Hindawi Publishing Corporation
Science and Technology of Nuclear Installations
Volume 2013, Article ID 473687, 5 pages
http://dx.doi.org/10.1155/2013/473687

Research Article

Systems Thinking Safety Analysis: Nuclear Security Assessment of Physical Protection System in Nuclear Power Plants

Tae Ho Woo

Systemix Global Co. Ltd., Third Floor, 494-48 Yonggang-dong, Mapo-Gu, Seoul 121-876, Republic of Korea

Correspondence should be addressed to Tae Ho Woo; thw_kor@hotmail.com

Received 16 May 2013; Revised 17 September 2013; Accepted 18 September 2013

Academic Editor: Bing Li

The dynamical assessment has been performed in the aspect of the nuclear power plants (NPPs) security. The physical protection system (PPS) is constructed by the cyber security evaluation tool (CSET) for the nuclear security assessment. The systems thinking algorithm is used for the quantifications by the Vensim software package. There is a period of 60 years which is the life time of NPPs' operation. The maximum possibility happens as 3.59 in the 30th year. The minimum value is done as 1.26 in the 55th year. The difference is about 2.85 times. The results of the case with time delay have shown that the maximum possibility of terror or sabotage incident happens as 447.42 in the 58th year and the minimum value happens as 89.77 in the 51st year. The difference is about 4.98 times. Hence, if the sabotage happens, the worst case is that the intruder can attack the target of the nuclear material in about one and a half hours. The general NPPs are modeled in the study and controlled by the systematic procedures.

1. Introduction

The dynamical assessment is investigated for the security in the nuclear power plants (NPPs). The nonlinear dynamic algorithm is applied to the advanced security assessment, which is called the systems thinking analysis. The cyber security evaluation tool (CSET) gives operators a repeatable and systematic ways for assessing the cyber security state of the industrial control system networks which is shown in Figure 1, where it provides the tools of both high-level and detailed questions applicable to all industrial control systems (ICSs) [1]. The CSET was developed under the direction of the Department of Homeland Security (DHS) Control Systems Security Program (CSSP). It is shown that CSET is a designed desktop software that makes users assess their network and ICS security practices regarding identified industrial and governmental regulations [1]. This completed CSET assessment means a suggested list that enhances the security state for ICS of organization or network of company and also recognizes the achievement of the designed security level in the standards [1].

Information about the security in NPPs is available in the literature. Safeguard modeling is conducted for the successful operations in the NPPs [2]. Also, Pei et al. compared their method with some existing methods for nuclear safeguard evaluations in an example, which supports and clarifies the method of their paper [3]. The characteristics of the secure operation in NPPs are investigated using the network effect method which is quantified by the Monte-Carlo algorithm. Also, the study analyzes some potential security risks, concerning terrorism or more routine incidents like any crimes, and management of nuclear waste using a PEST scan which is formed by political, economic, social, and technical matters, and some insights of criminologists on crime prevention where nuclear waste is produced by the spent fuel by electricity production and its related contaminations and decommissions [4]. Finally, the basic object of an effective emergency system of regulation is to supply a sustained emergency response and to prohibit an emergent circumstance as during the emergency the regulatory purpose is to control the incidents and to guide people and to keep the environment safe in order not to be in catastrophic nuclear and radiological hazards [5].

There is the background for the modeling which is shown in Section 2. Section 3 explains the method of the study.

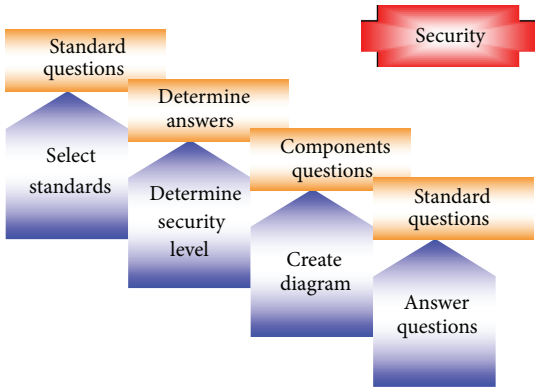

Figure 1: Configuration for the path of cyber security evaluation tool (CEST).

