DOI: https://doi.org/10.37075/EA.2024.4.08 Economic Alternatives, 2024, Issue 4, pp. 829-845

An Innovative Approach for Vulnerability Assessment of a Nuclear Facility's Physical Protection System

Received: 05.04.2023
Available online: 31.12.2024

Tsvetan Tsvetkov*

Abstract

The main idea of the article is to propose a framework for assessing the vulnerability of a nuclear facility's physical protection system (PPS) by applying an innovative approach using a simulation model.

The proposed framework includes the following steps: a scenario tree development that reflects the possible situations of attempted theft / sabotage in a nuclear facility; development of a simulation model for the reaction time of reaction forces for each of the scenarios; development of a simulation model of the time it takes for intruders to achieve their goal according to each scenario by using the CPM / PERT network model; determination of a critical detection point; calculating the probability that the reaction time of reaction forces after critical detection point will be longer than the time required for intruders to achieve their goal, according to each scenario; defining a critical path; sensitivity assessment of the times according to the developed models in relation to their input indicators. The aim is to determine to which input indicators the reaction forces time and the intruders time are the most sensitive. Based on the simulations and analyses one can draw conclusions and recommendations for the practice.

Keywords: vulnerability assessment, physical protection system, nuclear facility, simulation

JEL: C53

I. Problem identification

Nowadays, a country's critical infrastructure is crucial to its security, economic development, and competitiveness. The protection of critical infrastructure facilities is a complex and multifaceted research problem. The complexity arises from the fact that the objects of the critical infrastructure are many in number, they are diverse in their technical nature and there are various and difficult to trace interconnections between them. The protection of critical infrastructure can be studied from various aspects – political, legal, technical, economic, organizational and others. Each of the aspects is a significant research area.

Nuclear facilities are an important part of critical infrastructure. They perform socially significant functions in various directions. Nowadays, the application of radioactive materials and ionizing radiation is very wide.

[1] Professor, PhD at the University of National and World Economy, Department of National and Regional Security

People use similar materials in many areas. Of course, the intensity of radiation in different processes is different. Research nuclear reactors for example emit significantly less than much more powerful nuclear power plants reactors.

Nuclear security issues are gaining increasing priority worldwide. The International Atomic Energy Agency (IAEA) aims to promote the peaceful uses of nuclear energy and to prevent its use for military purposes. Over the last decade, the IAEA has focused significant resources on nuclear security research and regulation. A series of publications on the most important issues of nuclear security (Nuclear Security Series), which are published in different languages – English, French, Russian, Chinese, and Arabic – has become widespread.

II. Literature Review

The analysis of security threats to nuclear facilities is the focus of many institutions and researchers. Broadly speaking, the threat can be defined in various ways, but in any case, it is a factor, circumstance, or event that may have adverse consequences for the functioning of an organization or other entities. It is important for this article that the threat is perceived as an element of risk. Hayden (2020) for example, assumes that risk is determined by the following factors: threat, vulnerability, consequences, or impact. The same author also identifies the threats sources: man-made, accidental, structural, natural. Man-made threats are of major interest in this study. These are threats that are determined by individuals, groups, organizations, or states seeking to exploit or disrupt the organization's or facility's dependence upon resources such as other critical infrastructure and supply chains.

In the practice of nuclear facilities physical security, two types of threats are considered. The first is threat type 1 (TT-1), which is: "a threat posed to the nuclear facility by insiders or by adversaries intending to intrude into the facility to commit their act (with or without insider assistance)". The second type, threat type 2 (TT-2) is "a threat posed to the nuclear facility initiated outside the plant boundary that does not require the presence of the adversaries on-site", IAEA (2007). In this article I limit my research only to the study of TT-1.

In the literature on the discussed issues, the term nuclear security is understood as "the prevention and detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities". In turn, the term nuclear facility means "a facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored, or disposed of", IAEA (2022).

States have a responsibility to identify and assess threats to the security of nuclear facilities. Documents are usually developed – such as Design basis threat, which should include all attributes and characteristics of potential insider and / or external adversaries, who might attempt an act of unauthorized removal or sabotage against which a nuclear security system is designed and evaluated and that an operator, is expected to be able to counter, IAEA (2013).

It is not possible to protect all facilities and assets in the same way. The resources that organizations and the state can devote to physical security are limited. Therefore, it is necessary to identify those assets that are critical to the functioning of organizations and society. There are different methods for

assessing criticality, but in all of them the main idea is to determine what the consequences would be if one or a series of risky events occur. Biringer, Vugrin and Warren (2013) define critical assets as follows: "what specific assets must be protected to prevent the undesired event from occurring. These assets are labeled the critical assets; protection of these critical assets will be important in the security risk assessment".

Norman (2016) offers an interesting tool that allows to assess the assets in terms of their criticality in the functioning of the organization and the consequences if they are affected or destroyed. This is the matrix "Asset Criticality – Consequences". As assets in this case are perceived people, property, proprietary information, business reputation. The criticality of an asset is assessed in terms of its importance for the performance of the organization's operations and its sustainability. Norman offers a series of criteria for assessing the criticality of assets.

In the field of nuclear security, an important concept has been introduced – the "vital area". The "vital area" is an "area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences", IAEA (2018). In this sense, we can say that the vital area is one of the most important targets for the potential intruder and therefore one of the most critical assets for nuclear facilities. The process of identifying vital areas is presented in detail in: IAEA (2012) and includes nine steps.

