Chapter 12

Analysis of Terrorist Attack Scenarios and Measures for Countering Terrorist Threats

Dmitry O. Reznikov, Nikolay A. Makhutov and Rasim S. Akhmetkhanov

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75099

Abstract

The chapter will present the classification of the types of modern terrorism and describe scenarios and probabilistic models of ordinary, technological, and the so-called intelligent terrorism that are distinguished by their triggering events, propagation modes, damaging factors, probabilities, and consequences. A comparative assessment of these three types of terrorism is presented. Dynamic three-sided models allow assessing the situation from standpoints of terrorists and law enforcement agencies, the administration of the complex engineering system, and analyzing actions and counteractions of various sides involved. A new comprehensive approach to ensuring complex engineering system security is described. This approach is focused not only on the development of protection barriers and safeguards against predetermined list of design-basis scenarios of terrorist attacks but also on increasing the system's resilience toward beyond design-basis attack scenarios.

Keywords: complex engineering system, terrorist attack, risk assessment, protection barrier, resilience

1. Introduction

Complex engineering systems (CESs), such as nuclear and thermal power stations; hydro engineering facilities; chemical, metallurgical, and oil refinery plants; etc., are critical in terms of population life support and ensuring sustainable economic development. The functioning of complex engineering systems is connected with storing, processing, and transportation of huge amounts of energy and hazardous materials. The unauthorized

release of energy and hazardous material at a CES may cause disastrous consequences and trigger cascading failures in interrelated infrastructures. This makes complex engineering systems attractive targets for terrorists and requires special attention in countering terrorist threats [1–8].

Complex engineering systems are characterized by a complex structure, complicated behavior, and interaction between their components, which determine the ability of systems to redistribute loads and to resist cascading failures occurring after local failure of their individual components. Owing to the high level of uncertainty concerning the governing parameters of CESs, environmental conditions, and external impacts, the estimation of the complex engineering system performance should be probabilistic. Their evolution should be described by multivariate scenario trees [9–11].

Through the efforts of specialists from many countries, an extensive bank of knowledge has been developed for analyzing accidents and catastrophes at complex engineering systems, studying scenarios by which they might be initiated, and reducing the vulnerability of CESs with regard to natural and man-made disasters [12]. This bank of knowledge should be used as widely as possible to ensure security against the impacts of terrorism. This approach to analyzing terrorism-related threats presupposes that emergency situations triggered by terrorist attacks develop according to laws analogous to the development of emergency situations caused by natural or industrial disasters. Therefore, they may be analyzed by methods and models used to address classical problems in risk and safety theory [13–16].

The threat of terrorist attacks must be included in the system of studies of possible scenarios of how emergency situations might develop. In particular, event trees used in risk analysis at critically important infrastructure sites must be augmented with scenarios taking into account the possibilities of terrorist attacks that substantially change the scenarios themselves as the structure of primary initiating factors in emergency situations. They also lead to the initiation of cascading processes in the development of accidents and catastrophes with the most serious losses to the population, economic objects, and other vital resources. A classification and probabilistic models of basic scenarios of terrorist attacks were developed (**Figure** 1).

The need to include in the range of problems being considered the analysis of terrorism risks and terrorist mechanisms for initiating extreme situations requires developing and adapting existing models and methods for studying catastrophes with the aim of taking into account the special characteristics of their initiation with the help of unauthorized and terrorist actions that could be taken to attack at the most vulnerable and significant targets critically important for the national security infrastructure.

As it is imperative that terrorist risks and terrorist mechanisms of triggering emergencies be included into the framework of traditional risk assessment, the existing models and methods for analysis of accidents at CES should be modified, and new ones have to be developed in order to take into account specific properties of emergency initiation by terrorist impacts which can be targeted at the most vulnerable facilities of critical infrastructures. Most of the

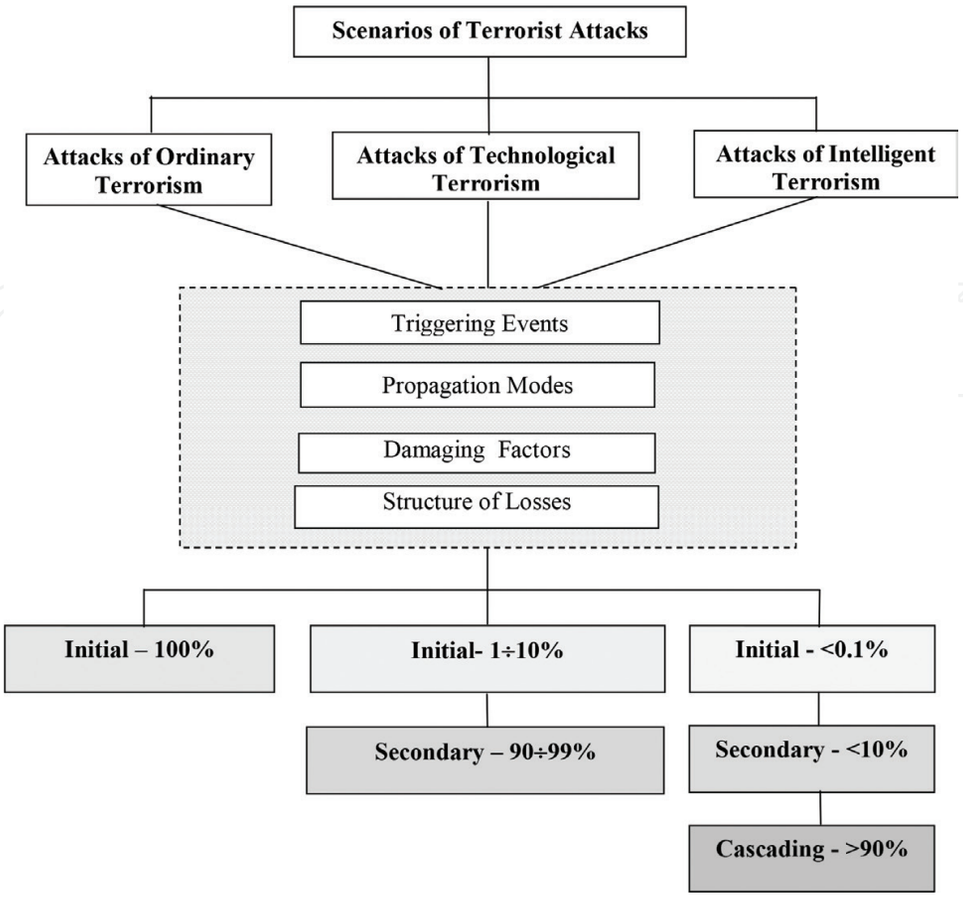

Figure 1. Basic scenarios of terrorist attacks.

components of complex engineering systems were however constructed in conformity with national and international regulations and norms for design, construction, and maintenance without direct consideration of terrorist threats [17, 18]. In this context, two major security-related problems arise:

1. Ensuring protection of the existent CES against terrorist attacks
2. Designing and constructing of a new CES with special protection barriers against terrorist attacks

To cope with these fundamental problems, it is necessary that a special analysis of methods and scenarios of terrorist acts be carried out and a study into how the existing and new protection barriers respond to terrorist attacks be conducted.

Conventional safety analysis for CES is to be focused on the question: What is the way for an accident scenario to be realized in the given system?

When addressing security problems for complex engineering systems, one should also consider the situation from the terrorist's standpoint. Hence, the modified question for security analysis should be: What is to be done for the given scenario to be realized at a CES?

2. General risk assessment model

According to the traditional risk assessment model, risk is considered to be a function of threat T, vulnerability V, and consequences C: $R = f(T, V, C)$. The model was developed to assess risks of technological catastrophes and natural disasters and now is widely used in terrorist risk assessments. Here threat is defined as probability of terrorist attack on a certain complex engineering system, $T = P(A)$; vulnerability is estimated as conditional probability of a system's failure given the attack occurs, $V = P(F \mid A)$ and consequences are defined as losses that occur as a result of the attack and the system failure, $C = E(U \mid A, F)$. Then terrorist risk index is determined by Eq. (1):

$$R = P(A) \cdot P(F \mid A) \cdot E(U \mid A, F). \tag{1}$$

For complex engineering systems that are subjected to multiple threats and multiple failure scenarios, risk assessment implies assessment of a scenario tree (**Figure** 2). This is being done using graph models called scenario trees [6, 7, 9]. The system is designed to fulfill the so-called success scenario S_0 (i.e., a transition from its initial state IS to the designed end state ES_0). Since any failure scenario S_* presents a deviation from the success scenario S_0 that corresponds to the successful functioning of the *CES*, the scenario S_* must have a disturbance point at which an extreme event, or, in case of terrorism, a terrorist attack (A_k), occurs (**Figure** 2). Each attack gives rise to a branch of a scenario tree that has a corresponding set of scenarios S_i that ends with an end state (ES_i). In this case, one can get a similar risk index using matrix expression:

$$R = \underbrace{\{P(A_1); P(A_2); \ldots; P(A_n)\}}_{\text{Threat } \mathbf{T}} \times \underbrace{\begin{bmatrix} P[ES_1 \mid A_1]\, P[ES_2 \mid A_1] \cdots P[ES_m \mid A_1] \\ P[ES_1 \mid A_2]\, P[ES_2 \mid A_2] \cdots P[ES_m \mid A_2] \\ \cdots \\ P[ES_1 \mid A_n]\, P[ES_2 \mid A_n] \cdots P[ES_m \mid A_n] \end{bmatrix}}_{\text{Vulnerability } \mathbf{V}} \times \underbrace{\begin{Bmatrix} U_{ES_1} \\ U_{ES_2} \\ \cdots \\ U_{ES_m} \end{Bmatrix}}_{\text{Consequences } \mathbf{C}} \tag{2}$$

Eqs. (1) and (2) give first-order indicators of terrorist risk. They also determine three main ways of risk reduction: Reduction of terrorist threat is in the sphere of responsibility of law enforcement and intelligence communities, while reduction of vulnerability and consequences are the domains of engineering community and emergency management agencies, respectively.

