Arab J. Nucl. Sci. Appl., Vol. 56, 2, 57-67 (2023)

10th African Conference on Research Reactor Safety, Operation & Utilization, Cairo (Egypt) 27 to 29 Nov. 2022

ISSN 1110-0451

Arab Journal of Nuclear Sciences and Applications

Web site: ajnsa.journals.ekb.eg

IAEA

Using Systematic Analysis for Stealth Elements Against Intrusion of Research Reactors

A. A.Wadoud[1*], S.S.Hussein[2], Nehal Ali[3],

(1) *Egyptian Atomic Energy Authority, Reactors Department, P.O. Box 13759*
(2) *Egyptian Nuclear Power Plant Authority, Abbasia, P.O. Box: 108*
(3) *Faculty of Engineering, Tanta University, Tanta, Egypt*

ARTICLE INFO

Article history:

Received: 26th Oct. 2022

Accepted: 7th Jan. 2023

Keywords:

Systematic Analysis;
Stealth Elements;
SAVI Module;
Physical Protection Evaluation;
Intrusion Detection.

ABSTRACT

Many of the nuclear and radiological facilities have Physical Security System (PSS). It has been installed from long time; the security systems include many different types of cluster sensors, components and control devices. It should keep the security system component valid and updated, and follows procedures, rules and requirements of the Nuclear Regulatory Authority at the national level and meets IAEA concept and recommendations at the international level. The Evaluation of the PSS efficiency is very necessary requirements, and should be determined. This paper introduces a Hypothetical Nuclear Site for PSS analysis and evaluation process. The work developed an analytical methodology for the evaluation. The Systematic Analysis of Vulnerability to Intrusion (SAVI) computer program is used in PSS evaluation. SAVI determines the most vulnerable paths of an adversary sequence diagram as a measure of effectiveness. The paper determines the vulnerabilities and threat of some physical protection element on the nuclear site and calculates the system win probability. This work explains; the adversary scenario for the most vulnerable path and determine the PSS effectiveness. Each of Time remaining after interruption, and cumulative path delay after critical detection point will be calculated. SAVI Outsider module enables the likelihood of attack interruption to be calculated &finds the set of the most vulnerable 10th worst paths. This work will serve as base guidelines for the decision makers, the application, and evaluation of PSS and provision of counter measure strategies in the nuclear energy facilities

1. INTRODUCTION

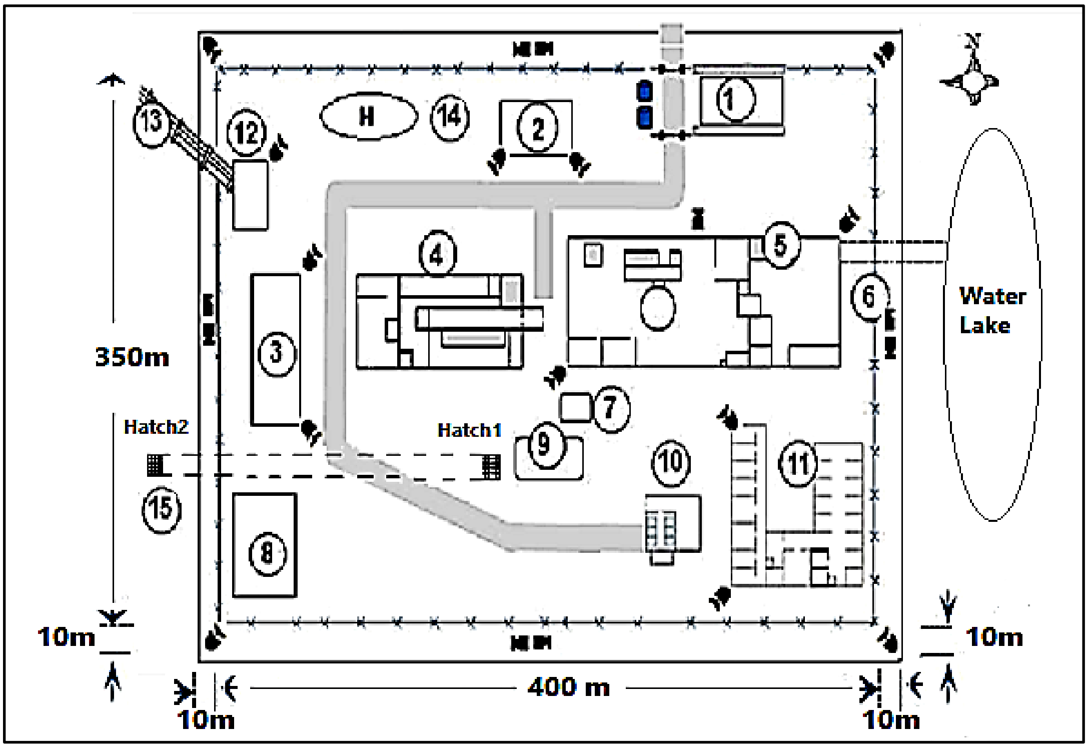
The physical protection system is designed to defeat any theft or sabotage actions carried out by one or more persons from outside or inside the site. This paper introduces a Hypothetical Atomic Research Institute (HARI) for PPS analysis and evaluation process [1].

