Reducing the Vulnerability of Critical Facilities by Improving the Protection of their Critical Elements from Terrorist Attacks

E F Dubinin1 and V I Kuksova1

1Mechanical Engineering Research Institute, RAS, 4, M. Kharitonyevsky Pereulok, Moscow 101990, Russia

E-mail: mibsts@mail.ru

Abstract. The vulnerability of a critical facility depends to a large extent on the protection of its critical elements (structural or technological). Their failure leads to termination of normal functioning of facility or to emergency situations. Therefore, first of all, it is necessary to identify critical elements and analyze their vulnerability with regard to the most probable spectrum of terrorism-related threats, determined on the basis of scenario analysis taking into account new methods of technological terrorism. It is useful to divide critical elements into categories in accordance with physicochemical processes taking place in them and design features. The results of vulnerability analysis and identification of critical elements to be additionally protected are the initial data for improving the facility’s protection system. The decision as to whether additional costs should be incurred to ensure security of facility is made on the basis of a quantitative assessment of the ratio of corresponding costs, risks and losses.

1. Introduction
The safety of social-natural-technogenic systems is largely determined by protection level of critical facilities (CF) that comprise them. Among the main systemic factors that adversely affect the safety of CFs is the possibility of terrorist attacks.

Most of CFs, for which terrorist attacks might have large-scale destructive consequences, is well protected. These include enterprises of nuclear industry, oil refinery plants, terminals for storage and pumping of liquefied gas, etc. The facts of serious disruption of such facilities operation as a result of terrorist attacks are very rare [1]. However, one should consider the possibility of realization terrorist threats to the listed facilities.

At the present stage, one can very likely expect a transition from ordinary to technological terrorism with the use of new types of possible terrorist attacks [2]. This is the use of unmanned aerial vehicles (drones), the use for terrorist purposes of new types of toxic chemicals and highly dangerous bacteriological materials, the impact of electromagnetic radiation on safety systems, personnel, security guards of facilities, etc.

Technological terrorism implies organization of powerful external unauthorized impacts at CFs, ensuring breakthrough of their protection system. Secondary catastrophic processes due to stocks of hazardous substances ($W$), energy ($E$), and information ($I$), stored or processed at the facilities are initiated. The catastrophe then escalates outside the CF boundaries with substantially increase in secondary and cascade losses. Primary losses caused by the damaging factors of terrorist impact is up
to 10%, and secondary losses associated with escalation of the accident at a facility accounts for up to 90% of total losses from a terrorist attack [3, 4].

As a rule, technological terrorism involves:

- preliminary analysis of the CF structure and vulnerabilities, the potential sources of secondary catastrophic processes (stocks \(W, E, I\), the weak points in the protection systems, and selection of the most efficient attack scenarios;
- identification of key elements and links of the CF, at the destroying of which the system will not be able to perform its functions;
- use of the vulnerabilities and powerful initiating impacts at the CF to break through protection systems;
- assessment of events development scenarios and determination of such end states of the CF that are capable of initiating powerful secondary catastrophic processes outside the facility.

In order to ensure protection of CFs, a special analysis of methods and scenarios of possible terrorist acts and the respond of CFs to terrorist impacts is required, with a determination of their vulnerability level. This will make it possible to determine the degree of discrepancy of the taken protection measures with expected threats or specified safety requirements.

Complex technical system, including CF, can be considered as a set of structurally interconnected elements. This approach involves two directions to reducing vulnerability:

- reduction of local vulnerability of elements and links of system;
- reduction of structural vulnerability of system [5, 6, 7].

To reduce the local vulnerability of CF elements, the most significant are the critical elements of CF (structural or technological). Their failure leads to termination of normal functioning of the facility as a whole, or emergency situations. If critical elements (CE) are not resilient enough or weakly protected, they become the most vulnerable places of facility.

