The development of multi-path adversary analysis tool for vulnerability assessment of physical protection systems (MAVA)

D Andiwijayakusuma[1,3,*], A Mardhi[1], T Setiadipura[1], A Purqon[2], and Z Su'ud[3]

[1]*Center for Nuclear Reactor Technology and Safety, Badan Tenaga Nuklir Nasional, Gedung 80 Kawasan PUSPIPTEK Serpong, South Tangerang, Banten 15310, Indonesia*

[2]*Earth Physics and Complex System Research Division, Department of Physics, Institut Teknologi Bandung Gedung Fisika, Jalan Ganesha 10, Bandung 40132, Indonesia*

[3]*Nuclear Physics and Bio Physics Research Division, Department of Physics, Institut Teknologi Bandung Gedung Fisika, Jalan Ganesha 10, Bandung 40132, Indonesia*

[*]*Email: riset.dinan@gmail.com*

Article Information:

Received:
10 August 2021

Received in revised form:
22 November 2021

Accepted:
5 December 2021

Volume 3, Issue 2, December 2021
pp. 71 – 79

`http://doi.org/10.23960/jesr.v3i2.92`

Abstract

The Physical Protection System (PPS) is an important component in each nuclear facility security aspect. We must regularly evaluate the effectiveness of PPS to ensure the system can anticipate every enemy attack; therefore, a PPS vulnerability assessment is needed. In this study, we develop a Multi-path Analysis tool for Vulnerability Assessment of PPS (MAVA) based on the Adversary Sequence Diagram (ASD) implemented in python computer code. We examined for feasibility by applying the code to a hypothetical facility (National Nuclear Research Facility - NNRF). The results of calculations compared to single-path analysis (EASI) show the advantages of MAVA, which can calculate the probability of interruption simultaneously on multi-path analysis. MAVA also predict the adversary's most vulnerable paths (MVP) with its various strategies for intrusion path. MAVA results show that multi-path calculations help analysts obtain information faster in evaluating to improve the effectiveness of PPS.

Keywords: *physical protection system, multi-path analysis, nuclear security.*

I. Introduction

Implementing nuclear technology in various nuclear facilities must apply the standards of Safety-Security-Safeguard (3S) [1]. The general objective of 3S standards is to protect the public and the environment from radiological hazards. One of the standards is nuclear security, and it is related to theft, sabotage, illegal transfer, unauthorized access, or other illegal actions related to nuclear materials and facilities; it involves physical protection system (PPS) as an essential part of it[1][2]. Since 1972 the International Atomic Energy Agency (IAEA) has recommended its member countries to implement the PPS concept through the IAEA international standard certification guidelines INFCIRC/225[3]. Evaluating the effectiveness of PPS is not a simple one because of the PPS characteristics and adversary abilities (the quantity and quality of the adversary, their capability, knowledge, and equipment, etc.). One of the main perspectives in evaluating the effectiveness of PPS is to analyze pathways that have the potential to attack facilities from outside. Due to the complexity of PPS, computer modeling techniques are usually required for pathway analysis. It analyzes the sequence of adversary actions in a path (adversary-path) and estimates a response force team's probability to neutralize the adversaries before completing their attack mission [4].

There are several tools for PPS effectiveness evaluation has been developed. The pioneer of this research was started in 1960 by Sandia National Laboratory (SNL); it is called EASI (Estimate of Adversary Sequence Interruption) [5]. EASI determines the probability of adversary interruption for a single path. The analyst must determine one by one the predicted paths that the adversary will use in carrying out its mission. Each path is analyzed by calculating the probability of interruption value. The lowest probability of interruption value is the most vulnerable path (MVP) and should be done with the security upgrade. EASI is quite simple and easy to use. Both of these are the advantages and disadvantages of this tool. The use of EASI tools for the analysis of extensive facilities that potentially have more adversary paths will possibly make it difficult for analysts to evaluate them.

Several studies have reported EASI-based PPS evaluation tools, such as SAPE, HAPPS, and HPEP [6–8]. Almost all evaluation tools use the same basic criteria to evaluate the PPS. It is to determine the most vulnerable adversary path to accomplish his/her mission [8]. In this study, we developed a Multi-path Analysis tool for Vulnerability Assessment of PPS (MAVA) based on EASI and implemented it in python computer code. This tool uses a one-dimensional (1D) model approach. It can perform the probability of interruption calculations on multi-paths (adversary-path) simultaneously, so that faster analysis results can be obtained. The code is implemented to assess the PPS with various strategies that the adversary can carry out. The feasibility of this multi-path code is confirmed through an example assessment using a hypothetical nuclear reactor facility.

II. Materials and Methods

A. The PPS Effectiveness Measure

The PPS combines people, equipment, and procedures in recognize the adversary presence (detect), slowing their movements (delay), and intercept (response) any threats to protect facilities against all illegal acts, i.e., theft, sabotages, or another illegal breach of security. Measuring the effectiveness of PPS can be done quantitatively through a performance-based analysis approach. This approach assesses the effectiveness of PPS by calculating the probability of interruptions (PI) along the most vulnerable paths. In addition to the (PI) parameters, consideration is also given to the probability of neutralization (PN) carried out by the response team in intercepting adversary action. Therefore, to calculate the effectiveness of PPS depends on two parameters, PI and PN. The product of those two parameters is the value of Probability Effectiveness (PE).

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

However, neutralization calculations were not carried out in this study. The PN value should be near 1.0; thus, we will calculate the PI only. We can calculate the PI values using EASI [5]. PI is determined from Probability of Detection (PD), delay time (TR), and response force team (RFT). We can use the equation below to calculate the PI value.

$$P_I = P(D_1)P(R|A_1)$$
$$+ \sum_{i=2}^{n} P(D_i)P(R|A_i) \prod_{j=1}^{i-1}(1-P(D_j)) \tag{2}$$

P(Di) is the probability of detection at the i-th element location, and n is the total number of elements. P(R|A1) is the probability of the response team to interrupts an adversary. The probability has a continuous value because time has a deviation. The time delay value is assumed to have a normal distribution, and:

$$T = RFT - T_R \tag{3}$$

The P(R|Ai) is calculated by other [4] as follo:

$$P(R|A_i) = \frac{1}{\sqrt{2\pi\left({d_R}^2+{d_{A_i}}^2\right)}} \int_0^0 e^{-2{d_R}^2+{d_{A_i}}^{2^{T^2}}} \tag{4}$$

where,
dR : deviation of response time
dAi : deviation of adversary task time.