In terrorist risk assessment framework, the main challenge is to estimate the probability of a terrorist attack. Some specialists believe that probabilistic measure is not adequate for the terrorist risk assessment since terrorist attack is not a stochastic event but a deliberate action based on the assessment made by terrorists regarding their skills and capabilities and the system's vulnerabilities.

Assignment of probabilities to the terrorist attack is a task which has a substantial human and behavioral dimension. The main problem is to describe the intentions of terrorists, their preferences, system of values (i.e., utility function), and decision rule. This allows one to assess the probability of different attack scenarios. The probability of each attack scenario is a function of the scenario's successful realization and their preferences regarding the expected consequences of that scenario.

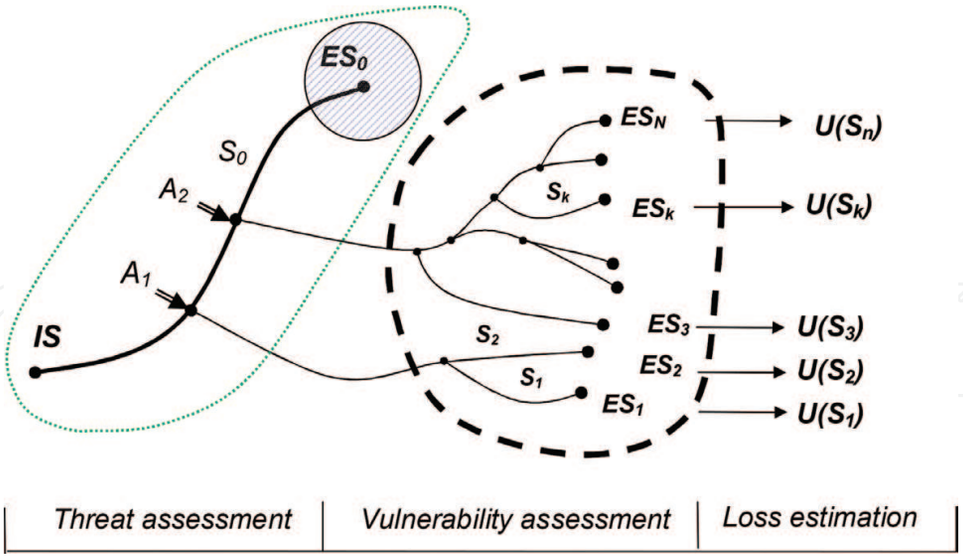

Figure 2. General risk assessment framework.

Unfortunately, Eqs. (1) and (2) could only be considered first-order indicators of the terrorist risk. The problem is that these equations do not allow one to account for a number of specific features of terrorism.

3. Specific features of terrorist threats

When assessing security-related problems for complex engineering systems, one should take into account the following characteristics of the terrorist threat [17, 19, 20].

High level of uncertainty: In modeling terrorist scenarios, we encounter a higher level of uncertainty. In addition to the uncertain factors inherent in threats of a natural or man-made nature, terrorist threats entail new factors of uncertainty resulting from the complexity of evaluating terrorists' system of values and behavioral logic as well as their organizational-technical potential and the resources at their disposal.

High level of dynamism: Terrorist attack scenarios and impact factors are more dynamic by nature than scenarios and impact factors for natural and man-made disasters to which the system is subject. A change in the spectrum and intensity of terrorism-related extreme effects on the system is significantly more rapid than in the case of natural or man-made threat. This is due to the terrorists' capacity for constantly expanding their arsenal of mechanisms for initiating emergency situations using modern means of attack, reacting to changes in protection barriers, and learning lessons from mistakes made during previous attacks on the system similar to it.

The capability of terrorists to choose attack scenarios deliberately: This refers to terrorists' deliberate selection of attack scenarios (places, times, and types of actions), taking into account the system vulnerability parameters and the losses expected if an attack is successfully carried out. That is, terrorists are capable of analyzing the vulnerability matrix and structure of losses for various types of actions against the CES and selecting the attack scenario that maximizes the harm to society (taking into account secondary and cascading losses). Here, in addition

to probability analysis, it is also necessary to apply the tools of game theory, which makes it possible to take into account the intentional actions of terrorists.

Complex nature of the terrorist threat: The presence of a terrorist organization in a region may give rise to the possibility of a broad spectrum of attack scenarios. Thus, to counter terrorist threats and terrorist mechanisms for initiating emergency situations to an even greater degree than for natural and man-made risks, a systemic approach is needed for ensuring security and developing an optimal strategy for counterterrorism force and resource deployment. Inasmuch as concentrating resources on protecting one system element (or protecting a target from one scenario of terrorist action) could prove useless because, after evaluating the situation, the terrorists could redirect the attack against another element of the system or switch to a different attack scenario. In this case, counterterrorism efforts will fail to reduce risk and increase the system's level of protection.

Presence of two-way linkages between the terrorist threat and system vulnerability: The structure of linkages among the risk factors for the given *CES* in case of natural or manmade catastrophes is presented in **Figure** 3**a**. One differentiating feature of a terrorist risk assessment is the presence of two-way linkages (feedbacks) between the terrorist threat and (a) vulnerability of the system to the threat and (b) the magnitude of expected losses if the threat is successfully realized (see **Figure** 3**b**). This characteristic of terrorism must be examined in detail. In particular, reducing the vulnerability of a given system makes it possible to reduce substantially the level of the terrorist threat it faces.

In terrorist risk assessment framework, the main challenge is to estimate the probability of a terrorist attack. Some specialists believe that probabilistic measure is not adequate for the terrorist risk assessment since terrorist attack is not a stochastic event but a deliberate action based on the assessment made by terrorists regarding their skills and capabilities and the system's vulnerabilities.

Assignment of probabilities to the terrorist attack is a task which has a substantial human and behavioral dimension. The main problem is to describe the intentions of terrorists, their preferences, system of values (i.e., utility function), and decision rule. This allows assessing probability of different attack scenarios.

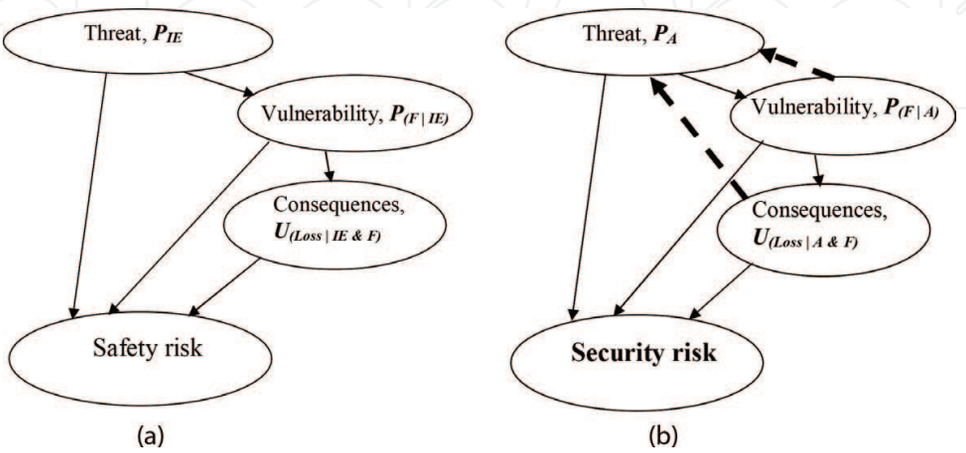

Figure 3. (a) System of linkages among risk factors for natural or man-made hazards (safety context). (b) System of linkages among risk factors for terrorist threat (security context).

Terrorists' capacity for self-learning: Because terrorists are capable of analyzing the results of previous attacks and drawing conclusions from them, their experience in "successful" and "unsuccessful" attacks can have a noticeable effect on the selection of a scenario for the next attack. Attack scenarios that proved their effective in the past are most likely to be repeated by terrorists in the future, while scenarios that ended unsuccessfully will most likely to be less attractive to terrorists and consequently are less likely to be repeated. Therefore, in assessing the chances that various attack scenarios will be realized, statistical self-learning models are more effective than traditional frequency methods.

In solving the above problem of security analysis, it is necessary to assess the resources the terrorists possess. In security analysis, by resources we mean a broad set of factors that determine the potential of a terrorist organization. These include:

- Material resources: technical means, equipment, and "human material" that can be used for terrorist attack
- Nonmaterial resources: experience and skills of terrorists, their knowledge, and access to the CES internal procedures

To answer the question of security analysis, experts should consider the quality of equipment the terrorists have, their skills and knowledge of *CES*, and their ability to take advantage of the existing vulnerabilities (and even create new ones) in order to organize the attack.