2. Identification of critical elements of facility

To define the critical element, it is advisable to use the theory of reliability, which introduces the corresponding concept in the analysis of technical systems. According to GOST 27.310-95 3.7, this is such an element of system, the failure of which is critical. The severity of this failure consequences is considered inadmissible and requires special measures to reduce the probability of given failure and / or the possible damage associated with its occurrence [8]. For each specific system (including CF), the individual signs of identifying critical elements may be established.

Table 1 shows main critical elements of various types of CF. Materials of works [5, 9, 10, 11] were used in its preparation. The list of CE (objects likely to be targeted by terrorists) is determined on the basis of expert assessments, analytical and statistical data, quantitative indicators.

With pre-planned terrorist attacks, there is a high probability that attacks will be targeted primarily at the CEs, as they are most important for the safe functioning of CFs. With the advent of new technical means and the development of new terrorist attack scenarios, existing protections may not be sufficient, and CF will become vulnerable without additional protective measures. Therefore, in the first place, it is necessary to develop measures to reduce the vulnerability of critical elements of facility. First of all, it is necessary to analyze the vulnerability of CEs with regard to the most probable spectrum of terrorist threats determined on the basis of scenario analysis.

In the analysis, it is advisable to divide critical elements into categories in accordance with physicochemical processes taking place in them and design features. Elements belonging to the same category may be characterized by the same set of possible accident initiation models. For each category, its own specific triggering events and a model of destruction under the action of damaging factors (shock and thermal effects, fragment impacts, etc.) should be developed.
Table 1. Main critical elements of various types of CF

| Type of CF                                | Sample list of critical elements                                                                 |
|------------------------------------------|--------------------------------------------------------------------------------------------------|
| Hydroelectric power stations and hydro   | Dams; poternas; power-house permanent equipment; central control panel; cable tunnels; dikes; floodgates |
| engineering facilities                   |                                                                                                 |
| Nuclear power plants                     | Reactor and reactor elements; steam turbines; cable lines; spent fuel storage                      |
| Chemically hazardous facilities          | Warehouses and storage tanks; process equipment; pipelines; hazardous chemical waste repositories |
| Petrochemical facilities                 | Pressure vessels; columns; compressors; heat exchangers; turbines; pumps; reservoirs; trunk pipelines |
| Facilities of transport infrastructure    | Places of mass concentration of people (train stations, airports, etc.); vehicles with passengers; subways |
| Russian information infrastructure       | Information and telecommunication systems of all levels of state power, financial sphere, communications, Ministry of Emergency Situations and other emergency response services |
| Automated hazardous manufacturing        | Database servers; application servers; programmable logic controllers; switching nodes; data collection sensors; execution mechanisms |
| management systems                       |                                                                                                 |

3. Directions for reducing vulnerability of CF

Thus, measures for reducing vulnerability of CFs it seems advisable to carry out in two directions (figure 1).

The first direction involves development of a set of measures aimed at protecting critical elements from extreme impacts in order to prevent local damages in the system.

Implementation of the second direction provides for improvement of the system structure, introduction of reservation, creation of active and passive means of protection aimed at localization of failures, prevention of cascade effects and reduction of probability of the most catastrophic scenarios after local damages to the system [5, 7].

As can be seen from figure 1, measures to reduce local vulnerability of CF critical elements advisable to carry out in three stages, which include:

- identification of facility critical elements;
• assessment of vulnerability (resilience) of facility critical elements to the most probable types of possible destructive impacts;
• selection of critical elements characterized by increased vulnerability to deliberate destructive impacts.

Identification of CEs according to results of studying the influence of a particular technological element on stability of operation of the entire facility is carried out when analyzing technological scheme of facility. In particular, the protections and blockings provided for in design and technology from emergency situations are considered, and such points are identified, the impact on which is guaranteed to interrupt the technological process.

Identification of critical elements to be protected is aimed, inter alia, at the maximum reduction in complexity and cost of security system. This system should protect the necessary number of identified elements, while ensuring the high efficiency and security of CF as a whole.

