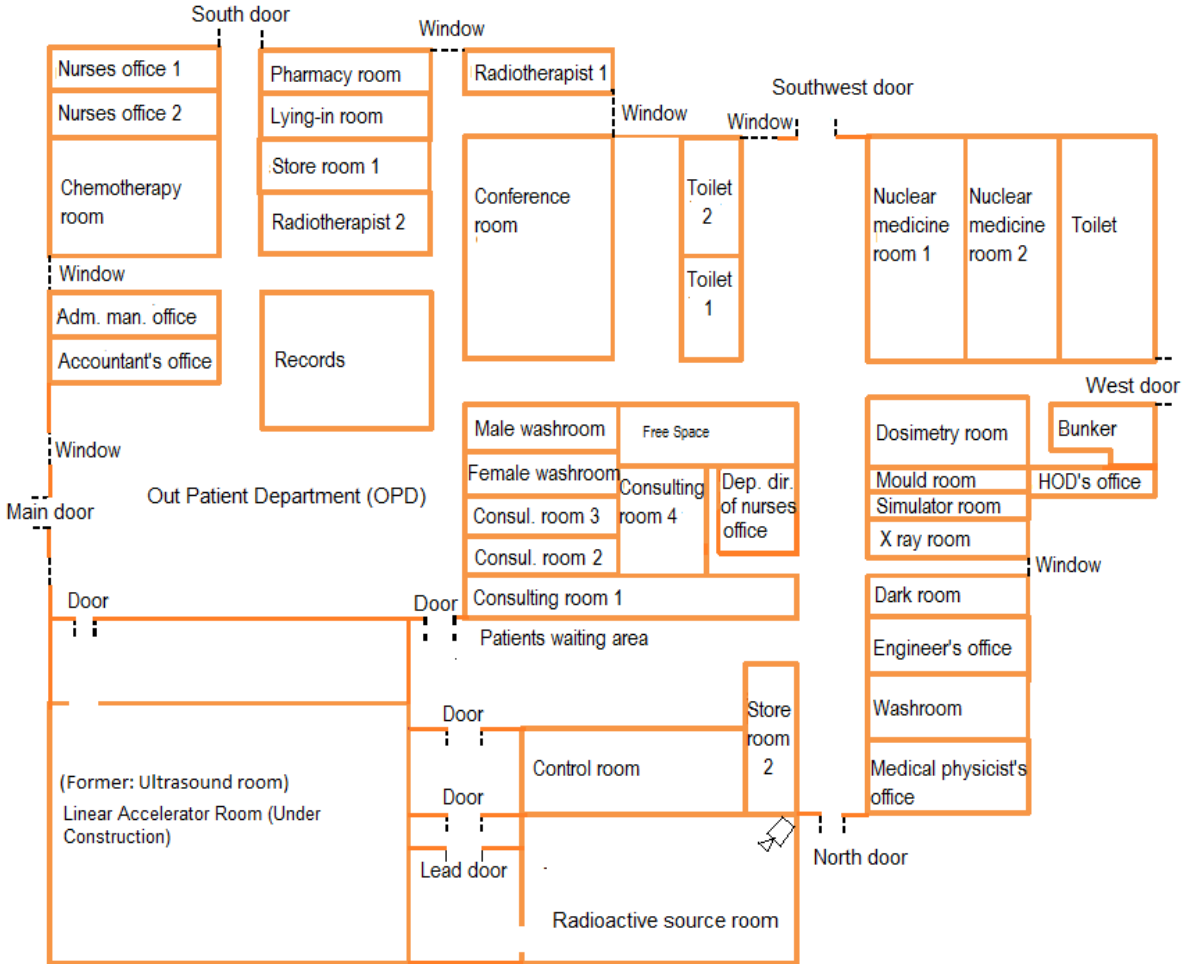

Figure 1. Showing detailed layout of the radiotherapy facility and its current physical protection systems.

E. Risk Assessment for a Single Asset with Multiple Intrusion Paths

Risk assessment approach employed to safeguard the radiation source in the oncology

directorate are as follows:

- Identification of the assets (radiation source) to be assessed.

In this stage, the target for which an adversary tends to sabotage or steal was identified and analyzed to acquire basic information such as the risk factor and its danger to people.