1.1 Hypothetical Atomic Research Institute (HARI) Description

HARI complex was established by Sandia National Laboratory (SNL), USA, to serve as the State's premier nuclear energy research facility. HARI describes a hypothetical nuclear security program that meets the international recommendations for an institute with a 10 MW research reactor (RR), a radioisotope production facility (RPF), a low-enriched uranium fuel fabrication facility (FFF), Interim Storage Facility (ISF) and a waste treatment and storage facility (WPF) [1]. HARI complex is surrounded by1500 meters external double fences enclosed 10m isolation area, which considers the first delay barriers & it divided into two security areas: A limited Access Area (LAA) that includes administrative, general operations, staff training and shipping and receiving facilities, & a high-security Protected Area PA, which is the scope of the work.

Figure (1) shows HARI site general view. HARI security system includes; intrusion detection system, closed circuit television system, access control system, and alarm system and security control centers distributed over all the HARI [2].

Corresponding author: amirwadood@gmail.com
DOI: 10.21608/ajnsa.2022.170999.1655



[1] Central Alarm Station (CAS) [2] PA Admin Annex [3] Fuel Fabrication Facility (FFF) [4] Radioisotope Production Facility (RPF) [5] Research Reactor (RR) [6] PA Fence [7] Interim Storage Facility (ISF) [8] Waste Processing Facility

Fig. (1): HARI Site General View

1.2 Response Forces teams at HARI-Site

1st team is formed by post guards or watchmen, their number is 7 (three shifts)

2nd team is hard tower security guards equipped with pistol, and 4 hard towers equipped with Telephone lines that can communicate to any emergency place if the response forces not reply.

3rd team (Special Response Team) is composed of 10 members each member is military trained and have the authority to enter target locations to ensure the safety of critical assets and target materials, this team is located about 1000 m far from the R.R site and have an armed vehicle. They are equipped with an Automatic Rifle

HARI Site has two redundancy central alarm stations [6]

The Main Central Alarm Station (CAS): is located in the R.R building and it is staffed by a minimum of one security guard at all times this man is responsible for the assessment of alarms and communication to the response forces.

The secondary Central Alarm Station (SAS): is located in guard building and staffed by a minimum of one guard The average times are listed in Table (1).

Table (1): Average Times for Response Functions [10]

no	Descriptions	The R.R Times (sec)
1	Alarm communication Time	5 seconds
2	Alarm assessment Time	25 seconds
3	Communication time to guards, police, and military	25 seconds
4	Guard preparation time	15 seconds
5	Response force preparation time	60 seconds
6	Travel Time by vehicle	36 seconds
7	Travel Time by foot	500 seconds
8	On-site deployment time (after arrival)	100 seconds

2. PHYSICAL SECURITY SYSTEM EFFECTIVENESS

For Physical Protection Systems to be effective against sabotage threat, the response force must both interrupt and neutralization the adversary. Interruption means the response force deploys before the adversary mission is complete and in adequate numbers that the adversary must interrupt the mission and engage with the response force. Neutralization means that the response force stops or permanently interrupts the adversary, who either surrenders, attempts to flee, is captured, or killed. Both interruption and neutralization are necessary for the PSS to be effective [3].

2.1 Probability of Interruption (PI)

P_I is defined based on the principle of timely detection and a critical detection point for any adversary path. P_I is the cumulative probability of detection along the path up to the critical detection point (CDP). The CDP is the last PPS detection component along that path for which the response force time is less than the remaining adversary task completion time [4].

If there is one sensor on the path, this probability of interruption is calculated as:

$$P_I = P_C * P_D$$

Where: P_C: Probability of guard communication, **P_D:** Probability of detection. And,

The general formula for P_I [41]:

$$PI = P(D_1) \times P(C_1) \times P(R|A_1) + \sum_{i=2}^{n} P(D_i) \times P(C_i) \times P(R|A_i) \times \prod_{i=1}^{i-1} \left(1 - P(D_i)\right)$$

P(R/A): Probability of response force arrival prior to the end of the adversary's action sequence given an alarm [23].

$$P_{(R/A)} = \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \, exp\left[-\frac{(x-\mu x)2}{2\sigma^2}\right]$$

2.2 Probability of Neutralization (PN)

The probability of neutralization P_N is the probability, given interruption of the adversary by response forces, that the response force will gain complete physical control of the adversary force. Then the system effectiveness P_E along this path is defined as the product of these two probabilities, P_I and P_N. The overall PPS effectiveness is conservatively defined as the lowest P_E for all adversary paths [3].