To protect their assets, nuclear facilities build their own physical protection systems. This term includes "a combination of hardware (security devices), procedures (including the organization of guards and the performance of their duties) and facility design (including layout)", IAEA (2007). The main functions that perform physical protection systems are related to the implementation of preventive and protective measures. Preventive measures are aimed at reducing or eliminating internal and external threats, while protective measures are associated with actions to be implemented in type 1 threats appearance. They are expressed in the implementation of the functions: "detect, delay, and respond to malicious acts as well as mitigate or minimize the consequences of the malicious act", IAEA (2012). Garcia (2006) includes the following actions in the detect function: intrusion sensing, alarm communication, alarm assessment. To the delay function she includes barriers and response force, and to the respond function – interruption (communication to response force, deployment of response force), neutralization (tactics, training). In the present article, the emphasis is on the time required for the implementation of possible malicious acts, considering all the actions of the physical protection system to perform the detection, delay and respond functions.

Biringer, Matalucci, and O'Connor (2007) see detection and delay analysis as elements of the physical security system's performance analysis. According to them, detection (with assessment) is the discovery of adversary action and includes sensing covert or overt actions. Delay is any physical protection feature that impedes adversary progress.

For the effective functioning of a physical protection system to be possible, it is necessary for it to have clearly formulated protection objectives, which should include threat definition, target identification, and facility characterization, Garcia (2006). The literature recommends application of the following three principles: risk management,

graded approach, and defense in depth. The latter principle is essential for this article. It provides for the application of "a concept of several layers and methods of protection (structural, other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives", IAEA (2011). Garcia (2006) also analyses a similar set of features of a well-engineered physical protection system – protection-in-depth, minimum consequence of component failure, and balanced protection.

In her very useful book, Garcia (2006) offers the following steps in performing performance-based vulnerability analysis, the logic of which will be used in this article: 1. Create an adversary sequence diagram for all asset locations. 2. Conduct a path analysis, which provides P_I (probability of interruption). 3. Perform a scenario analysis. 4. Complete a neutralization analysis, if appropriate, which provides P_N (probability of neutralization). 5. Determine system effectiveness, P_E. 6. If system effectiveness (or risk) is not acceptable, develop and analyze upgrades.

Once all the assets to be protected have been identified, it is possible to develop adversary sequence diagrams. For each of them a path analysis must be performed. To this end, a set of scenarios must be developed that reflect the possible types and directions of attack. Scenarios should reflect the available elements of the physical security system, their location, the available layers of protection, the available vulnerabilities. Scenario analysis is a popular analytical method in economics and management. Many authors have explored various aspects of the application of this method. As a result of the adversary sequence diagrams analysis, path analysis and the identified scenarios, the critical path can be determined. This is the path that is characterized by the lowest probability of interruption.

Adversary path includes the actions that the intruder must perform and the obstacles that he must overcome in order to reach the object – the goal of its invasion and to fulfill its purpose. Garcia (2001) defines the concept as: "an ordered series of actions against a facility, which, if completed, results in successful theft, sabotage, or other malevolent outcome". The performance of the detect, delay, and respond functions will largely depend on the characteristics of the adversary path. Efficiency is determined by comparing adversary time and PPS timeline. Garcia (2001) also identifies as critical the path with the lowest probability of interruption.

In order to comply with the principle of timely detection, it is necessary to detect the adversary early enough so that the response forces have sufficient time to react before the adversary has fulfilled its purpose.

In practice, another term is used related to Adversary Path. This is the Adversary Sequence Diagram. Such a diagram must be developed for each critical asset. Biringer, Matalucci, and O'Connor (2007) recommend the following steps to develop the Adversary Sequence Diagram: 1. Model the facility by separating it into adjacent physical areas. 2. Define the system features between the adjacent areas. 3. Construct the Adversary Sequence Diagram. The Adversary Sequence Diagram is displayed graphically, defining the individual physical areas separated by Protection Layers. Garcia (2001) provides detailed information on the development of the Adversary Sequence Diagram procedure. She emphasizes that in the analysis of the sabotage scenarios only the penetration path is analyzed, and in the theft scenario – the

protection elements are traversed twice — on entry to the asset and on exit from the asset.

The nature and method of application of Layers of protection analysis is presented in detail by Fennelly (2017). He takes this tool more broadly, considering that "by using the layers of protection analysis (LOPA) the concept of a security professional can reduce or mitigate the risk as low as reasonably manageable.

The response function is important for the effectiveness of PPS analysis, because it is necessary to make a comparison between the adversary time and response force time. According to Snell and Winblad (1990), response force time measures how long it takes after an intrusion is correctly assessed for the response force to deploy and interrupt the forward progress of the intruders. Garcia (2006) perceives response force time as a key aspect of the vulnerability evaluation and considers that the PPS response function includes the following components: Communicate to Response Force, Deploy Response Force, Interrupt Adversary Attempt.

Many authors agree that security risk associated with the adversary attack can be assessed or measured based on the following equation (Biringer, Matalucci and O'Connor (2007), Garcia (2008), Vintr, Vintr and Malach (2012) and others):

$$R = P_A(1-P_E)C \quad (1)$$

where:

R - risk associated with adversary attack,

P_A - likelihood of attack,

P_E - probability that the security system is effective against the attack,

C - consequence of the loss from the attack.

In turn:

$$P_E = P_I \,.\, P_N \quad (2)$$

where:

P_I - probability if interruption,

P_N - probability of neutralization.

In fact, the efficiency of the system can be assessed by the value of P_E. According to Biringer, Matalucci, and O'Connor (2007) "An effective PPS must be able to detect the adversary early, delay the adversary long enough for the security response force to arrive, and neutralize the adversary before the undesired event is accomplished".