B. Vulnerability Assessment Using Multi-Path Analysis

The vulnerability assessment MAVA code that we present in this study was based on the EASI model. The code can perform both: the PI calculations on single-path and multi-path (adversary path) simultaneously. In this study, we also adopt the method from other to model the various adversary strategies in the calculations [8].

1. EASI model

There are three primary calculations performed by EASI, which are also implemented in this MAVA code. The first is the PD value calculation of every single layer of protection. The second calculation is to determine the cumulative delay time (TC) from the first protection layer to the end along the adversary path. TC value and TC variance are calculated based on the TR data along with the standard deviation determined by the PPS designer. There is a correction factor in calculating true delay time, depending on the detection element associated with the delay element. The location of the detection also influences the calculation, whether the detection occurs at the beginning of adversary movement ("B"), at the middle adversary action ("M"), or detection occurred when the adversary has finished the action ("E"). The last calculation is to determine the precise PI value for every single layer of protection and the total PI value of PPS. This location parameter is related to the response function employ the results of the detection and delay function calculations. The EASI model can determine the MVP by obtaining the path with the lowest PI value. Another method to calculate the MVP by using a timely detection method. This method combines the cumulative PD value, TC along the path, and RFT. This concept pays attention to the critical detection point (CDP). The point on the path where the remaining time the adversary should complete his mission surpasses the response force constrains reaction time (see Fig.1).

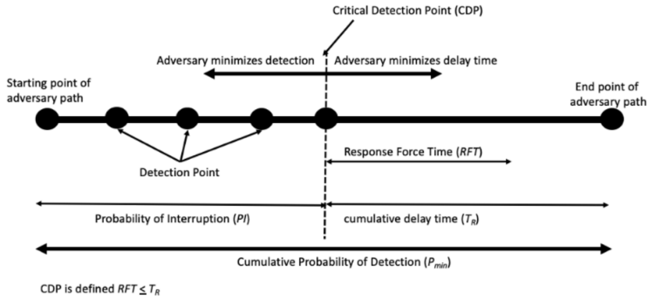

Critical Detection Point (CDP)
Adversary minimizes detection
Adversary minimizes delay time
Starting point of adversary path
End point of adversary path
Detection Point
Response Force Time (RFT)
Probability of Interruption (PI)
cumulative delay time (T_R)
Cumulative Probability of Detection (P_{min})
CDP is defined $RFT \leq T_R$

Figure 1. Illustration of timely detection.

The traditional EASI model with all of its capabilities is currently still widely used to study the effectiveness of PPS, but EASI still has limitations. This tool is a single path modeling, so analysis must be done one by one for each adversary path. That limitation makes it difficult for analysts to use the EASI model to analyze extensive facilities with as many adversary paths as possible. In this study, MAVA performs a vulnerability assessment of the adversary path, based-on traditional EASI using the multi-path analysis to solve these problems. The multi-path analysis code that we developed can be employed to examine the PPS in the entire facility through numerous adversary multi-path combination simulation.

2. Adversary Strategies

There are four types of strategy modeling in the assessment of vulnerable paths presented in this study. The adversary's strategy is based on their knowledge and priorities taken by the adversary in accomplishing their mission to sabotage the facility. Adequate knowledge of the targeted facilities to know the elements of detection and the estimated time delay at each layer of protection. The priority referred to here is the selection, whether the mission will be completed as soon as possible or carried out as carefully as possible, with the main priority is completing the mission in sabotaging the facility.

The first strategy is a deep strategy, where the adversary has adequate knowledge about the facilities to be attacked. The adversary knows the estimated possibility of detection and the time delay in each stage of carrying out its mission. In this strategy, the algorithm will direct the adversary to select the protection segment path with the smallest PD value at every layer of protection before reaching the layer of CDP. This strategy is done to minimize the occurrence of early detection in completing their mission. After passing through the CDP, the adversary will be looking for the protection element with the lowest time delay value. It aims to complete its mission immediately and or avoid confrontation with the response force team if their movements have been detected before CDP. The second strategy is that the adversary will eschew detection as high as possible; we called this a covert strategy. This strategy means that the algorithm will direct the adversary to go through each protection layer with the lowest PD value. The third is a rushing strategy: the adversary will accomplish their mission to attack the facility as fast as possible. This strategy means that the algorithm will direct the adversary to go through each protection layer with the smallest td value. The last is a random strategy; this is based on inadequate adversary knowledge about the targeted facilities. The adversary will not consider the probability of detection capabilities or the estimated time delay on each protection element. The adversary's selection of paths is carried out randomly, with the main target being to reach the target to complete its mission to sabotage the facility. The program algorithm will provide the same possibility for each protection element, which means it will be given the same weight.

III. Results and Discussions

A. The Hypothetical Facility, Adversary and Scenario

It is difficult to get an actual model in an actual nuclear reactor facility due to security reasons. However, we will model it with a hypothetical facility that is close to the real situation. This study used the National Nuclear Research Facility (NNRF), described as hypothetical nuclear facilities equipped with a detection, delay, and response system. NNRF consists of limited areas, protected areas, controlled area, and vital areas. The Limited area consists of one personnel gate, one main vehicle gate, and one emergency vehicle gate. A limited area fence is the nuclear facility's outer fence as a guardrail for a facility that aims to prevent intruders from entering the facility. The protected area is more restricted. There are office rooms, Central Alarm Station (CAS) room, and reactor buildings along with vital facilities inside as vital areas in the protected area. There is the main door at the front of the building, and at the back of the building, there is an access door as an emergency exit and vehicle door. There are several rooms in the vital area, including the spent fuel room, fresh fuel room, reactor pool, control room, and product vault. This vital area is usually the adversary's main target to carry out its mission, both theft and or sabotage. The 2-D layout of the NNRF is shown Fig. 2.

B. Adversary and Scenario

Based on information derived from the assumption of design-based threat documents, the scenario postulated in this study is sabotage of the nuclear reactor by exploding it. Adversaries' personnel's number up to five-person with semi-military capabilities semi-automatic rifles and handguns equipped. The adversaries do not have the skills to hack the system but may collusion possibility with insiders; thus, they may employ covert or brute force attack. They also have portable power tools, radio communications, and limited explosives materials to break the doors/walls and explode nuclear reactors.

The adversary sequence diagram (ASD) of the NNRF is shown in Figure.3. It describes all possible paths chosen by the adversary, from the off-site to the target. PI calculation on this tool uses the value PD, td, location (B, M, E), response and communication on the system. The value of the PD and td for every single protection element was acquired from other [10]. All these values are the parameter inputs that refer to specific adversary paths. The probability of communication (PC) is 0.95 (the most system operates that design and implements by SNL) [4]. The the PD and td where the system uses several sensors. Response Force Time equal to 700s, with the standard deviation, is approximated as 30% form mean value.

