

Received April 19, 2019, accepted June 6, 2019, date of publication June 21, 2019, date of current version July 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2924239

Development of an Interaction Simulator for the Scenario Analysis of Physical Protection Systems

ZOU BOWEN¹, LIU JIAN², WANG WENLIN³, YAN ZHENYU²,
LIU GAOJUN², YANG JUN¹, AND YANG MING¹

¹School of Electric Power, South China University of Technology, Guangzhou 510641, China

²State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Guangdong Nuclear Power Engineering, Design Company Ltd., Shenzhen 518116, China

³School of Automation, Wuhan University of Technology, Wuhan 430070, China

Corresponding author: Wang Wenlin (wangwenlin@whut.edu.cn)

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

ABSTRACT Scenario analysis is used for the simulation of the physical protection system (PPS) by considering several credible intrusion and defense scenarios. A practical interaction simulator is developed for the scenario analysis of the PPS. The interaction simulator integrates all discrete subsystems of the PPS to form an intermodulation chain of intrusion-detection-response-interruption. Adversary intrusion strategies and defense strategies are regarded as knowledge bases in the interaction simulator. Moreover, agents in the simulator can graphically travel dynamically. Thus, this simulator is used to verify and validate the daily operation flows of each subsystem, applied for long-term management of intrusion consequences, and helped the relevant staffs for training and vulnerability analysis of the PPS.

INDEX TERMS Physical protection system, scenario analysis, adversary intrusion.

I. INTRODUCTION

A Physical Protection System (PPS) is used to protect critical facilities from malevolent adversary's use and destruction. National Academy of Sciences [1] in 2002 indicated that the nuclear power vulnerabilities to potential adversary intrude include nuclear power plants (NPPs), research reactors, spent nuclear fuel, and radioactive waste.

A PPS is defined as an integrated collection of components or elements designed to interrupt adversary intrusion according to the specific regulations. PPS has three primary functions include detection, delay and response. These three functions contain a sizeable amount of states to graphical describing dynamic behavior of the entire PPS.

All state transitions describe the adversary intrusion strategies and the defense strategies in PPS. The transition logic of PPS states has a lot of statement coding of "if-else" judgment which are similar to rule reasoning. Thus, based on the state machine diagram [2], finite-state machines [3] and basic theory of Petri net [4], this paper develops a scenario analysis method which is used security risk simulation system for the dynamic simulation of the process of adversary intrusion and the process of defense. The scenario analysis is

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed M. Elmisery.

defined as a methodology for analyzing effectiveness of PPS by considering several possible adversary intrusion scenarios and response of defense [5].

Bassam *et al.* [6] proposed a model-based system engineering models for PPS evaluation and used SysML for the vulnerability assessment of PPS. SysML is defined as an extension of a subset of the unified modeling language (UML) using UML's profile mechanism. Uke *et al.* [7] used the state machine diagram to model behavioral on critical security attacks residing in the physical and data link layer. Similarly, Wang *et al.* utilized UML method for modeling of the cases of cross-layer attack to better understand the behaviors of the adversary.

Annarita *et al.* proposed a model-driven approach which is based on the UML method and BBN model to design and evaluate the modern PPS. Annarita transformed the structure of the UML specification into BBN model for the background analysis of PPS in an automatic way. Haq *et al.* [8] characterized a physical infrastructure and proposed a meta-model which was based on UML to describe the basic structure and attributes of infrastructure.

MacDonald *et al.* [9] presented a discrete event simulation model for the integration analysis of physical and cyber security systems. The discrete event simulation model is based on the graphical configuration. Some scholars use the Petri net

to describe the security system, Chen *et al.* [10] investigated the used the Petri net for the model of coordinated physical and cyber-attacks on the smart grid.

The method mentioned above using the visually modeling tools for the design and evaluation of physical security or cyber security. The specific analysis of the procedure and potential upgrade are less analyzed and studied. This paper proposed a security risk simulator (or simulation system) for the dynamic simulation of the intrusion scenarios and defense scenarios to prevent the severe intrusion event in daily simulation and mitigate the intrusion hazard after intrusion event happens. In addition, this approach can be applied in the field of cyber security [23], the protection system for cyber security also includes [25] detection function [24], delay function, and response function.

The traditional PPS consists of a series of scattered independent systems such as video surveillance, patrol management, access control management, intrusion detection system, information dissemination, security communications, etc. The security risk simulator integrates the all subsystems and analyzes the linkage of each subsystem to form an inter modulation simulation chain of intrusion-detection-response-interruption. In addition, hierarchical interaction of comprehensive information, emergency response implementation status and event recording criteria are established in the simulation platform for the scenario analysis of PPS.

The security risk simulator can also be used as emergency decision supports system to obtain the optimal countermeasures based on the back-end knowledge base. The system provides virtual contingency plan and actions (knowledge base) to help analyst or users to comprehend the behavior of agents. The system is updated with the upgrade program of PPS to ensure all the subsystems are the latest state and mine the vulnerability protection elements, suspicious staff, error regulations, etc.

II. OVERVIEW OF SECURITY RISK INTERACTION SIMULATOR

Security risk [11] means the potential for an unwanted outcome resulting from a security event. In this paper, the security risk interaction simulator is developed for the prevention of intrusion event and served as a learning approach of PPS for relevant staffs. The general design and evaluation process outline of PPS is divided into four parts, definition of PPS requirements, design, evaluation, and final design or redesign of PPS. The process of scenario analysis is in the period of the evaluation of PPS.