An important element of the physical security system analysis is the establishment of a critical detection point. According to Garcia (2001), the critical detection point is "the point on the path where the delay time remaining first exceeds the response force time". Vintr, Vintr, and Malach (2012) also emphasize the importance of this element, recognizing that "as long as the attack is detected behind this point, the response force will not have enough time to act against an adversary effectively before he reaches his target".

At the heart of the ideas for this article is the logic of probability and probability distributions. There are a huge number of publications on this topic and here I do not intend to analyze them in depth. When talking about threats, risk, vulnerability, it is inevitable to consider the fact that we are talking about random events and processes. Enrico Zio (2007) provides very valuable information in this area. In his publication he presents basic definitions related to basics of probability theory for applications to reliability and risk analysis, probability laws, random variables, probability distributions. He also presents interesting methods that can be used in hazard identification: Checklists, Hazard index method, Hierarchical trees, System Identification of Release Points (SIRP), Failure

Mode and Effect Analysis (FMEA), HAZard and Operability analysis (HAZOP).

The idea proposed in this article envisages the development and use of a Monte Carlo simulation model. In another publication, Enrico Zio (2013) offers in-depth information on the possibilities of applying Monte Carlo simulations for Risk Analysis. In his book, he presents the content of the method, the approaches for generating random numbers (which is the basis of the method) and the ways in which it can be applied to System Reliability and Risk Analysis. Other authors who publish in this field are Paolo Brandimarte (2014), Johnathan Mun (2010), Christopher Chung (2004) and many others.

III. Proposed Methodology

The methodology I propose in this article aims to assess the vulnerability of a nuclear facility's physical security system to TT-1 threats – those that require the enemy to intrude into the facility.

The methodology includes the following steps:

1. Development of a scenario tree.
2. Development of a simulation model.
3. Determination of Critical Detection Point (CDP).
4. Evaluation of the effectiveness of the physical security system
5. Sensitivity assessment.

The methodology is presented in more detail below.

1. Development of a scenario tree that may arise in terms of physical security.

The first node for branching the scenario tree is recommended to be the number of intruders. Suppose their number can vary between one and four. The number of intruders will strongly influence the way the penetration proceeds. If there are two or more intruders, they will be able to perform some of the necessary actions in parallel, which will reduce the total time to perform the act. On the other hand, it is possible that when intruders must sneak through a narrow facility or for some other reason move or perform a certain action sequentially, this will increase their total time.

The second node, which will be developed on each of the branches of the tree will reflect whether the intruders are violent or nonviolent. This will affect the way reaction forces will have to react, their actions and, accordingly, the time they need for deployment.

The third node of the scenario tree will reflect the various possible targets of intruders – theft or sabotage. In order to steal intruders will have to have time to penetrate the site, take radioactive material and leave the facility. For the purpose of sabotage for intruders it is enough to have time to penetrate the object and perform the act.

The fourth node reflects the various possible paths that intruders can choose to enter the territory of the facility, move to the target and possibly (in case of theft) to leave the facility. Paths can be numerous, especially when it comes to a large facility, such as a nuclear power plant. This may increase the number of scenarios to be analyzed. If we assume that the preliminary analyses have identified five possible paths, this means that the scenarios to be analyzed are 4 x 2 x 2 x 5 = 80.

2. Development of simulation models for calculating the time required for intruders to achieve their goal and, accordingly, for the response of the physical security system.

In order to develop an individual model for each of the scenarios included in the scenario

tree it is necessary to perform the following steps:

- determination of the list of actions that intruders must perform according to the respective scenario and respectively reaction forces to stop intruders;
- determining the duration of those actions for which the duration is considered to be a deterministic variable;
- identification of those actions whose duration is considered to be a random variable;
- determination of the type of probability distribution of these durations and other probabilistic characteristics of these durations;
- determining the way of combining the actions of intruders and respectively of reaction forces in time – in parallel, sequentially, or otherwise;
- creation of a CPM / PERT model for calculation of the intruder's total time and respectively of reaction forces to neutralize intruders;
- construction of the model for calculation of the intruder's time and reaction forces time considering the determined probabilistic characteristics.

To build the described model can be used specialized software, such as GPSS and Simula, "@Risk", "Crystal Ball" and many others. For the purposes of this article, the models were developed using @Risk from Palisade.

Determining the probability distribution type and the probabilistic characteristics of the activities' duration, which are considered to be random variables, are key decisions in model development. This can be done in two ways. The first way is possible if the organization has collected information about past events, which is sufficient for statistical processing with reliable results. Such information can be gathered from repeated reaction force drills by measuring the results obtained. Based on this information, the average duration of each of the actions included in the model can be calculated. The proposed software has specialized tools through which the available statistical information can be processed to calculate the probabilistic characteristics of random variables. The choice of distribution will depend on the selected criterion to fit distribution. This requires some knowledge in the field of statistics.

The second way is to use expert opinions. It is possible to conduct an individual or group assessment. Participating experts must be well acquainted with the ways, methods, and practice of physical protection of the facility, as well as to have knowledge of the statistical and probability distributions and the peculiarities of their probability characteristics.

3. Critical Detection Point determination

The simulation models developed for each of the scenarios calculate several trials using @Risk software. The intruder time, the reaction force time and the difference between these times are calculated. The obtained results are analyzed statistically. The probability the reaction force time to be shorter than the intruder time is calculated. In this way, a CDP is defined for each scenario. This is the element of the PPS in the intruder path in which the violation must be detected, in order the response forces time to be less than the intruder time.