We converted ASD scheme into a 1-D sketch in the form of a directed-graph. This model has ten layers with a twenty-one position (node). Layer 0 is located at the furthermost layer (off-site area node), and layer 9 is the target node, it is shown in Figure 4. Based on the 1-D sketch, it can be estimated that there are several path combinations from the initial node (off-site) to the end node (target), which is 240 path combinations. MAVA code as a multi-path analysis tool will calculate the PI value for each path combination, including various strategies and determine the most vulnerable path.

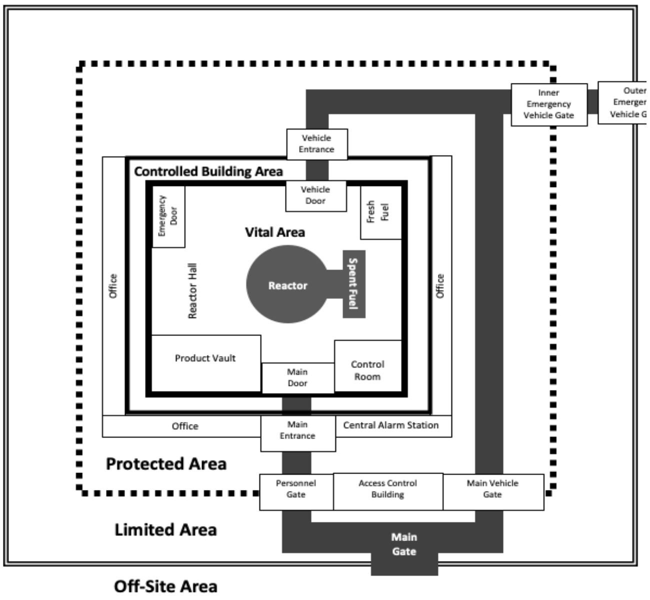


Figure 2. The schematic 2D layout of the National Nuclear Research Facility (NNRF).

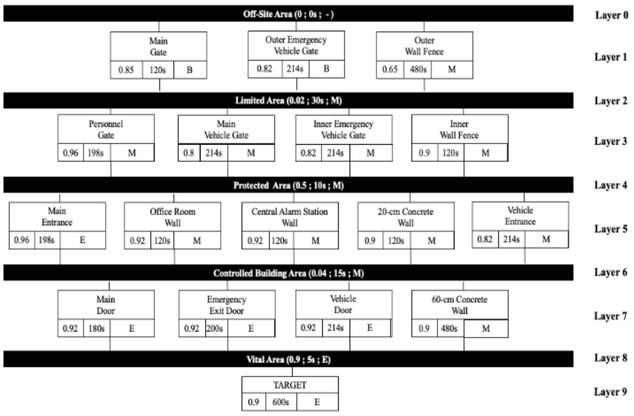
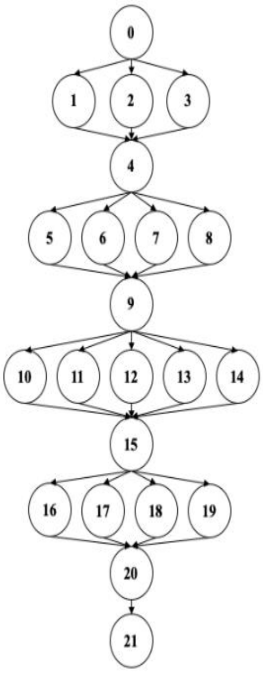


Figure 3. The adversary Sequence Diagram of the hypothetical facility.



Node 0 : Off Site Area
Node 1 : Main gate
Node 2 : Outer Emergency Vehicle Gate
Node 3 : Outer Fence
Node 4 : Limited Area
Node 5 : Personnel Gate
Node 6 : Main Vehicle Gate
Node 7 : Inner Emergency Vehicle Gate
Node 8 : Inner Fence
Node 9 : Protected Area
Node 10 : Main Entrance
Node 11 : Office Room Wall
Node 12 : Central Alarm Station Wall
Node 13 : 20-cm Concrete Wall
Node 14 : Vehicle Entrance
Node 15 : Controlled Building Area
Node 16 : Main Door
Node 17 : Emergency Exit Door
Node 18 : Vehicle Door
Node 19 : 60-cm Concrete Wall
Node 20 : Vital Area
Node 21 : Target

Figure 4. Directed-graph based on The Adversary Sequence Diagram (ASD).

C.Vulnerable Assessment Results

There are 240 intrusion path combinations for the adversary to get to the target (shown in appendix A). The calculation is implemented for the interruption probability of the intrusion path. Table 1 shows the calculation results of the PI from the simulations of the various adversary strategies. The calculated PI is 88% for the most vulnerable path (MVP). The results of the calculated MVP path shown in Table 2. The other calculations for various of strategies: deep strategy, covert strategy, rushing strategy, and random strategy are shown in Table 3 to Table 6, respectively, as well as presented on Figure 5.

Table 1 – Results of adversary strategies simulations

Adversary Strategy	Mean P_I Value (%)
MVP	88
Rush Strategy	89
Deep Strategy	91
Covert Strategy	94
Random Strategy	94

Table 2 – Calculated P_I for the most vulnerable path (MVP)

Task	***Node***	***Task Description***	***P_D* (%)**	***Location***	***t_d*(s)**
1	0	off-site area	0	End	0
2	3	infiltrate the outer wall fence	65	Middle	480
3	4	towards the limited area	2	Middle	30
4	8	infiltrate inner wall fence	90	Middle	120
5	9	towards the protected area	50	Middle	10
6	13	infiltrate the 20-cm wall	90	End	120
7	15	towards the controlled area	4	Middle	15
8	16	break down the main door	92	End	180
9	20	towards the vital area	90	End	5
10	21	sabotage the target	90	End	600
		Result Probability of Interruption (%)			88

Table 3 – Calculated PI for deep strategy

Task	***Node***	***Task Description***	***P_D* (%)**	***Location***	***t_d*(s)**
1	0	off-site area	0	End	0
2	3	infiltrate the outer wall fence	65	Middle	480
3	4	towards the limited area	2	Middle	30
4	6	infiltrate the main vehicle gate	80	Middle	214
5	9	towards the protected area	50	Middle	10
6	14	infiltrate the vehicle entrance	82	Middle	214
7	15	towards the controlled area	4	Middle	15
8	16	break down the main door	92	End	180
9	20	towards the vital area	9	End	5
10	21	sabotage target	9	End	600
		Result Probability of Interruption (%)			91