IAEA [12] indicated that the life cycle of PPS for critical infrastructure includes six steps, design, implement, sustain, evaluate and redesign. The sustain phase of PPS encompasses six processes, that is, the operating procedures (instructions); human resource management and training; equipment updating, maintenance, repair and calibration; performance testing, operational simulation; configuration management; resource allocation and operational cost analysis. These six processes can be written in the simulator as an electronic procedure.

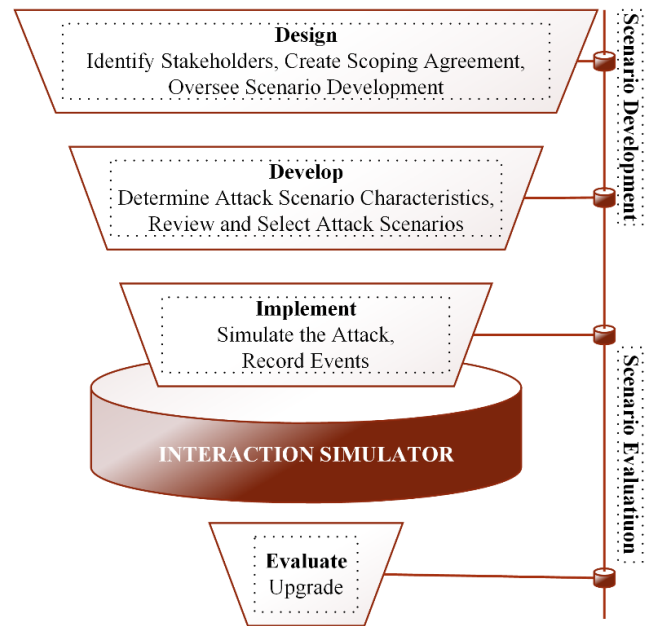


FIGURE 1. Process of scenario analysis in interaction simulator.

Figure 1 shows the improvement on scenario analysis process which includes four steps, design, develop, implement and evaluate [5]. In the phase of scenario development, the security risk simulator constructs a knowledge base for the description of the current status of PPS. This knowledge base is based on the expert knowledge and long-term experience accumulated by skilled staffs. Security risk simulation system defines various states of agent and transition conditions between states, and defines execution logic and jump statements between various states. The knowledge bases in the interaction simulator are organized, processed, and refined according to the human intuition.

The PPS is kind of responsive system that includes adversary, detection staff, response force, protection elements, etc. From the view of the agent, PPS includes the process of intrusion, process of detection, detection staff and response force cooperate to interrupt the adversary intrusion.

The security risk simulator shows the different states of the agents in different scenarios and displays the changes in the state which are caused by the handling of some events. In the simulation system, behavior modeling on each agent is the foundation of virtual scenario analysis. This paper defines behavior modeling on an agent which is that the agent executes the relevant sequence of actions in response to different events throughout its lifecycle.

III. DEVELOPMENT OF SECURITY RISK SIMULATOR

This paper uses the principle of state machine for the scenario analysis of PPS. The elements of state machine are called behavioral elements which represent the state of elements transit with the time and events. State machine is used to simplify the complex intrusion events and defense strategies of the PPS into several state sets. The state transitions simulate

the process of adversary intrusion and process of intrusion prevention, that is, the attack and defense scenarios. When an input event is received, the system produces an output accompanied by a transition of the state.

The complex scenarios are decomposed into a finite number of states with graphical security risk simulation system. The specific terminologies of security risk simulation system in PPS are:

State: means the state of the agent during its life cycle (such as the adversary intrusion state include climbing, jogging, running, etc.). Content of a state include name (for distinguishing the state from other states), entry and exit actions (actions performed when entering and exiting the current state), internal transition (do not change the state), deferred event (suspend the current state, and wait for other states to be processed).

Agent: intelligent agent, interact with the environment. All types of agents as shown in table 1, including human and devices.

TABLE 1. Category of agent.

Category	Content
Human	Detection Staff, Response Force, Management Staff, Adversary
Device	Detection Element, Delay Element







Event: is a notable occurrence at a particular point in time. There are four types event in risk simulation system, include external event is an explicit signal from outside the system, internal event means an invocation from the system, the timer event means the passage of a designated period of time and the primary event is an internal transition in one state (only the primary event hold in the state).

Transition: refers to a directed relationship between two states. The transition is used to display the control flow from the initial state to the target state, represented by a solid connecting line with parameters. Transition indicates the transition of the actors between the two states.

Basic components of an interaction simulator are shown in table 2. The control node of state machine diagram include: decision node, merge node, fork node, and join node. The decision node selects the direction of the output based on the dynamic evaluation of the guards of the triggers of its outgoing transitions. The merge node is composing of one input node and multiple output nodes. Once an input signal enters the merge node, the signal is output directly without any analytical process.

Fork state makes parallel processing states. An event generates multiple parallel events at the fork state and processes the state in parallel. That is, all of the states connecting the output side of the fork state will be active when the event hold in the input side is fired. Join state synchronizes all input side parallel state and makes a transition to one state. That is, multiple accurate completed parallel input side states enter the unique output side state.

