Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Development of a structure analytic hierarchy approach for the evaluation of the physical protection system effectiveness

Bowen Zou [a, *], Wenlin Wang [b], Jian Liu [c], Zhenyu Yan [c], Gaojun Liu [c], Jun Wang [a], Guanxiang Wei [a]

[a] *School of Electric Power, South China University of Technology, Guangzhou, 510641, China*
[b] *School of Automation, Wuhan University of Technology, Wuhan, 430070, China*
[c] *State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Guangdong Nuclear Power Engineering, Design Co. Ltd., Shenzhen, 518116, China*

ARTICLE INFO

Article history:
Received 16 March 2019
Received in revised form
17 December 2019
Accepted 31 January 2020
Available online 4 February 2020

Keywords:
Physical protection system
Structure analytic hierarchy approach
Community algorithm

ABSTRACT

A physical protection system (PPS) is used for the protection of critical facilities. This paper proposes a structure analytic hierarchy approach (SAHA) for the hierarchical evaluation of the PPS effectiveness in critical infrastructure. SAHA is based on the traditional analysis methods “estimate of adversary sequence interruption, EASI”. A community algorithm is used in the building of the SAHA model. SAHA is applied to cluster the associated protection elements for the topological design of complicated PPS with graphical vertexes equivalent to protection elements.

1. Introduction

The physical protection system (PPS) of critical infrastructure is a security defense system utilizes the equipment, procedures, and people for the protection of facilities and assets against theft, sabotage and terrorist attacks. The PPS establishes a state of security with a purposeful arrangement of set of protective measures [1]. Three depth measures, “Defence in Depth”, “Protection in Depth” and “Security in Depth [3]”, are used in the design of PPS to protect the critical facilities, systems, or devices in complex infrastructures [2].

Various kinds of security risk tools are developed for the analysis of an area of PPS. Some of the tools are used in low-consequence facilities that rarely address the three components of risk, threat, vulnerability, and consequence, in the analysis process. For a higher-consequence facility in critical infrastructure, Sandia National Laboratories (SNL) developed an automated security risk assessment methodology tool for the assessment and management of security risk from malevolent threats [4].

The evaluation tools for the protection of higher-consequence facilities use qualitative-quantitative methods. Francesca et al. studied the performance assessment of anti-terrorism physical protection systems in chemical plants resorted to experts’ consultation [5]. Zdenek et al. summarized the current common evaluation theory, algorithms, models and software tools [6]. The EASI model (Estimate of Adversary Sequence Interruption) was a stochastic method using the mean values and standard deviations and was developed in the SNL [7–9]. EASI method is used to assess one adversary path of the attack selected beforehand and cannot find vulnerable paths.

The traditional graphic representation method uses adversary sequence diagram (ASD) to identify the adversary paths which adversaries can follow to accomplish intrusion. The physical protection areas are divided into 7 levels, including Off-site, Limited Area, Protected Area, Controlled Building, Controlled Room, Target Enclosure, Target, etc. All potential adversary paths through a facility establish the effectiveness of the PPS which can be modeled by the ASDs. A SAVI (Systematic Analysis of Vulnerability to Intrusion) method is on the basis of the ASD has been widely used, such as the current handbook for analyzing nuclear power plant security in the USA [10,11]. SAVI calculates the likelihood of attack interruption and finds the set of the most vulnerable adversary paths on a facility model from the protection elements [6]. Other methods like ASSESS (Analytic System and Software for Evaluating

[*] Corresponding author.
E-mail address: zoubowen@scut.edu.cn (B. Zou).

https://doi.org/10.1016/j.net.2020.01.033

Safeguards and Security) [12], SAPE (Systematic Analysis of Physical Protection Effectiveness) [13], VEGA, MAPPS [25], BN [26], etc.

The aforementioned methods (EASI, SAVI, ASSESS, etc.) based on ASD rarely consider the association of protection elements and is difficult to evaluate a complicated PPS effectiveness hierarchically. In the design and analysis of complicated PPS, abundant protection elements influence the analysis and evaluation efficiency, so that the design, optimal installation, maintenance process of protection elements will be affected.

In general, the protection elements of PPS are inter-associated rather than separated. The associated data between the protection elements need to be analyzed and evaluated with a systematic method. In this paper, an undirected graph is used for the graphical representation of networks and formed by the PPS protection elements. The protection elements denote nodes or vertexes of the graph, the intrusion paths denote the set of edges. The adversaries determine the intrusion path based on the difficulty of accomplishing the tasks along the path. Thus, the adversary path between the two protection elements has weight value to assess their association.

In this paper, a novel structure analytic hierarchy approach (SAHA) based on the community structure algorithm is proposed for the modeling of PPS protection elements. SAHA is an agglomerative analysis method for the evaluation of the PPS effectiveness and addresses the vulnerable group of protection elements. The agglomerative method and division method are the common types of community algorithms. Popular community analysis algorithms include fast unfolding of community algorithm [14], Label Propagation Algorithm [15] (LPA), Normalized Cut algorithm [16], Kernighan-Lin algorithm [17], etc. However, the research on the community analysis method is explained briefly, only one of community algorithms Newman is discussed in this paper.

How to accurate divide protection elements into corresponding protection areas for modeling and analysis is a practical engineering problem. One of the SAHA functions is clustered with the associated elements at a different level. The cluster-level corresponding to maximum modularity that is a better module structure in the process of cluster analysis. Another theoretical basis of SAHA is EASI method for the evaluation of the PPS effectiveness. SAHA is a data miner so that the vulnerable adversary path can be mined. In this paper, section 2 introduces the SAHA of PPS, and section 3 elaborates on the effectiveness evaluation method. In the end, a minimum case system is illustrated for the feasibility evaluation.

2. Structure analytic hierarchy approach of physical protection system

The analysis process diagram of the structure analytic hierarchy approach is shown in Fig. 1, the input sources of the protection elements in each level are installation sites, protection regions, and evaluation parameters. The basic element level contains all protection elements information, the upper levels are the clustered unit block.