Table 4 – Calculated P_I for covert strategy

Task	***Node***	***Task Description***	***P_D* (%)**	***Location***	***t_d*(s)**
1	0	off-site area	0	End	0
2	3	infiltrate the outer wall fence	65	Middle	480
3	4	towards the limited area	2	Middle	30
4	6	infiltrate the main vehicle gate	80	Middle	214
5	9	towards the protected area	50	Middle	10
6	14	infiltrate the vehicle entrance	82	Middle	214
7	15	towards the controlled Area	4	Middle	15
8	19	infiltrate the 60-cm wwall	90	Middle	480
9	20	towards the vital Area	90	End	5
10	21	sabotage target	90	End	600
		Result Probability of Interruption (%)			94

Table 5 – Calculated P_I for rushing strategy

Task	***Node***	***Task Description***	***P_D(%)***	***Location***	***t_d(s)***
1	0	off-site area	0	End	0
2	1	infiltrate the main gate	85	Begin	120
3	4	towards the limited area	2	Middle	30
4	8	infiltrate the inner wall fence	90	Middle	120
5	9	towards the protected area	50	Middle	10
6	13	infiltrate the 20-cm wall	90	Middle	120
7	15	towards the controlled area	4	Middle	15
8	16	break down the main door	92	End	180
9	20	towards the Vital Area	90	End	5
10	21	sabotage target	90	End	600
				Result Probability of Interruption (%)	89

Table 6 – Calculated P_I for random strategy

Task	***Node***	***Task Description***	***P_D(%)***	***Location***	***t_d(s)***
1	0	off-site area	0	End	0
2	3	infiltrate the outer wall fence	65	Middle	480
3	4	towards the limited area	2	Middle	30
4	8	infiltrate the inner wall fence	80	Middle	120
5	9	towards the protected area	50	Middle	10
6	14	infiltrate the vehicle entrance	82	Middle	214
7	15	towards the controlled area	4	Middle	15
8	19	infiltrate the 60-cm Wall	90	Middle	480
9	20	towards the vital area	90	End	5
10	21	sabotage target	90	End	600
				Result Probability of Interruption (%)	94

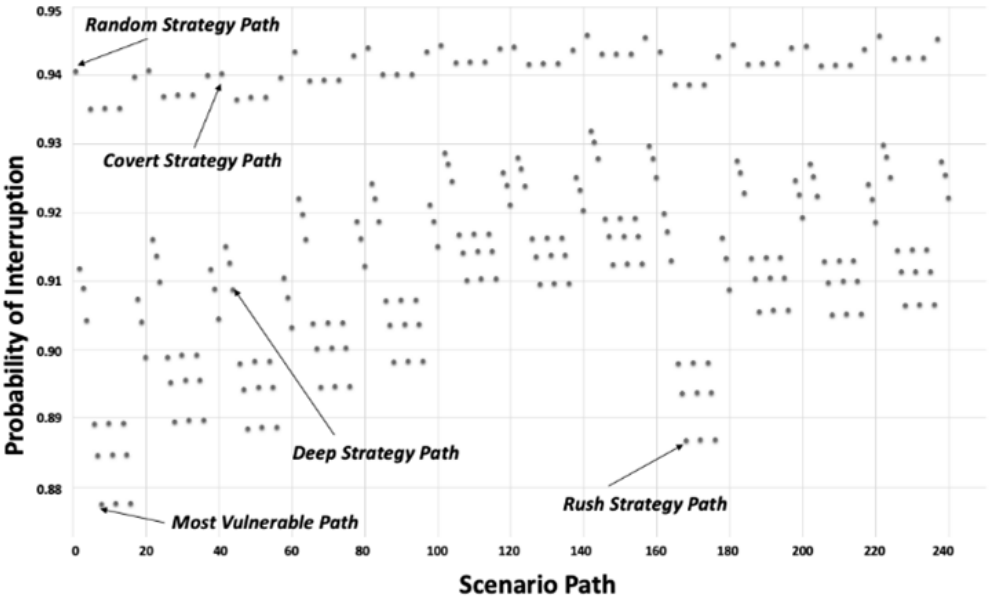


Figure 5. The Calculated Probability of Interruption of NNRF over various pathways.

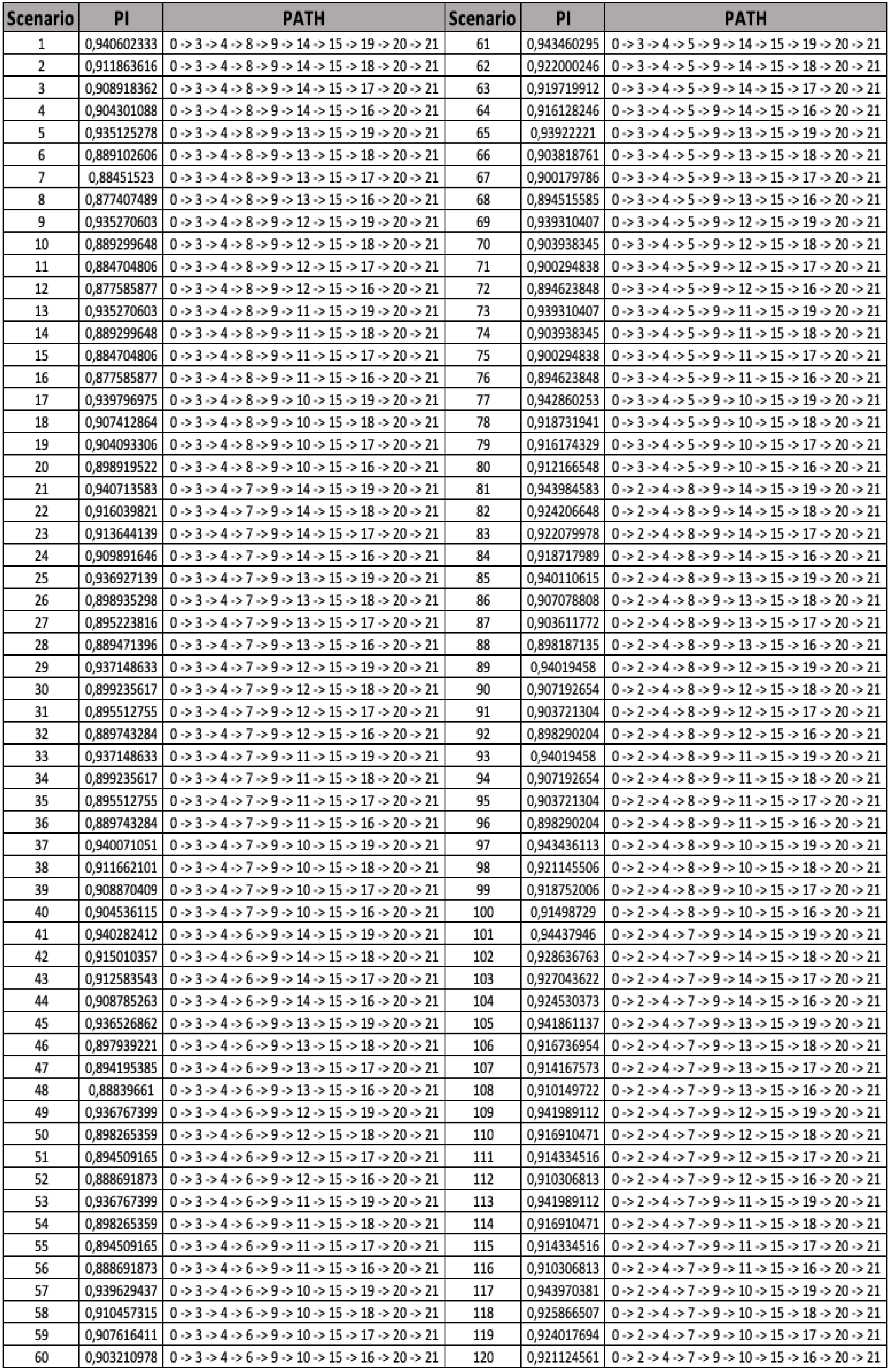
In general, as shown in Figure 5, PI value for all intrusions path, and those various strategies is greater than 80%, and it is considered as high value. These values mean that the effectiveness of PPS at these facilities has good performance in anticipating various attack strategies, including the most vulnerable paths.