TABLE 2. Basic components of an interaction simulator for modeling the PPS scenarios.

SYMBOL	TERM	DEFINATION
	State	State represents the condition of an object at a particular point in time, including simple state, initial state, final state, composite State.
	Decision	Decision state accepts tokens on one or two incoming edges and selects one outgoing edge from one or more outgoing flows.
	Merge	Merge state brings together multiple incoming alternate flows to accept one outgoing flow.
	Fork	Fork state makes parallel processing states.
	Join	Join state synchronizes all input side parallel state and makes transition to one state.
	Transition	Transition is an arrow line connecting between states. Events and actions are hold in the transition line.

The process of scenarios analysis includes the agent of characters and sequence of events. In the human category, the agent of a person is divided into different behaviors to distribute execute the sequence of events. In general, the regulations of meta-model of human are complex, which are necessary to refine regularly.

IV. INTERACTION OF AGENTS

Figure 2 is the interactive simulation process of agents which integrates intrusion and defense. The agents include adversary, response force, detection staff, delay element, etc. When the adversary penetrates an area successfully, the state of detection and state of delay turn into failure. In addition, section 5 explains the transfer of parameters to calculate the risk in the figure 2.

In this paper, the key staffs involved in the PPS include NPPs managers, detection staffs and response forces. Figure 2 shows the different responsibilities of management staff, detection staff, and response force at the time of intrusion happened. The detection staff directly access alarm and analyzes the intrusion information. The analysis results of alarm will be transferred to the response forces and management staffs. The response force gets the optimal scheme to interrupt the adversary. The management staffs use the intrusion information for the generation of comprehensive emergency programs to prevent internal and external adversary intrusion while upgrading the protection element of PPS. The above description is the most basic functions of the staffs. For the nuclear power plants, the staffs have many daily procedures for repetitive operations to ensure the security of the nuclear power plant.

A scenario analysis of PPS, as showed in figure 3, can effectively bundle management staff, detection staff and response force to achieve real time cooperation, interaction of comprehensive information and response of emergency. In engineering, the nuclear power plant develops an integrated management platform to supervise and manage the

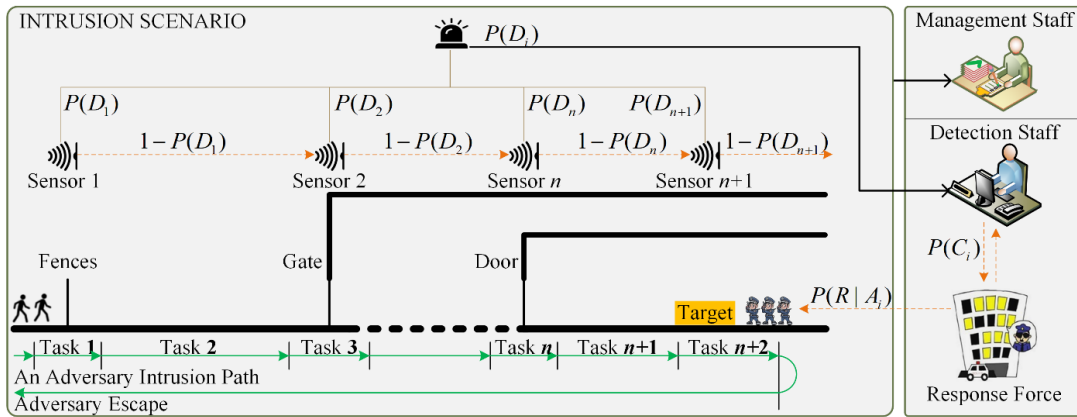


FIGURE 2. Interaction simulation of nuclear staff.

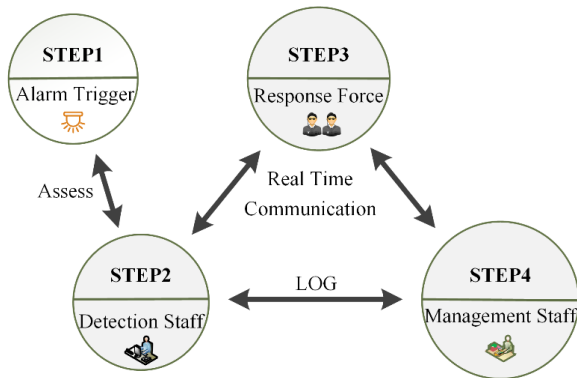


FIGURE 3. Security management methods in NPPs.

three roles which can reduce the consequences of failure of defense against adversary intrusion caused by human error.

Figure 3 is the security management methods in NPPs, including the basic four steps:

STEP 1: According to the trigger information of the detection elements, the detection system will generate an alarm signal and transmit the alarm signal to the server. Detection staffs estimate the validity of alarm (determine whether it is a false alarm). Simultaneously, detection staff extracts other information such as location of the alarm signal, the alarm level, etc.

STEP 2: According to the estimation results of the alarm, when the alarm is a false alarm, eliminates it. Then log and upload to the management department for reporting. The management staff performs further maintenance to eliminate the false alarm. When the alarm is not a false alarm, detection staff analyzes and processes the causes of the alarm according to the alarm level and alarm type, records the log and eliminates the alarm.