- Acquisition of operational and physical data and in addition analysis of the facility and its operations.

Physical protection functions such as detection, guard communication values in the form of probabilities, response time and delay values in the form of mean times were measured. Probabilityof Guard Communication value: A standard value of 0.95 was used (Sandia National Laboratories in the USA).

Probability of Detection values: It was based on the availability and non-availabilty of cameras or sensors on the adversary intrusion paths.

Delay time: The delay time values were obtained by measuring the time taken for an adversary to travel a given path to the target (radiation source).

Response force time: The response force time values were obtained by measuring the time taken for the response force to halt the progress of adversary activity. The actual value for the response force time and the delay time were obtained from the average value of 30 data points taken for the response force time and the adversary delay time.

- Development of adversary intrusion path sequence diagram.

This section was based on complete knowledge of the radiotherapy facility and reasonable assumptions about the intrusion paths the adversary will take to access the facility. The security elements along the various intrusion paths were also taken in account. The main asset within the oncology facility was a Cobalt-60 teletherapy machine. The various intrusion paths for sabotaging and/or theft of the Cobalt-60 source are depicted in figure 2.

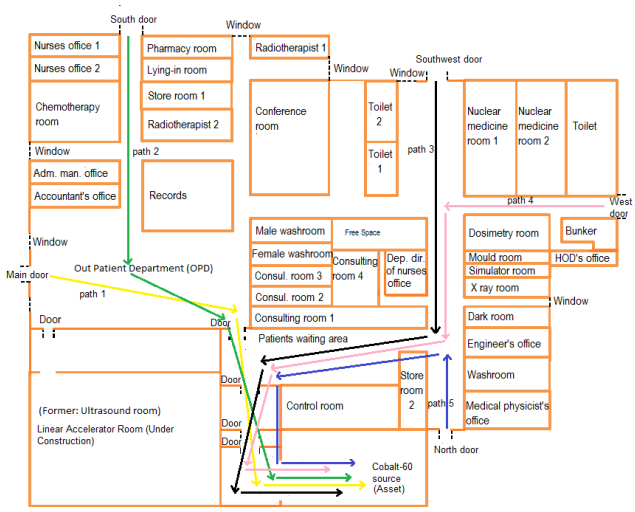

Figure 2. Adversary intrusion paths to sabotage the Cobalt-60 source.

- Prediction of the probability of interruption using the Estimate of Adversary Sequence

Interruption (EASI) model.

The EASI model was then applied to estimate the probability of intercepting adversary activities by varying the physical protection functions along a particular intrusion path.

- Finding the protection effectiveness of the security elements.

The effectiveness of the security elements were estimated by the level of protection capabilities of the physical protection elements to moderates the vulnerability of the security system. Suppose a security element has n-factors for a known protection task. The probability is 1 if theprotection task is successful and is 0 if the task is unsuccessful. The ratio of m factors on a security element can be expressed as Ri; where i = 1, 2, 3..., n, the weight of each factor is given as wi; where i = 1, 2, 3..., n. For a particular task, the protection effectiveness of one security element j can be estimated as [8]:

$$U_j = \sum_{i=1}^{n\sum\frac{1}{1-R_i}} w_i log \qquad (2)$$

Where j = 1, 2, 3…, m and i = 1, 2, 3..., n. Uj is the protection effectiveness of unit j, Ri = Probabilities of i (i=detection, delay or response), 1 - Ri is the degree of failure to achieve protection task of factor i, wi denotes the effect weight of factor-i, and is given as:

$$w_i = R_i / \sum_{i=1}^{n} R_i \qquad (3)$$

- Finding the protection effectiveness of the adversary intrusion paths.

The higher the performance of a security element protection, the greater the cost an adversary must pay to overcome it, so we characterize unit cost as theestimation of security element

adequacy. The estimation of unit cost is expressed as C(Uj) (j = 1, 2, 3…, m) is proportional to the unit effectiveness C(Uj) = Uj (j = 1, 2, 3..., m). The estimation of the path cost is equivalent to the aggregate of unit costs which is given as:

C(Path (U1, U2, U3… ,Ui)) = C(U1) + C(U2) + C(U3) + … + C(Ui) (4)

where i = 1, 2, 3…, k

- Assessment of the risk and if necessary revise the assumptions, operations and design of the facility.