IV. Conclusions

The purpose of the current study was to develop the vulnerability assessment tool, and it was carried through to the MAVA code. The feasibility of this code was implemented on NNRF. This code can perform the calculation of the probability of interruption values simultaneously and perform multi-path analysis through an ASD. The assessment results provide the vulnerability pathway information to the analysts to improve the effectiveness of PPS. Several limitations to this code need to be acknowledged. Additional features include the effect of insider involvement and theft scenarios for more in-depth analysis. Furthermore, the current implementation of a vulnerability assessment is still in the 1-D model approach. This analysis can be improved by a 2-D model approach that provides an intuitive view of PPS, and realistically represents the adversary's position and the protection elements.

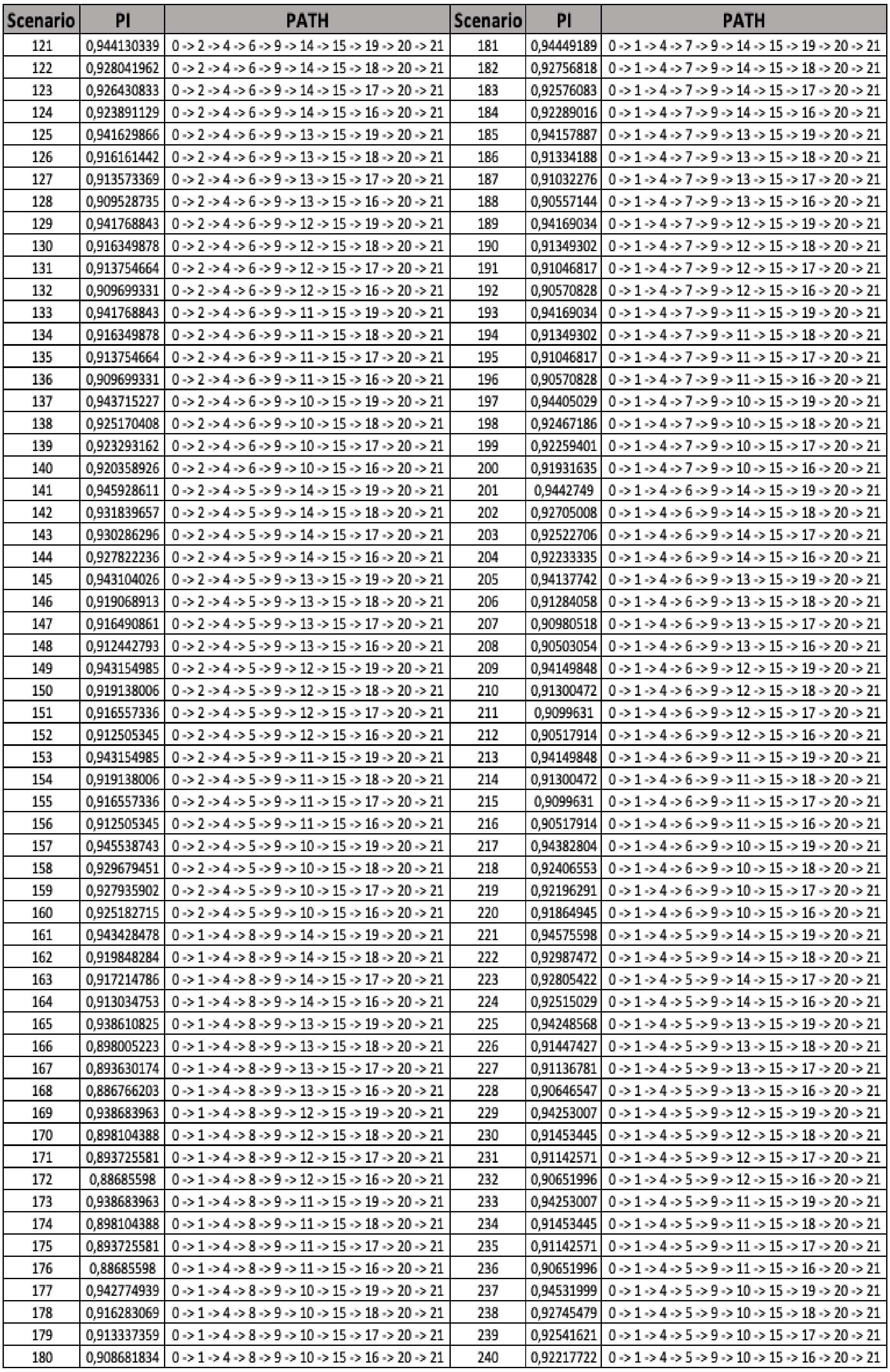
APPENDIX

Table A.1 – Calculated PI for path combination from scenario 1-120



Scenario	PI	PATH	Scenario	PI	PATH
1	0,940602333	0 -> 3 -> 4 -> 8 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21	61	0,943460295	0 -> 3 -> 4 -> 5 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21
2	0,911863616	0 -> 3 -> 4 -> 8 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21	62	0,922000246	0 -> 3 -> 4 -> 5 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21
3	0,908918362	0 -> 3 -> 4 -> 8 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21	63	0,919719912	0 -> 3 -> 4 -> 5 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21
4	0,904301088	0 -> 3 -> 4 -> 8 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21	64	0,916128246	0 -> 3 -> 4 -> 5 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21
5	0,935125278	0 -> 3 -> 4 -> 8 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21	65	0,93922221	0 -> 3 -> 4 -> 5 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21
6	0,889102606	0 -> 3 -> 4 -> 8 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21	66	0,903818761	0 -> 3 -> 4 -> 5 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21
7	0,88451523	0 -> 3 -> 4 -> 8 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21	67	0,900179786	0 -> 3 -> 4 -> 5 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21
8	0,877407489	0 -> 3 -> 4 -> 8 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21	68	0,894515585	0 -> 3 -> 4 -> 5 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21
9	0,935270603	0 -> 3 -> 4 -> 8 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21	69	0,939310407	0 -> 3 -> 4 -> 5 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21
10	0,889299648	0 -> 3 -> 4 -> 8 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21	70	0,903938345	0 -> 3 -> 4 -> 5 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21
11	0,884704806	0 -> 3 -> 4 -> 8 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21	71	0,900294838	0 -> 3 -> 4 -> 5 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21
12	0,877585877	0 -> 3 -> 4 -> 8 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21	72	0,894623848	0 -> 3 -> 4 -> 5 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21
13	0,935270603	0 -> 3 -> 4 -> 8 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21	73	0,939310407	0 -> 3 -> 4 -> 5 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21
14	0,889299648	0 -> 3 -> 4 -> 8 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21	74	0,903938345	0 -> 3 -> 4 -> 5 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21
15	0,884704806	0 -> 3 -> 4 -> 8 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21	75	0,900294838	0 -> 3 -> 4 -> 5 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21
16	0,877585877	0 -> 3 -> 4 -> 8 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21	76	0,894623848	0 -> 3 -> 4 -> 5 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21
17	0,939796975	0 -> 3 -> 4 -> 8 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21	77	0,942860253	0 -> 3 -> 4 -> 5 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21
18	0,907412864	0 -> 3 -> 4 -> 8 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21	78	0,918731941	0 -> 3 -> 4 -> 5 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21
19	0,904093306	0 -> 3 -> 4 -> 8 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21	79	0,916174329	0 -> 3 -> 4 -> 5 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21
20	0,898919522	0 -> 3 -> 4 -> 8 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21	80	0,912166548	0 -> 3 -> 4 -> 5 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21
21	0,940713583	0 -> 3 -> 4 -> 7 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21	81	0,943984583	0 -> 2 -> 4 -> 8 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21
22	0,916039821	0 -> 3 -> 4 -> 7 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21	82	0,924206648	0 -> 2 -> 4 -> 8 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21
23	0,913644139	0 -> 3 -> 4 -> 7 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21	83	0,922079978	0 -> 2 -> 4 -> 8 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21
24	0,909891646	0 -> 3 -> 4 -> 7 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21	84	0,918717989	0 -> 2 -> 4 -> 8 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21
25	0,936927139	0 -> 3 -> 4 -> 7 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21	85	0,940110615	0 -> 2 -> 4 -> 8 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21
26	0,898935298	0 -> 3 -> 4 -> 7 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21	86	0,907078808	0 -> 2 -> 4 -> 8 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21
27	0,895223816	0 -> 3 -> 4 -> 7 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21	87	0,903611772	0 -> 2 -> 4 -> 8 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21