The association between the protection elements are estimated based on the input information. Then, clustering analysis of the protection elements, includes relevancy between the protection elements, matching protection elements estimation of modularity and production of “New” protection elements.

In the upper level, the output information is used as the input information of the upper level to perform the analysis process and estimate the effectiveness of the PPS. The cluster analysis can be performed multiple times at the upper level until the analysis requirements are met and the correlation of protection elements are obtained.

2.1. Analysis of physical protection elements

The physical protection system is divided into two basic systems, mechanical barrier system and technical protection system [18]. The protection elements of the mechanical barrier system are walls, roofs, floors, doors, windows objects, etc. The technical protection system includes the intruder alarm system, security camera system, access control system, etc.

In this paper, the protection elements are some mechanical barrier elements and intrusion-detection sensors. The mechanical barrier system is used to delay the process of adversary intrusion. The intrusion detection sensors are used for the detection of adversary intrusion actions, and a camera system is used for the verification of the alarm information. The vulnerabilities of sensors are the physical components, the detection signal processing process, the installation, the false alarm rate (FAR), the nuisance alarm rate (NAR). The adversaries general utilize the electronic interference devices to affect the normal detection function of the sensors or bypass the sensor detection areas to avoid triggering the alarm.

The basic protection elements of PPS which are used in the effectiveness evaluation are shown in Fig. 2. A 2D map of the critical facility site is analyzed and the adversary sequence diagram (ASD) [19] is established based on the element properties.

ASD is an auxiliary graphical modeling method used for evaluating the effectiveness of the PPS at a facility. ASD has two basic functions, graphically represent the PPS elements and intrusion direction along adversary paths. The steps for establishing the ASD at a specific site are as follows.

1. Identify the characteristics of all physical areas for the separation of a facility into adjacent physical areas, Table 1 enumerates the critical physical areas and the definitions.
2. Define the protection layers and path elements between the adjacent physical areas. A protection layer is formed from more than one protection element. A protection element in the protection layer has its marks of entry and exit. The adversary should through all the protection elements along the intrusion path to reach a target;
3. Assign the correlation parameters of system effectiveness analysis for each path element and physical area, such as the probability of detection, delay time, location, etc.

The adversary path general intrudes from the outside to the target area along with the delay elements, and the intrusion detection elements are deployed on all possible intrusion paths for the detection of adversary actions. According to the adversary path, the deployment of the mechanical barrier elements and the intrusion detection elements are abstracted into network hierarchy. The community detection algorithm is used for the cluster analysis of the associated elements. The final layer is abstracted to a complete community, i.e. the protection elements covering an entire critical infrastructure facility.

2.2. Community structure model

This paper uses the method of community detection method for the hierarchy partition of PPS protection elements. Vulnerability evaluation of the PPS from the basic protection elements layer to the top layer. The structure analytic hierarchy approaches graphically represents the data, where the nodes are protective elements and the edges mean the degree of association between the protection elements. The clusters are defined as connected elements, i.e. the element groups that communicate with each other but do not communicate with the elements outside the group.

Newman et al. [22,23] proposed a community detection

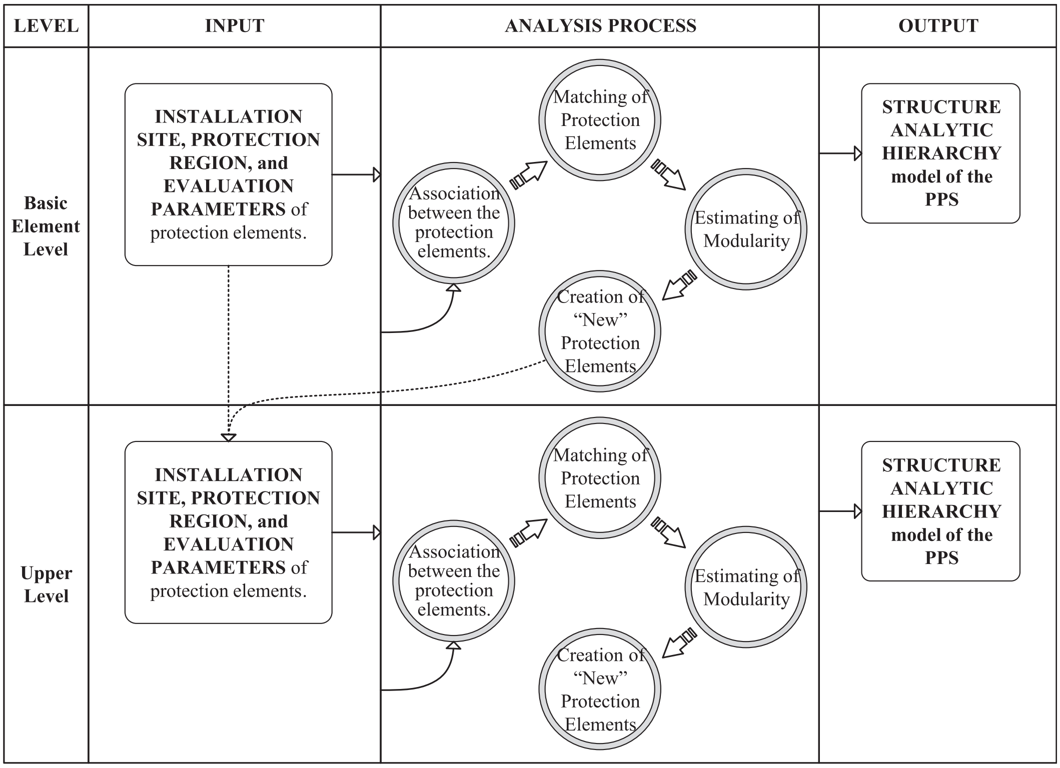

LEVEL
INPUT
ANALYSIS PROCESS
OUTPUT
Basic Element Level
INSTALLATION SITE, PROTECTION REGION, and EVALUATION PARAMETERS of protection elements.
Matching of Protection Elements
Association between the protection elements.
Estimating of Modularity
Creation of "New" Protection Elements
STRUCTURE ANALYTIC HIERARCHY model of the PPS
Upper Level
INSTALLATION SITE, PROTECTION REGION, and EVALUATION PARAMETERS of protection elements.
Matching of Protection Elements
Association between the protection elements.
Estimating of Modularity
Creation of "New" Protection Elements
STRUCTURE ANALYTIC HIERARCHY model of the PPS

Fig. 1. The analysis process diagram of SAHA. The analysis process includes four steps, assessment of association, matching of protection elements, estimation of modularity, and creation of new elements. The final output is the hierarchical PPS.