The ability of terrorists to select the most vulnerable and critical elements of *CES*, choose the time and place of an attack, adapt to changes of safety barriers and defense strategies, and learn lessons from previous attacks requires that the game theory approaches be included into probabilistic risk assessment models. That means that (a) traditional scenario trees used in safety risk assessment, which include only chance nodes, have to be supplemented by decision nodes that describe rational deliberate actions and counteractions of terrorists and counterterrorists; (b) models for terrorist risk assessment should be multi-sided and describe the situation from the perspective of terrorists and counterterrorist forces [11]; (c) these models should be dynamic and allow one to update actions and counteractions of various sides involved at different time steps.

4. Three types of terrorist attack scenarios

Scenarios of terrorist attacks can be divided into three types, scenarios of ordinary, technological, and intelligent terrorism, that differ in resources used by terrorists to carry out the attacks and structure of losses inflicted by the attacks (**Figure** 1) [17–19].

Scenarios of ordinary terrorism imply organization of explosions, fires, and assassinations of officials, public figures, and people at large in order to intimidate people and destabilize political situation in the country or region. Scenarios of ordinary terrorism are not considered in this paper since these scenarios are not focused on complex engineering systems. We are going to deal with two other types of terrorist attack scenarios that are directly related to *CES.*

4.1. Scenarios of technological terrorism

Scenarios of technological terrorism (*STT*) imply powerful unauthorized impacts at complex engineering system capable of:

- Breaking through the *CES* protection system
- Initiating secondary catastrophic processes due to hazardous substances (*W*), energy (*E*), and information (*I*) stored or processed at the *CES*
- Escalation of the accident outside the *CES* boundaries with substantially increased secondary and cascade losses

Technological terrorism is based on taking advantage of the existing vulnerability of the system. To perform an attack of technological terrorism, it is necessary to preliminarily:

- Analyze the *CES* structure and vulnerability, i.e., to reveal potential sources of secondary catastrophic processes (stocks of *W,E,I*), the weak points in the *CES* protection systems, and to devise the most efficient attack scenarios.
- Identify the *CES* key elements and links whose failure would disrupt the system.
- Calculate the strength of the initial impacts that might break through the *CES* protection barriers.
- Assess the *CES* scenario tree and determine the end states ES_* capable of initiating major secondary catastrophic processes outside the *CES.*

Scenarios of technological terrorism do not require that the attacking party have any insider information and can inflict point impacts imperceptible by the *CES* monitoring systems;

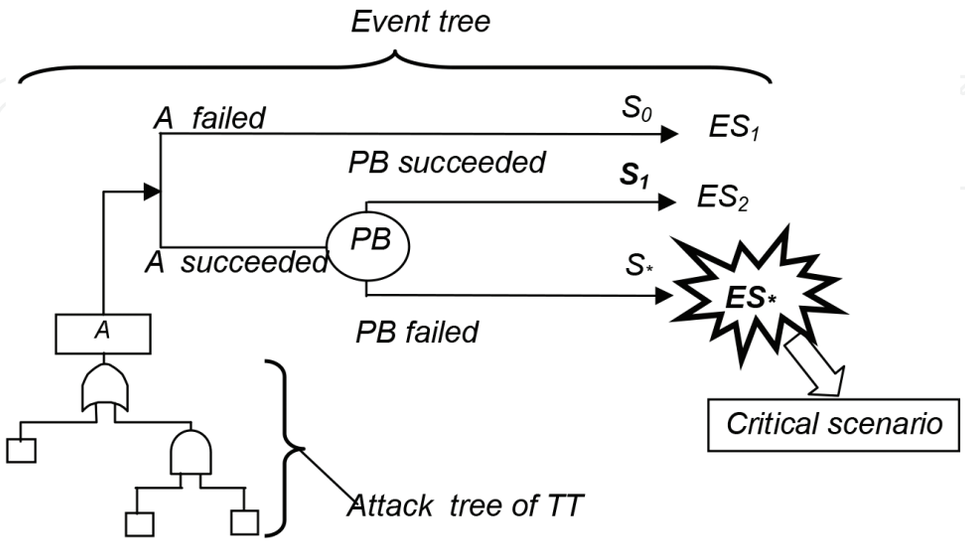

Figure 4. The scenario tree for technological terrorism.

therefore, they have to prepare a powerful action capable of breaking through the *CES* protection barriers [20]. It is necessary for the terrorist to select the method for the attack resulting in the CES end state that would initiate the accident propagation outside the *CES* boundaries.

The selection of the attack scenario is made through a hybrid scenario tree that in case of *TT* could be quite simple. It incorporates several attack trees describing the abilities and resources of terrorists and the event tree describing the *CES* vulnerability (**Figure** 4).

4.2. Scenarios of intelligent (or highly sophisticated, insiders') terrorism

Intelligent terrorism (*IT*) is a deliberate unauthorized interference into the process of designing, building, and/or operating the CES aimed at increasing its existing vulnerabilities and creating new ones in the system so that these input vulnerabilities, insider's knowledge of the system, and access to its elements are used for future realization of most disastrous scenarios of a terrorist attack.

IT implies:

- A comprehensive vulnerability assessment of a system under design, construction, or operation with respect to various scenarios of terrorist impacts and identification of the most effective way of realization of the initiating impact upon the system
- Insertion of latent changes into the system at the stage of its being designed, built, or operated, in order to give rise to new vulnerabilities in the CES
- Disconnection or disruption of the *CES* monitoring and protection systems
- Triggering cascading failures in the system and the environment

As a rule, scenarios *of IT* require that a member of a terrorist group penetrate into the staff of the organization that is designing, building, or operating the *CES*. The terrorist must possess insider's information on the *CES* and be able to perform well-camouflaged actions in order to weaken protection systems and create latent defects undetectable by the existing monitoring systems.

Consequently intelligent terrorism implicates detailed knowledge of the *CES* structure and working principles. It also implies awareness of its existing and potential vulnerabilities, possible end states, possible scenarios of accident propagation, and initial impacts that can trigger them. Additionally, *IT* can anticipate distortion of the success scenario, formulate false targets, and generate new disastrous scenarios.

Attacks of intelligent terrorism can be carried out at any stage of the *CES*'s life cycle:

- At the stage of design, some latent defects can be intentionally introduced into the system.
- At the stage of construction, additional vulnerabilities can be input into the *CES* through intentional violations of the technological processes.
- At the stage of operation, some maintenance procedures that are critical for the *CES*'s safety can be intentionally violated.

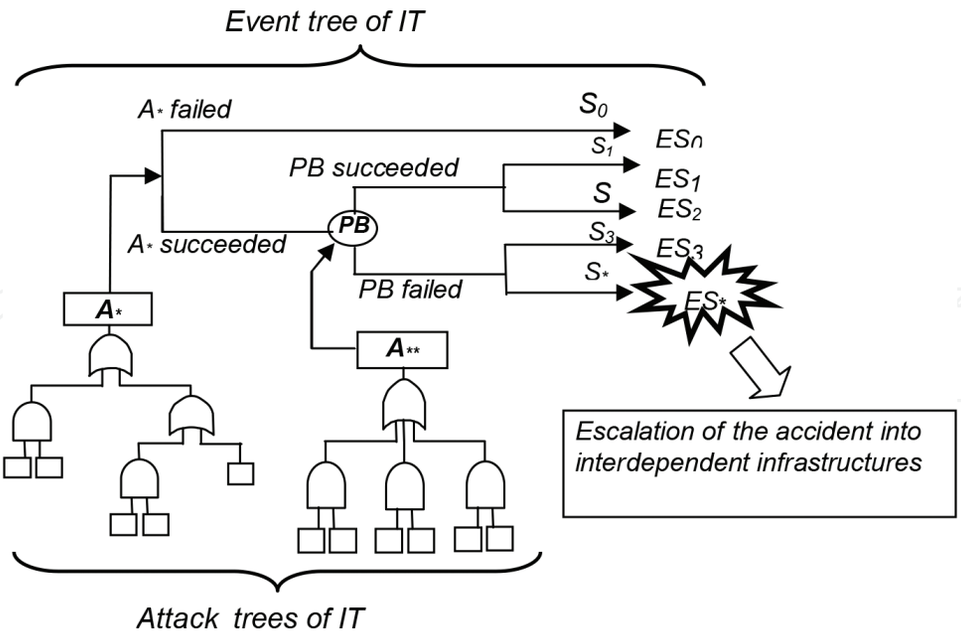

Figure 5. The scenario tree for intelligent terrorism.

Intelligent terrorism implies maximal level of the terrorist competence (comprehensive knowledge of the *CES* and its control, operation, and protection barriers), which enables it to select the most disastrous accident scenarios and find the most effective way of their initiation, disconnection, or disruption of the *CES* monitoring systems in order to prevent prompt response to failures. The assessment of the attack scenarios is made through a hybrid scenario tree that in case of *IT* could be more complicated (**Figure** 5). It incorporates several attack trees describing the abilities and resources of terrorists and the decision tree describing the system's vulnerability.