The worst scenario of the state of a physical protection system is a clever adversary who can find the weakest paths to the asset(s) and decimate it. The most vulnerable adversary path is the lowest cost of intrusion paths for the asset(s). Hence, the protection effectiveness for the asset(s) is given as:

E(Asset) = Min(C(Path1), C(Path2),…, C(Pathn)) (5)

The estimation of risk of the physical protection system (security systems) can be expressed as follows, with respect to the risk definition of physical protection system that [9] proposed:

Risk = PA x Pr x C (6)

Where PA is the probability of attack against a critical asset, C is the consequence and Pr is the probability of successful attack. The two concepts in assessing the risk of the physical protection system can be expressed as:

$$P_r = \exp^{E(Asset)} \quad (7)$$

II. Results and Discussion

A. Results of the Threat Assessment of the Cobalt-60 Radioactive Source

In assessing the Cobalt-60 teletherapy machine, the current source activity was found to be 80.35 TBq with a risk factor (Df) of 2678.3 as shown in table 1. The risk factor was very highand the danger associated with the radioactive source is considered to be extremely hazardous and could cause permanent damage or death to a person who handles it or touch it for more than a couple of minutes. An evaluation of the risk factor of the radioactive source in the KATH radiotherapy revealed that the nature and form of the Cobalt-60 source is such that it could be dispersed with ease through an explosion or other destructive devices when assessment was conducted on the probable consequences of illicit acquisition of the Cobalt-60 source from the radiotherapy facility. In view of this, a specific design basis threat was made on the current physical protection systems to upgrade it based on the vulnerabilities of the physical protection systems. This was to keep the radioactive source away from insider adversary, an outsider adversary assisted by an insider or an outsider adversary (that is people who enter the facility as visitors, patients or contractors).

Table 1: Showing the activity and risk factor of the radioactive source at the radiotherapy facility.

Activity (TBq)	Risk factor (D_f)	Associated risk
80.35	2678.3	This amount of radioactive material is considered to be hazardous and could cause fatal injury to persons who come in contact with it or handle it if not managed safely and securely.

B. Results of the Current State of the Physical Protection System (PPS) at the Radiotherapy Facility

Table 2 and 3 depicts the current state of the PPS of the radiotherapy facility and the estimated probability of interruption. From the evaluation of the security systems, it took an adversary a total time of 191 seconds for path 1 and path 2 and 189 seconds for path 3, path 4 and Path 5 to sabotage the asset; which was less than the time of 600 seconds taken by the nearby response force team to provide initial denial before the adversary removes the shield protecting the radioactive material and along the line bring to a halt the operation of the teletherapy unit. However, the response team would be able to provide some level of final denial and consequently escape denial since it will take the adversary an additional 600 seconds to dismantle the teletherapy machine. The probability of interruption of 0.427500000 by the response force team to neutralize the malicious act was below the medium range of 0.50 to 0.70 for physical protection systems [10]. This is because the PPS ability to provide immediate detection of any unauthorized access to vital areas was very low despite some level of low to medium denial in the initial stage of the intrusion. This indicates that in general the PPS failed to produce enough resources to protect its radioactive source. Considering an insider, it was impossible for the response force team at KATH to respond in time to achieve an initial denial position. Also, there is no reasonable chance they would achieve a final and escape denial position especially if the adversary has the necessary knowledge and skills to deactivate the teletherapy machine on time. This is an inherent problem when dealing with insider threat, as they tend to have at least some level of access to vital areas of the facility; in this way bypassing procedures for search, or simply circumventing physical protection or access control. Considering an outsider adversary, it was again impossible the KATH response force team would respond in time to achieve an initial denial position, especially if the adversary is assisted by an insider. Achieving a final denial position is also highly unlikely since the adversary has an insider for assistance. Escape denial is

also impossible even if the response force team took the maximum expected response time of 300 seconds; they are still not able to provide escape denial. Considering an outsider adversary, again the KATH personnel would not be able to provide initial denial. However, if the adversary does not have any technical skills to deactivate the teletherapy machine within the facility, there is a low-medium (43%) chance the response force team would be able to respond in time to provide final denial and in turn escape denial if they have prior knowledge of the intended target, which is very likely in this case. Hence, an insider or an outsider assisted by insider adversary would succeed in sabotaging the asset and use it for malicious purpose. For an outsider adversary who has no skills, knowledge and unauthorized access to the facility or the radioactive source would fail in using the radioactive source for malicious purposes but sabotaging the target would be successful since escape denial does not prevent sabotage and consequently the adversary will achieve his or her objective if it is to sabotage.