STEP 3: If the alarm level is the second and third level alarm, and the alarm UI is approved, the detection staff should communicate the response force to interrupt the adversary intrusion in time. If the alarm level is the first level alarm, the alarm UI is approved. The subsequent steps are processed by the PPS emergency regulations. It is found that the

adversary is intruded, the response force need to be called in time to interrupt the adversary intrusion.

STEP 4: Deploy of the response force according to the regulations and actual situation. Management staffs need to analyze the log after an intrusion event occurs and to upgrade the PPS in time to prevent the next intrusion of the adversary.

A. ADVERSARY

According to the threat assessment and design basis threat [13], attack scenarios should consider external and insider adversaries. The insider threat is the most risky and easiest to intrude the NPPs. In the design basis threat, the adversaries are divided into at least eight categories, including international terrorist (may include an insider colluding), domestic terrorist: Eco and Militia (may include an insider colluding), criminal, extremists, vandals or hackers, foreign intelligence officer, psychotic, and insider. As the initial event of the intrusion, the type of adversary is difficult to estimate because of human behavior is unpredictable. For the different type of adversary, the diverse intrusion information includes number of adversaries, equipment, vehicles, weapons, motivation, tactics, targets of interest, etc. For example, the international terrorist with the motivation of mass casualties, generally consists of 3-10 members and equips with unlimited hand or power tools.

Adversary intrusion behavior includes walking, running, crawling, climbing (up or down), and driving (pick up), etc. The consequence of adversary intrusion is mainly penetrating without alarm successful, continue to penetrate ignore the alarm, escape with alarm. The state transition modes of adversary task are the protection areas and the protection elements. The intrusion process [14] for an adversary follows these basic steps: the selection of a target for attack, the selection of an attack scenario, and choose a critical (vulnerability) adversary path to reach the target at the end.

B. RESPONSE FORCE

The response forces may include proprietary or contract guards, local and state police, etc. In view of various types

of response force are used, it is important to train to improve the effective guard. The specific functions of response force are the interruption and neutralization of adversary intrusion actions. The effectiveness analysis method of response force is the ability assessment to arrive in time and prevent completion of the adversary.

IAEA stated that the guard and response force should respond effectively and promptly to prevent adversary from completing the intrusion task. PPS should be performing a performance test at least once a year include appropriate exercises, such as actual combat exercises, to determine whether the response force can interrupt the adversary.

When the response forces are communicated and how they are arrived at the target area are the main problem of response force module of PPS. In the event of a security emergency, security risk simulation system helps the decision making team to give a contingency plan. The analysis process of security risk simulation system act as a decision support system can give response force detailed interruption information.

The utility evaluation of response force includes response force time to the target area and effectiveness of interrupting the adversary. The goal of the response force training is to maximize the utility of PPS and exert the capabilities of the response force to protect the critical assets. In the evaluation of effectiveness of PPS, it is known that the response force time is shorter in the limited response time, the probability of interruption and neutralization of adversary is greater.

C. DETECTION STAFF

In order to deal with the internal and external threats, once there is an alarm triggered, the investigation of unauthorized actions should be carried out by continuous simulation. Two-person rule is utilized to prevent compromising facility security which required two knowledgeable staffs to be involved in a detection activity. Functions of permanently staffed central alarm station are required simulation and assessment of alarms, initiation of response, and communication with the guards, response force and facility management.

Detection regulation is used to assist detection staff to analyze the alarm information and handle emergency information reasonably. Detection is one of the main functions in PPS, which determines the capability of PPS to protect critical facilities. Detection regulation is relatively complicated. Training of detection is required to perform multiple times to eliminate the error rate of detection staff.

D. MANAGEMENT STAFF

In this paper, the key responsibilities of the management staff are analysis of log and upgrade of PPS. For the false alarm of sensor, the staff should notify the designer for the redesign of PPS. If it is a product problem, the maintenance department upgrades the protection elements. If it is a layout problem, re-layout the protection elements to ensure the detection requirement is reached in the false alarm area. In case of accidental intrusion, if there is no accompanying staff, the detection staff should raise the

threat level to critical reflects, verify and review the identity of visitor; if there is an accompanying staff, the staff should be re-educated security to eliminate the probability of internal adversary.

E. PROTECTION ELEMENT

1) DETECTION ELEMENT

The intrusion detection sensors are used for detection of an adversary action [15]. In critical infrastructure, exterior sensors typically included fence sensors, line of sight sensors and video motion sensors [16] are installed on the exterior of the critical building, which have capacity to resist the weather conditions and nuisance alarms from external disturbances. The interior sensors are categorized by the structure for barriers and interior spaces and placed on the interior of the building, include boundary penetration sensors, volumetric motion sensors, point sensors, etc.

The states of the normal operation detection sensors are *detect* and *undetected*.

2) DELAY ELEMENT

Delay device is used to control, limit, or exclude access to the critical physical areas. After an adversary has been detected, the delay element will prevent completion of the malevolent act and provide sufficient delay until the threat is removed. A delay element is penetrated when an individual (or adversary) can pass through, over, under, or around the protective structure.

States of delay element are *penetration* and *non-penetration*.