3. PHYSICAL PROTECTION EVALUATION PROCESS

The physical security system effectiveness (P_E) along a specific path is defined as the product of two probabilities, P_I, which is calculated by SAVI model and P_N, which determined by the neutralization module, PE= P_I*P_N [3].

3.1 The Systematic Analysis of Vulnerability to Intrusion (SAVI)

SAVI is computer program used to evaluate the physical protection system's effectiveness. SAVI determines the most vulnerable paths of an adversary sequence diagram (ASD) as a measure of effectiveness. An analysis using SAVI begins with identifying a target and constructing a site-specific ASD for that target. Next, the characteristics of the threat must be specified. The response force deployment time, delay and detection values for each protection element on ASD must be defined. All of this information is used as input to the SAVI code. The code calculates the probability of interruption for each path on the ASD [1]. Features of SAVI include analysis of all adversary paths, a safeguards-component catalog with a detection/delay performance database, results in graphic form, and path-upgrade recommendations. Software of SAVI consists of two modules [4]

1. ***Facility Module;*** enables a facility in to be modeled from protective elements & spaces.
2. ***Outsider Module;*** enables the likelihood of attack interruption to be calculated &finds the set of the most vulnerable paths.

3.2 PI Calculation using SAVI Modules

a. HARI-site modeling:

SAVI employs an **ASD** diagram to model HARI-site and its physical security system. The ASD diagram includes designated areas and protection layers located on the HARI. The layers consist of protection elements and path segments which configure the adversary path element [1] Fig.4

b. Facility module:

The facility module is the tool to specify the facility and its physical security system, and enable the user to specify the classifications of each layer and protection element. In our work the HARI facility has 7 layers starting with the off-site layer which is the area outside the HARI, then the protected area, there are 6 protection elements between the out site and protected area (Personnel gate, Vehicle gate, Isolation zone, Cooling tunnel, Helicopter land base, and Electric duct) then the reactor ground level. There are 4 protection elements between the protected area and the reactor ground level (personnel gate, emergency gate, cooling duct which is coming from off-site layer, and the wall of the reactor building as a way to be penetrated to enter the reactor ground level, then the reactor level 1, 2, and 3 which have the same protection elements in between (Door, Window, Wall surface, and Elevator).Then the target area which is the reactor hall that contain the nuclear fuel [4], as shown in Fig.4. SAVI facility module used to specify the dimension, characteristics, safeguard and condition state of each protection element and the Dimensions of the layers. In addition, computation of delay time and probability of detection of all layers and areas will be specified and calculated by SAVI model,

3.3 The Adversary Path, characteristics and Tactics

The adversary beginning from the off-site and ending when locate his target (main tank of the reactor). Layers A, B, C, and D are the reactor levels floors (Levels 0, +1, +2, and +3). In the SAVI model, an adversary path consists of a sequence of areas and protection elements traversed by the adversary from offsite to the target and back offsite. SAVI considers all possible adversary paths in its analysis. Each path is transformed into a time line that consists of delay segments separated by detection points. In the ASD Diagram, the physical areas calculated as delay segments [11].

4. SAVI OUTSIDER MODULE

The outsider analysis (Outsider) module is part of the analytic system which output the results and adversary vulnerability of 10 worst paths upon the specification of the facility and its layers and protection elements [3]. First step is to characterize the adversary. Adversary attributes are defined as possession of metal (weapons and tools), explosives, and transportation (foot, truck, or helicopter). The mode of transportation determines the speed in which the area can be traversed in our facility 4m/seconds adversary speed selected [8]. The computation of delay time and probability of detection of all layers and areas must be specified and calculated by SAVI model. Adversary objective is specified either as theft or hands-on sabotage and corresponds to entry/exit or entry-only path analysis, respectively. Adversary tactics are either force-only or mixed, i.e., force and deceit. Deceit is defined as an adversary imitating an employee in protection elements with an authorized entry procedure [7]. As shown in Fig.3, which showed that the threat type is terrorist foot and the response strategy is Denial. For a denial strategy the adversary must be interrupted before completing tasks at the target, which is appropriate when protecting against sabotage or hand-on theft. For containment strategy, the adversary must be stopped before leaving the facility, which is appropriate to protect against theft. Table 2 shows the P_D and DT delay time of the protection element currently used [9] [12].