5. Development of dynamic multi-sided models for analyzing scenarios of terrorist attacks and developing counterterrorist measures

In view of the specific features of terrorist threats addressed in p.3 and the analysis of the scenarios of terrorist attacks on CESs presented in p.4 of this chapter, an integrated (three-sided) terrorist risk model based on the approaches developed in Bayesian networks and game theory has been developed [8, 21–23]. The schematic representation of the model is given in **Figure 6**. Each of the three graphs represents an influence diagram from the perspective of the following players: terrorist group, administration of industrial facility subjected to terrorist threat, and municipal authorities. These three diagrams are separated to keep the decisions made by different parties separate. Oval nodes represent random variables or events with their possible realizations and probabilities assigned. Rectangular nodes represent decisions and are characterized by possible options. The arrows represent probabilistic dependences between the events, state of variables or decision variables.

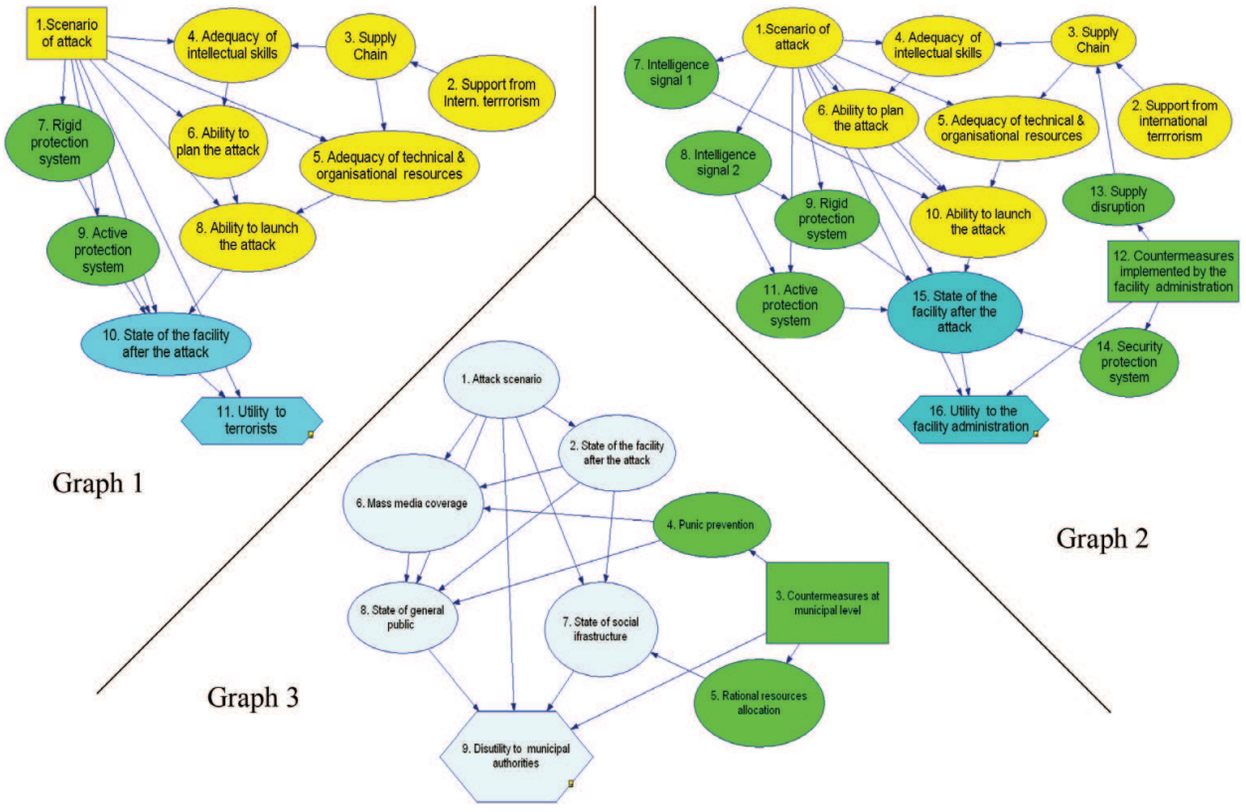

Figure 6. Multi-sided terrorist risk assessment model.

The model is based on the assumption that all the players act in such a way as to minimize their maximum losses. This strategy is governed by so-called minimax criterion: Counterterrorist players don't know which attack scenario the terrorist group will select, that is why they should choose the defense strategy that results in the lowest possible worst-case expected losses.

Graph 1 (**Figure** 7) represents an influence diagram from the perspective of terrorists. It allows one to assess (a) the probabilities that the specified attack scenario will result in damage and (b) the expected utility of terrorist of different attack scenarios[1].

$$EU(s_i) = \sum_{j=0}^{m}\left[Ut(s_i; v_j) \times P\left(V = v_j \mid S = s_i\right)\right] \ (i = 1,\ 2,\ \ldots,\ n), \tag{3}$$

where $Ut_{(s_i; v_j)}$ is an element of utility matrix.

$$\begin{bmatrix} W(s_1; v_0) - Z(s_1) & W(s_1; v_1) - Z(s_1) & \cdots & W(s_1; v_m) - Z(s_1) \\ W(s_2; v_0) - Z(s_2) & W(s_2; v_1) - Z(s_2) & \cdots & W(s_2; v_m) - Z(s_2) \\ \quad \cdots & & & \\ W(s_n; v_0) - Z(s_n) & W(s_n; v_1) - Z(s_n) & \cdots & W(s_n; v_m) - Z(s_n) \end{bmatrix} \tag{4}$$

[1]Figures on the diagram are conditional and are presented for the illustrative purpose.

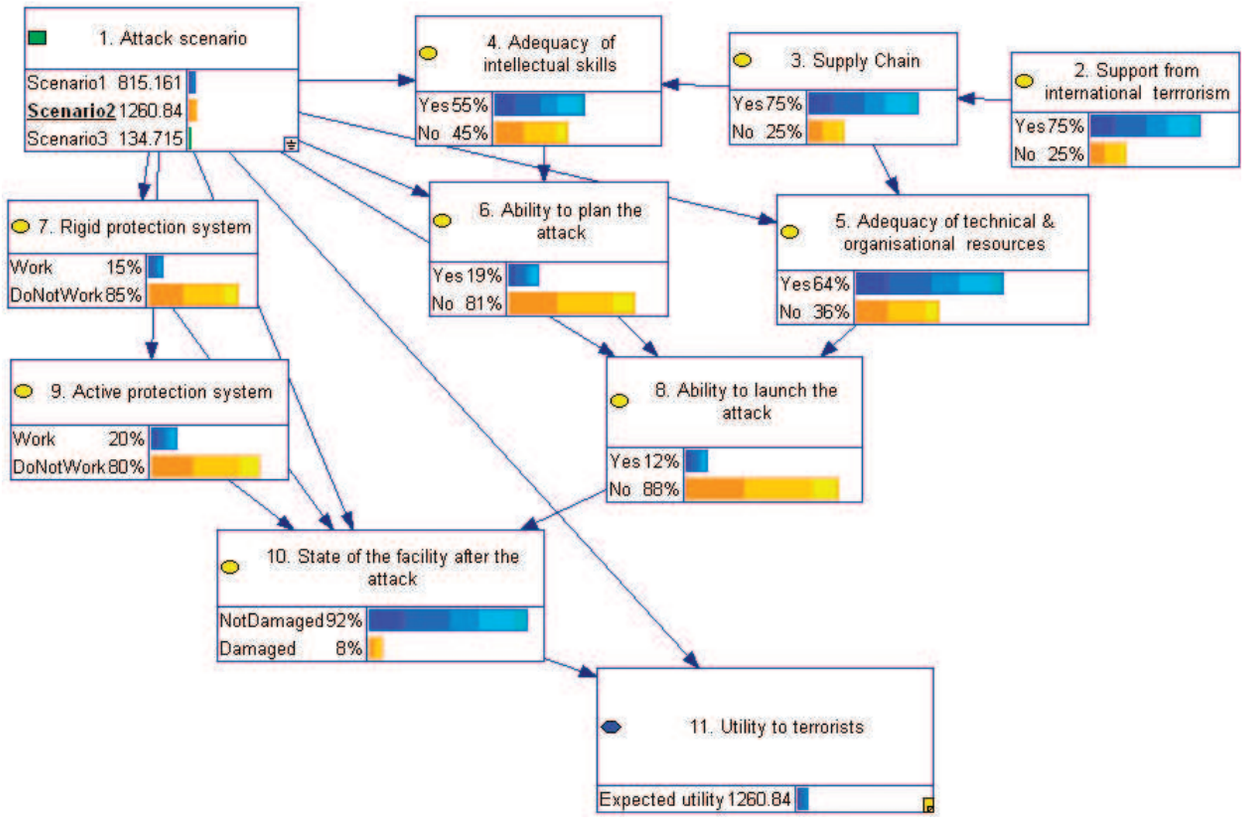

Figure 7. An illustrative example of the influence diagram from the perspective of terrorist group.

s_i is attack scenario; v_j is damage factor of the facility inflicted by the attack ($j = 0, 1, \ldots n$: $j = 0$ corresponds to a not damaged system, while $j = n$ corresponds to completely destroyed system); $P(V = v_j \mid S = s_i)$ is conditional probability of inflicting damage factor j to the facility provided that attack scenario i was carried out; $W_{(s_i; v_j)}$ is the outcome in case of attack scenario i and damage state j; $Z_{(s_i)}$ are the costs of implementing attack scenario i.