F. RISK ASSESSMENT

The figure 4 is an analytic process of system risk under different design basis threats. The results of risk assessment are used to assist managers for analysis. The steps include optional screening analysis, facility characterization,

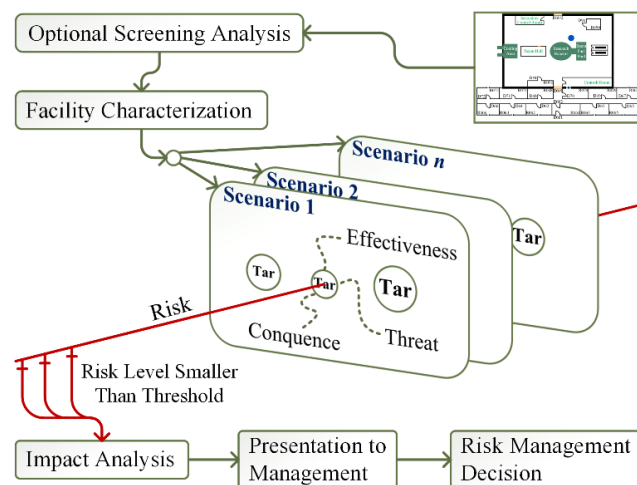


FIGURE 4. Risk assessment process. The risk estimation equation contains three parameters, threat, consequence and effectiveness.

(threat analysis, consequence analysis, effectiveness analysis), impact analysis, presentation to management, and risk management decision. The basic risk equation proposed by Sandia Laboratory is

$$R = P(A) * [1 - P(E)] * C = P(A) * [1 - P(I) * P(N)] * C \tag{1}$$

where, $P(A)$ is the likelihood of attack (design basis threat) qualitative evaluation; $P(E)$ is the effectiveness of PPS (effectiveness); C is the consequence of the loss (consequence), qualitative evaluation; $P(I)$ is the probability of interruption; $P(N)$ is the probability of neutralization.

The evaluation process of effectiveness of PPS is simplify to calculate the probability of interruption and the probability of neutralization. The probability of interruption equation [17] is

$$P(I) = P(D_1) * P(C_1) * P(R|A_1) + \sum_{i=2}^n P(D_i) * P(C_i) * P(R|A_i) * \prod_{j=1}^{i-1} (1 - P(D_j)) \tag{2}$$

where, $P(D_i)$ is probability of detection at i -th location, $P(C_i)$ is probability of communication to the response force, $P(R|A_1)$ is the probability of response force arrival prior to the interruption of the adversary's action sequence, n is the total number of tasks.

The probability of neutralization equation [18] is

$$P(N) = N(W)/N(E) \tag{3}$$

where, $N(W)$ is the number of the following outcomes of the $N(E)$, the adversary is killed, is captured, or abandons the attack and flees; $N(E)$ is the number of events where two opposing forces, such as response force and adversary, use tools to achieve their respective purposes.

In the security risk analysis, the quantitative parameters include delay time of each protection element, probability of detection, probability of communication, response force time. In the interaction simulator, those parameters can be assigned in advance and analyzed directly during the simulation.

G. CASE STUDY

Security risk simulation system is utilized to simulate the adversary intrusion scenario. The eight intrusion scenarios proposed by NCPA [19], [20] as design basis threats can be considered as intrusion drills, namely, a truck bomb, attack by boat, suicide attack by small aircraft, frontal assault with small arms, attack with rockets or medium artillery, sabotage of the power lines to and from the plant, infiltration and sabotage, suicide crash of a hijacked commercial airliner into the reactor building and spent-fuel storage.

During the simulation of security risk, the required time for each state is set on the security risk simulation platform. In the case of considering internal threats, it can be assumed that a protection device has failed. For example, an alarm occurs in D61/2, if D60/1 element is the internal insider's

jurisdiction or the adversary can easily penetrate, the delay time is set to 0.0s on the security risk simulation platform to simulate the internal threat mode as shown in figure 5.

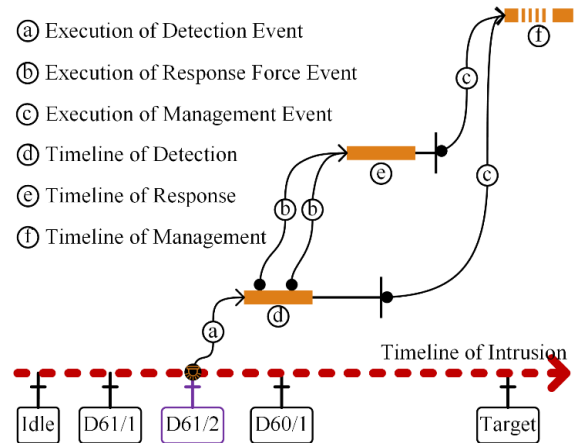


FIGURE 5. An area where adversary is detected in the adversary intrusion path.

1) ADVERSARY

The adversary is normally characterized into three broad groups, outsiders, insiders, and outsiders working in collusion with insiders. States of intrusion include continuous intrusion, intrusion interrupted, and escape. Depending on the design basis threat, the tools of attack include hand tools, power tools, burn bars, as well as any tools located at the facility. The behavior of attack along the vulnerable adversary path includes running, walking, climbing, etc.

2) DETECTION STAFF

Detection is one of the main functions to detect the adversary. The detection staff performs the assessment of alarm. Two purposes of assessment are: determine the cause of each sensor alarm and provide additional intrusion information to the response force. A key principle for the detection staff is that detection is not complete without an assessment. Thus, detection regulation is relative complicated. The regulation of the level I alarm is different from the level II and level III. Level II and III alarms are the most serious alarm. After the alarm is audited by UI, one-touch called response force to provide sufficient time for the interruption of the adversary. After the detection procedure is completed, the analysis data are stored in the database as evidence for post-mortem investigation and as a basis for the upgrade of the PPS.