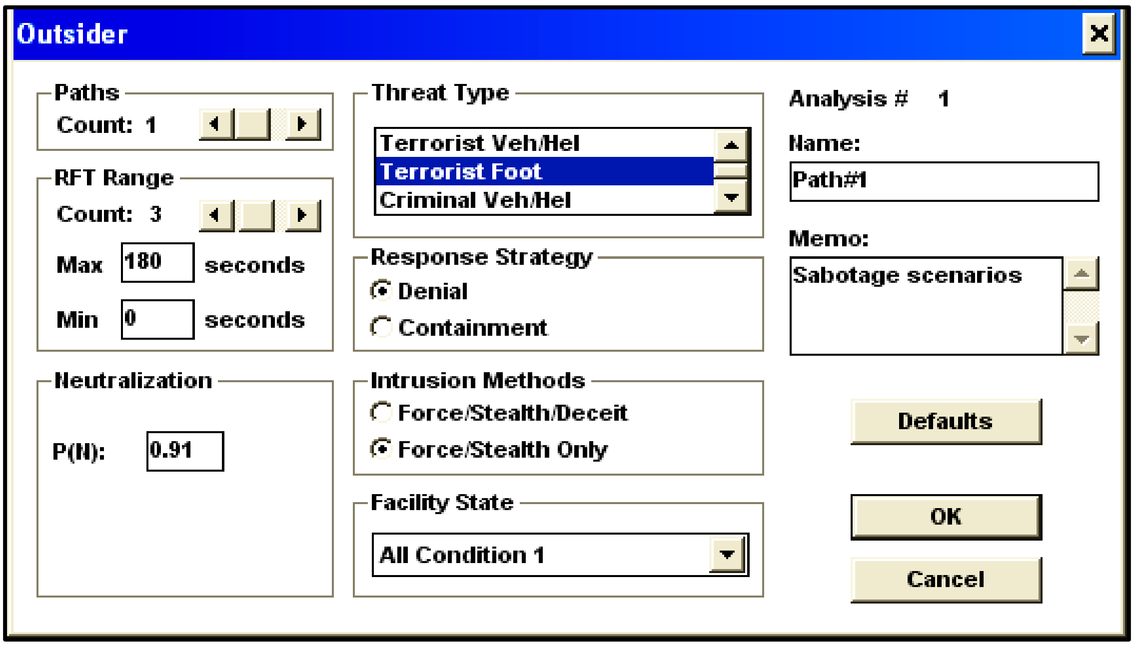


Fig. (2): Adversary Path, characteristics and Tactics

Table (2): The probability of detection and the delay time of the PSS protection elements

Area	Protection element	Type	Applied component	P_d	Delay time (sec)
Off-site to PA	PER	Dimensions	5 m	--	--
		Characteristics	CCTV with instance reply	0.60	--
		Passage	Persons-pedestrian		--
		Access Delay	Finger print and PIN	0.95	--
		Sec inspector	Inner- schedule	0.01	--
	VEH	Dimensions	20 m		--
		Characteristics	CCTV with instance reply	0.6	--
		Passage	VEH-Shipment		--
		Access Delay	Serial no verification	.45	--
		Intrusion detection	Micro wave Multi complimentary sensor Electric field	0.7 0.75 0.45	--
		Access Delay	VEH rollup Train barrier		108 1440
		Sec inspector	Duress LAW protected	0.8	--
	Cooling tunnel	Dimensions	200m-60cm diameter		--
		Characteristics	CCTV with instance reply	0.60	--
		Access Delay	12 inch filled rebar block 12 inch filled rebar block		900 900
	ISO isolation zone	Dimensions	10m		--
		Characteristics	CCTV with instance reply	0.60	--
		IDS	Micro wave Multiple sensor Personnel always in vicinity	0.70 0.50	-- -- 0.02
		Sec inspector	LAW resistance tower		0.05
	HEL	Dimensions	600m		--
		Characteristics	CCTV with instance reply	0.60	--
		IDS	Radar Multi complimentary sensor Electric field	0.50 0.75 0.45	--
		Access Delay	Min unload time Min Load time		15 15
		Sec inspector	Random	0.02	--
	Electric Duct	Dimensions	300m-90cm diameter		--
		Characteristics	No assessment		--
		Access Delay	High security pad lock		90
		IDS	Multi complimentary sensor	0.90	--
		Access Delay	Heavy Grid		720
PA-RR Ground level	EMX	Passage	Prohibited		--
		Characteristics	CCTV with instance reply	0.60	--
		Access Delay	Electronically coded		300
		Intrusion detection	Vibration BMS	0.90 0.80	--