4. Assessment and reduction of vulnerability of critical elements and CF as a whole
As a result of vulnerability analysis, the following should be obtained:

• list of threats, ranked by degree of hazard;
• types and dimensions of possible losses and damages;
• list of protection objectives with determination of their priority;
• categories of system elements taking in account the level of potential damages;
• protection criteria defined by category of system elements and expressed in quantitative (time and probabilistic) indicators;
• list of vulnerable places of system and list of measures to achieve specified level of protection.

As indicators of vulnerability of critical elements, one can use the degree of vulnerability in the ordinal rating scale or the probability of successful realization of damaging impact in the probability scale.

The cumulative probability of vulnerability realization \( P \) to identified threats can be defined as:

\[
P = 1 - \prod_{i=1}^{n} (1 - p_i)
\]

where \( p_i \) is the probability of realizing of the \( i \)-th threat through the corresponding vulnerability.

The results of vulnerability analysis of critical elements and the structure of CF are the initial data for development of the facility protection system [12, 13]. The following types of protection are used to protect CFs from initiating impacts and development of emergency situations: rigid protection; constant functional protection; natural protection; security guards; combined protection. Risk reduction for CFs, as a rule, is achieved by applying a complex of all the listed protection systems.

In view of the foregoing, when developing a protective complex for the entire CF, it is advisable to create additional protection barriers around its critical elements (figure 2).

Barriers are set in the way of possible external impacts, thus creates a series of successive levels of protection. It includes:

• creation of additional successive physical barriers on the way of possible external impacts in the direction of facility protected elements;
• development of technical and administrative measures to maintain the integrity and efficiency of these barriers.

When developing additional protection barriers, it is necessary that the most important security zone is inside other zones.
The probability that terrorists will be able to break through protection barriers of the CF element of interest to them is a quantitative indicator of vulnerability. With the increasing number of protection barriers, the level of vulnerability of the facility decreases.

Let, for example, the safety barriers of critical element divide the protected space into 5 zones. At that the critical element of the facility is located in zone 5. In this case, the probability of the threat $H$ being realized in zone 5 (the most important area) will depend on the probabilities of breaking through the protection lines $R_1, R_2, R_3, R_4, R_5$:

$$H_5 = P(R_1) \cdot P(R_2) \cdot P(R_3) \cdot P(R_4) \cdot P(R_5)$$

(2)

Because $P(R_i)<1$, the probability $H$ decreases with the increase in the number $i$ of lines of protection.

In order to create additional lines of protection for CEs, it is possible to include additional subsystems of various operating principle in the existing CF protection system. These can be additional guarded zones, checkpoints, personnel access control and management systems, security alarms, television surveillance, operational communications and alerts, security lighting, etc.

5. Additional measures to assess protection of CF and its critical elements

The CF protection level is not a constant value [9] because:

- the value of the integral risk varies over time due to changes in technological processes, physical and moral wear of the facility, improvement of protection systems, changes in environment parameters and external impacts;
- changing the regulatory-legal framework for risk management is possible.

Therefore, the protection level of CF and its critical elements should be considered as a dynamic characteristic. In order to ensure the necessary protection level and continuous improvement of CF protection systems, periodic assessment of the sufficiency of these systems, continuous monitoring of CF, and additional measures to ensure the specified level of protection of facility are necessary.

The decision as to whether additional costs should be incurred to ensure security of CF is made on the basis of a quantitative assessment of the ratio of corresponding costs, risks and losses [14]. This compares the estimated cost of preventable damage $C_{PD}$ and the cost of creating additional protection subsystems $C_{PS}$. The criterion of expediency of additional financial investments is fulfillment of the condition $C_{PD} > C_{PS}$. According to some estimates [15], security costs amounting to 5-10% of the losses predicted in the event of a terrorist act may be considered justified.
6. Conclusions
The local vulnerability of CF depends to a large extent on the protection of its critical elements. To identify them, it is advisable to use the theory of reliability. With the advent of new methods of technological terrorism, to ensure security of CEs, it is necessary to analyze their vulnerability with regard to the most probable spectrum of terrorist threats determined on the basis of scenario analysis.