Section 4 describes the results of the study. There are some conclusions in Section 5.

2. Background

It is examined that the literature investigations for the nuclear security which is related to the topic of this paper. So, the historical and analytic reviews are introduced. Then, the basic explanations of the systems thinking are done.

2.1. Nuclear Security. For several years following 9/11 terror attack, the Nuclear Regulatory Commission (NRC) required many security enhancements on commercialized nuclear power reactors, decommission of old reactors, nuclear spent fuel storage facility, research and multipurpose reactors, uranium fuel manufacturing facilities, nuclear fuel gaseous diffusion plants, nuclear fuel fabrication facilities, industrial distribution parts, transportation systems, and permitted licensees who can treat nuclear material greater than IAEA category II [6]. It has been done as the NRC directed NPPs and fuel fabrication facilities to improve physical security planning, and security officer training and uncertain planning where several facilities are shown as follows [6]:

(i) larger standoff distances for vehicle checks,

(ii) much more restrictive site access controls,

(iii) many patrols,

(iv) stronger and more capable security forces,

(v) enough physical barriers,

(vi) enhanced emergency preparedness and response plans.

It is important that NPPs and category I fuel fabrication facilities must show that they can defend against a set of adversary characteristics outlined in the NRC's design basis threat (DBT) [6]. In 2003 and 2006, the NRC supplemented the DBT to incorporate insights from the 9/11 attacks [6]. In 2007, the NRC amended 10 CFR 73.1 and issued a final rule consolidating the supplemental requirements established by DBT's orders with the existing DBT requirements following NRC regulations [6].

In 1996 in Russia, the 48 nuclear power reactors were operating in five newly independent states (NISs) of the former Soviet Union: 29 units at nine sites in Russia, 15 units at five sites in Ukraine, a double-unit plant in Lithuania, and one unit each in Armenia and Kazakhstan [7]. According to the International Atomic Energy Agency (IAEA) regulation, the objective of the State's nuclear security regime is to protect persons, property, society, and the environment from malicious acts involving nuclear material and other radioactive materials [8]. That is, the purposes of the physical protections are an essential component of the nuclear security regime. So, the physical regime should prevent a dangerous act by relevant information and system.

Using the above objectives, it is needed to be addressed in an integrated and coordinated manner taking into account the different risks covered by nuclear security. It is necessary for these nuclear power facilities to be reliably protected against possible radiological sabotage or terrorism. The nation has been marked by ethnic and political conflicts, crime, and societal instabilities. These power facilities have great tendencies to have these maladies and face a broad range of threats. In fact, the potentially catastrophic releases of radioactivity and resultant global societal dislocations make the national nuclear industry a particularly attractive target in case of industrial sabotage.

2.2. Systems Thinking. The systems thinking is defined as the thinking about how things interact with one another [9]. One can use the phrase systems thinking to refer to a set of tools such as causal loop diagrams, stock and flow diagrams, and simulation models that help us map and explore dynamic complexity [10]. In addition, the systems thinking could use specified vocabulary where one can represent its understanding of dynamic complexity as feedback of event for expressing the affection to future event by the past event. The systems thinkers often describe the world by several logics like feedback, delay, dynamical behavior, and so on. System dynamics (SD) is basically and technically similar to systems thinking and produces the causal loop diagrams of systems with feedback where the event flows to the designed modeling. This event can express several variables like the population, speed, temperature, pollution, contamination, and so on. The variables are quantified by the random sampling based Monte-Carlo methods. The SD was created during the mid 1950s by Dr. Jay Forrester of the Massachusetts Institute of Technology (MIT). However, SD typically goes further and utilizes simulation to study the behavior of systems and the impact of alternative policies [11]. The systems thinking can be realized by the SD due to the similarity of the algorithm. The relevant software packages are used for the simulations. The calculations with the generated random numbers are performed by the Vensim code system. The Vensim is made for developing, analyzing, and packaging high quality dynamic models [12]. The models are constructed graphically or in a text editor. The features include dynamic functions, subscripting (arrays), Monte-Carlo sensitivity analysis, optimization, data handling, and application interfaces [12].