28	0,889471396	0 -> 3 -> 4 -> 7 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21	88	0,898187135	0 -> 2 -> 4 -> 8 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21
29	0,937148633	0 -> 3 -> 4 -> 7 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21	89	0,94019458	0 -> 2 -> 4 -> 8 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21
30	0,899235617	0 -> 3 -> 4 -> 7 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21	90	0,907192654	0 -> 2 -> 4 -> 8 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21
31	0,895512755	0 -> 3 -> 4 -> 7 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21	91	0,903721304	0 -> 2 -> 4 -> 8 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21
32	0,889743284	0 -> 3 -> 4 -> 7 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21	92	0,898290204	0 -> 2 -> 4 -> 8 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21
33	0,937148633	0 -> 3 -> 4 -> 7 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21	93	0,94019458	0 -> 2 -> 4 -> 8 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21
34	0,899235617	0 -> 3 -> 4 -> 7 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21	94	0,907192654	0 -> 2 -> 4 -> 8 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21
35	0,895512755	0 -> 3 -> 4 -> 7 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21	95	0,903721304	0 -> 2 -> 4 -> 8 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21
36	0,889743284	0 -> 3 -> 4 -> 7 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21	96	0,898290204	0 -> 2 -> 4 -> 8 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21
37	0,940071051	0 -> 3 -> 4 -> 7 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21	97	0,943436113	0 -> 2 -> 4 -> 8 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21
38	0,911662101	0 -> 3 -> 4 -> 7 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21	98	0,921145506	0 -> 2 -> 4 -> 8 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21
39	0,908870409	0 -> 3 -> 4 -> 7 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21	99	0,918752006	0 -> 2 -> 4 -> 8 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21
40	0,904536115	0 -> 3 -> 4 -> 7 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21	100	0,91498729	0 -> 2 -> 4 -> 8 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21
41	0,940282412	0 -> 3 -> 4 -> 6 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21	101	0,94437946	0 -> 2 -> 4 -> 7 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21
42	0,915010357	0 -> 3 -> 4 -> 6 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21	102	0,928636763	0 -> 2 -> 4 -> 7 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21
43	0,912583543	0 -> 3 -> 4 -> 6 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21	103	0,927043622	0 -> 2 -> 4 -> 7 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21
44	0,908785263	0 -> 3 -> 4 -> 6 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21	104	0,924530373	0 -> 2 -> 4 -> 7 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21
45	0,936526862	0 -> 3 -> 4 -> 6 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21	105	0,941861137	0 -> 2 -> 4 -> 7 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21
46	0,897939221	0 -> 3 -> 4 -> 6 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21	106	0,916736954	0 -> 2 -> 4 -> 7 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21
47	0,894195385	0 -> 3 -> 4 -> 6 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21	107	0,914167573	0 -> 2 -> 4 -> 7 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21
48	0,88839661	0 -> 3 -> 4 -> 6 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21	108	0,910149722	0 -> 2 -> 4 -> 7 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21
49	0,936767399	0 -> 3 -> 4 -> 6 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21	109	0,941989112	0 -> 2 -> 4 -> 7 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21
50	0,898265359	0 -> 3 -> 4 -> 6 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21	110	0,916910471	0 -> 2 -> 4 -> 7 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21
51	0,894509165	0 -> 3 -> 4 -> 6 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21	111	0,914334516	0 -> 2 -> 4 -> 7 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21
52	0,888691873	0 -> 3 -> 4 -> 6 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21	112	0,910306813	0 -> 2 -> 4 -> 7 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21
53	0,936767399	0 -> 3 -> 4 -> 6 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21	113	0,941989112	0 -> 2 -> 4 -> 7 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21
54	0,898265359	0 -> 3 -> 4 -> 6 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21	114	0,916910471	0 -> 2 -> 4 -> 7 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21
55	0,894509165	0 -> 3 -> 4 -> 6 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21	115	0,914334516	0 -> 2 -> 4 -> 7 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21
56	0,888691873	0 -> 3 -> 4 -> 6 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21	116	0,910306813	0 -> 2 -> 4 -> 7 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21
57	0,939629437	0 -> 3 -> 4 -> 6 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21	117	0,943970381	0 -> 2 -> 4 -> 7 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21
58	0,910457315	0 -> 3 -> 4 -> 6 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21	118	0,925866507	0 -> 2 -> 4 -> 7 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21
59	0,907616411	0 -> 3 -> 4 -> 6 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21	119	0,924017694	0 -> 2 -> 4 -> 7 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21
60	0,903210978	0 -> 3 -> 4 -> 6 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21	120	0,921124561	0 -> 2 -> 4 -> 7 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21