Table 2: The estimated probability of interruption for the proposed PPS of the KATH radiotherapy facility for path 1 and 2 to the teletherapy machine.

Estimate of Adversary Sequence Interruption	**Probability of Guard Communication 0.95**		**Response Force Time (s) Mean 600**	**Standard Deviation 180**
			Delays (in Seconds):	
Description	P(Detection)	Location	Mean:	Standard Deviation
Break oncology fence	0	B	6	1.8
Move to oncology center door	0	B	15	4.5
Break door to the oncology center	0	B	20	6
Move to door to the patient waiting area	0	B	4	1.2
Break door to the patient waiting area	0	B	20	6
Move to door to the control room	0	B	3	0.9
Break door to the control room	0	B	30	9
Move to 1st door to the target	0	B	2	0.6
Break 1st door to the target	0	B	30	9
Move to 2nd door to the target	0	B	1	0.3
Break 2nd door to the target	0	B	60	18
Sabotage the target	0.9	B	600	180
Probability of Interruption:	0.427500000			

able 3: The estimated probability of interruption for the proposed PPS of the KATH radiotherapy facility for path 3, 4 and 5 to the teletherapy machine.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication 0.95		Response Force Time (s) Mean 600	Standard Deviation 180
			Delays (in Seconds):	
Description	P(Detection)	Location	Mean:	Standard Deviation
Break oncology fence	0	B	6	1.8
Move to oncology center door	0	B	25	7.5
Break door to the oncology center	0	B	20	6
Move to door to the control room	0	B	15	4.5
Break door to the control room	0	B	30	9
Move to 1st door to the target	0	B	2	0.6
Break 1st door to the target	0	B	30	9
Move to 2nd door to the target	0	B	1	0.3
Break 2nd door to the target	0	B	60	18
Sabotage the target	0.9	B	600	180
Probability of Interruption:	0.427500000			

C. *Proposed Physical Protection System and Design Criteria*

In upgrading the PPS, an element-based design and a performance-based design were considered to defeat the following adversary acts: radiological sabotage or unauthorized removal through direct physical attack or covert access that could cause radiological consequences by a determined violent external assault or attack by stealth or deceptive actions. Based on the worst-case scenario of the threat in figure 3, a proposed PPS was outlined to defeat the adversary. This system integrates 3 important physical protection functions (detection, delay and response) which have the ability to provide in-depth and balanced protection. The security system was useful in two protection zones (zone 1 and zone 2) within the facility. Zone 1 is from the exits of the facility to the Out Patient Department (OPD)/patient waiting area and zone 2is from the control room to the radioactive source room (vital areas).

1) ***Detection Function:*** The effectiveness of the detection function is based on the probability of sensing adversaryactivity;the time needed to report and evaluate the alarm and the nuisancealarm rate [11]. This suggested security system will provide balanced and in- depth physical protection.

- Zone 1: Glass break sensors, Duress button and Cameras. These physical functions are connected to alarm assessment for all cameras and sensors and also connected to video monitors and sirens in two positions (the security room within the facility and the response force office outside the facility).
- Zone 2: Vibration sensor, Balanced magnetic door, Duress button, Dialer and cameras. All cameras in the radiotherapy are connected to a CCTV to assess an unauthorized entry. CCTV is also located throughout the vital areas and rooms to assess unauthorized activities.

2) ***Delay Function:*** The effectiveness of the delay function is based on its ability to slow down adversary progress by increasing the time needed by an adversary (after detection) to bypass each delay element [12]. An effective delay system consists of two key elements:

1) ***Physical Barriers:***

- Zone 1: Hardened doors in the 5 entrances, keypad password lock for the three doors (the southwest, west and the north door), hard steel on the windows.
- Zone 2: Hardened and highly secured password lock for 1st and 2nd door to the asset and hardened door with key control for the other doors.