4. Evaluation of the effectiveness of the physical security system

The results of the analyses for each of the scenarios are compared with each other. The path in which there is a minimum probability

that the reaction force time is shorter than the intruder time to achieve its goal is determined.

5. Sensitivity assessment of the indicators calculated in items 2 and 3 to the individual times included in the model.

The functionality of the @Risk software is used. The software offers various analytical and graphical possibilities to assess the strength with which changes in input variables affect output variables, i.e., adversary time, reaction force time, and others.

IV. Results and comments

For the purposes of this article, I have built a model that presents the logic of development, calculations, and analysis of the results in assessing the vulnerability of a hypothetical nuclear facility. One scenario was selected, and one possible adversary path was evaluated. The scenario envisages an intruder that aims to sabotage an equipment in vital area. My recommendation is that the procedure discussed below be applied to each of the identified scenarios.

A simulation model has been developed using the @Risk software. A system for physical security of a hypothetical nuclear object – a research reactor – has been modeled. The times required to calculate the adversary and reaction force time, as well as their probabilistic characteristics, are also hypothetical. I accept that they are determined using expert opinions (see Tables 1 and 2).

I entered the data in Tables 1 and 2 as input variables in the model. The model calculates Intruder's Time as the sum of the times required for intruder's activity. This is because according to the assessed scenario the intruder is only one and performs its activities necessarily consecutively.

In scenarios that involve two or more intruders that can perform two or more activities in parallel calculations are different. To calculate Intruder's Time, it is necessary to develop a PERT / CPM model.

The model also calculates Reaction Forces Time as the sum of the activity times required by Reaction Forces to neutralize the intruder. Third, the model calculates the difference between Reaction Forces Time and Intruder's Time. I define these three indicators – Reaction Forces Time, Intruder's Time, and their difference as output variables

Table 1. Probabilistic characteristics of the duration time for Intruder's Activities

Intruder's Activity	Distribution type	Mini-mum Time, seconds	Mean Time, seconds	Maxi-mum Time, seconds
Climbing Administrative Area fence	PERT	8	10	15
Run through Administrative Area	PERT	6	8	15
Penetrating door to protected area	PERT	20	60	90
Run through protected area	PERT	8	10	15
Penetrating wall from reinforced concrete	PERT	40	180	400
Run through vital area	PERT	8	10	15
Sabotage vital equipment	PERT	10	20	40

Table 2. Probabilistic characteristics of the duration time for Reaction Forces Activities

Reaction Forces Activity	Distri-bution type	Mini-mum Time, seconds	Mean Time, seconds	Maxi-mum Time, seconds
First sensing time	PERT	7	10	40
Detection time	PERT	9	10	30
Assessment detection	PERT	4.5	5	12
Muster time	PERT	18	20	50
Preparation time	PERT	9	10	30
Traveling time	PERT	54	60	120
Deployment time	PERT	11	15	40

Table 3. Results of statistical processing of the values of the initial variables as a result of the simulation

Parameter	Intruder's Time	Reaction Forces Time	Difference
Minimum	153.50	130.957	-19.28
Maximum	518.46	224.863	353.62
Mean	315.21	173.532	141.68
90% Confi-dence Interval	± 3.55	± 0.889	± 3.66
Mode	284.69	180.248	71.97
Median	312.68	172.712	139.63
Standard Deviation	68.13	17.074	70.36
Skewness	0.1141	0.2763	0.1231
Kurtosis	2.3794	2.7425	2.4682

in the model. The model is set up to perform a 1000 iterations simulation. The summarized simulation results in numerical form are presented in Table 3, and in graphical form – in Figures 1, 2 and 3.

The resulting statistics and graphical images allow the analyst to draw important conclusions about the effectiveness of the physical protection system. It is possible to estimate the probability distribution of Intruder's Time and compare it with the probability distribution of Reaction Forces Time. Graphically, this comparison is presented in Fig. 4.

For each of the output variables it is possible to calculate what is the probability that the variable will take values higher or lower than a certain value, i.e., in a certain range. These assessments provide an opportunity to justify management decisions about the possibilities for improving the efficiency of the physical security system in various directions – for example, in the direction of reducing the response time or increasing the intruder time.

Very important information one can obtain by calculating the probability that the difference between Reaction Forces Time and Intruder's Time is negative. This is the probability that the Reaction Forces will not