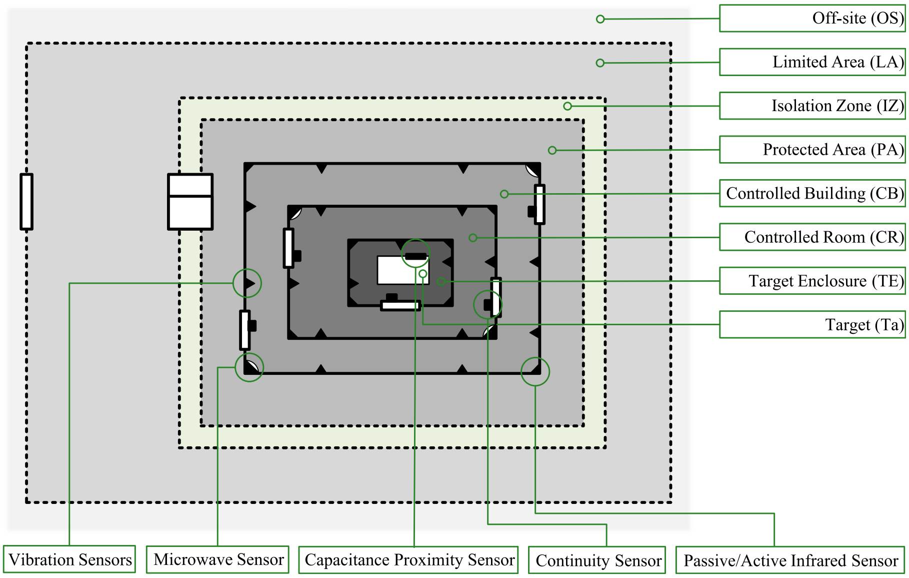


Fig. 2. Sketch of the minimum physical protection system.

algorithm based on the idea of a greedy algorithm for the measurement of the partition quality of community structural. The initial modularity formula is as follows:

$$Q = \frac{1}{2m}\sum_{i,j}\left[A_{i,j} - p_{i,j}\right]\delta(c_i, c_j) \tag{1}$$

where, Q is the modularity, the greater the modularity, the better the community partition. In the graph $G = (V, E)$, the adjacent matrix $A_{i,j}$ is the weight of connection from vertex i to j; $2m = \sum_{i,j} A_{i,j}$ represents all the degree of edges in the graph (weights of all edges in the network); the probability that an edge is connected to vertex i is $p_i = k_i/2m$; the probability that an edge is connected to vertex j is $p_j = k_j/2m$; the expected value of edge is $p_{i,j} = 2mp_ip_j = k_ik_j/2m$; $k_i = \sum_j A_{i,j}$ means the degree of the edges connected to the vertex i

Table 1
The definitions or characteristics of critical physical areas in the critical infrastructure.

Terms	Definitions/Characteristics
Off-site	An area outside a facility's land boundaries, not just exterior to the buildings.
Limited Area [20]	The designated area containing targets to which access is limited and controlled for physical protection purposes.
Protected Area	A specifically defined area inside a limited area containing targets, enclosed by at least one physical barrier, to which access is controlled.
Controlled Building	The controlled building is the vital areas and is located within protected areas and have additional barriers and alarms to protect vital equipment. (see 10 CFR 73.2, "Definitions")
Controlled Room [21]	A room serving as a central space where a large physical facility can be monitored and controlled.
Target Enclosure	Similar to material access areas, no one is allowed to be alone in a material access area (two-person rule). (see 10 CFR 73.2, "Definitions")
Target	An objective of an attack like critical facilities

(the sum of the weights); c_i is the community i; c_j is the community j; $\delta(c_i, c_j)$ is used to determine whether vertex i and j are partitioned into a unified zone, if so, $\delta(c_i, c_j) = 1$, if not, $\delta(c_i, c_j) = 0$.

$C = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$ is the index vector.

This paper uses the Newman community detection algorithm for the vulnerability analysis of the protection elements of PPS, the analysis steps are as follows:

1) Each protection element is assigned to a "unique" community then matched in order for each community. As shown in Fig. 3, the element i in the community i and has three adjacent communities j, k, l, and calculate the change modularity ΔQ of community i and community j, k, l.
2) Place the adjacent communities in the same cluster. If the change modularity is negative, the merge process is aborted. Aggregates all vertexes in the same cluster as a single vertex. Iterate the above step and reassess the changing community until any two matched communities cannot improve the overall modularity value.
3) The successful matched community is defined as "new" vertex in step 1. Reconstruct the sub-graph, and reassess each community. The final result is that all the vertexes are aggregated to a "big" community.

The Newman detection algorithm shows that the largest degree of modularity, the best structure is. Everitt [24] proposed a tree diagram named dendrogram for the illustration of the clusters produced by the hierarchical clustering. And a dendrogram will be established which obtained any level of sub-layer community structure and recorded the division results.

2.3. PPS hierarchical structure model

This paper uses a network structure for the illustration of the topological design of a complicated PPS with graphical vertexes equivalent to protection elements. The hierarchical structure model (HSM) is based on the community partition/detection algorithm proposed by Newman for the agglomerative modeling of PPS from the basic layer to the top layer.