2) ***Protective Force:***

- Two trained security guards should be available at the radiotherapy facility to patrol closed doors.
- Two trained computer experts to be available at the radiotherapy facility for quick communication evaluation and response to any adversary threat.

3) ***Response:*** The effectiveness of the response function is based on the actions of the response force to stop adversaries from accomplishing their mission. This involves interrupting adversary's activities to halttheir progress in carrying out malevolent act. The effectiveness of the response function is the likelihood of deployment at the adversary zone and the time between receipt of a communication of adversary activity and the interception of the adversary activity [10]. The effectiveness of the response function may be implemented through the following process:

- Memorandum of Understanding (MOU) should be developed between security guards and response force team.
- Effective training of security guards and response force team.
- Implementation of authorized security devices to detect and respond quickly to adversary actions.
- Documentation of all procedures.

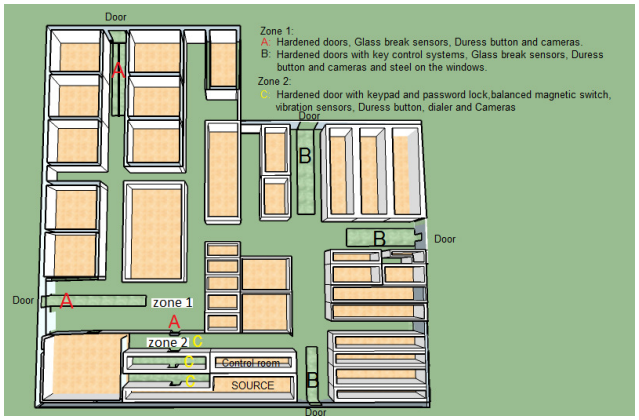

Figure 3. Suggested access with their locations in the radiotherapy facility.

D. *Result of the Upgraded Physical Protection Systems for the Radioactive Source using the Estimated Adversary Sequence Interruption(EASI) Model*

Using figure 3, the various intrusion paths to sabotage the teletherapy machine by an adversary is indicated. The likelihood of detection values, measured delay and response force time values, detector location and the estimated probability of interruption for path 1, path 2, path 3, path 4 and path 5 are indicated in table 4, 5, 6, 7 and 8 respectively. The probability of intercepting the adversary before any sabotage or theft of the teletherapy machine occur was 0.949999133 for path 1, 0.949999690 for path 2, 0.949997580 for path 3, 0.949997513 for path 4 and 0.949997079 for path 5. These values showed that the security systems are high enough and there is low risk for the radioactive source since the probabilities of interruption were higher than the medium range of 0.50-0.75 for physical protection systems [10]. These upgraded systems provide enough resources to protect the radioactive source and would be difficult for an adversary to sabotage it. Approximating from the EASI model, there is a high (95%) chance the security personnel would have the capacity to respond in time to provide initial denial, final denial and in turn escape denial. Hence, an outsider, an insider or an outsider assisted by insider adversary would not succeed in sabotaging the asset and use it for malicious purpose. Therefore, the adversary will not achieve his or her objectives whether it being sabotage or theft.

Table 4: The estimated probability of interruption for the proposed PPS of the KATH radiotherapy facility for path 1 to the teletherapy machine.

Estimate of Adversary Sequence Interruption	**Probability of Guard Communication 0.95**		**Response Force Time (s) Mean 300**	**Standard Deviation 90**
			Delays (in Seconds):	
Description	**P(Detection)**	**Location**	**Mean:**	**Standard Deviation**
Break oncology fence	0.2	B	6	1.8
Move to oncology center door	0.2	B	15	4.5
Break main door to the oncology center	0.7	B	180	54
Move to door to the patient waiting area	0.2	B	4	1.2
Break door to the patient waiting area	0.9	B	180	54
Move to door to the control room	0.9	B	3	0.9
Break door to the control room	0.9	B	180	54
Move to 1st door to the target	0.9	B	2	0.6
Break 1st door to the target	0.9	B	180	54
Move to 2nd door to the target	0.9	B	1	0.3
Break 2nd door to the target	0.9	B	240	72
Sabotage the target	0.9	B	600	180
Probability of Interruption:	0.949999133			

Table 5: The estimated probability of interruption for the proposed PPS of the KATH radiotherapy facility for path 2 to the teletherapy machine.