3) RESPONSE FORCE

In the virtual scenario, the regulations for the response force are as follows:

After receiving the alarm signal, analyzer determines the number of attendances according to the alarm level and risk level. The response force repeatedly verify the location of the target to the detection staff for timely arrival. The analyst should estimate the path between the target and station of

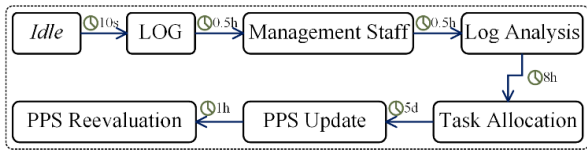


FIGURE 6. Simplified drilling regulation of management department.

response force, and search for the optimal route to the destination. If multiple locations are invaded, the number of response force should be reasonably allocated according to the priority of the target.

4) MANAGEMENT STAFF

As shown in figure 6, management analyzes the log to find out the vulnerability and errors of PPS. After upgrading the PPS, the analyst reevaluate the effectiveness of PPS to form a closed loop of design-analysis-design. In addition, administrative procedures should be revised for the better regulation of staff behavior.

Figure 7 shows integrated security risk system of PPS which effectively integrates the decentralized subsystems of PPS. The detection regulation is based on a NPP comprehensive security management patent [21] which proposed by Shanghai Nuclear Engineering Research & Design Institute.

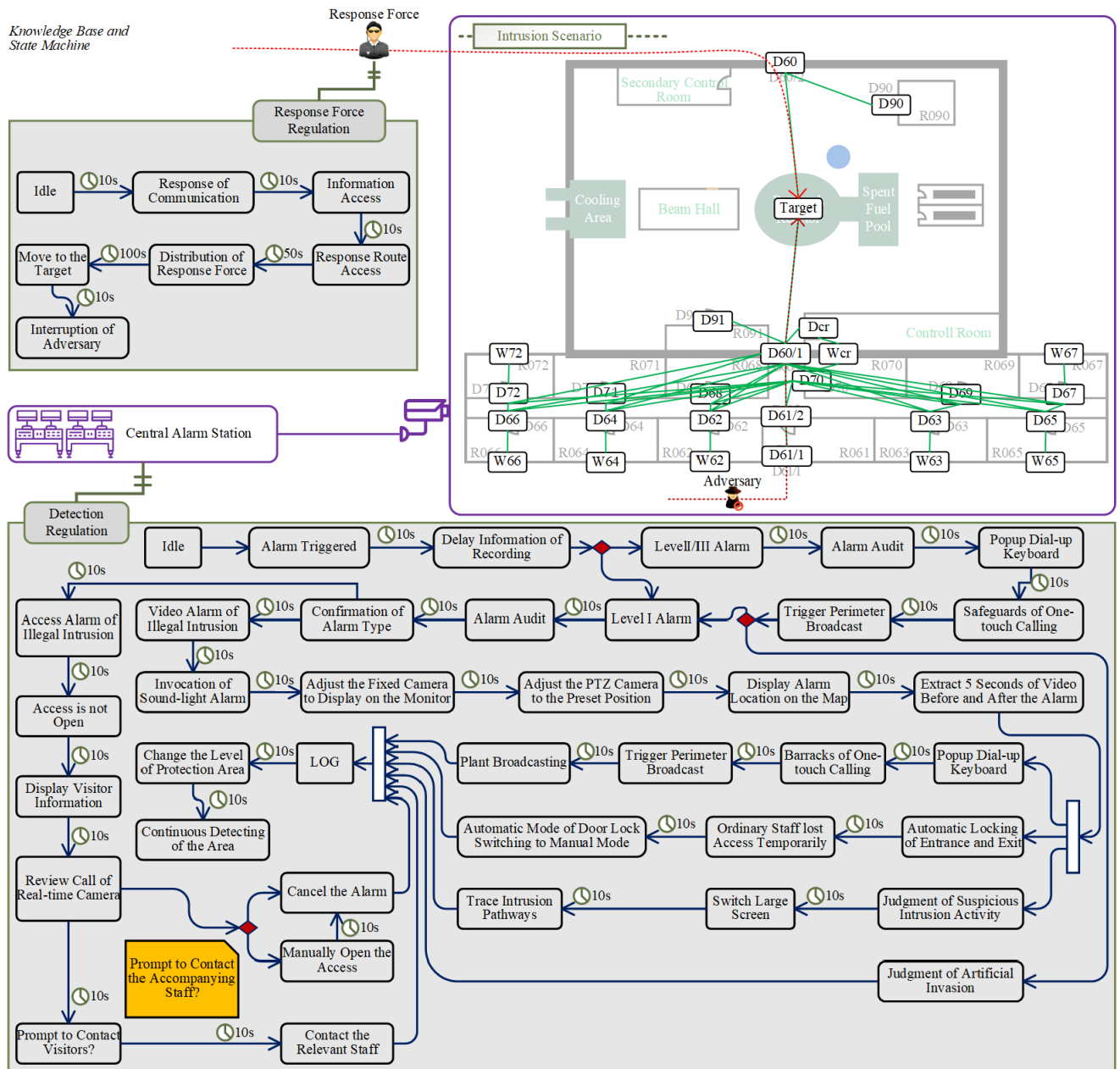


FIGURE 7. Detailed flowchart of integrated security management methods for NPPs. This process management handles the collaboration of independent systems.