Calculation of expected utility values for different attack scenarios allows one to estimate probabilities of these scenarios (Eq. (5)) [8, 11]:

$$P_t(S = s_i) = \frac{EU_t(s_i)}{\sum_{k=1}^{n} EU_t(s_k)} \; (i = 1, 2, \ldots n). \tag{5}$$

Eq. (5) assumes that (a) different attack scenarios are mutually exclusive and (b) the decision taken by terrorists is rational (i.e., they chose attack scenarios that maximize the expected utility). The results obtained in Graph 1 are then used as inputs to Graphs 2 and 3. The results of Graph 2 are then used in Graph 3.

Graph 2 (**Figure 8**) represents an influence diagram from the perspective of administration of industrial facility subjected to terrorist threat. It allows one to assess expected disutilities related to various countermeasures made by the administration of the facility involved. The probabilities $P_t(S = s_i)$ (Eq. (5)) are used in Graph 2 as state probabilities of the chance node 1.

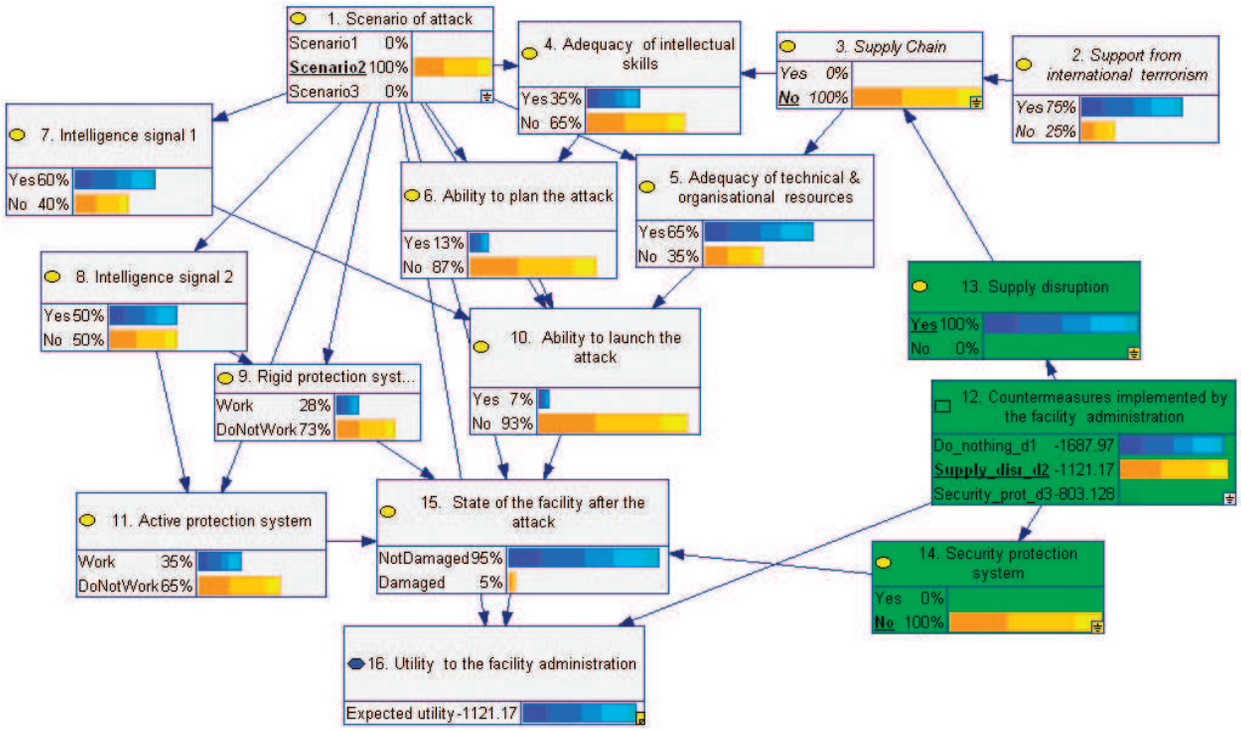

Figure 8. An illustrative example of the influence diagram from the perspective of CES's administration.

The graph permits estimation of expected disutilities to facility administration in case of various countermeasures adopted by the facility administration, to rank countermeasures.

Graph 3 (**Figure 9**) represents an influence diagram from the perspective of local community authorities. Graph 2 and Graph 3 permit assessment of risk reduction benefits of different countermeasures and their costs.

The structure of the influence diagrams and probabilistic dependences between the variables should be developed by the joint efforts of specialists representing a broad spectrum of disciplines (these include specialists in terrorist threat assessment, reliability theory, social sciences, loss estimation), each providing insights in their relevant area of expertise. The model permits identification of effects of different factors and parameter values on the likelihood of success of different attack scenarios and on the expected utilities to different sides involved.

The model described above can be used in dynamic fashion via discrete time steps. At each step, each player updates his beliefs, objectives, and decisions based on his previous step. Each of the players is uncertain about the other's actions and state of knowledge. To address the dynamics of security problem, one needs to model moves and countermoves of all three sides involved, changes in the structure of terrorist organizations and systems of protection, and lessons learned by all parties from previous attacks.

At each consecutive time period, all three parties make decisions regarding their actions in the upcoming time period based on the information accumulated so far (Blocks I_{t_k} and $I_{t_{k+1}}$, **Figure 10**). Estimations of probabilities of various attack scenarios and countermeasures adopted by facility administration and community authorities obtained at time step t_k could be treated as prior

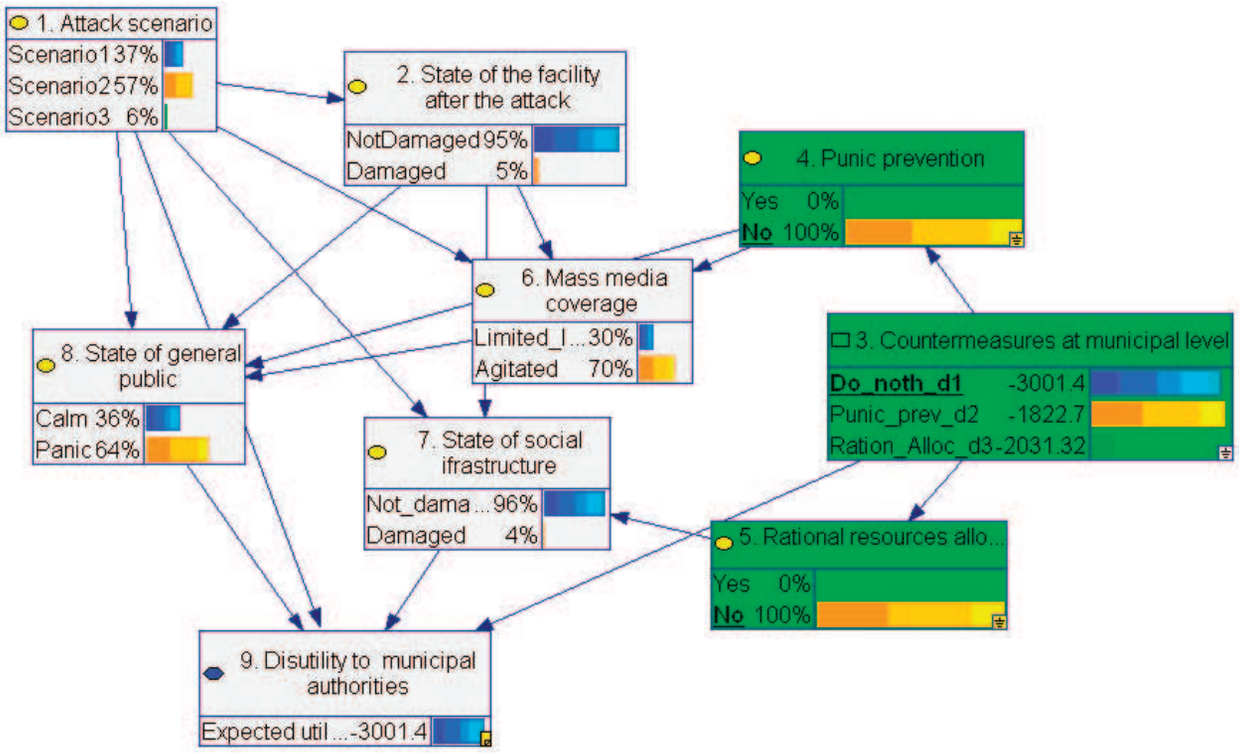

Figure 9. An illustrative example of the influence diagram from the perspective of community authorities.

