IOP Conf. Series: Materials Science and Engineering **135** (2016) 012050 doi:10.1088/1757-899X/135/1/012050

Ways of improvement of methodological approaches to the assessment of the effectiveness of physical protection systems of nuclear facilities in consideration of modern requirements and threats

E A Vlasenko[1], A V Nikienko[1] and D G Demyanuk[2]

[1] Mining and chemical combine, Lenina street, 53, 662970, Zheleznogorsk, Krasnoyarsk region, Russia
[2] Physical Technical Institute of National research Tomsk Polytechnic University, Lenina avenue, 30, 634050, Tomsk, Russia

E-mail: atomlink@mcc.krasnoyarsk.su

Abstract. Methodological approaches to the assessment of the effectiveness of physical protection systems developed by Russian and foreign researchers are reviewed. Some ways of improvement of these approaches are offered. They consider tactics overview, application of two-person rule, aspects of inherent safety of nuclear materials, proposals on the use of test reliability data.

1. Introduction

Due to international agreements Russian authorities run state system of physical protection to prevent acts of nuclear sabotage and proliferation of nuclear materials. The operating organizations create physical protection systems (PPS) at nuclear sites including nuclear power plants. PPS is a set of organizational and technical measures taken by an administration of a nuclear site, its security department, guards forces with a help of technical means of physical protection. There is a set of state and departmental requirements to PPS. Fulfillment of these requirements and system design based on certain principles help to build an effective PPS which means that it can resist unauthorized actions of adversaries against objects of physical protection taking into account a design basis threat (DBT). DBT is usually defined during a vulnerability assessment of a nuclear facility. PPS effectiveness can be measured quantitatively as well as qualitatively. Quantitative measure of PPS effectiveness is called an efficiency indicator.

Efficiency assessment results are used to determine if PPS has to be improved or not. If yes, it helps to understand essentially important ways of improvement. When funding is limited it has a vital meaning.

2. Probabilistic-temporal analysis as a primary method of PPS efficiency assessment

Probabilistic-temporal analysis is a primary method of PPS efficiency assessment in Russia as well as in other countries. Researches all over the world develop and use similar techniques to perform it.

A.V. Boyarintsev, A.N. Brazhnik, A.G. Zuev say that efficiency indicator is a probability of suppression of unauthorized actions of intruders:

$$P = P_{\text{det}} \times P_{del} \times P_n \tag{1}$$

where P_{det} is a probability of detection, P_{del} is a probability of delay, and P_n is a probability of neutralization. To define P_{det} it is offered to refer to technical specifications of intrusion sensors that are used at a site. At the same time, it is allowed to competently decrease a value of probability of detection compared to the one mentioned in manuals considering condition of communication lines and other equipment as well as a "human factor" caused by a need to assess an alarm by an operator [1].

S.V. Skryl, A.V. Dushkin and V.V. Gaifullin offer a probability of protection of a nuclear site against unauthorized actions of adversaries as an efficiency indicator:

$$P = P_i \cdot P_{fo} \tag{2}$$

where P_i is a probability of interception of adversaries by rapid response forces and P_{fo} is a probability that rapid response forces win an armed clash against adversaries.

$$P_i = P_{\text{det}} \cdot P_{tr} \cdot P_{nfo} \cdot P_{dgrr} \tag{3}$$

where P_{det} is a probability of timely intrusion detection by an intrusion sensor system, P_{tr} is a probability of credible alarm signal transition to rapid response forces, P_{nfo} is a probability of no-failure operation of equipment, P_{dgrr} is a probability that rapid response forces deploy at a point of interception of adversaries before an armed clash after receiving an alarm signal.

It is stated that P_{tr} and P_{nfo} can be ignored because at a design stage they may be taken equal to 1. Authors say that P_{fo} can also be taken equal to 1 if a set of organizational measures is taken so that rapid response forces definitely win adversaries in an armed clash. Therefore, an efficiency indicator can be defined as:

$$P_i \approx P_{\text{det}} \cdot P_{dgrr} \tag{4}$$

where P_{det} depends on characteristics, number of intrusion sensors and their location at a site. P_{dgrr} depends on tactics of rapid response forces as well as location and delay parameters of physical barriers that adversaries meet moving towards an object of physical protection [2].

M.L. Garcia offers two basic measures of PPS efficiency. The first one is based on comparison of minimal total delay time throughout the adversary path (TMIN) and response forces time (TG). PPS should provide sufficient delay so that response forces are able to intercept an adversary. The second measure is a total probability of detection of an adversary before he reaches his goal. To consider both measures during the PPS efficiency assessment, it is estimated in at a specific point of the adversary path which is called critical detection point (CDP). CDP is a point where an adversary delay time at the rest of the path (TR) just exceeds response forces time (TG).

$$P_I = 1 - \prod_{i=k}^{k-1} P_{NDi} \tag{5}$$

where P_I is a probability of interception of an adversary by response forces, k is a point where TR just exceeds TG, P_{NDi} is a probability that element i does not detect an adversary [3].