The association rules between any two protection elements are relied on whether the protection elements prevent or deter the intrusion actions in one area are unified or not. A case shown in Fig. 2 is taken for the vulnerability evaluation of PPS protection elements. The association weight indicates that the protection elements have a certain similarity functions to the same protection area.

The preparatory work for the hierarchical structure modeling of the PPS is the association judgment of protection elements, including the mechanical barrier elements and intrusion detection elements, and the estimation of the associated weight value. The pairwise association values of the protection elements are determined by the association rules which in terms of the distance of each protection area and the protection functions.

2.3.1. Association rules

This paper proposes the following association rules to estimate the associated weight values between protection elements. Considering the delay of time is the most sensitive factor in PPS and the sphere of action of the protection elements, only the task time between two protective elements is estimated as the weight value. The minimum time between the two protection elements is calculated to represent the maximum associated weight.

There are two hypothetical situations shown in Fig. 4, the time estimation methods are as follows: 1) Assume that there are no obstacles between the two elements, time $= \text{distance}/_{\text{velocity}}$; 2)

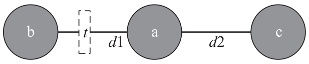


Fig. 4. The assessment of association value in both cases. Assume that the distance between protection element a and b is $d1$, the distance between a and c is $d2$. The task passed through the obstacle requires t minutes. The total time moved from element a to b is $d1/_v + t$.

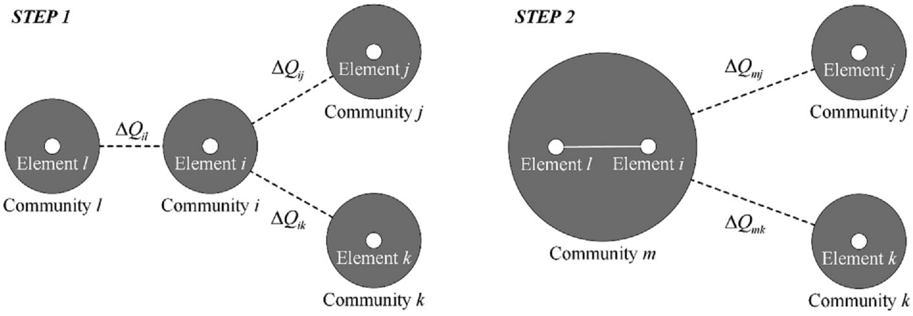


Fig. 3. Visualization of the illustration of the community structure model.

Assume that there are some obstacles, time $=$ time through the obstacles $+$ distance$/_{\text{velocity}}$.

In this paper, the associated weight is only related to the task time. The Poisson distribution is used to estimate the associated weight value.

$$A_{i,j} = 1 - \left(1 - \frac{\lambda^k}{k!}e^{-\lambda}\right) = \frac{\lambda^k}{k!}e^{-\lambda} \tag{2}$$

where, k is the number of adversary intrusion, $k = 0$ when there is no intrusion; λ is the average incidence of random intrusions per unit time.

$$\lambda = \frac{T_{i,j} + T_{obstacles}}{RFT} \tag{3}$$

where $T_{i,j}$ is the task time between the element i and j without obstacles; $T_{obstacles}$ is the task time for the obstacles;

$$A_{i,j} = e^{-\frac{T_{i,j}+T_{obstacles}}{RFT}} \tag{4}$$

The INPUT parameters of association rules include, 1) the characteristic of protection devices; 2) the physical area controlled by the protection device.

The OUTPUT: association value of any two protecting devices.

The associated weight matrix between element a and b is as follows:

$$A_{a,b} = \begin{array}{cc} \begin{array}{cc} a & b \end{array} & \\ \begin{pmatrix} 0 & f_{b-a} \\ f_{a-b} & 0 \end{pmatrix} & \begin{array}{c} a \\ b \end{array} \end{array} \tag{5}$$

3. Effectiveness evaluation of the PPS using SAHA method

The structure analytic hierarchy approach replaces the ASD for the structural division of PPS protection elements. The sub-elements are clustered upwards to update a parent-element to get the final results. Thus, the uppermost element is the whole basic protection elements based on the strictness and integrity of the critical infrastructure PPS.

3.1. Analysis of general method

The EASI method [7] is used to evaluate the effectiveness of the sub-element system. The criterion for successful interrupting the adversary intrusion is that the delay time of protection element should be longer than the response force time.

$$X = TR - RFT > 0 \tag{6}$$

where TR is the remaining time of the adversary's successful intrusion; RFT is the time for response force to reach the target; The critical detection point (CDP) defines the remaining time TR exceeds RFT for the first time. The CDP is used to initially determine whether the adversary can be interrupted or neutralized. Prior to the CDP, the adversary was found to give sufficient alarm evaluation and RFT to interrupt the adversary.

Assuming that TR and RFT are independent and normally distributed, the variable X is also independent and normally distributed. The mean and variance of variable X are:

$$\mu_X = E(TR - RFT) = E(TR) - E(RFT) \tag{7}$$

$$\sigma_X^2 = Var(TR - RFT) = Var(TR) + Var(RFT) \tag{8}$$

The task time the adversary passed through the protection elements is related to factors such as the skills and intrusion tools, thus, the average task time from area p to area n is:

$$E(TR) = E(TAD_p) + \sum_{i=p+1}^{n} E(T_i) \tag{9}$$

where, $E(TAD_p)$ is the average dwell time at the area p after the adversary is detected (ie, the defense measure effectively blocks the adversary intrusion at the area p); $E(T_i)$ is the task time at area i.