Security risk simulation model establishes a clear responsibility management and simulates the emergency scenarios to strengthen the capability of relevant staffs to handle emergency events. A hypothetical intrusion path is D61/1-D61/2-D60/1-Target and a hypothetical optimal response path is D60-Target as shown in figure 7. In the security risk simulation system, the agents are dynamic transition from the current place to the next place, which are displayed on the map.

The event which is held in the Transition and State handlers is used to model behaviors of the state. The external event, internal event, timer event, and the primary event are frequently used in this system for the implementation of state transitions. The time event is used to implement the delay function of protection elements and limited time of per task. The minimal case system is showed in figure 7. In fact, the regulations are knowledge base for all kinds of actors which are invisible. The simulator provides a database for the store plural places. The agent of adversary will penetrate the protection elements as the transition process of states followed the specific path.

5) RISK ASSESSMENT

Suppose an adversary path is Idle-D61/1-D61/2-D60/1-Target as shown in figure 7, the adversary actions to achieve the goal are penetrate D61/1, penetrate D61/2, penetrate D60/1 and sabotage Target. The main calculated parameters in this actions are listed in the table 3, all data is hypothetical.

TABLE 3. Use EASI method to estimate the probability of interruption.

Probability of Guard Communication			Response Force Time (s)		
0.95			Mean	SD	
			300	90	
Task	Description	$P(D)$	Location	Mean	SD
1	penetrate D61/1	0.95	B	50	5
2	penetrate D61/2	0.90	B	160	16
3	penetrate D60/1	0.90	B	170	17
4	sabotage Target	0.95	B	180	18
Probability of Interruption $P(I)$			0.944974		

The value of $P(N)$ is assigned to 1.0 usually. The values of other parameters are assigned by qualitative analysis. The threat spectrum [13], [20] is divided into four levels, LOW (0.05), MEDIUM (0.3), HIGH (0.65), HIGH Plus (0.9). The consequence [22] is divided into 4 ranges, NO (0.1), LOW (0.2), MEDIUM (0.5), HIGH (0.9). In this case, the $P(A) = 0.65$, $C = 0.9$. Thus, $R = 0.03219$, which needs to be less than the threshold.

In addition, the key parameters of risk assessment as extended attributes are set for symbols in simulator. The results of risk assessment can be evaluated after the scenario analysis. The review of scenarios should be performed to

determine that all analysis objectives are covered in the credible scenarios.

V. CONCLUSION

A PPS is an integration of complex security system strictly in accordance with various standards from design and evaluation to use. Scenario analysis is used for the evaluation of the effectiveness of PPS. This paper proposes an interactive simulator which contributes to interactive simulating the scenarios of adversary intrusion, response and defeat. This interaction simulator integrates the knowledge bases of security management and simulates the intermodulation process of related agents.

In the scenario analysis process of design, develop and implement, the agents, including adversary, response force, detection staff, delay element, etc. are considered in the interactive simulator for the establishment of more complete attack scenario and defense scenario. The proposed method enables the user to create a range of scenarios to identify more vulnerabilities, including vulnerability of strategy, vulnerability of design, etc.

Risk analysis is the result of simulation. Risk analysis is used to calculate the risk level of the intrusion scenario and assess whether the intrusion scenarios are controllable.

Future work may include comprehensive analysis of the proposed method, construct a knowledge base, establish an intrusion and defense system, and simulate the PPS on the interaction simulator. The calculation of the probability of interruption may be combined with IoT and big data technology [26], [27] for synthetic evaluation.

REFERENCES

- [1] National Research Council. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, DC, USA: The National Academies Press, 2002.
- [2] G. Booch, J. Rumbaugh, and I. Jacobson, *The Unified Modeling Language Reference Manual*. Reading, MA, USA: Addison Wesley, 2017.
- [3] V. Ulyantsev, I. Buzhinsky, and A. Shalyto, "Exact finite-state machine identification from scenarios and temporal properties," *Int. J. Softw. Tools Technol. Transf.* vol. 20, no. 1, pp. 35–55, Feb. 2018.
- [4] W. Reisig, *A Primer in Petri Net Design*. Berlin, Germany: Springer, 2012.
- [5] T. M. Scenario, *Twenty-Sixth International Training Course*. Albuquerque, NM, USA: Sandia National Laboratories, 2016.
- [6] S. Bassam, J. W. Herrmann, and L. C. Schmidt, "Using sysML for model-based vulnerability assessment," *Procedia Comput. Sci.*, vol. 44, pp. 413–422, Jan. 2015.
- [7] S. N. Uke and A. R. Mahajan, and R. C. Thool, "UML modeling of physical and data link layer security attacks in WSN," *Int. J. Comput. Appl.*, vol. 70, no. 11, pp. 1–4, May 2013.
- [8] Ul Haq, Sami, "A Novel Approach for Modeling Security Aspects of Physical Infrastructures," in *Proc. Int. Conf. High Perform. Compilation, Comput. Commun.*, Mar. 2017, pp. 39–44.
- [9] D. MacDonald, S. L. Clements, S. W. Patrick, C. Perkins, G. Muller, M. J. Lancaster, and W. Hutton, "Cyber/physical security vulnerability assessment integration," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2013, pp. 1–6.
- [10] T. M. Chen, J. C. Sanchez-Aarmouse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Trans. Smart Grid* vol. 2, no. 4, pp. 741–749, Dec. 2011.
- [11] International Atomic Energy Agency, International Criminal Police Organization-Interpol, *Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control*, IAEA Nucl. Secur., Vienna, Austria, 2015.