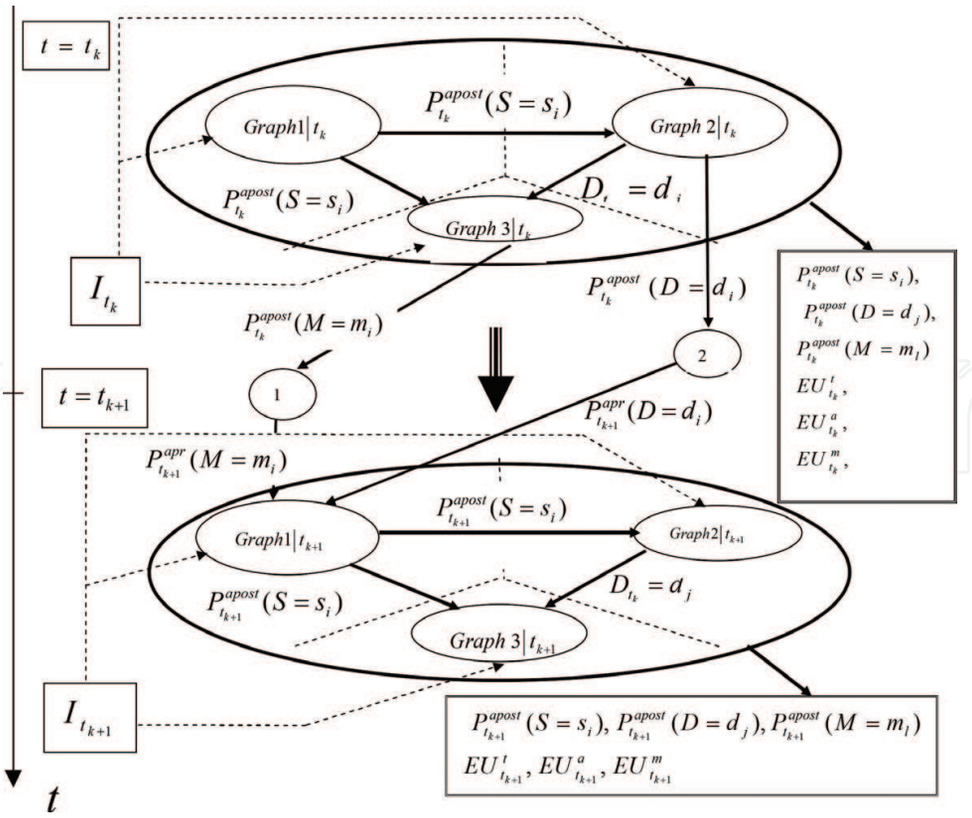

Figure 10. Dynamic multi-sided terrorist assessment model.

http://dx.doi.org/10.5772/intechopen.75099

estimates for the time period t_{k+1}. Terrorist may take into account countermeasures of counterterrorist forces by including the respective chance nodes into Graph 1 at time step t_{k+1} and estimate probabilities of countermeasures adopted by facility administration d_j and municipal authorities m_l using Eq.(6) similar to Eq.(5):

$$P_a(D = d_j) = \frac{EU_a(d_j)}{\sum_{g=1}^{3} EU_a(d_g)}, k = 1, 2, 3; P_m(M = m_l) = \frac{EU_m(m_l)}{\sum_{f=1}^{3} EU_m(m_f)}, l = 1, 2, 3 \quad (6)$$

6. Measures for countering terrorist threats

6.1. Measures aimed at increasing protection of a CES from terrorist threats

The complexity of modern engineering systems and their interdependence with other systems make them vulnerable to attacks of technological and intelligent terrorism. This complexity stems largely from the vast functional and spatial dependencies and nonlinear interactions between the components of CES as well as from interdependencies that exist among the CESs which enable failures to cascade within one system and pass from one system to another.

Different historical, economic, political, social, as well as cultural traditions have formed different approaches to ensuring safety of complex engineering systems. Contemporary CESs, i.e., power, transport, and telecommunication networks, are becoming transboundary. Their significant spatial extension makes their functioning dependent on many factors and events in different parts of the world. The ensuring of CES's security is a complex interdisciplinary problem. It is impossible to solve this problem without joining efforts of experts in different fields and taking into account technical, social, psychological, and cultural-historical aspects.

Analysis of major disasters at CES in different countries shows that high-risk engineering systems in many cases are being designed and constructed according to traditional design codes and norms that are based on common and quite simple linear "sequential" risk assessment models and employ traditional design, diagnostics, and protection methods and procedures. This is being done in the assumption that a bounded set of credible design-basis impacts and subsequent failure scenarios could be determined for the CES, thus allowing one to create a system of protection barriers and safeguards that could secure the CES from the identified impacts with required substantially and high probability. This bounded set of impacts referred to as design-basis impacts includes normal operation events as well as abnormal events (component failures, human errors, extreme environmental loads, attacks of technological terrorism on CES) that are expected to occur or might occur at least once during the lifetime of the CES.

The currently available approach to ensuring security of complex engineering systems is based on the so-called protection approach that provides for the development of a set of protection barriers against the list of terrorist attack scenarios that were identified in advance. Within this approach, attacks of technological terrorism should be included into the list of

design-basis events. To protect CESs from these scenarios of terrorist attacks, the following types of protection barriers should be developed (see **Figure 11**):

- Rigid protection barrier (protection barrier that requires a powerful impact to be broken)
- Functional protection barrier (protection barrier that in case of an accident could take on certain system's functions for a limited time or could prevent an accident from progressing further)
- Natural protection barrier (involves the use of passive natural phenomena and processes aimed at limiting the scales of the accident)
- Security guards

Circles "1," "2," and "3" stand for separate types of protection barriers. Areas of intersection ('1-2," "2-3," "1-3," and "1-2-3") – correspond to combination of correspondent types of protection barriers. Security guard barrier "4" is organized to ensure protection of all of the above mentioned barriers ("1," "2," "3," "1-2," "2-3," "1-3," and "1-2-3").

Application of this protection approach allows one to reduce risks of design-basis scenarios of technological terrorism (compare FN curves 1 and 2; **Figure 12**). However, it should be noted that this protection-based approach does not allow one to reduce risk of unforeseen "low-probability-high-consequence" scenarios of intelligent terrorism that could not be included into the list of design-basis events.

In currently applied protection-based approach, a number of low-probability impacts of extreme intensity are neglected as being practically incredible. Other impacts (such as attacks of intelligent terrorism) are not identified and, consequently, not analyzed. Such impacts are classified as beyond design-basis impacts. Thus, the issue of protection of CES from beyond design-basis impacts has not been addressed in a proper manner. These impacts however can cause large-scale disasters of extreme severity and induce tremendous property losses and a great number of victims.

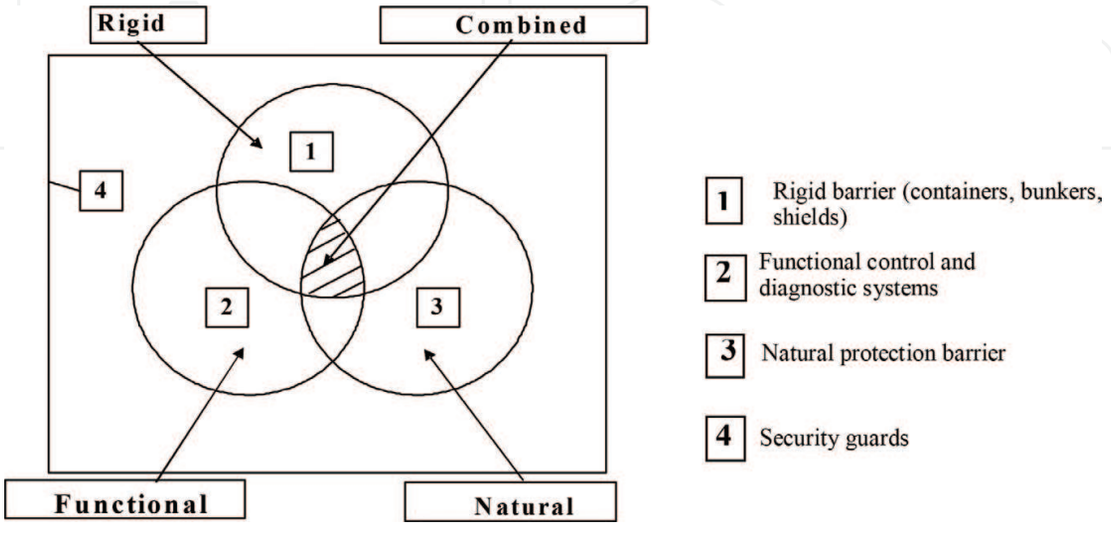

Figure 11. Types of protection barriers.