Table A.2 – Calculated PI for path combination from scenario 121-240



Scenario	PI	PATH	Scenario	PI	PATH
121	0,944130339	0 -> 2 -> 4 -> 6 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21	181	0,94449189	0 -> 1 -> 4 -> 7 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21
122	0,928041962	0 -> 2 -> 4 -> 6 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21	182	0,92756818	0 -> 1 -> 4 -> 7 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21
123	0,926430833	0 -> 2 -> 4 -> 6 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21	183	0,92576083	0 -> 1 -> 4 -> 7 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21
124	0,923891129	0 -> 2 -> 4 -> 6 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21	184	0,92289016	0 -> 1 -> 4 -> 7 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21
125	0,941629866	0 -> 2 -> 4 -> 6 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21	185	0,94157887	0 -> 1 -> 4 -> 7 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21
126	0,916161442	0 -> 2 -> 4 -> 6 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21	186	0,91334188	0 -> 1 -> 4 -> 7 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21
127	0,913573369	0 -> 2 -> 4 -> 6 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21	187	0,91032276	0 -> 1 -> 4 -> 7 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21
128	0,909528735	0 -> 2 -> 4 -> 6 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21	188	0,90557144	0 -> 1 -> 4 -> 7 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21
129	0,941768843	0 -> 2 -> 4 -> 6 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21	189	0,94169034	0 -> 1 -> 4 -> 7 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21
130	0,916349878	0 -> 2 -> 4 -> 6 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21	190	0,91349302	0 -> 1 -> 4 -> 7 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21
131	0,913754664	0 -> 2 -> 4 -> 6 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21	191	0,91046817	0 -> 1 -> 4 -> 7 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21
132	0,909699331	0 -> 2 -> 4 -> 6 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21	192	0,90570828	0 -> 1 -> 4 -> 7 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21
133	0,941768843	0 -> 2 -> 4 -> 6 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21	193	0,94169034	0 -> 1 -> 4 -> 7 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21
134	0,916349878	0 -> 2 -> 4 -> 6 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21	194	0,91349302	0 -> 1 -> 4 -> 7 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21
135	0,913754664	0 -> 2 -> 4 -> 6 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21	195	0,91046817	0 -> 1 -> 4 -> 7 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21
136	0,909699331	0 -> 2 -> 4 -> 6 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21	196	0,90570828	0 -> 1 -> 4 -> 7 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21
137	0,943715227	0 -> 2 -> 4 -> 6 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21	197	0,94405029	0 -> 1 -> 4 -> 7 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21
138	0,925170408	0 -> 2 -> 4 -> 6 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21	198	0,92467186	0 -> 1 -> 4 -> 7 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21
139	0,923293162	0 -> 2 -> 4 -> 6 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21	199	0,92259401	0 -> 1 -> 4 -> 7 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21
140	0,920358926	0 -> 2 -> 4 -> 6 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21	200	0,91931635	0 -> 1 -> 4 -> 7 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21
141	0,945928611	0 -> 2 -> 4 -> 5 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21	201	0,9442749	0 -> 1 -> 4 -> 6 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21
142	0,931839657	0 -> 2 -> 4 -> 5 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21	202	0,92705008	0 -> 1 -> 4 -> 6 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21
143	0,930286296	0 -> 2 -> 4 -> 5 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21	203	0,92522706	0 -> 1 -> 4 -> 6 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21
144	0,927822236	0 -> 2 -> 4 -> 5 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21	204	0,92233335	0 -> 1 -> 4 -> 6 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21
145	0,943104026	0 -> 2 -> 4 -> 5 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21	205	0,94137742	0 -> 1 -> 4 -> 6 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21
146	0,919068913	0 -> 2 -> 4 -> 5 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21	206	0,91284058	0 -> 1 -> 4 -> 6 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21
147	0,916490861	0 -> 2 -> 4 -> 5 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21	207	0,90980518	0 -> 1 -> 4 -> 6 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21
148	0,912442793	0 -> 2 -> 4 -> 5 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21	208	0,90503054	0 -> 1 -> 4 -> 6 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21
149	0,943154985	0 -> 2 -> 4 -> 5 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21	209	0,94149848	0 -> 1 -> 4 -> 6 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21
150	0,919138006	0 -> 2 -> 4 -> 5 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21	210	0,91300472	0 -> 1 -> 4 -> 6 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21
151	0,916557336	0 -> 2 -> 4 -> 5 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21	211	0,9099631	0 -> 1 -> 4 -> 6 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21
152	0,912505345	0 -> 2 -> 4 -> 5 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21	212	0,90517914	0 -> 1 -> 4 -> 6 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21
153	0,943154985	0 -> 2 -> 4 -> 5 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21	213	0,94149848	0 -> 1 -> 4 -> 6 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21