Assume that the adversary is independent through the defense elements, the remaining time variance from area p to area n:

$$Var(TR) = Var(TAD_p) + \sum_{i=p+1}^{n} Var(T_i) \tag{10}$$

Hence, under the premise of the effective detection of the adversary intrusion (defined as event A), the probability that response forces reach the target area to interrupt in advance is:

$$P(R|A) = P(X > 0) = \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_X^2}} e^{-\frac{(X-\mu_X)}{2\sigma_X^2}} dX \tag{11}$$

In the case of conservative evaluation of $P(R|A)$, SNL report indicates that $P(R|A) = 0$ if the detection after the CDP, i.e. the response force cannot reach the target area to interrupt or neutralize the adversary intrusion; on the contrary, the detection triggered before the adversary reached CDP, $P(R|A) = 1$. Thus, the detection probability of CDP is higher than that of other areas.

The probability of effective detection (event A) is:

$$P(A) = P(D)P(C) \tag{12}$$

where P(D) is the probability that the PPS detects the adversary intrusion. The detection probability consists of four parameters, $P(D) = f[P(D_S), P(D_T), P(D_A)]$. $P(D_S)$ is the probability that the PPS detects an adversary's abnormal or unauthorized intrusion event; $P(D_T)$ is the probability that the alarm information into evaluation information; $P(D_A)$ is the probability of the alarm is accurately evaluated. The detection probability is

$$P(D) = P(D_S) \times P(D_T) \times P(D_A) \tag{13}$$

Fig. 5 shows the detection process of PPS, the steps are as follows:

Step 1: PPS detects the adversary intrusion, the probability is $P(D_S)$;
Step 2: Generate an alarm signal;

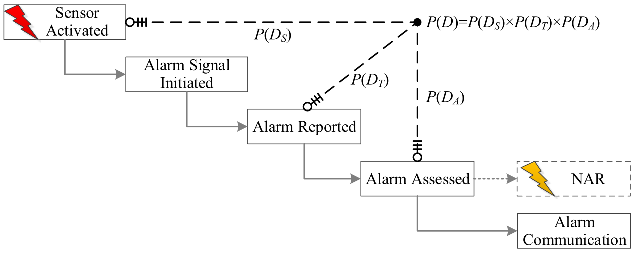


Fig. 5. Process of the detection of the sensor in PPS.

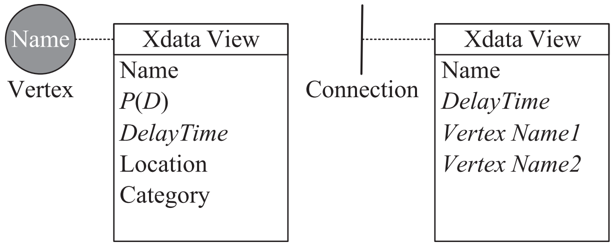


Fig. 6. Graphical representation and attribute definition of the protection element.

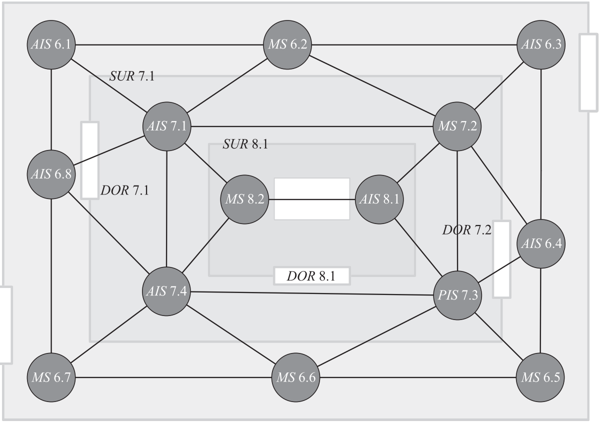


Fig. 7. The layout of the main sensor in the minimum system Community structure of the minimum case system.

Step 3: The alarm signal is converted into an evaluation signal, the probability is $P(D_T)$;
Step 4: Alert assessment, the probability is $P(D_A)$;
Step 5: Alarm evaluation ends until alarm communication.

P(C) is the probability of responding to an adversary intrusion.

When only one effective protection layer is set in the PPS (referring to the defense measures of the detection device and the defense measures not detected are deemed to be invalid defenses), the probability of interrupting the adversary intrusion is:

$$P(I) = P(R|A)P(A) \tag{14}$$

Thus, when multiple effective protection layers are set in the PPS, $P(I)$ is calculated as follows:

$$P(I) = P(A_1)P(R|A_1) + \sum_{i=2}^{n} P(R|A_i)P(A_i)\prod_{j=1}^{n-1}[1 - P(D_j)] \tag{15}$$

where, the $P(D_j)$ is the detection probability at the jth task, and the probability of undetected is $1 - P(D_j)$.

3.2. Clustering process of effectiveness evaluation

In this paper, the structure analytic hierarchy approach is proposed for the vulnerability evaluation of the PPS. Only two elements are considered for clustering and divided into series and parallel clusters. The serial-parallel connection mode of protection element is determined by the intrusion process. If the protection elements are required to pass through in sequence, it is equivalent to the serial connection. If not, it is equivalent to the parallel connection.

The equivalent processes of two parameters, task time and detection probability, are as follows:

(1) Task time

Serial state: the mean task time of an adversary through two protection elements in sequence is calculated as:

$$E(T_{a+b}) = E(T_a) + E(T_b) \tag{16}$$

The task time variance of an adversary through two protection elements is:

$$Var(T_{a+b}) = Var(T_a) + Var(T_b) \tag{17}$$

Parallel state: the mean task time of an adversary through two protection elements is equivalent to the element with the minimum task time:

$$E(T_{a+b}) = Min(E(T_a), E(T_b)) \tag{18}$$

The parallel variance is equal to the variance of the element with the minimum task time.

(2) Detection probability

Serial state: the mean detection probability of an adversary through two protection elements is calculated as:

$$P(D_{a,b}) = 1 - (1 - P(D_a)) \times (1 - P(D_b)) \tag{19}$$

Parallel state: under conservative conditions, the equivalent detection is the minimum detection probability of the two protection elements:

$$P(D_{a,b}) = Min(P(D_a), P(D_b)) \tag{20}$$

The probability of detection is calculated when each two protection elements are clustered according to formulas (19, 20).