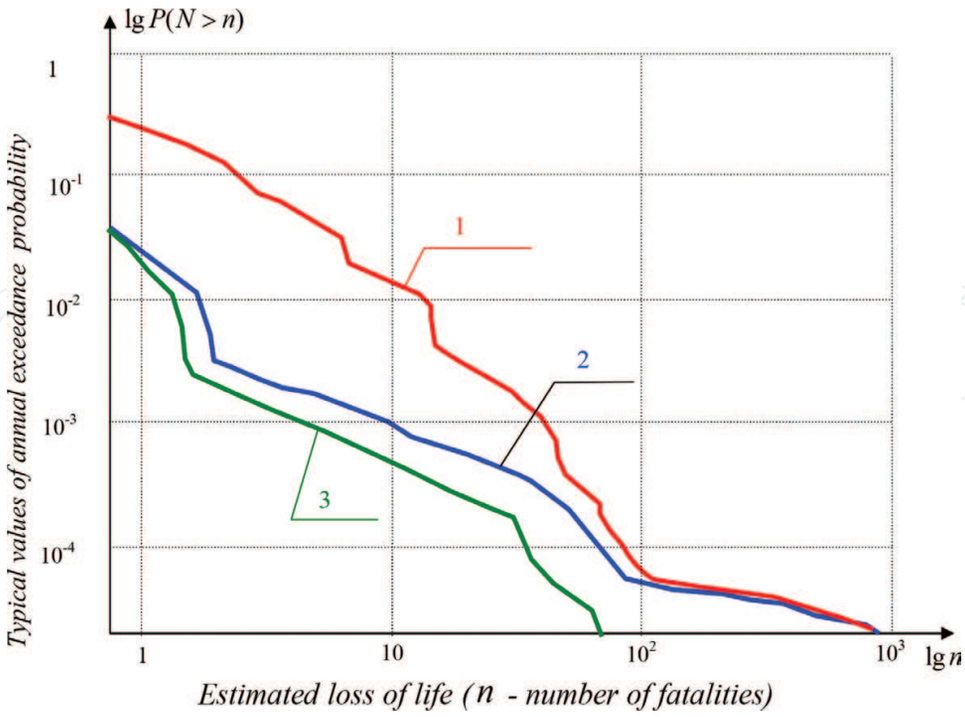

Figure 12. FN curves before and after realization of protection and resilience measures. (1) FN, curve before realization of any measure; (2) FN, curve after realization of protection measures; (3) FN, curve after realization of protection and resilience measures.

6.2. Measures focused on ensuring CES's resilience to beyond design-basis events

Complex engineering systems are becoming global networks. The currently available methodologies of risk assessment and reliability engineering were developed for technological systems with fixed boundaries and well-specified hazards for which exists statistical and/or actuarial data on accident initiation events, component failure rates, and accidents' consequences which allow one to quantify and verify models taking into account uncertainties deriving from both natural variations of the system parameters (and performance conditions) and from lack of knowledge of the system itself.

The protection-based approach is focused on developing safety barriers for countering the identified scenarios of terrorist attacks that were included in the list of design-basis events. This approach however has the weakness of neglecting the possibility of beyond design-basis events. To overcome this weakness, a new comprehensive strategy is needed. This strategy should not only include measures aimed at development protection barriers against design-basis attacks of technological terrorism but also development of special measures aimed at increasing the system's resilience to future yet-to-be-determined scenarios of attacks of intelligent terrorism (**Figure 13**) [24, 25].

The current accident models and risk assessment techniques such as fault and event tree analysis are not adequate to account for the complexity of modern engineering systems. Due to rapid technological and societal developments of the recent decades, modern engineering systems are becoming steadily more complex. It means that (a) in safety assessments for CES, there are too many details to be considered, and (b) some modes of CES's operation may

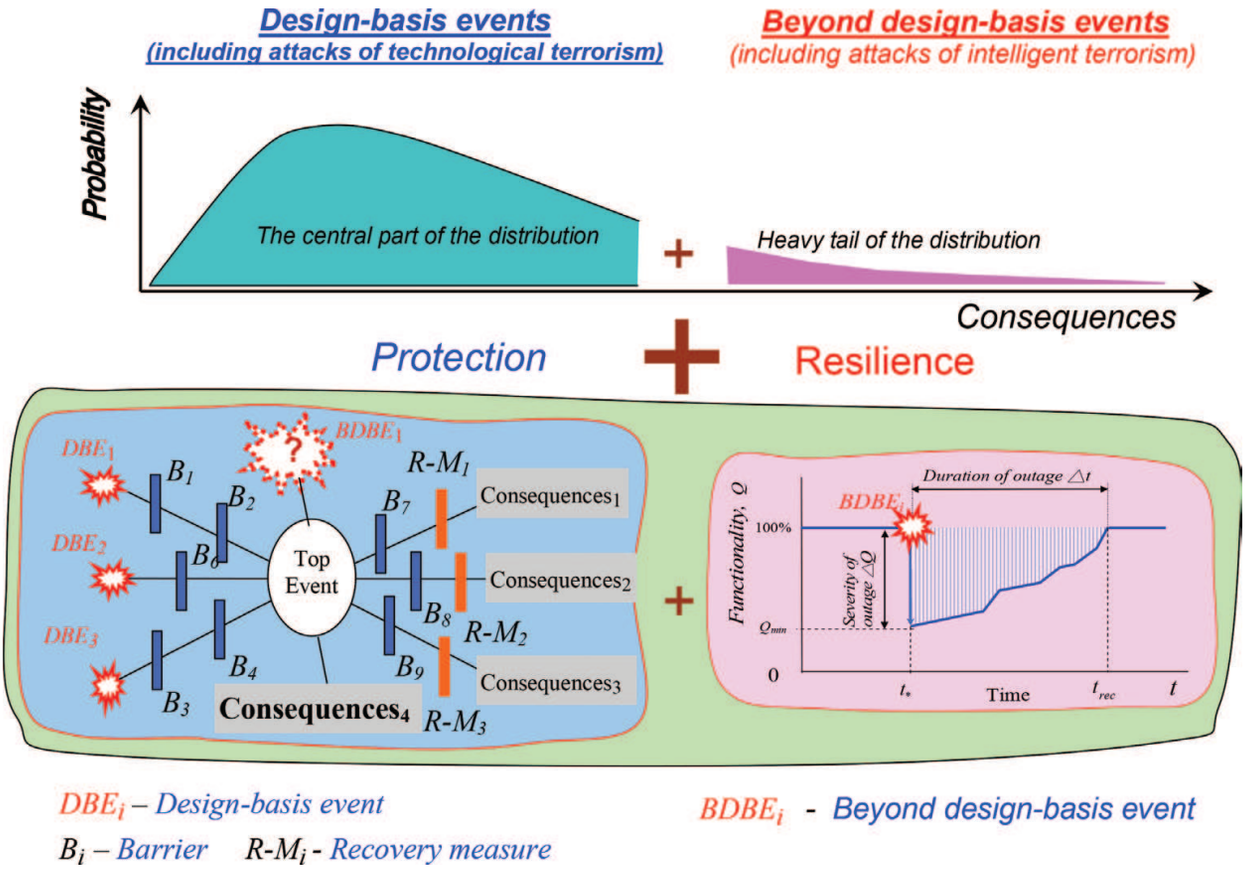

Figure 13. A new comprehensive approach to ensuring CES's security based on implementation of protection measures and measures for improving resilience of CES.

be incompletely known due to complex nonlinear interactions between components of CES, due to tight couplings among different systems, and because CES and its environment may change faster than they can be described. As a result, it is impossible to describe the performance of CESs in every detail. In other words for complex engineering systems, it is practically impossible to define a bounded set of design-basis impacts that are expected to occur or might occur at least once during the lifetime of the CES.

This problem can be solved by including the concept of resilience in the processes of designing and ensuring the safety and security of CESs [26, 27]. The proposed approach should not be considered as a substitute but rather a supplement to the traditional one. Adopting this view creates a need to move beyond traditional "threat-vulnerability-consequence" models that are limited to analyzing design-basis events and deal with beyond design-basis impacts and impact combinations. This comprehensive approach will be based on such concepts as resilience to provide more adequate explanations of accidents as well as identify ways to reduce risks caused by beyond design-basis impacts.

In other words, the new security paradigm for complex engineering systems should focus the efforts not only on development of protection barriers and safeguards against design-basis accidents but also on increasing the CES's resilience toward beyond design-basis impacts (**Figure 13**).

The CES's resilience is the capacity of the system potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning. This is determined by the degree to which the CES is capable of organizing itself to increase its capacity, of learning from past disasters for better future protection, and to improve risk reduction measures.

Figure 14 presents the so-called resilience profile of the system: a powerful beyond design-basis event (BDBE) occurs at the time moment t_* resulting in a slump of the system's performance characteristics Q which recovers at the time moment t_{rec}. A ratio of the square F_e of the figure BDEF that is located under the chart of the CES's performance characteristics in the period between the time moment t_*, when the beyond design-basis event occurs, and the moment t_{rec} when the system returns to its normal operation level and the square F_n of the rectangular ADEF can be considered as a quantitative measure of the system's resilience [26, 28]:

$$Res = \frac{F_e}{F_n} = \frac{\int_{t_*}^{t_r} Q(t)dt}{(t_{rec} - t_*) \cdot Q_n} \times 100\% \tag{7}$$

Two groups of measures aimed at increasing the CES resilience can be identified:

- Measures focused on reducing the severity of outage ΔQ (**Figure 15a**)
- Measures focused on the reducing the duration of the outage Δt (**Figure 15b**)

As previously stated, due to the complexity of modern engineering systems and their potentially large-scale catastrophes, in order to ensure security of such systems, one needs to move beyond traditional design-basis risk management framework. The new paradigm needs to be focused on increasing CES's resilience (**Figure 13**). That means that if the beyond design-basis accidents are to be considered, the scope of the analysis should be widened. Security-related efforts should be focused not only on the development of protection barriers and safeguards from predetermined (postulated) set of design-basis attacks of technological terrorism but

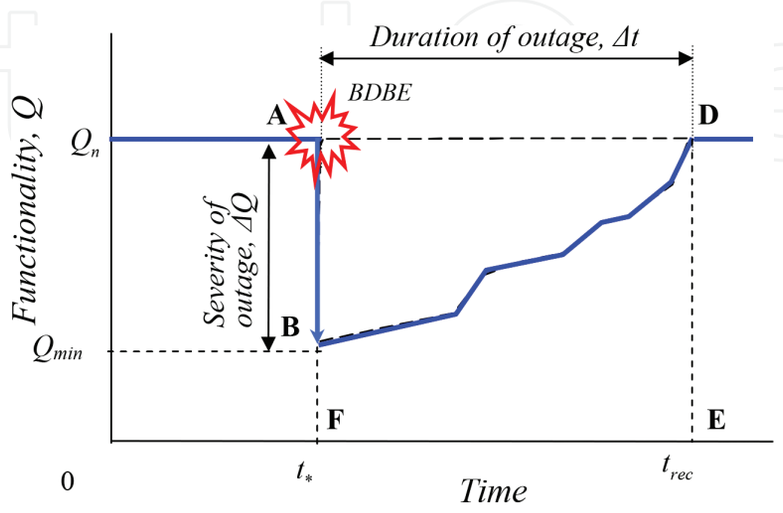

Figure 14. Resilience profile of CES.