		Access Delay	9 gauge wire mish		30
		Sec inspector	Duress unprotected LAW	0.80	--
	SUR	Dimensions	20cm wall		--
		Characteristics	CCTV with instance reply	0.60	--
		IDS	Outer Multi complimentary sensor Inner Multi complimentary sensor	0.95 0.95	--
		Access Delay	24 inch reinforced concrete		Inf
	PER Personal gate	Dimensions	5 m		--
		Characteristics	CCTV with instance reply	0.60	--
		Passage	Persons-pedestrian		--
		Access Delay	Finger print and PIN	.95	--
		Sec inspector	Inner- schedule	.01	--
	ventilation Duct	Dimensions	300m-90cm diameter		--
		Characteristics	No assessment		--
		Access Delay	High security pad lock		90
		IDS	Multi complimentary sensor	0.90	--
		Access Delay	Heavy Grid		720
RR Ground floor to Level#1	DOR door	Dimensions	0.3 m		--
		Characteristics	CCTV with instance reply	0.60	--
		Passage	Persons-pedestrian		--
		Access Delay	Finger print and PIN	.95	--
		Sec inspector	Inner- schedule	.01	--
	SUR surface	Dimensions	20cm wall		--
		Characteristics	CCTV with instance reply		--
		IDS	Outer Multi complimentary sensor Inner Multi complimentary sensor	0.95 0.95	--
		Access Delay	24 inch reinforced concrete		Inf
	SHD elevator	Dimensions	2 m		--
		Characteristics	CCTV with instance reply	0.60	--
		Passage	Persons-pedestrian		--
		Access Delay	Serial number verification	0.45	100
Level#1 to Level#2	DOR door	Dimensions	0.3 m		--
		Characteristics	CCTV with instance reply	0.60	--
		Passage	Persons-pedestrian		--
		Access Delay	Finger print and PIN	0.95	--
		Sec inspector	Inner- schedule	0.01	--
	SUR surface	Dimensions	20cm wall		--
		Characteristics	CCTV with instance reply	0.60	--
		IDS	Outer Multi complimentary sensor Inner Multi complimentary sensor	0.95 0.95	--
		Access Delay	24 inch reinforced concrete		Inf

	SHD Elevator	Dimensions	2 m		--
		Characteristics	CCTV with instance reply	0.60	--
		Passage	Persons-pedestrian		--
		Access Delay	Serial number verification	.45	--
Level#2 to Level#3	DOR door	Dimensions	0.3 m		--
		Characteristics	CCTV with instance reply	0.60	--
		Passage	Persons-pedestrian		--
		Access Delay	Finger print and PIN	.95	100
		Sec inspector	Inner- schedule	.01	--
	SUR surface	Dimensions	20cm wall		--
		Characteristics	CCTV with instance reply	0.60	--
		IDS	Outer Multi complimentary sensor Inner Multi complimentary sensor	0.95 0.95	--
		Access Delay	24 inch reinforced concrete		Inf
	SHD elevator	Dimensions	2 m		--
		Characteristics	CCTV with instance reply	0.60	--
		Passage	Persons-pedestrian		--
		Access Delay	Serial number verification	.45	100
Level#3 to RR Hall	DOR door	Dimensions	0.3 m		--
		Characteristics	CCTV with instance reply	0.60	--
		Passage	Persons-pedestrian		--
		Access Delay	Finger print and PIN	.95	100
		Sec inspector	Inner- schedule	.01	--
	SUR surface	Dimensions	20cm wall		--
		Characteristics	CCTV with instance reply	0.60	--
		IDS	Outer Multi complimentary sensor Inner Multi complimentary sensor	0.95 0.95	--
		Access Delay	24 inch reinforced concrete		Inf
	WND	Dimensions	60 m		--
		Characteristics	CCTV with instance reply	0.60	--
		Access Delay	Outer Combination Inner Combination		300 300
		Intrusion detection	Infrared	0.80	--
		Access Delay	9 gauge wire mish		30
Open Target	Open target fuel rods	Access Delay	Authorization verification Dedicated observation	0.60 0.95	100
		Characteristics	CCTV with instance reply	0.60	--
		IDS	Video motion sensor Personnel always in vicinity	0.50 0.02	--
		Access Delay	Wire secure with bolt		30
		Sec inspector	Duress unprotected LAW	0.45	--

4.1. Determination of Probability of Neutralization PN using Neutralization Module

The user should input the probability of neutralization as delivery information to the program. The probability of neutralization entered to SAVI determined by a neutralization module. The neutralization module consists of three parts [5]:

1st: the threats which defined the type of thread,

2nd: the guards which describe the type, number, weapons and guards delay time

3rd: the Result section which shows the output of the estimation of PN

The output value of the probability of neutralization PN is 0.99 as shown in Figure 3.

4.2 Outsider Module Output Results

After finishing the HARI-Site modeling, facility setting, and adversary characterize, and response forces data input information, we choose the number of paths and run the analysis from the control panel. After the analysis is finished, the outsider module analysis result shows the most ten vulnerable paths in the HARI PSS Figure (4) shows the scenario of the most vulnerable path could be use by the advisory to achieve his task, which is inter the protected area from the offsite through the cooling tunnel directly to the reactor building ground level then through the elevator will reach the reactor level#3 then the reactor area through the door then to the reactor pool (which is the sabotage target).

The control panel is used to select any path. And any editor information can be achieved and the output graphs (sensitivity, distribution and vulnerability) can be shown.

A detailed textual description of the path including intrusion methods and individual safeguard performance values is shown in the results window. The graphs window displays user selectable information about sets of paths, including a graph of the protection system's sensitivity to response force deployment time. Figure 4 shows the most vulnerable path (worst path) which is the path#1.