Estimate of Adversary Sequence Interruption	**Probability of Guard Communication 0.95**		**Response Force Time (s) Mean 300**	**Standard Deviation 90**
			Delays (in Seconds):	
Description	**P(Detection)**	**Location**	**Mean:**	**Standard Deviation**
Break oncology fence	0.2	B	6	1.8
Move to oncology center door	0.2	B	17	5.1
Break south door to the oncology center	0.9	B	180	54
Move to door to the patient waiting area	0.2	B	12	3.6
Break door to the patient waiting area	0.9	B	180	54
Move to door to the control room	0.9	B	3	0.9
Break door to the control room	0.9	B	180	54
Move to 1st door to the target	0.9	B	2	0.6
Break 1st door to the target	0.9	B	180	54
Move to 2nd door to the target	0.9	B	1	0.3
Break 2nd door to the target	0.9	B	240	72
Sabotage the target	0.9	B	600	180
Probability of Interruption:	0.949999690			

Table 6: The estimated probability of interruption for the proposed PPS of the KATH radiotherapy facility for path 3 to the teletherapy machine.

Estimate of Adversary Sequence Interruption	**Probability of Guard Communication 0.95**		**Response Force Time (s) Mean 300**	**Standard Deviation 90**
			Delays (in Seconds):	
Description	**P(Detection)**	**Location**	**Mean:**	**Standard Deviation**
Break oncology fence	0.2	B	6	1.8
Move to oncology center door	0.2	B	20	6
Break southwest door to the oncology center	0.9	B	180	54
Move to door to the control room	0.9	B	28	8.4
Break door to the control room	0.9	B	180	54
Move to 1st door to the target	0.9	B	2	0.6
Break 1st door to the target	0.9	B	180	54
Move to 2nd door to the target	0.9	B	1	0.3
Break 2nd door to the target	0.9	B	240	72
Sabotage the target	0.9	B	600	180
Probability of Interruption:	0.949997580			

Table 7: The estimated probability of interruption for the proposed PPS of the KATH radiotherapy facility for path 4 to the teletherapy machine.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication 0.95		Response Force Time (s) Mean 300	Standard Deviation 90
			Delays (in Seconds):	
Description	P(Detection)	Location	Mean:	Standard Deviation
Break oncology fence	0.2	B	6	1.8
Move to oncology center door	0.2	B	22	6.6
Break west door to the oncology center	0.9	B	180	54
Move to door to the control room	0.9	B	26	7.8
Break door to the control room	0.9	B	180	54
Move to 1st door to the target	0.9	B	2	0.6
Break 1st door to the target	0.9	B	180	54
Move to 2nd door to the target	0.9	B	1	0.3
Break 2nd door to the target	0.9	B	240	72
Sabotage the target	0.9	B	600	180
Probability of Interruption:	0.949997513			

Table 8: The estimated probability of interruption for the proposed PPS of the KATH radiotherapy facility for path 5 to the teletherapy machine.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication 0.95		Response Force Time (s) Mean 300	Standard Deviation 90
			Delays (in Seconds):	
Description	P(Detection)	Location	Mean:	Standard Deviation
Break oncology fence	0.2	B	6	1.8
Move to oncology center door	0.2	B	25	7.5
Break north door to the oncology center	0.9	B	180	54
Move to door to the control room	0.9	B	15	4.5
Break door to the control room	0.9	B	180	54
Move to 1st door to the target	0.9	B	2	0.6
Break 1st door to the target	0.9	B	180	54
Move to 2nd door to the target	0.9	B	1	0.3
Break 2nd door to the target	0.9	B	240	72
Sabotage the target	0.9	B	600	180
Probability of Interruption:	0.949997079			