4. Feasibility evaluation of the effectiveness of the minimum case system

In this paper, the protection elements and critical targets are properly initialized. Fig. 2 is used as a minimal case analysis system for the modeling and feasibility analysis of the hierarchical structure of PPS. Each protection element is represented as circle, the main xdata is stored connection circle and line, such as the detection probability, the delay time, and the location, etc. All of those are used for the basic elements definition as shown in Fig. 6. The thickness of the graphic lines indicates the degree of association between the two protection elements. Connection lines from thick to fine indicate the associated weight from strong to weak.

The hierarchical structure modeling and analysis platform is developed for the automatic identification of the installation area and relative installation position. The attributes are set synchronized with the process of modeling. Thus, a network structure diagram of PPS has the main original attributes after generation.

SAHA method is used to initialize the attributes of the protection elements and clustering analyze the protection elements that act on the same area shown in Fig. 7, element *AIS* means a group of active infrared sensors and element *MS* means a group of microwave sensors. Whenever a layer is clustered, the xdata of "new" protection element are updated. Identify the association of adjacent elements for the next cluster analysis.

Table 2 shows the basic attribute values of the protection element, including the probability of detection, delay of the meantime. The probability of communication and response force time are assessed from engineering experience.

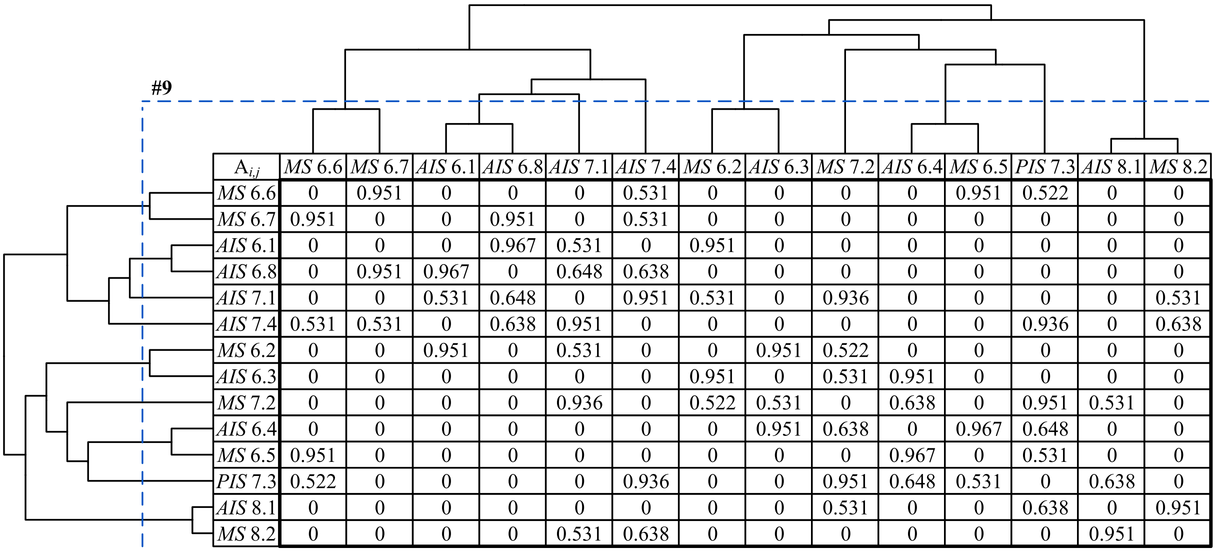
In addition, the SAHA method is applied to two-dimensional

Table 2
Essential input values of protection elements.

Probability of Communication *P*(*C*)				Response Force Time (*RFT*, s)			
				Mean Time (s)		Standard Deviation (s)	
0.95				300		90	
Elements	*P*(*D*)	Mean Time (s)	Standard Deviation (s)	Elements	*P*(*D*)	Mean Time (s)	Standard Deviation (s)
AIS 6.1	0.6	60	6	*PIS* 7.3	0.5	50	5
MS 6.2	0.7	70	7	*AIS* 7.4	0.6	60	6
AIS 6.3	0.6	60	6	*DOR* 7.1	0	120	12
AIS 6.4	0.6	60	6	*DOR* 7.2	0	120	12
MS 6.5	0.7	70	7	*SUR* 7.1	0	180	18
MS 6.6	0.7	70	7	*AIS* 8.1	0.6	60	6
MS 6.7	0.7	70	7	*MS* 8.2	0.7	70	7
AIS 6.8	0.6	60	6	*DOR* 8.1	0	120	12
AIS 7.1	0.6	60	6	*SUR* 8.1	0	180	18
MS 7.2	0.7	70	7				

Table 3
Hypothetical travel time between two protection elements.

Path Segment	Mean Time (s)	Path Segment	Mean Time (s)	Path Segment	Mean Time (s)	Path Segment	Mean Time (s)
AIS 6.1-*MS* 6.2	15	*AIS* 6.1-*AIS* 6.8	10	*AIS* 6.1-*AIS* 7.1	10	*MS* 6.2-*AIS* 6.3	15
MS 6.2-*AIS* 7.1	10	*MS* 6.2-*MS* 7.2	15	*AIS* 6.3-*AIS* 6.4	15	*AIS* 6.3-*MS* 7.2	10
AIS 6.4-*MS* 7.2	15	*AIS* 6.4-*PIS* 7.3	10	*AIS* 6.4-*MS* 6.5	10	*MS* 6.5-*PIS* 7.3	10
MS 6.5-*MS* 6.6	15	*MS* 6.6-*PIS* 7.3	15	*MS* 6.6-*AIS* 7.4	10	*MS* 6.6-*MS* 6.7	15
MS 6.7-*AIS* 6.8	15	*MS* 6.7-*AIS* 7.4	10	*AIS* 6.8-*AIS* 7.1	10	*AIS* 6.8-*AIS* 7.4	15
AIS 7.1-*MS* 7.2	20	*AIS* 7.1-*MS* 8.2	10	*AIS* 7.1-*AIS* 7.4	15	*MS* 7.2-*AIS* 8.1	10
MS 7.2-*PIS* 7.3	15	*PIS* 7.3-*AIS* 8.1	15	*PIS* 7.3-*AIS* 7.4	20	*AIS* 7.4-*MS* 8.2	15
AIS 8.1-*MS* 8.2	15	/	/	/	/	/	/