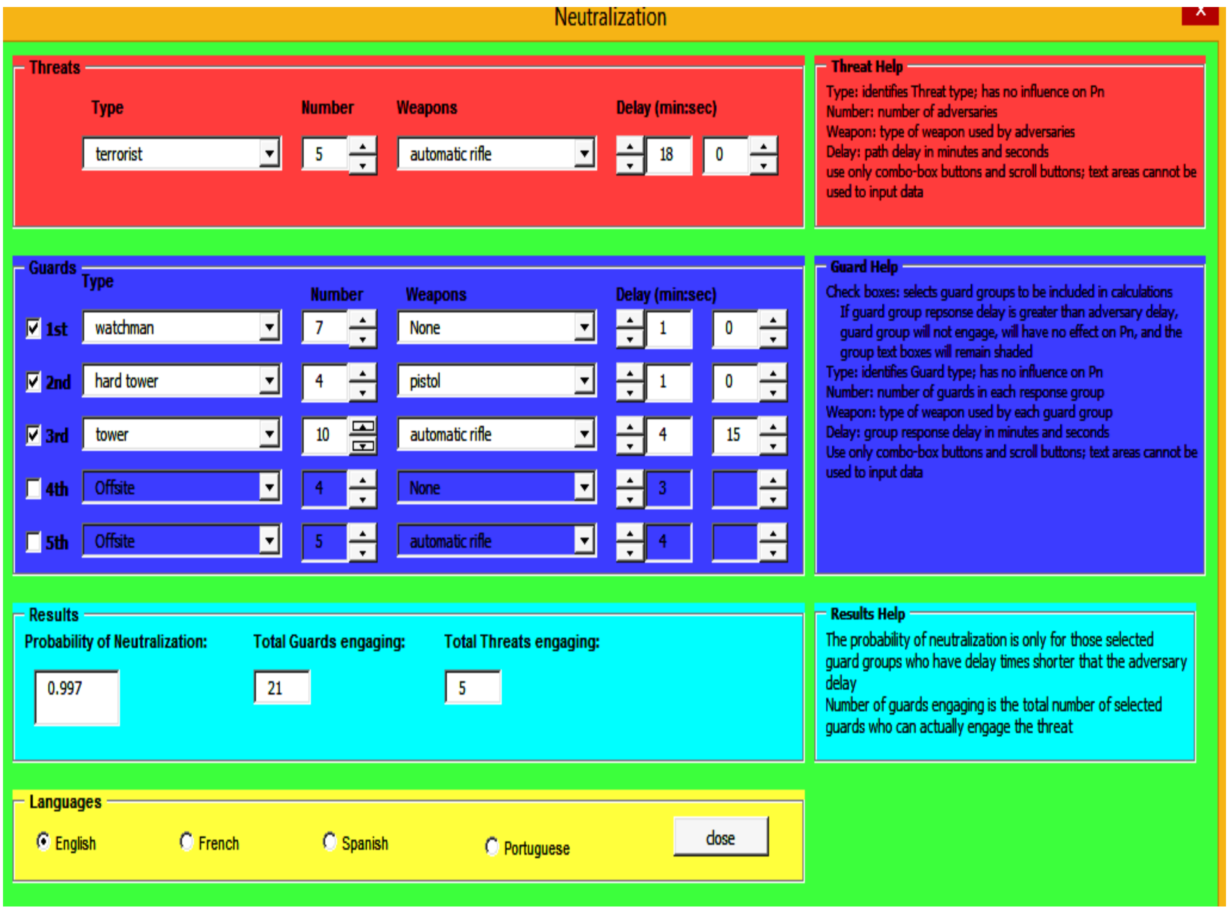


Fig. (3): The Neutralization Module for the HARI [5].

5. SAVI RESULTS: THE PHYSICAL PROTECTION SYSTEM EVALUATION

The SAVI outsider analysis result determined the most vulnerable path which is the path#1 shown in the figure (4). The computation of the probability of interruption, the probability of Neutralization and the system win probability as follow (see table.3):

- Probability of interruption is PI = 0.71.
- Probability of Neutralization is PN = 0.92.
- System win probability is P_W =0.66.
- Time remaining after interruption TRI=13 Seconds
- Detection potential (points) is =10 points along paths which is the points that the adversary supposed to be interrupted at these point through the ten vulnerable paths.

The effectiveness of the physical protection system P_E = P_I*P_N, in this case is = 0.66 which is the system potential that adversaries can be detected and assessed in sufficient time for security forces to intervene and neutralize them before they can seize or sabotage nuclear material. The SAVI evaluation of the current PPS showed that the probability of interruption is 0.71 which is Not Sufficient and although the probability of neutralization is quite high 0.92. The conclusion of this analysis is the PSS system should be upgrade. The outsider graph result As shown in figure (5), shows the relation between the probability of interruption Pi and the time remaining after interruption TRI before the system improving which was Pi = 0.71 for TRI = 110 sec.