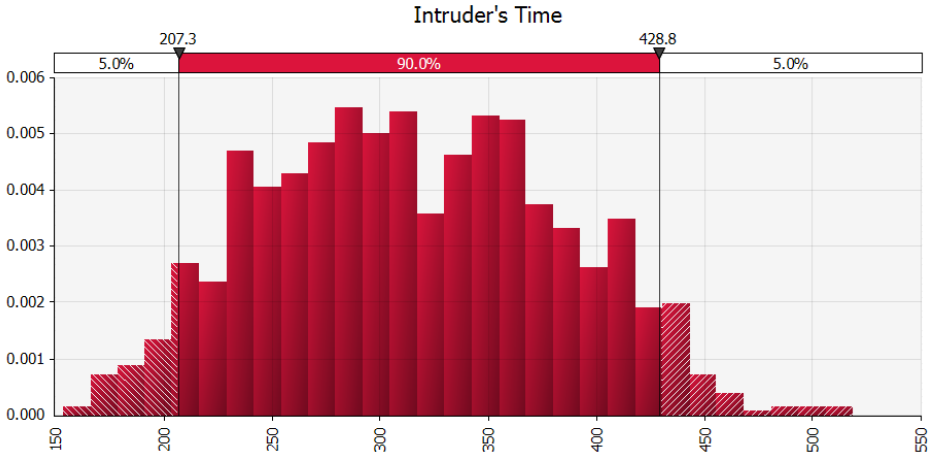


Fig. 1. Results of the simulation of the Intruder's Time variable

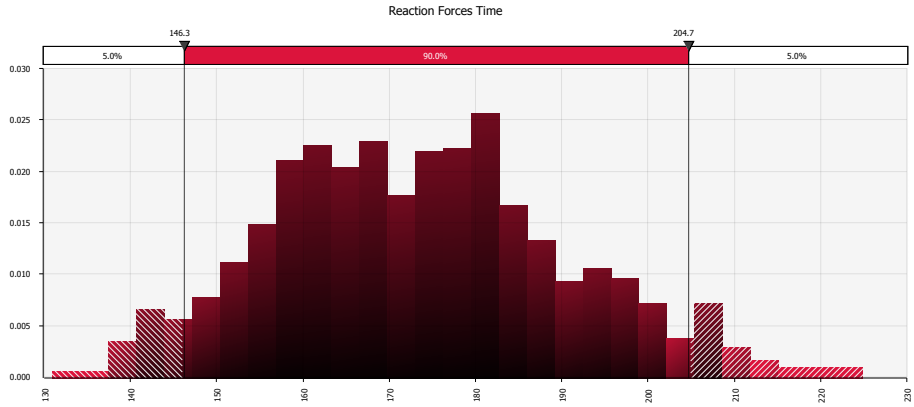


Fig. 2. Results of the simulation of the Reaction Forces Time variable

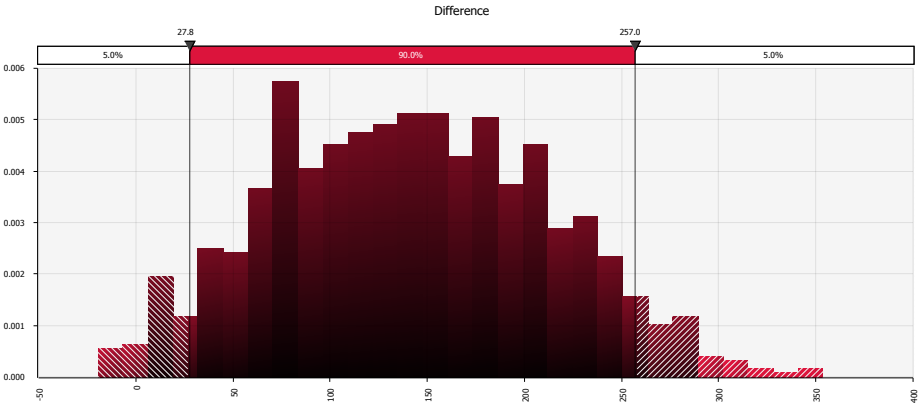


Fig. 3. Results of the simulation of the Difference Between Reaction Forces Time and Intruder's Time variable

be able to neutralize the intruder before it has carried out the sabotage. In the studied model this value is 1.2% (see Fig. 5). This indicator is very often used to assess the effectiveness of the physical security system.

The model calculates the probabilistic characteristics of the Critical Detection Point. To do this, for each iteration, the accumulated amount of Intruder's Time is calculated as a sum of the delay times for each of the delay elements, starting with the last one.

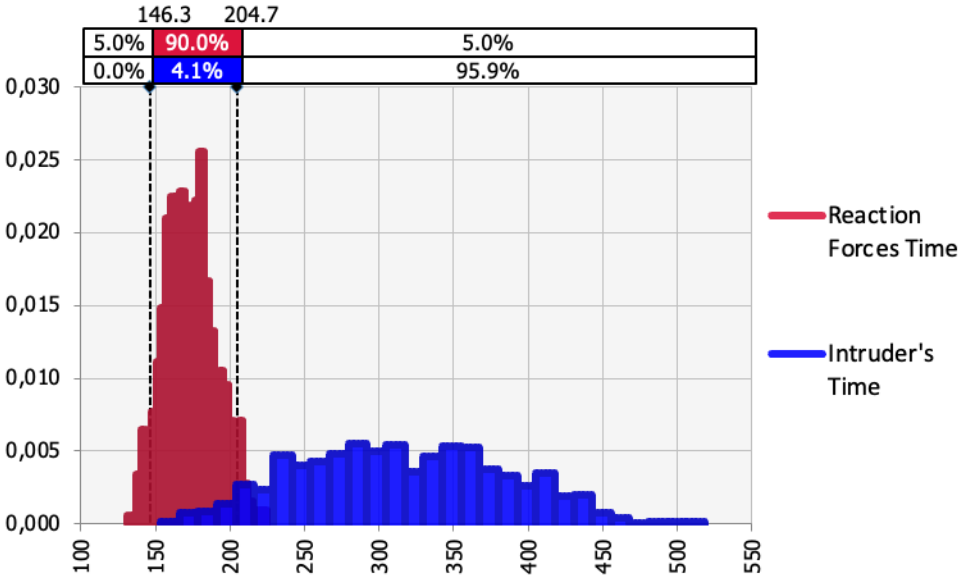


Fig. 4. Comparison between the probability distributions of Intruder's Time and Reaction Forces Time.