Table 1: List of numeric values.

Path for sabotage	Value
Pass of fence	Random number between 0 and 1
Pass of outer door	(Random number between 0 and 1, mean: 0.8, and st. deviation: 0.2) + pass of fence
Pass of wall	(Random number between 0 and 1, mean: 0.6, and st. deviation: 0.3) + pass of outer door
Pass of inner door	(Random number between 0 and 1, mean: 0.4, and st. deviation: 0.3) + pass of wall
Attack of target	(Random number between 0 and 1, mean: 0.2, and st. deviation: 0.1) + pass of inner door

3. Method

The analysis is done by the physical protection system (PPS) in NPPs which is in Figure 2 [13]. This is the systematic procedures of the PPS where the figure explains the design of PPS incorporated with the PPS body selection and PPS formation. This is followed by the CEST in Figure 1. Using the PPS, one can make the path for sabotage in NPPs. Figure 3 shows the modified path for sabotage in NPPs in which the person of sabotage could go through from the fence to target to make the terror [13]. So, the diagram is modified from the original algorithm. For the calculation, the SD method is applied to this sabotage case. Figure 4 is constructed for the SD using Figure 3. That is, the event sequence is connected by the arrow line. The addition is denoted by plus sign which also means the multiplication. If the subtraction is needed, the minus sign will be shown. Each box gives the numeric values of the events. In this work, there are several random number quantifications. Table 1 shows the list of numeric values, where the numeric values are decided by expert's judgment. In addition, Figure 5 shows the diagram which is incorporated with the time delay where the detection and action are considered in Table 2. The detection means the detection method of the intruder, and the action means the guarding ways against the enemy who is a possible terrorist. Table 3 shows the related time for the step. The list of the numeric values is obtained by the random number of Table 1 incorporated with the expert judged time, which is in Table 4. In the case of the pass of fence, random numbers between 0 and 1 are multiplied by 10 (minutes). The time list with delays is shown in Table 5.

4. Results

The attack of target is quantified by the dynamical consequences in Figure 6 which is the result of the Vensim simulation. The period is considered as 60 years. The maximum possibility happens as 3.59 in 30th year. The minimum value is done as 1.26 in 55th year. The difference is about 2.85 times. The results of the case with time delay are in Figure 7 where the maximum possibility happens as 447.42 in 58th year and the minimum value happens as 89.77 in 51st year. The difference is about 4.98 times. So, if the sabotage happens,

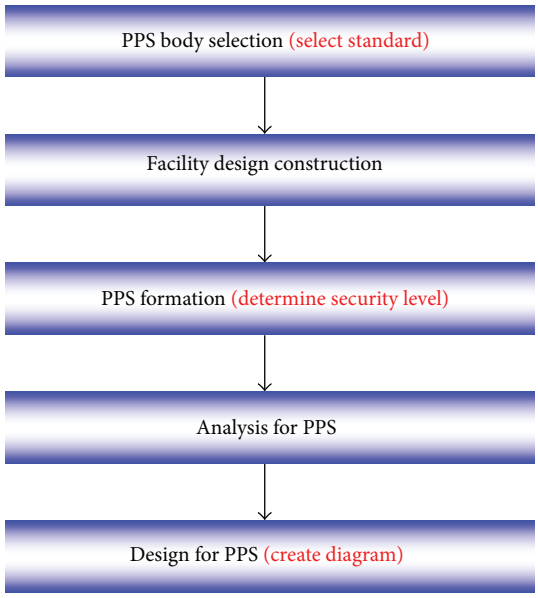

Figure 2: Modified physical protection system (PPS) in nuclear power plants (NPPs).