Taking into account a probability that response forces win an adversary in an armed clash an efficiency indicator may look like:

$$P_E = P_I * P_N \tag{6}$$

where P_N is a probability that an adversary is neutralized in case of interception. P_E characterizes vulnerability to a specific threat [4].

The methodical approach used by the State Corporation "Rosatom" is also based on a probability temporal analysis. Following indicators are used to assess the efficiency:

- Differential indicators that characterize probabilities of prevention of unauthorized actions against every object of physical protection.
- An integrated indicator that characterizes an ability of PPS to protect all the objects of physical protection [5].

An integrated indicator is calculated using differential indicators.

Efficiency assessment is carried out for various scenarios of actions of an outside adversary, an inside adversary and their combination.

A differential indicator of PPS efficiency against an outsider is defined as:

$$P_{out} = \max(f(P_{\det}, P^{i}_{inrf})P^{n}_{inrf}, f(P^{i}_{exrf}, P^{n}_{exrf}) \quad (7)$$

where f is a function that depends on tactics of response forces, P_{det} is a probability of detection of an adversary, P^{i}_{inrf} is a probability of interception of an adversary by internal response forces, P^{n}_{inrf} is a probability of neutralization of an adversary by internal response forces, P^{i}_{exrf} is a probability of interception of an adversary by external response forces, P^{n}_{exrf} is a probability of neutralization of an adversary by external response forces.

A probability of detection of an outsider overpassing a layer of physical protection is estimated as:

$$P_{\det} = 1-(1-P_{\det.before})\times(1-P_{\det.after}) \quad (8)$$

where $P_{\det.\text{before}} = 1-\prod_{i=1}^{k}(1-P_i)$ is a probability of detection of an outsider before he overpasses a layer of physical protection, k is a total number of intrusion sensors which have a detection zone allowing to detect an adversary before he overpasses a layer of physical protection, P_i is a probability of detection of an intrusion sensor i that has a detection zone allowing to detect an adversary before he overpasses a layer of physical protection; $P_{\det.after} = 1-\prod_{j=1}^{m}(1-P_j)$ is a probability of detection of an outsider after he overpasses a layer of physical protection, m is a total number of intrusion sensors which have a detection zone allowing to detect an adversary after he overpasses a layer of physical protection, P_j is a probability of detection of an intrusion sensor j that has a detection zone allowing to detect an adversary before he overpasses a layer of physical protection.

A differential indicator of PPS effectiveness is taken equal to a minimal value of probability of prevention of unauthorized actions taken by an adversary using a variety of scenarios [6].

When assessing PPS effectiveness against an insider threat it is assumed that an adversary scenario consists of two parts: moving to a certain layer of physical protection using his own authorization and then a "force" breakthrough. In some cases second part of scenario may not be realized.

3. Ways of improvement of methodology

The assessment of PPS effectiveness based on probabilistic-temporal analysis helps to evaluate an ability to withstand unauthorized actions of different types of adversaries quantitatively. Along with this, a set of proposals to enhance methodology is formulated. Implementation of following suggestions may lead to better objectivity of results of assessment:

- When analyzing scenarios of actions of adversaries and guard forces it is advisable to model actions of several groups of guard forces (alarm group, reserve group) and potential adversaries (main group, cover group). Besides this, different tactics of actions should be considered. These tactics may vary depending on circumstances. Results of armed clashes should also vary depending on weapons and equipment of specific groups taking part in an action.

- Two-person rule should be considered when assessing an action in a zone or a vault where a rule is implemented. If a model of an insider consists of a single person it should be assumed that he is not allowed to such zones. As soon as he gets into a zone a single insider should be considered an outsider.
- When assessing an effectiveness of PPS against an insider that works with another person (colleague) in a zone following a two-person-rule a probability of generating an alarm by a partner should be taken into account.
- The inherent safety of an object of physical protection should be considered when assessing a probability of stealing. The main measure in this case is an equivalent dose level generated by an object of physical protection. If a time of an action is greater than a time required to achieve a certain level of dose a stealing may be considered impossible. E.g., for adversaries who are ready for self-sacrifice (according to a model) a level of dose can be extremely high. For those adversaries who are not ready to risk their health (according to a model) a level of dose should not exceed levels stated in radiation safety instructions.
- When assessing a stealing scenario it is advisable to overlook different paths of adversaries heading to an object of physical protection and back. For instance, when an insider approaches an object of physical protection he is most likely to go through an entry control point legally. However, he is not likely to go the same way back. To minimize a risk of being arrested, he may go back through an evacuation door escaping examination by a guard.
- During the calculation of a probability of detection it is advisable to take into account a probability that a complex of technical means of physical protection is in a state of operability at a moment of an attack. Such probability can be calculated using reliability data, information about periodicity and duration of maintenance, number of maintenance parties, maintenance prioritization, and spare parts delivery period. Reliability theory is a powerful instrument for calculation. State Corporation "Rosatom" collects data on reliability of technical means of physical protection [7]. However, collected data is not used for enhancing believability of results of assessment of the effectiveness of PPS. Some researches try to take into account a probability that a complex of physical protection devices is in a state of operability at a moment of an attack. For instance, P.G. Gorlach offers to use probability of successful data transition P_{dt} as well as availability ratio K when calculating probability of detection. He mentions that P_{dt} is a feature of a data processing system and $P_{dt} \to 1$ because of the modern protective coding methods and repeated look-up. To calculate K he suggests to use a formula:

$$K = \frac{T_f}{T_f + T_m} \tag{9}$$

where T_f is mean time between failures and T_m is mean time of restoration. It is mentioned that modern complexes of technical means of physical protection have $K \approx 0{,}99...0{,}999$ because of repeated look-ups, small time of restoration (several hours), and high mean time between failures of details and devices [8]. Similarly, other researchers suggest to use following multipliers when calculating probability of neutralization: probability of successful data transition to alarm forces, probability of no-failure operation of technical means of physical protection. They mention that these probabilities can be ignored at an early state of designing of PPS. Nevertheless, practice of exploitation of PPS in real conditions proves that values of probability of successful data transition to alarm forces and probability of no-failure operation of physical protection devices may vary drastically because of imperfection of maintenance, spare parts supply system, poor inspections at a site, run-out of equipment and mechanisms, and other reasons.

- During the calculation of a probability of detection it is advisable to take into account an efficiency of compensative measures that are taken for the period of restoration of main components. Usually allocation of guards at certain points, patrolling, buildup of temporary detection sensors and systems, buildup of temporary physical barriers are used at nuclear sites

as compensative measures. Compensative measures are especially actual when considering a mutual action of an insider and outside adversaries. Such threat is absolutely real. For instance, in October, 2014 Belgium authorities found that during 3 years a jihad devotee had been working in one of NPP departments as a security technician [9]. Famous assault on Pelindaba in 2007 could have been organized with a help of an insider [10]. An insider familiar with a state of an operability of PPS can transfer an information about location of a broken sensor to an outsider. The risk is too high that an outside adversary will try to attempt his assault before a broken device is restored.

4. Conclusion

Despite a wide set of instruments and algorithms, modern methods and computer programs designed to assess effectiveness of PPS have plenty of assumptions. Some of these assumptions forbid to consider individual features of a nuclear site (i.e., geographic position, technological features, etc.), guard force tactics, adversary tactics. Eventually, it affects result of an assessment significantly.

On this basis, development of methods of PPS efficiency assessment should be continued in order to provide objective results based on a whole set of individual features of a nuclear site.

References

[1] A V Boyarintsev, A N Brazhnik, A G Zuev 2006 *Issues of anti-terroristic activity: Categorization and vulnerability analysis of facilities* (Saint-Petersburg: JSC "NPP "ISTA-Systems") pp 98-101

[2] S V Skryl, A V Dushkin and V V Gaifullin 2011 Considering physical protection system efficiency evaluation *Information and security. Issue 2 293-96*

[3] Garcia M.L. 2001 *The design and evaluation of physical protection systems* (Burlington, MA, USA: Elsevier Butterworh-Heinemann) pp 243-246

[4] Garcia M.L. 2006 *Vulnerability assessment of physical protection systems* (Burlington, MA, USA: Elsevier Butterworh-Heinemann) p 382

[5] *Guidelines on efficiency evaluation of physical protection systems of nuclear objects* 2015 (Moscow: Rosatom) p 8

[6] *Guidelines on efficiency evaluation of physical protection systems of nuclear objects* 2015 (Moscow: Rosatom) p 18-9

[7] *Guidelines on collection, processing and distribution of information on reliability of technical means of physical protection* 2011 (Moscow: Rosatom)

[8] P G Gorlach 2009 Functional efficiency assessment of a complex of technical means of physical protection *T-Comm – Telecommunication and transport. Issue S2 56-7*

[9] http://rg.ru/2016/03/24/celiu-teraktov-v-belgii-dolzhny-byli-stat-aes.html

[10] https://www.washingtonpost.com/world/how-armed-intruders-stormed-their-way-into-a-south-african-nuclear-plant/2015/03/13/470fc8ba-579d-4dba-a0c0-f0a1ed332503_story.html