$A_{i,j}$	*MS* 6.6	*MS* 6.7	*AIS* 6.1	*AIS* 6.8	*AIS* 7.1	*AIS* 7.4	*MS* 6.2	*AIS* 6.3	*MS* 7.2	*AIS* 6.4	*MS* 6.5	*PIS* 7.3	*AIS* 8.1	*MS* 8.2
MS 6.6	0	0.951	0	0	0	0.531	0	0	0	0	0.951	0.522	0	0
MS 6.7	0.951	0	0	0.951	0	0.531	0	0	0	0	0	0	0	0
AIS 6.1	0	0	0	0.967	0.531	0	0.951	0	0	0	0	0	0	0
AIS 6.8	0	0.951	0.967	0	0.648	0.638	0	0	0	0	0	0	0	0
AIS 7.1	0	0	0.531	0.648	0	0.951	0.531	0	0.936	0	0	0	0	0.531
AIS 7.4	0.531	0.531	0	0.638	0.951	0	0	0	0	0	0	0.936	0	0.638
MS 6.2	0	0	0.951	0	0.531	0	0	0.951	0.522	0	0	0	0	0
AIS 6.3	0	0	0	0	0	0	0.951	0	0.531	0.951	0	0	0	0
MS 7.2	0	0	0	0	0.936	0	0.522	0.531	0	0.638	0	0.951	0.531	0
AIS 6.4	0	0	0	0	0	0	0	0.951	0.638	0	0.967	0.648	0	0
MS 6.5	0.951	0	0	0	0	0	0	0	0	0.967	0	0.531	0	0
PIS 7.3	0.522	0	0	0	0	0.936	0	0	0.951	0.648	0.531	0	0.638	0
AIS 8.1	0	0	0	0	0	0	0	0	0.531	0	0	0.638	0	0.951
MS 8.2	0	0	0	0	0.531	0.638	0	0	0	0	0	0	0.951	0

Fig. 8. The weight matrix $A_{\mathrm{i,j}}$ and the dendrogram of the minimum system.

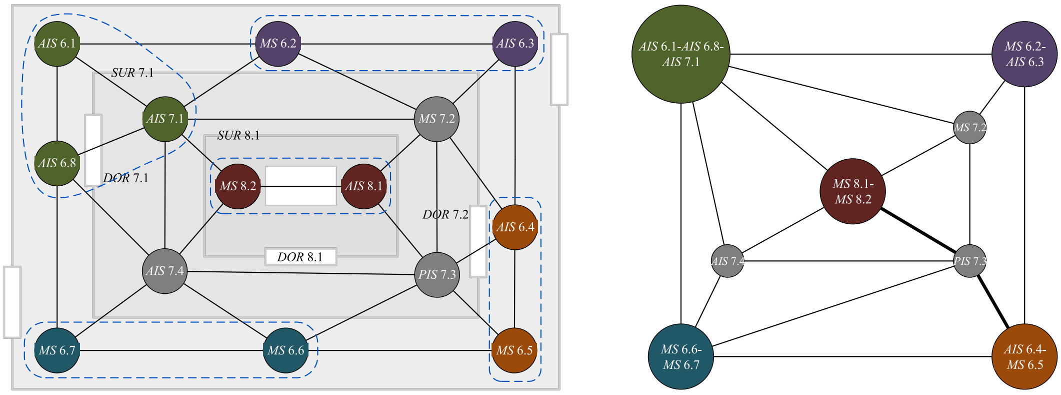
and three-dimensional model of critical facility. Thus, the mean travel time from one area to another with accurate graphics programming and simulation can be calculated. The hypothetical travel time between two protection elements shown in Table 3.

Fig. 8 display the datasheet of the weight matrix $A_{i,j}$ and the dendrogram. The dotted line is the pruning line, the value next to the dotted line indicates the number of clusters starting from the current position of the line.

As shown in Fig. 9.a, associated protection elements marked with the dotted line for the partition of the minimum case system. Fig. 9.b is the abstract diagram of Fig. 9.a.

The associated weight matrix is used to determine the association of the protection elements. From the dendrogram, the protection element *AIS* 8.1 and *MS* 8.2 have the maximum degree of the association at the first cluster level. The *MS* 6.6, *MS* 6.7, *AIS* 6.1, *AIS* 6.8, *AIS* 7.1 and *AIS* 7.4 are aggregated into a group, the *MS* 6.2, *AIS* 6.3, *MS* 7.2, *AIS* 6.4, *MS* 6.5, *PIS* 7.3, *AIS* 8.1 and *MS* 8.2 are aggregated into another group. All the protection elements merged into an entirety, that is, PPS. Elements *AIS* 8.1 and *MS* 8.2 have the highest association among all the two elements.

The evaluation of a cluster group is equivalent from outside protection elements to the inside according to the intrusion



(a) SAHA for the partition of the minimum case system at the specified level.

(b) Abstract diagram of left figure (a).

Fig. 9. The graphical aggregation process of the minimum case system. The same color represents the association of protection elements will be clustered as a "new" element. As a replacement for ASD, the abstract diagram shows the internal structure of PPS protection elements. (For interpretation of the references to color in this figure legend, the reader is referred to the Web version of this article.)

direction and the equivalent processes. The vulnerable intrusion path is (*AIS* 6.4, *MS* 6.5), *PIS* 7.3, (*MS* 8.1, *MS* 8.2), the thick lines in Fig. 9.b, the probability of interruption $P(I) = 0.697594$.

