Assessment of large-scale catastrophes in complex engineering systems

N A Makhutov 1, D O Reznikov 2

1 Mechanical Engineering Research Institute of the Russian Academy of Sciences. 4 Maly Kharitonievsky lane, Moscow, 101990 Russia
2 Mechanical Engineering Research Institute of the Russian Academy of Sciences. 4 Maly Kharitonievsky lane, Moscow, 101990 Russia

E-mail: mibsts@mail.ru

Abstract. The paper considers a traditional approach to ensuring safety of complex technical system that is based on development of protection barriers against the bounding set of credible (design-basis) impacts and presents a modern approach. The approach is based on combined efforts to improve the system protection from design basis impacts and to increases the system resilience towards beyond design basis events allowing one to include low probability – high consequences (beyond design-basis) events into the scope of risk assessment and management framework.

1. Introduction

Modern society cannot exist without stable and reliable operation of complex engineering systems (CES) whose functioning is vital for any national economy and constitute the back-bone of modern industry and society. Such systems include electric power transmission and distribution; rail and road transportation systems; oil, gas, and water processing, storage and delivery; telecommunication and information networks. Their performance is commensurate with storing, processing and transmission of huge amounts of hazardous substances, energy and information. The unauthorized release of these substances, energy and information may cause disastrous consequences and trigger cascading failures in interrelated infrastructures.

An extensive bank of knowledge has been created by scientists of different countries for analysis and classification of natural and man-made emergencies, and in-depth study of the processes of their initiation and propagation in order to reduce vulnerability of CES in case of natural or manmade catastrophes. Currently available methodologies of risk assessment and CES design codes have however been developed without accounting for risks of beyond design-basis accidents. It means that these methodologies and codes should be revised to include into consideration risks of beyond design-basis impacts on complex engineering systems.

2. Fundamentals of safety analysis for complex systems

Complex engineering systems are referred to the group of high risk facilities. The failure to provide for basic characteristics of strength, reliability, resilience and robustness with regard to a range of criteria leads to the possibility of accidents and catastrophic situations arising and developing at all stages of the life cycle of high risk facilities. Over the past decade, institutes of the Russian Academy
of Sciences, the Russian Ministry of Emergency Situations, the Russian Ministry of Education and Science, have synthesized a substantial volume of fundamental information on accidents and catastrophes of an industrial and natural character as part of the State Scientific-Technical Program for Safety for Population and Economic Facilities Considering the Risk of Natural and Manmade Disasters ("SSTP Safety"). These efforts were continued in the frame of the Federal Research Program Reduction of Risks and Mitigation of Consequences of Natural and Manmade Emergencies in the Russian Federation. In carrying out these programs, participants analyzed and generalized information on the basic characteristics, conditions, and scenarios of accidents and catastrophes in the natural and industrial spheres engendered by complex dangerous phenomena and processes in various regions of the world. Hazardous components of high risk facilities (atomic power stations, petroleum chemical plants, hydropower engineering facilities, etc.) might create catastrophes in the following classes (from 7 to 1): planetary, global, national, regional, local, facility-level, and localized (Figure 1). The potential losses and periodicity of occurrence were evaluated depending on the class of accidents and catastrophes (beginning from the global and ending with the localized) [1].

Legislation and regulatory framework in the Russian Federation uses six classes of catastrophes (from 6 to 1): global, international, national, regional, local, facility-level.

![Figure 1. Losses and periodicity of natural and manmade catastrophes](image)

Based on the results of this summary analysis, a classification of catastrophes was constructed, taking into account the losses $U$ and the periodicity $\frac{1}{T}$ of their occurrence (see Table 1). Here losses $U$ for each catastrophe decreases from $10^{10}$ to $10^{11}$ to $10^3$ to $10^4$ dollars, while the periodicity of their occurrence declines from $(3\div 5)\cdot 10^1$ to $10^{-1}$ years. Thus, the variation in losses (dollars per catastrophe) for various types of disasters could reach seven orders of magnitude, while that of the probability of occurrence $P = \frac{1}{\bar{T}}$ (1/year) could reach three orders of magnitude.