From the estimated adversary sequence of interruption models, it took an adversary more than 300 seconds to sabotage the target (teletherapy machine). The values were greater than the time of 300 seconds taken by the nearby response force team to provide initial denial before the adversary starts to remove the radioactive material from the teletherapy unit as shown in table 4, 5, 6, 7 and 8. This indicates that it is very likely that the security personnel would intercept the adversary with the conceivable time of the 300 seconds. Initial denial would be provided before the adversary tries to remove the shield guarding the radioactive source and along causing the release of

radioactive material in the environment. Considering an insider, there is a high chance of providing an initial denial position as well as an excellent one of providing final denial, where an above average or better response time was sufficed. Escape denial is consequently very possible. For an assisted outsider, there is a high chance for the response team to achieve an initial denial position. Final denial is also much more likely to occur, because detection is early and the probability of interruption was above average. It was also similar for escape denial. The high probability of interruption would not allow theadversary to escape. For an outsider, the chance of the response force team providing final denial andescape denial isalmostcertain. Initial denial is also very likely, with the point of initial denial being detected early and responded before the adversary could penetrate the facility.

E. Results of the Physical Protection System Effectiveness using the Dai et al Model

From figure 3, there are five adversary intrusion paths to access the teletherapy machine in the radiotherapy facility. These intrusion paths are infiltration of the adversary through the main door, the south door, the southwest door, the west door and the north door. Table 9 depicts the various possible adversary paths an adversary may take to attack or sabotage the teletherapy machine.

Table 9: The protection elements of each intrusion path

Intrusion Path	Protection Elements					
Path 1 for Asset 1	Oncology fence	Main door	P.W.A door	Control room door	1st door to target	2nd door to target
Path 2 for Asset 1	Oncology fence	South door	P.W.A door	Control room door	1st door to target	2nd door to target
Path 3 for Asset 1	Oncology fence	South west door	Control room door	1st door to target	2nd door to target	-
Path 4 for Asset 1	Oncology fence	West door	Control room door	1st door to target	2nd door to target	-
Path 5 for Asset 1	Oncology fence	North door	Control room door	1st door to target	2nd door to target	-

The effectiveness of each of the physical protection element was estimated using equation 2 and shown in table 10. The North door and the 2nd door to the radioactive source showed the highest effectiveness with a value of 0.916680701. The effectiveness of the North door and the 1st doorto the asset were above the medium range of 0.50 to 0.70 for physical protection systems [10] and the probability of it preventing an adversary intrusion is very high. On the other hand, the oncology fence showed the lowest effectiveness with a value of 0.122815650. The effectiveness was below the medium security element range and the probability of it preventing an adversary intrusion is very low.

Table 10: Effectiveness of Each of the Security Element

Element	Detection (i=1)	Delay (i=2)	Response (i=3)	Effectiveness
Oncology fence	0.2	0.2	0.3	0.122815650
Main entrance door	0.7	0.2	0.2	0.369530002
South entrance door	0.9	0.3	0.5	0.645181052
Southwest entrance door	0.9	0.8	0.7	0.762294938
West entrance door	0.9	0.8	0.8	0.807340803
North entrance door	0.9	0.9	0.8	0.916680701
P.W.A door	0.9	0.3	0.2	0.686096813
Control room door	0.9	0.8	0.8	0.807340803
2nd door to target 1	0.9	0.4	0.4	0.636487400
1st door to target 1	0.9	0.9	0.8	0.916680701

Table 11 depicts the strength of the security systems for each of the intrusion paths. The effectiveness of each of the intrusion paths was estimated utilizing equation 4 and the outcome is shown in table 11. Path one (1) and path three (3) to the teletherapy machine showed the maximumand minimum effectiveness with a value of 3.888494371 and 3.245619492 respectively. This result indicates that the effectiveness of the security systems were high and the probability of successful attack on the asset is minimal with values of 0.020476152 and 0.038944431 for Path one (1) and path three (3) respectively. The higher the effectiveness of the intrusion path; the longer the time it will take an adversary or attacker to be successful in sabotaging the radioactive source. The probability of attack on the asset was below one (1) for the attack to be successful. From equation 5, the security system with the weakest path to the asset has effectiveness of 3.245619492. Assuming the yearly occurrence of an attack and consequences for the teletherapy machine to be 0.5 and 0.8 respectively; then

the calculated risk for the physical protection system in place is 0.015577772 using equation 6 and 7.