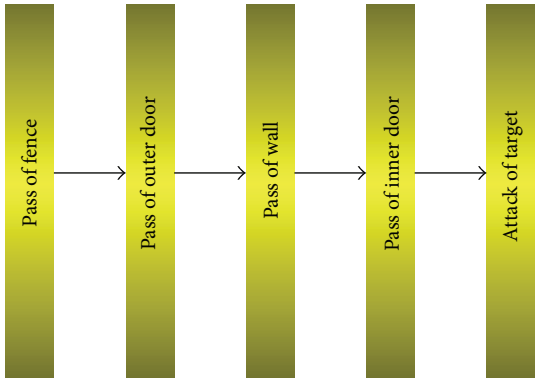

Figure 3: Modified path for sabotage in nuclear power plants (NPPs).

the worst case is that the intruder can attack the target of the nuclear material in about one and a half hours. Although the result of simulation to the target of the nuclear material is about one and a half hours, this value could be variable by physical protection systems from one plant to another, according to specific site and country conditions such as power reactors, decommissioning reactors, and spent fuel storage. Therefore, it is analyzed that the longer time values in the simulation are safer than the shorter time values, because the attack action needed to take much more time. One can prepare for the security in the period of the shorter time values. This is a particular assessment of SD method. In conventional safety assessment, the result of the event can show the frequency of the event by the probability values.

5. Conclusions

The dynamical quantification is done in the security of NPPs. The time delay is important to the security of

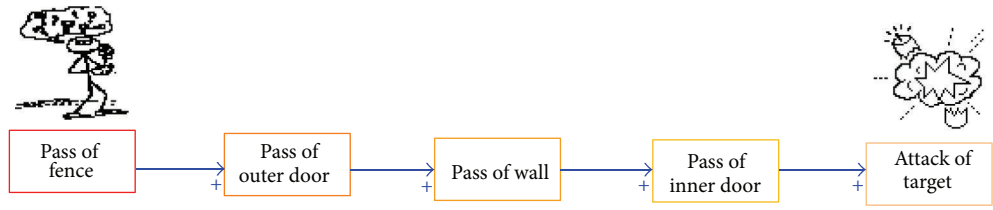

Figure 4: Modified path for sabotage by system dynamics (SD) diagram.

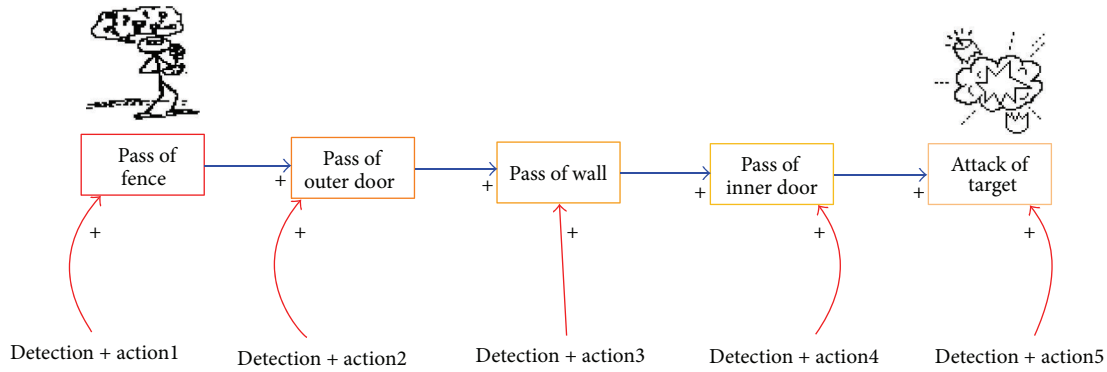

Figure 5: Path for sabotage with time delay by system dynamics (SD) diagram.