154	0,919138006	0 -> 2 -> 4 -> 5 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21	214	0,91300472	0 -> 1 -> 4 -> 6 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21
155	0,916557336	0 -> 2 -> 4 -> 5 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21	215	0,9099631	0 -> 1 -> 4 -> 6 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21
156	0,912505345	0 -> 2 -> 4 -> 5 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21	216	0,90517914	0 -> 1 -> 4 -> 6 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21
157	0,945538743	0 -> 2 -> 4 -> 5 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21	217	0,94382804	0 -> 1 -> 4 -> 6 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21
158	0,929679451	0 -> 2 -> 4 -> 5 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21	218	0,92406553	0 -> 1 -> 4 -> 6 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21
159	0,927935902	0 -> 2 -> 4 -> 5 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21	219	0,92196291	0 -> 1 -> 4 -> 6 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21
160	0,925182715	0 -> 2 -> 4 -> 5 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21	220	0,91864945	0 -> 1 -> 4 -> 6 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21
161	0,943428478	0 -> 1 -> 4 -> 8 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21	221	0,94575598	0 -> 1 -> 4 -> 5 -> 9 -> 14 -> 15 -> 19 -> 20 -> 21
162	0,919848284	0 -> 1 -> 4 -> 8 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21	222	0,92987472	0 -> 1 -> 4 -> 5 -> 9 -> 14 -> 15 -> 18 -> 20 -> 21
163	0,917214786	0 -> 1 -> 4 -> 8 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21	223	0,92805422	0 -> 1 -> 4 -> 5 -> 9 -> 14 -> 15 -> 17 -> 20 -> 21
164	0,913034753	0 -> 1 -> 4 -> 8 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21	224	0,92515029	0 -> 1 -> 4 -> 5 -> 9 -> 14 -> 15 -> 16 -> 20 -> 21
165	0,938610825	0 -> 1 -> 4 -> 8 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21	225	0,94248568	0 -> 1 -> 4 -> 5 -> 9 -> 13 -> 15 -> 19 -> 20 -> 21
166	0,898005223	0 -> 1 -> 4 -> 8 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21	226	0,91447427	0 -> 1 -> 4 -> 5 -> 9 -> 13 -> 15 -> 18 -> 20 -> 21
167	0,893630174	0 -> 1 -> 4 -> 8 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21	227	0,91136781	0 -> 1 -> 4 -> 5 -> 9 -> 13 -> 15 -> 17 -> 20 -> 21
168	0,886766203	0 -> 1 -> 4 -> 8 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21	228	0,90646547	0 -> 1 -> 4 -> 5 -> 9 -> 13 -> 15 -> 16 -> 20 -> 21
169	0,938683963	0 -> 1 -> 4 -> 8 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21	229	0,94253007	0 -> 1 -> 4 -> 5 -> 9 -> 12 -> 15 -> 19 -> 20 -> 21
170	0,898104388	0 -> 1 -> 4 -> 8 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21	230	0,91453445	0 -> 1 -> 4 -> 5 -> 9 -> 12 -> 15 -> 18 -> 20 -> 21
171	0,893725581	0 -> 1 -> 4 -> 8 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21	231	0,91142571	0 -> 1 -> 4 -> 5 -> 9 -> 12 -> 15 -> 17 -> 20 -> 21
172	0,88685598	0 -> 1 -> 4 -> 8 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21	232	0,90651996	0 -> 1 -> 4 -> 5 -> 9 -> 12 -> 15 -> 16 -> 20 -> 21
173	0,938683963	0 -> 1 -> 4 -> 8 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21	233	0,94253007	0 -> 1 -> 4 -> 5 -> 9 -> 11 -> 15 -> 19 -> 20 -> 21
174	0,898104388	0 -> 1 -> 4 -> 8 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21	234	0,91453445	0 -> 1 -> 4 -> 5 -> 9 -> 11 -> 15 -> 18 -> 20 -> 21
175	0,893725581	0 -> 1 -> 4 -> 8 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21	235	0,91142571	0 -> 1 -> 4 -> 5 -> 9 -> 11 -> 15 -> 17 -> 20 -> 21
176	0,88685598	0 -> 1 -> 4 -> 8 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21	236	0,90651996	0 -> 1 -> 4 -> 5 -> 9 -> 11 -> 15 -> 16 -> 20 -> 21
177	0,942774939	0 -> 1 -> 4 -> 8 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21	237	0,94531999	0 -> 1 -> 4 -> 5 -> 9 -> 10 -> 15 -> 19 -> 20 -> 21
178	0,916283069	0 -> 1 -> 4 -> 8 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21	238	0,92745479	0 -> 1 -> 4 -> 5 -> 9 -> 10 -> 15 -> 18 -> 20 -> 21
179	0,913337359	0 -> 1 -> 4 -> 8 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21	239	0,92541621	0 -> 1 -> 4 -> 5 -> 9 -> 10 -> 15 -> 17 -> 20 -> 21
180	0,908681834	0 -> 1 -> 4 -> 8 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21	240	0,92217722	0 -> 1 -> 4 -> 5 -> 9 -> 10 -> 15 -> 16 -> 20 -> 21

Acknowledgment

The first author thanks the Ministry of Research and Technology of the Republic of Indonesia for funding scholarships and research in this study

References

[1] Zakariya N I and Kahn M T E 2015 Safety, security and safeguard Ann. Nucl. Energy 75 292–302

[2] Schriefer D 2012 Safeguards, security, safety and the nuclear fuel cycle Nucl. Fuel Cycle Sci. Eng. 52–79

[3] International-Atomic-Energy-Agency 2011 Nuclear security recommendations on nuclear and other radioactive material out of regulatory control IAEA. Nuclear Security Series No. 15 Nuclear security recommendations on radioactive material and associated facilities IAEA vol 14873530.

[4] Garcia M L 2007 Design and evaluation of physical protection systems: Second edition (Butterworth-Heinemann).

[5] Bennett H A 1977 ″Easi″ - an Evaluation Method for Physical Security Systems. Nucl Mater Manag. 6 371–9

[6] Sung J S, Sung-Woo K, Hosik Y, Jung-Soo K and Wan Y K 2009 Development of a vulnerability assessment code for a physical protection system: Systematic analysis of physical protection Effectiveness (SAPE) Nucl. Eng. Technol. 41 747–52

[7] Zou B, Yang M, Guo J, Benjamin E R and Wu W 2017 A heuristic approach for the evaluation of Physical Protection System Effectiveness Ann. Nucl. Energy 105 302–10

[8] Zou B, Yang M, Zhang Y, Benjamin E R, Tan K, Wu W and Yoshikawa H 2018 Evaluation of vulnerable path: Using heuristic path-finding algorithm in physical protection system of nuclear power plant Int. J. Crit. Infrastruct. Prot. 23 90–9