Table 11: Effectiveness of Each Intrusion Path

Adversary Intrusion Path	Effectiveness
Path one (1) for asset one (1)	3.538951369
Path two (2) for asset one (1)	3.814602419
Path three (3) for asset one (1)	3.245619492
Path four (4) for asset one (1)	3.290665357
Path five (5) for asset one (1)	3.400005255

III.CONCLUSIONS

This study proposed a systematic and quantitative approach using information entropy to design security systems that protect a single asset with multiple intrusion paths in order to forestall the accomplishment of overt or covert malevolent actions. Four steps were employed in the effective evaluation for the security systems through quantitative approach and its corresponding risk. It used the concept of detection, followed by delay and response to propose and design a performance-based physical protection system which has the ability to defeat adversary activities.

The computerized EASI model and the Dai et al model were used to estimate the probability of interruption and the effectiveness of the PPS respectively at the oncology center for a single protected asset with multiple intrusion paths. The probabilities of interruption for the security systems using the EASI model were 0.949999133, 0.949999690, 0.949997580, 0.949997513 and 0.949997079 for path 1, path 2, path 3, path 4 and path 5 respectively. The probabilities of interruption were higher than the medium range of 0.50 to 0.70 for physical protection systems [10]. The system's effectiveness based on the Dai et al model for the asset was 3.888494371 for path 1, 3.814602419 for path 2, 3.245619492 for path 3, 3.290665357 for path 4 and 3.400005255 for path 5. The risk associated the PPS was found to be 0.015577772.The outcome revealed that the security systems are very high with low associated risk for the radioactive source. Due to the high probability of interruption and effectiveness of the intrusion paths; these methods used in this work will assist decision maker to make quantitative risk assessment for security systems protecting a single asset with multiple intrusion paths in medical and nuclear facilities in the near future.

ACKNOWLEDGMENT

The authors express their thanks to the Komfo Anokye Teaching Hospitalstaff for their cooperation and support to perform this research.

REFERENCES

[1] IAEA (2002). Inadequate control of world's radioactive sources. Press release PR 2002/09. Vienna: International Atomic Energy Agency; June 25, 2002.

[2] ICT (2003). Al-Qaida Supporters Threaten Nuclear Attacks. Herzliya, Israel: International Policy Institute for Counter-Terrorism, Interdisciplinary Center at Herzliya, Israel; January 10, 2003.

[3] Omotoso, O; Aderinto A. A (2012). Assessing the Performance of Corporate Private Security Organizations in Crime Prevention in Lagos State, Nigeria, Journal of Physical Security Vol.6:1, pp.73- 90.

[4] Sun, Y., Li, B., and Li, S. (2009). Quantitative evaluation of physical protection system in nuclear power plant. Nuclear Power Engineering, 30(1):20–25.

[5] Chen, Z.H. Research and practice of effectiveness evaluation of security system (in Chinese). China Security & Protection 2007, 11, 16–20.

[6] IAEA (2003). Emergency preparedness and response method for developing arrangements for response to a nuclear or radiological emergency updating iaeatecdoc-953.

[7] IAEA (2003). Tecdoc-1344 categorization of radioactive sources revision of iaea-tecdoc-1191, categorization of radiation sources July 2003.

[8] *Dai, J., Hu, R., Chen, J., and Cai, Q. (2012). Benefit-cost analysis of security systems for multiple protected assets based on information entropy. Entropy, 14(3):571–580.*

[9] Hicks, M., Snell, M., Sandoval, J., and Potter, C. (1998). Cost and performance analysis of physical protection systems-a case study. In Security Technology, 1998. Proceedings., 32nd Annual 1998 International Carnahan Conference on, pages 79–84. IEEE.

[10] Garcia, M. L. (2007). The Design and Evaluation of Physical Protection Systems, Second edition, Sandia National Laboratories, pp. 1-375.

[11] IAEA (1999). Infcircl 225/ rev.4 corrected, "the physical protection of nuclear materials and nuclear facilities" June 1999.

[12] *IAEA (2003e). Tecdoc-1355 security of radioactive sources interim guidanceforcomment, June 2003.*