[12] International Atomic Energy Agency, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*, IAEA Nucl. Secur., Vienna, VA, USA, 2011.

[13] International Atomic Energy Agency, *Objective and Essential Elements of a State's Nuclear Security Regime*, IAEA Nucl. Secur., Vienna, VA, USA, 2013.

[14] L. Zhang and G. Reniers, *Game Theory for Managing Security in Chemical Industrial Areas*. Cham, Switzerland: Springer, 2018.

[15] M. L. Garcia, *Vulnerability Assessment of Physical Protection Systems*. Burlington, VT, USA: Elsevier, 2005.

[16] D. J. Landoll and D. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. Boca Raton, FL, USA: CRC Press, 2005.

[17] M. L. Garcia, *Design and Evaluation of Physical Protection Systems*. Amsterdam, The Netherlands: Elsevier, 2007.

[18] S. L. O'Connor, D. W. Whitehead, and C. S. Potter, III, "Nuclear power plant security assessment technical manual," Sandia Nat. Lab., Albuquerque, NM, USA, Sandia Rep. SAND2007-5591, 2007.

[19] T. H. Woo, "Analytic study for physical protection system (PPS) in nuclear power plants (NPPs)," *Nucl. Eng. Des.*, vol. 265, pp. 932–937, Dec. 2013.

[20] *National Policy Analysis #374: Terrorism and Nuclear Power: What are the Risks? The National Center for Public Policy Research (NCPA)*, NCPA, Washington, DC, USA, 2001.

[21] M. G. Zhen et al., "Nuclear power comprehensive security management method," Shanghai Nucl. Eng. Res. Des. Inst., Shanghai, China, Tech. Rep. CN103390330A, 2013.

[22] H. Yoo, S.-W. Kwak, S.-S. Chang, J.-S. Kim, and W.-K. Yoon, "Development of PP measures for evaluating Nuclear Facility's Risk," in *Proc. Daejeon: Korea Inst. Nuclear Non-Proliferation Control*, Jan. 2009, p. 1.

[23] B. Gupta et al., *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*. Boca Raton, FL, USA: CRC Press, 2018.

[24] S. Gupta and B. B. Gupta, "Smart XSS attack surveillance system for OSN in virtualized intelligence network of nodes of fog computing," *Int. J. Web Services Res. (IJWSR)*, vol. 14, no. 4, pp. 1–32, 2017.

[25] B. Gupta, P. A. Dharma, and S. Yamaguchi, Eds. *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. Philadelphia, PA, USA: IGI Global, 2016.

[26] A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, and B. B. Gupta, "Efficient IoT-based sensor BIG data collection–processing and analysis in smart buildings," *Future Gener. Comput. Syst.*, vol. 82, pp. 349–357, May 2018.

[27] V. A. Memos, K. E. Psannis, Y. Ishibashi, B.-G. Kim, and B. B. Gupta, "An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework," *Future Gener. Comput. Syst.*, vol. 83, pp. 619–628, Jun. 2018.



WANG WENLIN was born in Shandong, China, in 1985. He received the B.S. degree in automation from the Harbin Institute of Technology, in 2008, and the M.S. and Ph.D. degrees in nuclear science and technology from the Harbin Engineering University, in 2013 and 2016, respectively. He is currently a Lecturer with the School of Automation, Wuhan University of Technology. His research interests include fault diagnosis, and system reliability analysis, and many academic papers were published.



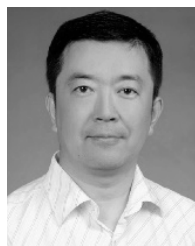
YAN ZHENYU was a Senior Engineer with the State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Guangdong Nuclear Power Engineering, Design Company Ltd. His research interest includes cyber security.



LIU GAOJUN received the bachelor's and M.S. degrees from the College of Computer Science and Technology, Harbin Engineering University, China, in 2004 and 2006, respectively. His research interest includes reliability analysis of I&C.



YANG JUN received the bachelor's degree from the College of Nuclear Science and Technology, University of South China, China, in 2010, and the Ph.D. degree from the College of Nuclear Science and Technology, Harbin Engineering University, in 2017. His research interest includes living PSA.



YANG MING received the bachelor's degree from the School of Electrical Engineering and Automation, Harbin Institute of Technology, China, in 1995, and the Ph.D. degree in nuclear science and technology from Harbin Engineering University, in 2014. His research interests include nuclear safety and security, and analysis of main control room.

...



ZOU BOWEN received the bachelor's and Ph.D. degrees from the College of Nuclear Science and Technology, Harbin Engineering University, China, in 2014 and 2018, respectively. His research interests include nuclear safety and security, and software reliability.



LIU JIAN received the bachelor's and M.S. degrees from the School of Automation Science and Engineering, South China University of Technology, China, in 2011 and 2013, respectively. His research interest includes physical protection systems.