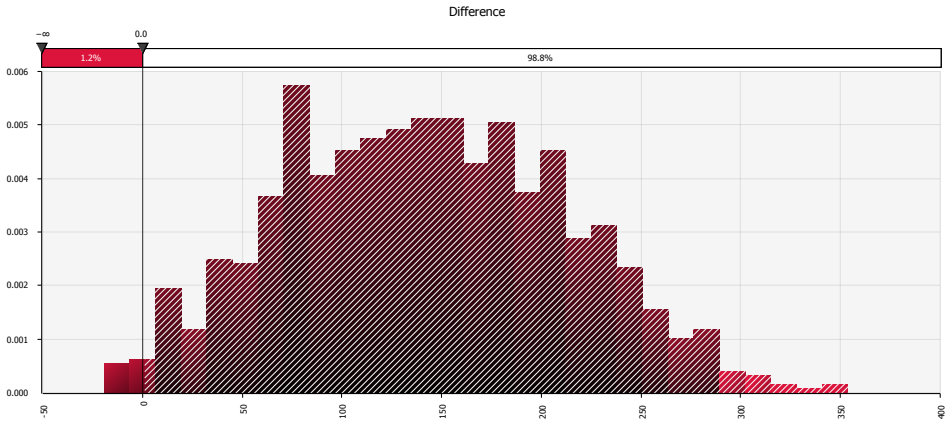


Fig. 5. Calculation of the probability that the Difference Between Reaction Forces Time and Intruder's Time indicator will take a negative value

It is determined at which delay element the intruder should be detected at the latest, so it can be neutralized before performing the sabotage. Possible Critical Detection Point are presented in Table 4.

The statistical analysis makes it possible to determine the probability distribution of the expectations for the Critical Detection Point. The results of this analysis are presented in Table 5 and Fig. 6.

Table 4. Numbering of possible Critical Detection Points

Value	Detection Point
1	Climbing Administrative Area fence
2	Run through Administrative Area
3	Penetrating door to protected area
4	Run through protected area
5	Penetrating wall from reinforced concrete

Table 5. Expectations for Critical Detection Point values

Parameter	Critical Detection Point
Minimum	1.0000
Maximum	5.0000
Mean	4.4810
90% CI	± 0.0501
Mode	5.0000
Median	5.0000
Std Dev	0.9615
Skewness	-1.7365
Kurtosis	5.1609

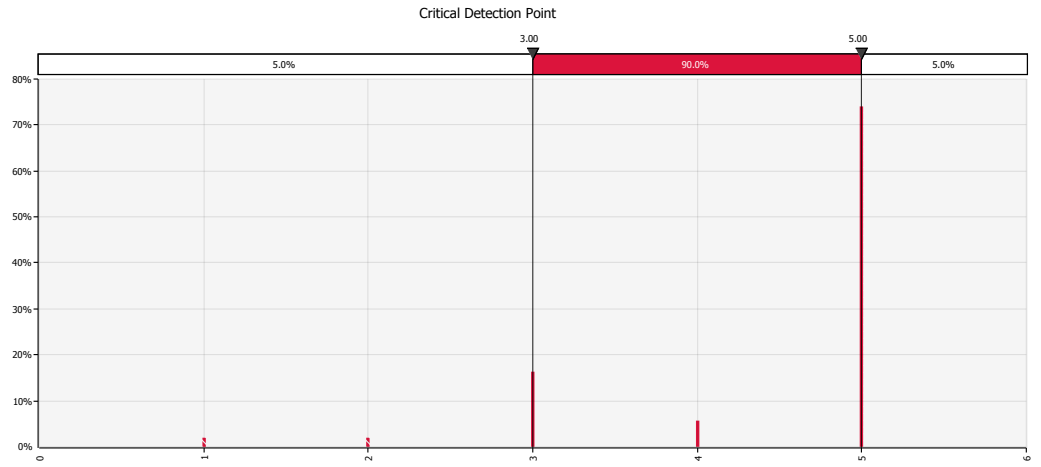
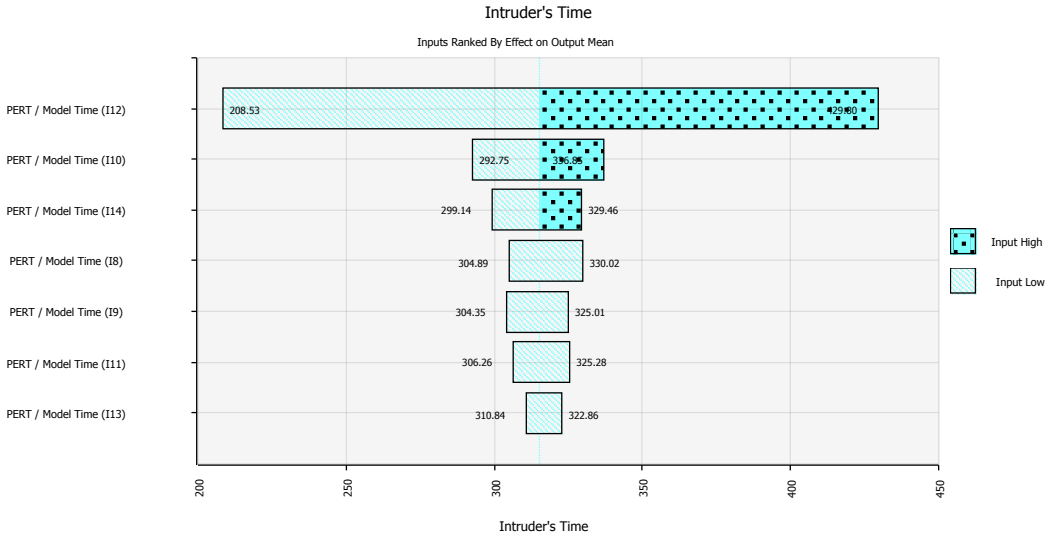


Fig. 6. Probabilistic distribution of expectations for Critical Detection Point

It is recommended that the procedure discussed so far be repeated for all identified scenarios and that the results be compared. The effectiveness of the physical security system can be assessed by determining the path and scenario in which there is a minimum likelihood that the Response Time will be shorter than the Intruder's time.