The effectiveness of PPS is evaluated according to the probability of interruption. The way to improve the effectiveness is to increase the interruption probability, that is, to upgrade the performance of the protection elements to detect and delay the adversary. At a certain level, a new sensitive area is redefined which involved more than one physical area.

5. Conclusion

In this paper, a novel method used structure analytic hierarchy approach is proposed for the vulnerability evaluation of the complicated PPS effectiveness. SAHA is used to cluster the adjacent protection elements based on the association rules. The association rules combined with the PPS is proposed to estimate the associated weight values between protection elements. The dendrogram displays different levels of aggregation. For the evaluation of the PPS effectiveness, an equivalent method is presented for the calculation of the main parameters of series and parallel clusters. A minimum case system is illustrated for the feasibility analysis of the SAHA method. The results displayed in graphical makes the association protection elements and the vulnerable protection areas clear.

Declaration of competing interest

The authors declare there is no conflicts of interest regarding the publication of this paper.

Acknowledgements

This work was supported by the China Postdoctoral Science Foundation, under Grant 2019M652906.

References

[1] T. Loveček, J. Vaculík, L. Kittel, Qualitative approach to evaluation of critical infrastructure security systems, Eur. J.Secur.Saf. 1 (1) (2012) 1–11.
[2] M. Coole, J. Corkill, A. Woodward, Defence in Depth, Protection in Depth and Security in Depth: A Comparative Analysis towards a Common Usage Language, 2012.
[3] R. Nunes-Vaz, S. Lord, Designing physical security for complex infrastructures, Int. J. Crit. Infrastruct.Protect. 7 (3) (2014) 178–192.
[4] C.D. Jaeger, N.S. Roehrig, T. Torres, Development of an Automated Security Risk Assessment Methodology Tool for Critical Infrastructures, Sandia report, 2008.
[5] F. Argenti, G. Landucci, V. Cozzani, et al., A study on the performance assessment of anti-terrorism physical protection systems in chemical plants, Saf. Sci. 94 (2017) 181–196.
[6] Z. Vintr, M. Vintr, J. Malach, Evaluation of physical protection system effectiveness. Security Technology (ICCST), in: 2012 IEEE International Carnahan Conference on, IEEE, 2012, pp. 15–21.
[7] M.L. Garcia, The Design and Evaluation of Physical Protection Systems, second ed., Elsevier Butterworth–Heinemann, Burlington, MA, 2008.
[8] M.L. Garcia, Vulnerability Assessment of Physical Protection Systems, Elsevier Butterworth–Heinemann, Burlington, MA, 2006.
[9] H.A. Bennett, EASI Approach to Physical Security Evaluation, Sandia National Laboratory, Albuquerque, NM, 1977. SAND-760500.
[10] D.W. Whithead, C.S. Potter, S.L. O'Connor, Nuclear Power Plant Security Assessment Technical Manual, Sandia National Laboratory, Albuquerque, NM, 2007. SAND-007-5591.
[11] S.A.V.I. Sandia National Laboratory, Systematic Analysis of Vulnerability to Intrusion, SAND89-0926, Sandia National Laboratory, Albuquerque, NM, 1989.
[12] R.A. Al-Ayat, T.D. Cousins, E.R. Hoover, ASSESS Update – Current Status and Future Developments, UCRL-JC-104360, Lawrence Livermore National Laboratory, Livermore, CA, 1990.
[13] S.S. Jang, S.W. Kwak, H. Yoo, J.S. Kim, W.K. Yoon, Development of a vulnerability assessment code for a physical protection system: systematic analysis of physical protection effectiveness (SAPE), Nucl. Eng.Technol 41 (5) (2009) 747–752.
[14] V.D. Blondel, J.L. Guillaume, R. Lambiotte, et al., Fast unfolding of communities in large networks, J. Stat. Mech. Theor. Exp. 2008 (10) (2008) P10008.
[15] U.N. Raghavan, R. Albert, S. Kumara, Near linear time algorithm to detect community structures in large-scale networks, Phys. Rev.E 76 (3) (2007), 036106.
[16] J. Shi, J. Malik, Normalized cuts and image segmentation, IEEE Trans. Pattern Anal. Mach. Intell. 22 (8) (2000) 888–905.
[17] B.W. Kernighan, S. Lin, An efficient heuristic procedure for partitioning graphs, Bell .Syst.Tech.J 49 (2) (1970) 291–307.
[18] F. Sayadi, Y. Said, M. Atri, et al., Physical Protection Systems and Critical Infrastructure Protection in the Czech Republic. Recent Researches in Automatic Control, Systems Science and Communications, 2012.
[19] Sadia, Adversary Sequence Diagram (ASD) Model, International Training Course on the Physical Protection of Nuclear Facilities and Materials, 2018 (Albuquerque, New Mexico, USA).
[20] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna, 2011.
[21] J. Wood, Control Room Design, Human factors for engineers, 2004, pp. 203–233.
[22] M.E.J. Newman, Fast algorithm for detecting community structure in networks, Phys. Rev.E 69 (6) (2004), 066133.
[23] M.E.J. Newman, Detecting community structure in networks, Eur. Phys. J.B 38 (2) (2004) 321–330.
[24] B. Everitt, A. Skrondal, The Cambridge Dictionary of Statistics, Cambridge University Press, Cambridge, 2002, p. 96.
[25] Y.A. Setiawan, S.S. Chirayath, E.D. Kitcher, MAPPS: a stochastic computational tool for multi-path analysis of physical protection systems, Ann. Nucl. Energy (2019) 107074.
[26] F. Argenti, G. Landucci, G. Reniers, et al., Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network, Reliab. Eng. Syst. Saf. 169 (2018) 515–530.