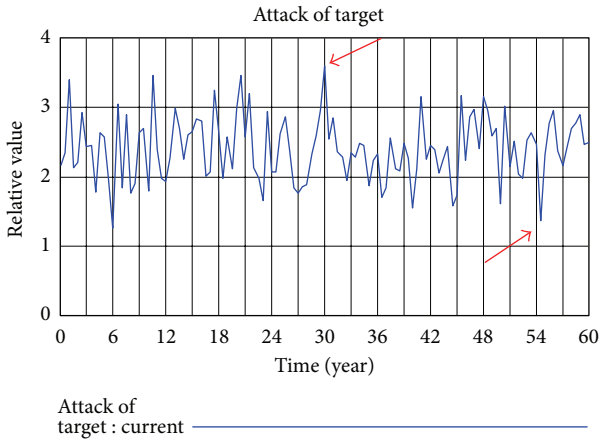

Figure 6: Results of path for sabotage.

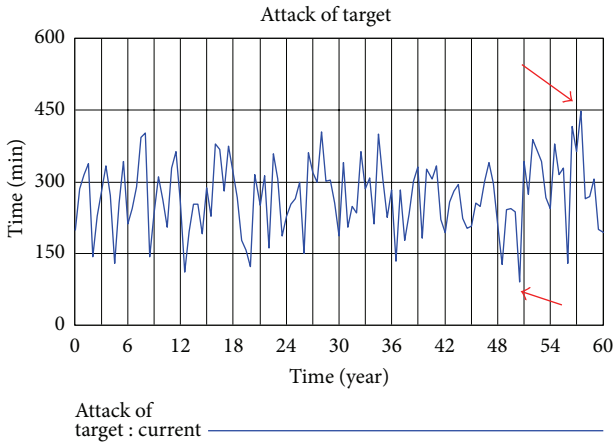

Figure 7: Results of path for sabotage with time delay.

the NPPs. How the defense against possible terror attack reacts could be analyzed by some aspects by several external impacts. The political, social, and technological aspects could be considered. In addition, the natural disaster could be another kind of matter, because this happens without anyone minding. Hence, the policy makers, security personnel, or owners and operators of the nuclear facilities should think of the possible terror related incidents as well as the natural disaster, because these incidents happen usually without prior notification. The method of this paper gives a quantified prediction which is different from the subjective description in the conventional ways. Several significant findings are obtained in the simulations as follows.

(i) The dynamical consideration of the security is considered.

(ii) The detection and action against the incidents are quantified.

(iii) SD method is applied to the security of NPPs.

(iv) General NPPs are modeled in the study.

(v) NPPs are controlled by the systematic procedures.

There are some more investigations in this work. The time-based analysis could be used for the possible procedures in the accident of the terror incidents. However, the steps of the events are variable by the characteristics of the plants. The nuclear materials are extremely prohibited from the public. But some other industrial facilities are placed to be reached by the public. Therefore, the analysis is able to be modified by the public facilities like the public communications and

Table 2: List of detection and action.

Path for sabotage	Detection	Action
Pass of fence	Elec. signal + CCTV + guard	Calling for guard or police
Pass of outer door	Elec. signal + CCTV + noise	Using weapon (hand gun, tear gas)
Pass of wall	Elec. signal + CCTV + noise	Using weapon (hand gun, tear gas)
Pass of inner door	Elec. signal + CCTV + worker	By physical defense
Attack of target	Elec. signal + CCTV	Impossible to defense

Table 3: Time for each step.

Path for sabotage	Detection	Action
Pass of fence	Immediately	Over several minutes
Pass of outer door	~minutes	Over several minutes
Pass of wall	Minutes~hours	Up to 1 hour
Pass of inner door	Over hours	Up to 1 hour
Attack of target	Over hours	Impossible

Table 4: List of numeric values.