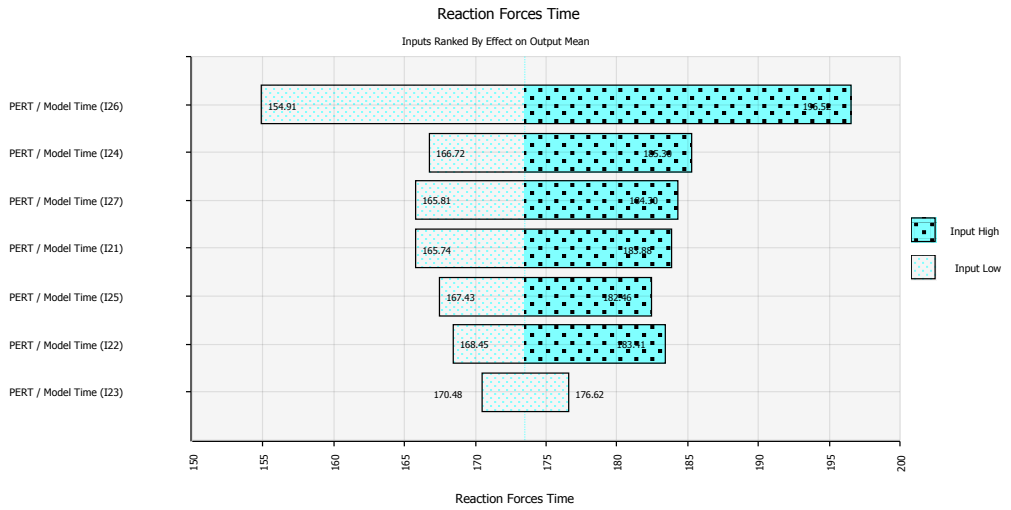
The results of the simulation and the functionalities of the software make it possible to assess the sensitivity of the output variables to changes in input variables. The results of the sensitivity assessment can be presented in different forms. For example, the sensitivity of Intruder's Time, Reaction Forces Time, and Critical Detection Point can be seen in Fig. 7, 8 and 9. Sensitivity analysis provides valuable information for managers when it comes to deciding to reduce the vulnerability of the PPS. It can be determined by changing which inputs can most strongly increase Intruder's Time and decrease Reaction Forces Time. When the necessary costs for the implementation of the possible actions to achieve these effects are considered, a comprehensive program for vulnerability reduction of the PPS can be developed in a rational way.



Legend for Fig. 7

Notations in the model and in the Fig. 7	Corresponding Critical Detection Point
PERT/Model Time (112)	Penetrating wall from reinforced concrete
PERT /Model Time (110)	Penetrating door to protected area
PERT /Model Time (114)	Sabotage vital equipment
PERT/Model Time (18)	Climbing Administrative Area fence
PERT/Model Time (19)	Run through Administrative Area
PERT /Model Time (111)	Run through protected area
PERT/Model Time (113)	Run through vital area

Fig. 7. Sensitivity analysis of the of the Intruder's Time indicator to changes in the input indicators



Legend for Fig. 8

Notations in the model and in the Fig. 8	Corresponding Critical Detection Point
PERT/Model Time (126)	Traveling time
PERT /Model Time (124)	Muster time
PERT /Model Time (127)	Traveling time
PERT /Model Time (121)	First sensing time
PERT /Model Time (125)	Preparation time
PERT /Model Time (122)	Detection time
PERT/Model Time (123)	Assessment detection

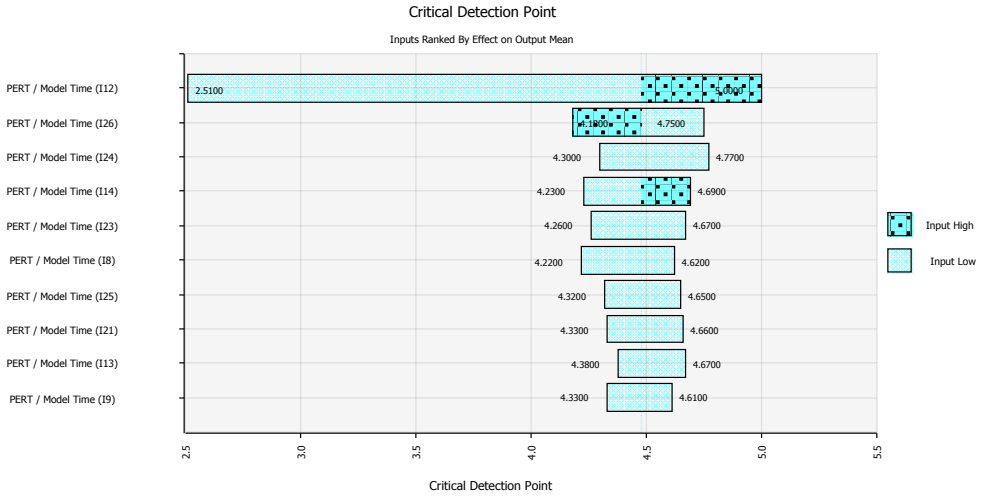
Fig. 8. Sensitivity analysis of the Reaction Forces Time indicator to changes in the input indicators

From Figures 7, 8 and 9 it can be seen that in the considered model Intruder's Time is most sensitive to changes in Penetrating wall from reinforced concrete, followed by changes in Penetrating door to protected area. Reaction Forces Time, on the other hand, is most sensitive to changes in Traveling time, followed by changes in Muster time. Critical Detection Point is most sensitive to changes in Penetrating wall from reinforced concrete, followed by changes in Traveling time and Muster time.