In the analysis, it is advisable to divide critical elements into categories in accordance with physicochemical processes and design features. For each category, its own specific triggering events and models of destruction under the action of damaging factors may be developed.

The results of vulnerability analysis of critical elements and the structure of CF are the initial data for improvement of the facility protection system. When developing CF protective complex, it is necessary to create additional protection barriers around its critical elements, taking into account the newly identified threats. At the same time, it is advisable to include additional subsystems of various operating principle in the existing CF protection system.

The protection level of CF and its critical elements should be considered as a dynamic characteristic. Therefore, periodic assessment of the sufficiency of CF protection system, continuous monitoring, and additional measures to ensure the specified level of protection of facility are necessary. The decision as to whether additional costs should be incurred to ensure security of CF is made on the basis of a quantitative assessment of the ratio of corresponding costs, risks and losses.

7. References
[1] Kamyshtansky M I et al. 2011 Organization of protection against terrorist acts, explosions, fires, epidemics and emergency situations caused by them. Practical guide (Moscow: Institut riska i bezopasnosti) p 512 (in Russian)
[2] Mozhayev N M 2011 Bulletin of the Academy of Military Sciences 3(36) 38-43 (in Russian)
[3] Dmitry O Reznikov, Nikolay A Makhutov and Rasim S Akhmetkhanov 2018 Analysis of Terrorist Attack Scenarios and Measures for Countering Terrorist Threats. http://dx.doi.org/10.5772/intechopen.75099
[4] Petrov V P, Reznikov D O, Kuksa V I and Dubinin E F 2007 Safety and emergencies problems 1 89-105 (in Russian)
[5] Makhutov N A, Akhmetkhanov R S, Dubinin E F and Kuksa V I 2018 Safety and emergencies problems 4 28-43 (in Russian)
[6] Makhutov N A and Reznikov D O 2011 J. of Machinery Manufacture and Reliability 6 92-98
[7] Makhutov N A, Petrov V P, Reznikov D O and Kuksa V I 2009 Safety and emergencies problems 2 50-69 (in Russian)
[8] Dependability in technics. Failure mode, effects and criticality analysisys. Basic principles: GOST 27.310-95 (int.1997) 2007 (Moscow: Standartinform) p 14 (in Russian)
[9] Makhutov N A, Pernyakov V N, Akhmetkhanov R S, Reznikov D O and Dubinin E F 2013 Risks Analysis and the Way to Protect Strategic Objects of Oil and Gas Sector. Student’s Book (Tyumen: TyumGNGU) p 560 (in Russian)
[10] Tsygichko V N, Chereshin D S and Smolyan G L 2018 Safety of critical infrastructures (Moscow: KRASAND) p 200 (in Russian)
[11] Pishchik B N 2013 Computational technologies 18 170-174
[12] Makhutov N A, Akhmetkhanov R S, Dubinin E F and Kuksa V I 2011 Safety and emergencies problems 6 51-67 (in Russian)
[13] Mozhayev N M 2009 Bulletin of the Academy of Military Sciences 2(27) 38-43 (in Russian)
[14] Isaev V S, Makiev Yu D, Malyshnev V P, Taranov A A and Kamzolkin V L 2014 Civil Protection Strategy: Problems and Research 2(7) 454-463 (in Russian)
[15] Makhutov N A et al., 2012 Safety of Russia. Safety and Protection of Strategic Objects, part 1: Scientific Foundations of Safety and Protection of Strategic Objects Critically Important for National Safety (Moscow: Znaniye) p 896 (in Russian)