Path for sabotage	Value (minute)
Pass of fence	(Random number between 0 and 1) $*$ 2
Pass of outer door	(Random number between 0 and 1, mean: 0.8, and st. deviation: 0.2) $*$ 10 + pass of fence
Pass of wall	(Random number between 0 and 1, mean: 0.6, and st. deviation: 0.3) $*$ 30 + pass of outer door
Pass of inner door	(Random number between 0 and 1, mean: 0.4, and st. deviation: 0.3) $*$ 60 + pass of wall
Attack of target	(Random number between 0 and 1, mean: 0.2, and st. deviation: 0.1) $*$ 90 + pass of inner door

Table 5: Time for each step.

Path for sabotage	Detection + action (minute)
Pass of fence	(Random number between 0 and 1) $*$ 10
Pass of outer door	(Random number between 0 and 1) $*$ 30
Pass of wall	(Random number between 0 and 1) $*$ 60
Pass of inner door	(Random number between 0 and 1) $*$ 120
Attack of target	(Random number between 0 and 1) $*$ 180

transportations like the bus, subway, or train. For the general goal, the safety of the facility is considered for the prevention against the incidents. So, the dynamical quantifications should imply the process of the catastrophic happening. There should be many possibilities to the extreme case. The security of the facility is related to the safe operations for the normal situation.

The dynamical assessment can show the operator to find the dangerous situation in the site. Then, the operator could prepare for possible incidents which could be a catastrophe for the NPPs. Generally, the terror attack of NPPs has not been considered significantly. Therefore, in the aspect of international policy aspect, the regulations could be constructed in the future.

Conflict of Interests

According to the editorial policy, "a conflict of interests exists when professional judgment concerning the validity of research is influenced by a secondary interest, such as financial gain." The author declares that there is no conflict of interests in this paper.

References

[1] Department of Homeland Security, *Cyber Security Evaluation Tool (CSET), Performing a Self-Assessment*, Department of Homeland Security, Washington, DC, USA, 2011.

[2] T. H. Woo and U. C. Lee, "Safeguard management for operation security in nuclear power plants (NPPs)," *Annals of Nuclear Energy*, vol. 38, no. 2-3, pp. 167–174, 2011.

[3] Z. Pei, D. Ruan, J. Liu, and Y. Xu, "A linguistic aggregation operator with three kinds of weights for nuclear safeguards evaluation," *Knowledge-Based Systems*, vol. 28, pp. 19–26, 2012.

[4] T. V. Beken, N. Dorn, and S. van Daele, "Security risks in nuclear waste management: exceptionalism, opaqueness and vulnerability," *Journal of Environmental Management*, vol. 91, no. 4, pp. 940–948, 2010.

[5] V. Kostadinov, "Developing new methodology for nuclear power plants vulnerability assessment," *Nuclear Engineering and Design*, vol. 241, no. 3, pp. 950–956, 2011.

[6] US NRC, *Backgrounder—Nuclear Security*, US NRC, Washington, DC, USA, 2008.

[7] O. Bukharin, "Upgrading security at nuclear power pants in the newly independent States," *The Nonproliferation Review*, pp. 28–39, 1997.

[8] IAEA, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*, (INFCIRC/225/REVISION 5), IAEA, Vienna, Austria, 2010.

[9] G. Bartlett, "Systemic thinking, a simple thinking technique for gaining systemic focus," in *Proceedings of the International Conference on Thinking*, Probsolv International, Auckland, New Zealand, 2001.

[10] B. Richmond, *Systems Thinking, Four Key Questions*, High performance systems, Hanover, NH, USA, 1991.

[11] System Dynamics Society, 2011, http://www.systemdynamics.org/.

[12] Vensim, *Vensim Simulation Software*, Ventana Systems, Inc., 2009.

[13] US DOE, "Nuclear power plant security assessment technical manual," Sandia Report, SAND 2007-5591, 2007.