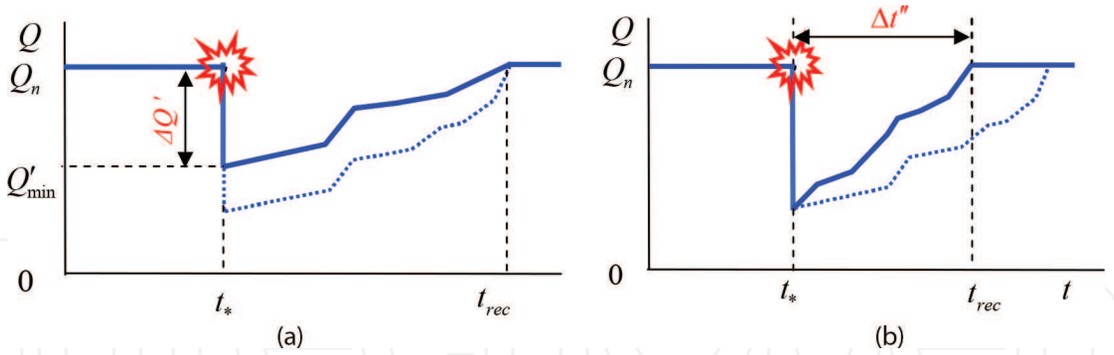

Figure 15. Measures to increase CES resilience. (a) Reduction of the outage severity. (b) Reduction of the outage duration.

also on additional set of measures aimed at increasing complex engineering system resilience that would prevent catastrophic failure and long-term dysfunctioning of CESs in case of beyond design-basis attacks. Application of such comprehensive (protection and resilience focused) approach allows one to reduce risks of beyond design-basis scenarios of intelligent terrorism (compare FN curves 2 and 3; **Figure 12**).

Acknowledgements

This work was financially supported by the Russian Foundation for Basic Research (grant no. 16-29-09575).

Author details

Dmitry O. Reznikov*, Nikolay A. Makhutov and Rasim S. Akhmetkhanov

*Address all correspondence to: mibsts@mail.ru

Mechanical Engineering Research Institute, Moscow, Russia

References

[1] Schweitzer G, Sharber C, editors. Countering Urban Terrorism in Russia and the United States: U.S.-Russian Workshop Proceedings. Washington: The National Academies Press; 2006. p. 241

[2] Schweitzer G, editor. Countering Terrorism: Biological Agents, Transportation Networks, and Energy Systems: Summary of U.S.-Russian Workshop. Washington: The National Academies Press; 2009. p. 239

[3] Terrorism: Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings. Washington: The Academies Press; 2004. p. 239

[4] Frolov K, Baecher G, editors. Protection of Civilian Infrastructure from Acts of Terrorism. Dordrecht: Springer; 2006. p. 244

[5] Makhutov N, Baecher G, editors. Comparative Analysis of Technological and Intelligent Terrorism Impacts on Complex Technical Systems. Amsterdam: IOS Press BV; 2012. p. 194

[6] Kaplan S. Applying the general theory of quantitative risk assessment (QRAC) to terrorism risk. In: Haimes Y, Moser D, editors. Risk-Based Decision-Making in Water Resources X: Proceedings of the Conference. Reston: ASCE Publications; 2002. pp. 77-81

[7] Garrick B, Hall J, et al. Confronting the risk of terrorism: Making the right decisions. Reliability Engineering and Safety Systems. 2004;**86**:129-1768

[8] Pate-Cornell E. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among counter-measures. Military Operations Research. 2002;**7**:5-23

[9] Berman A, Nikolaychuk O, Yurin A. Intellectual data system for analyzing failures. Journal of Machinery Manufacture and Reliability. 2012;**41**(4):337-343

[10] Makhutov N, Reznikov D. Assessment and regulation of risks related to operation of complex technical systems. Problems of Safety in Emergency Situations. 2012;**5**:3-9 (in Russian)

[11] Makhutov N, Reznikov D, Zatsarinny V. Two types of failure scenarios in complex technical systems. Problems of Safety in Emergency Situations. 2014;**2**:28-41 (in Russian)

[12] Frolov K, Makhutov N, editors. Multi-Volume Addition Safety of Russia. Legal, Social, Economic, Scientific and Engineering Aspects. Znanie publ. Vol. 1-54; 1997-2018 (in Russian)

[13] Akhmetkhanov R. Stability of social system under terrorist impacts. In: Makhutov N, Baecher G, editors. Comparative Analysis of Technological and Intelligent Terrorism Impacts on Complex Technical Systems. Amsterdam: IOS Press; 2012. pp. 157-166

[14] Akhmetkhanov R. Risk management in natural and societal systems: Taking into account terrorist threats. In: Frolov K, Baecher G, editors. Protection of Civilian Infrastructure from Acts of Terrorism. Dordrecht: Springer; 2006. pp. 7-20

[15] Makhutov N, Akhmetkhanov R, Dubinin E, Kuksova V. Problems of rationing of terrorist risks to critical facilities, taking into account the risks increase of regular functioning. Problems of Safety in Emergency Situations. 2017;**2**:30-44 (in Russian)

[16] Makhutov N, Reznikov D. Characteristics of technological terrorism scenarios and impact factors. In: Countering Terrorism: Biological Agents, Transportation Networks, and Energy Systems: Summary of a U.S.–Russian Workshop. Washington: The National Academy of Sciences Press. 2009. pp. 53-70

[17] Reznikov D. Technological and intelligent terrorism: Specific features and assessment approaches. In: Makhutov N, Baecher G, editors. Comparative Analysis of Technological and Intelligent Terrorism Impacts on Complex Technical Systems. Amsterdam: IOS Press; 2012. pp. 45-60

[18] Makhutov N, Reznikov D, Petrov V. Engineering infrastructures: Problems of safety and security. In: European Perspective on Security Research and Safety Aspects. Berlin/ Heidelberg: Springer; 2010. pp. 93-106

[19] Makhutov N, Reznikov D, Khaziakhmetov R. Basic scenarios of terrorist attacks at hydropower engineering facilities. In: Escuder-Bueno et al., editors. Risk Analysis, Dam Safety, Dam Security and Critical Infrastructure Management. London: Taylor & Francis Group; 2012. pp. 389-394

[20] Makhutov N, Reznikov D, Dubinin E, Kuksova V. Assessment of terrorist risk and making decision regarding the expedience of creation of protection systems against terrorist impacts. Problems of Safety in Emergency Situations. 2007;**1**:88-105 (in Russian)

[21] Woo G. Quantitative terrorism risk assessment. The Journal of Risk Finance. 2003;**4**(1): 15-24

[22] Makhutov N, Reznikov D. Application of Bayesian networks for assessment of terrorist risk and identification of optimal counterterrorist strategy. Problems of Safety in Emergency Situations. 2007;**1**:89-104 (in Russian)

[23] Makhutov N, Akimov V, Akhmetkhanov R, et al. Safety of Russia: Human Factor in Problems of Safety. Moscow: Znanie Publishing; 2008. p. 687 (in Russian)

[24] Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience. Critical infrastructure protection program. Discussion Paper Series. George Masson University [Internet]. 2007. p. 109. Available from: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=C359CF09E0E785A43C91C0A1871A9B4E?doi=10.1.1.169.9384&rep=rep1&type=pdf [Accessed: January 04, 2018]

[25] Makhutov N, Reznikov D, Petrov V. Specific futures of ensuring critical infrastructures safety. Safety in Technosphere. 2014;**3**(1):3-14

[26] Hollnagel E, Woods D, Leveson N, editors. Resilience Engineering: Concepts and Precepts. Farnham: Ashgate; 2007. p. 410

[27] Hollnagel E, Paries J, Woods D, Wreathall J, editors. Resilience Engineering in Practice: A Guidebook. Farnham: Ashgate; 2011. p. 362

[28] Cimellaro G, Reinhorn A, Bruneau M. Quantification of seismic resilience. In: Proceedings of the 8-th U.S. National Conference on Earthquake Engineering, USA [Internet]. 2006. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.538.8029&rep=rep1&type=pdf. [Accessed: January 04, 2018]