Conclusions

As a result of the performed research the following conclusions can be formulated:

The vulnerability assessment of PPS is an important methodological and practical issue that has a strong impact on security nationally and even globally. Therefore, the operators of nuclear facilities, as well as all players in this field, have a high responsibility on this issue. It is necessary to apply innovative tools and use the latest scientific advances to obtain accurate results.



Legend for Fig. 9

Notations in the model and in the Fig. 9	Corresponding Critical Detection Point
PERT/Model Time (112)	Penetrating wall from reinforced concrete
PERT /Model Time (126)	Traveling time
PERT/ Model Time (124)	Muster time
PERT/ Model Time (114)	Sabotage vital equipment
PERT /Model Time (123)	Assessment detection
PERT/Model Time (18)	Climbing Administrative Area fence
PERT/ Model Time (125)	Preparation time
PERT /Model Time (121)	First sensing time
PERT /Model Time (113)	Run through vital area
PERT/Model Time (19)	Run through Administrative Area

Fig. 9. Sensitivity analysis of the of the Critical Detection Point indicator to changes i n the input indicators

The vulnerability assessment of PPS requires the consideration of several indicators that are random in nature, such as the time during which intruder is expected to overcome the various obstacles in its path, as well as the different components of Reaction Forces Response Time. This requires the application of stochastic models.

The application of simulation models is a powerful tool with growing popularity worldwide. It can also be used successfully in assessing the vulnerability of PPS. The software products available on the market are powerful and have a wide range of applications.

The application of simulation models requires the use of both statistics (e.g., the results of reaction forces exercises) and expert's opinion data that cannot be determined by statistical analysis.

@Risk is a powerful software designed to develop a variety of simulation models. This allows for the development of complex models without necessarily the researcher being deeply acquainted with the theory of probabilities, statistics, modeling, and the methodology of simulation modeling.

The application of such models makes it possible to determine the current level of vulnerability, to establish the critical path and the Critical Detection Point, as well as to evaluate alternatives for improvement. This can be done in at least two ways: 1. By assessing the sensitivity of the resulting variables to changes in the input variables. 2. By systematically applying What-if analysis by playing technically and organizationally feasible alternatives to reduce vulnerabilities.

References

Beenhakker B. L., 1975.Capital investment planning for management, Roterdam University Press.

Biringer B. E., Matalucci R. V. and O'Connor S. L., 2007. Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures, John Wiley & Sons.

Biringer, B. E., Vugrin E. D. and D. E. Warren, 2013. Critical Infrastructure System Securityand Resiliency, CRC Press.

Brandimarte, P., 2014. Handbook in Monte Carlo Simulation. Applications in Financial Engineering, Risk Management, and Economics, Wiley.

Chung C. A., 2004.Simulation Modeling Handbook. A Practical Approach, CRC Press.

Fennelly L. J., 2017. Effective Physical Security, Fifth Edition, Elsevier.

Garcia M. L., 2001. The Design and Evaluation of Physical Protection Systems, Elsevier Science.

Garcia M. L., 2006. Vulnerability Assessment of Physical Protection Systems, Elsevier.

Garcia M. L., 2008. Physical Protection, Nuclear Safeguards, Security, and Nonproliferation. Achieving Security with Technology and Policy, Elsevier, pp. 87-96.

Vintr Z., Vintr M. and Malach J., 2012 . Evaluation of physical protection system effectiveness, International Carnahan Conference on Security Technology (ICCST), IEEE, Hayden, E., 2020. Critical Infrastructure Risk Assessment. The Definitive Threat Identification and Threat Reduction Handbook, Rothstein Publishing.

IAEA, 2007. Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA.

IAEA, 2013. Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme. Implementing Guide. IAEA Nuclear Security Series No. 19, IAEA.

IAEA, 2012. Identification of Vital Areas at Nuclear Facilities. Technical Guidance. Reference Manual. IAEA Nuclear Security Series No. 16., IAEA.

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

IAEA, 2018. Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA.

IAEA, 2020.Preventive and Protective Measures against Insider Threats, IAEA.

IAEA, 2022. IAEA Nuclear Safety and Security Glossary, Terminology Used in Nuclear Safety,

Nuclear Security, Radiation Protection and Emergency Preparedness and Response. 2022 (Interim) Edition, IAEA.

Mun J., 2010. Modeling Risk. Applying Monte Carlo Risk Simulation, Strategic Real Options, Stochastic Forecasting, and Portfolio Optimization, Wiley.

Norman, T., 2016. Risk analysis and security countermeasure selection, Second Edition, CRC Press.

Snell M. K., Winblad A. E., Bingham B., Key B. and Walker S., 1990. The ASSESS (Analytic System and Software for Evaluating Safeguards and Security) Outsider module with multiple analyses, Institute of nuclear materials management conference, Los Angeles, CA (USA), 15-18 Jul 1990, Los Angeles, CA,

Zio, E., 2007. An Introduction to the Basics of Rellablllty and Rlsk Analysls, World Scientific Publishing.

Zio, E., 2013. The Monte Carlo Simulation Method for System Reliability and Risk Analysis, Springe.