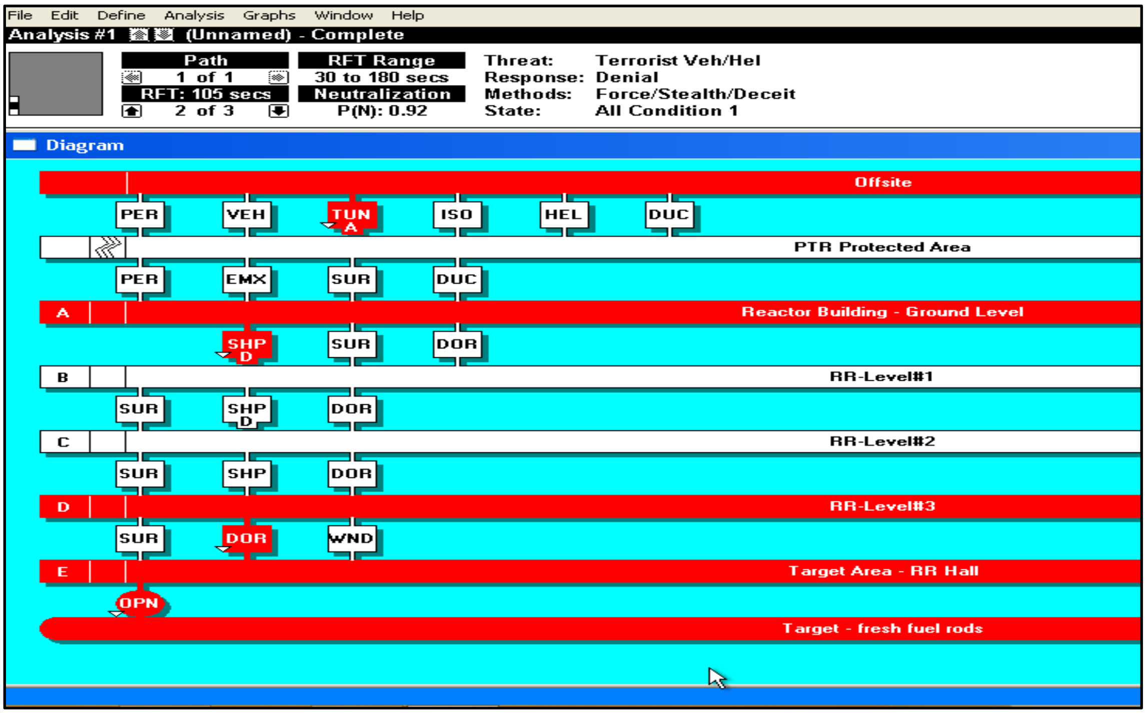


Fig. (4) the Most Vulnerable Path and Adversary Scenario

Table (3): the Outsider Analysis Result.

Results

Most Vulnerable Path
RFT - Response Force Time #1 (seconds): 45

P(I) - Interruption Probability: 0.7193
P(N) - Neutralization Probability: 0.9200
P(W) - System Win Probability: 0.6617

Detection Potential (points) : 13
TRI - Time Remaining after Interruption (seconds): 110

CDP - Critical Detection Point at Open Location - fuel rods in racks on Entry
Located in: Target Area - RR Hall

Cumulative Path Delay after CDP (seconds):155

ENTRY

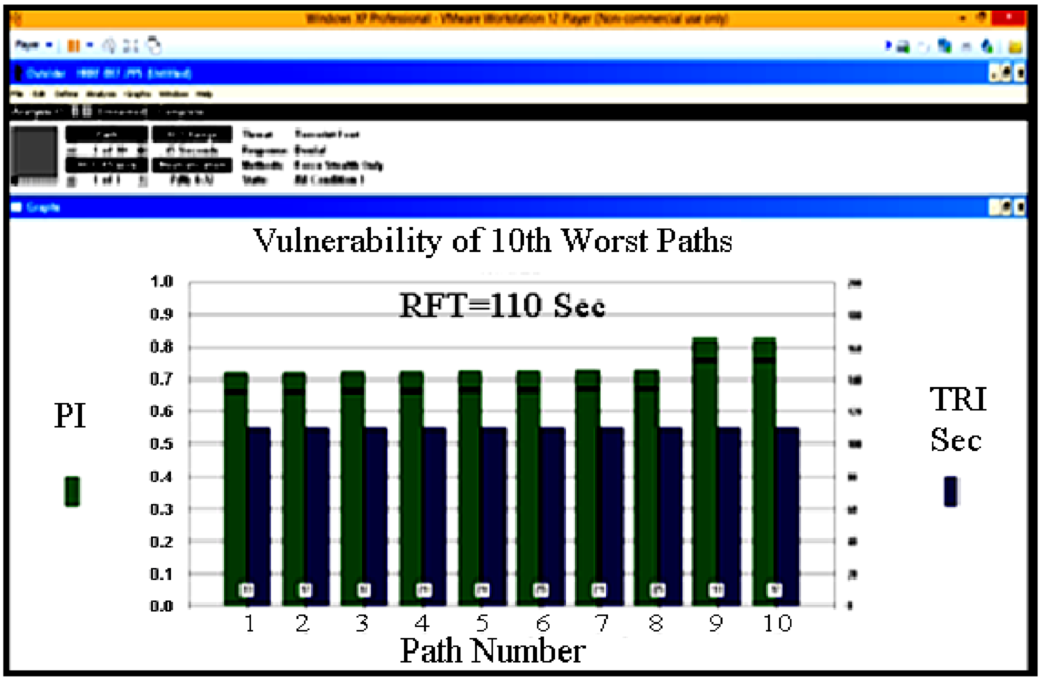


Fig. (5): the outsider analysis graph result of current PSS

6. CONCLUSION

The ultimate goal of a physical Security system (PSS) is to prevent the accomplishment of overt and covert malevolent actions. The Evaluation of the PSS efficiency is very necessary requirements, and should be determined. The Systematic Analysis of Vulnerability to Intrusion (SAVI) computer program is used in PSS evaluation. SAVI determines the most vulnerable paths of an adversary sequence diagram as a measure of effectiveness. The work, determines the vulnerabilities and threat of some physical protection element on the nuclear site. The work explain; the adversary scenario for the most vulnerable path and determine the physical protection system effectiveness. SAVI outsider analysis result determined the most vulnerable path and the computation of the probability of interruption, the probability of Neutralization and the system win probability, in this paper the results shows: The time remaining after interruption TRI=13 Seconds, and The detection potential (points) is =10 points along the paths which is the points that the adversary supposed to be interrupted at these point through the ten vulnerable paths, which is the system potential that adversaries can be detected and assessed in sufficient time for security forces to intervene and neutralize them before they can seize or sabotage nuclear material. The system effectiveness of the physical protection system, $P_E = P_I * P_N$, along the worst path was = 0.66 this depending upon, the probability of interruption is P_I =0.71 and the probability of Neutralization is PN = 0.92, the system win probability obtained is P_W =0.66. This work will serve as base guidelines for the decision makers for the application and evaluation of Physical Security systems (PSS) and provision of counter measure strategies in the nuclear energy facilities.

REFERENCES

[1] John C. Matter,"SAVI: A Pc-Based Vulnerability Assessment Program", Sandia National Laboratories, Albuquerque, New-Mexico 87185, July 1988.

[2] Hypothetical Atomic Research Institute (HARI) Hypothetical Facility Exercise Data Handbook, IAEA, .June, 2008

[3] Matter, J.C., SAVI: "A PC-Based Vulnerability Assessment Program", SAND88-1279, 1988.

[4] M. L. Garcia, Vulnerability Assessment of Physical Protection Systems. Burlington, MA: Elsevier Butterworth–Heinemann, 2006

[5] A. Abdel. Wadoud, "Developments of physical protection design tools in research reactors'' Doctor of philosophy of Engineering Science, (PhD.) Faculty of engineering, Al-Azhar University, 2009

[6] Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) January, 2011.

[7] Mary Lynn Garcia Butterworth-Heinemann, "Design and Evaluation of Physical Protection Systems", Second Edition, Sep 26, 2007.

[8] International Atomic Energy Agency, IAEA International Train the Trainers Course on the Physical Protection of Nuclear Material and Facilities. Ljubljana: Jozef Stefan Institute, 2010.

[9] A. E. Mansour and A. Abdel Wadoud, " Evaluation and Upgrading of Physical Protection System of a Hypothetical Nuclear Facility Sabotage Threat", Ninth International Conference, Faculty of Engineering, Al-Azhar University, Nasr City, Cairo, Egypt, 2007.

[10] Achumba, I.C. Ighomereho, O.S. Akpor-Robaro, M.O.M. "Security Challenges in Nigeria and the Implications for Business, Journal of Economics and Sustainable Development", Vol.4, No.2, 2013 pp.79-99. 2013.

[11] A. A. Wadoud, A. S. Adail, A. A. Saleh "Physical Protection Evaluation Process for Nuclear Facility via Sabotage Scenarios" Alexandria Engineering Journal, 2016

[12] A. A. Wadoud, S. Agamy1, H. A. Gabal, M. Trabelsi ''Physical Protection System Evaluation and Consequences Analysis at Research Reactor Facility via Sabotage Scenarios'' Journal of Electrical Engineering & Technology, Korea, 2019

[13] A. A. Wadoud IAEA'S Technical Support for Establishing Requirements for the security Up-Grades at Egypt's Research Reactor Complex "International Conference on Nuclear Security (ICONS2020), 10-14, February 2020 | IAEA, Vienna, Austria.