The concept of risk is the key one in resolving problems related to ensuring safety. Risk is defined by means of the functional $F_R$: 

$$R = F_R\{P, U\} = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} P_i \cdot U_i = \int U(P) \, dP = \int P(U) \, dU$$  \hspace{1cm} (1)
where \( R \) represents the risk associated with a natural or manmade catastrophe, \( P \) is its probability, and \( U \) is loss.

### Table 1. Risks of accidents and catastrophes

| No. | Class of accidents and catastrophes | \( P \) (1/year) | \( U \) (dollars) | \( R \) (dollars/year) |
|-----|-----------------------------------|-----------------|----------------|----------------------|
| 1   | Object                            | \( 5.0 \cdot 10^0 \) | \( 5.0 \cdot 10^3 \) | \( 2.5 \cdot 10^4 \) |
| 2   | Facility-level                    | \( 1.2 \cdot 10^0 \) | \( 4.0 \cdot 10^5 \) | \( 4.8 \cdot 10^5 \) |
| 3   | Local                             | \( 5.0 \cdot 10^1 \) | \( 7.0 \cdot 10^6 \) | \( 3.5 \cdot 10^6 \) |
| 4   | Regional                          | \( 1.6 \cdot 10^1 \) | \( 1.0 \cdot 10^8 \) | \( 1.6 \cdot 10^7 \) |
| 5   | National                          | \( 1.2 \cdot 10^1 \) | \( 1.5 \cdot 10^9 \) | \( 1.8 \cdot 10^8 \) |
| 6   | Global                            | \( 8.0 \cdot 10^{-2} \) | \( 1.0 \cdot 10^{10} \) | \( 8.0 \cdot 10^8 \) |

Here risks vary within the bounds of four orders of magnitude. For Russia, the probability of the occurrence of national and regional natural-manmade emergencies differ by 1.4 times and are approximately on the order of magnitude lower than the risk for local situations; the likelihood of local and facility-level accidents differ by 5 times.

The assessment of the probability \( P \), losses \( U \), and risks \( R \) of accidents and catastrophes involves a group of risk assessment methods, including various methods for analyzing statistical information on natural and manmade catastrophes of a particular type in the region being studied, as well as methods for analyzing the reliability of equipment and technological processes and the effectiveness of management and control. Methods for calculating the magnitude of loss substantially differ for various technical facilities and natural systems. Therefore, specialists in Russia and other countries have developed a group of special methods aimed at analyzing natural-manmade processes capable of leading to accidents and catastrophic situations at engineering infrastructures.

These methods are based on special graph models called scenario trees. The system is designed to fulfill a 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 \( S_j \) (Figure 2) presents a deviation from the success scenario \( S_0 \) that corresponds to the successful functioning of the CES, the scenario \( S_j \) must have a disturbance point at which an extreme event (loading regime) \( A_i \) \((i = 1, 2, \ldots, m)\), occurs (Fig. 2). Each attack gives rise to a branch of a scenario tree that has a corresponding scenario \( S_j (j = 1, 2, \ldots, n) \) that ends with an end state \( ES_j \) [2, 3].

In this case one can get a risk index using the following matrix expression:

\[
R = \left[ \frac{P(A_i)}{T} \right] \times \left[ \begin{array}{cccc}
P[ES_1 | A_1] & P[ES_2 | A_1] & \cdots & P[ES_m | A_1] \\
\vdots & \vdots & \ddots & \vdots \\
\end{array} \right] \times \left[ \begin{array}{c}
U_{ES_1} \\
U_{ES_2} \\
\vdots \\
U_{ES_m} \\
\end{array} \right]
\]

(2)
3. **New approach to ensuring safety of complex systems: moving from “Protection” to “Protection + Resilience”**

The complexity of modern engineering systems and their interdependence with other systems makes them vulnerable to emergency situations triggered by natural and manmade catastrophes or terrorist attacks. These complexities largely stem 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 from a system to other systems.

Different historical, economical, political, social as well as cultural traditions have formed different approaches to ensuring safety of CES. 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 complex engineering systems’ safety 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 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 bounding 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 high probability. This bounding set of impacts referred to as design-basis impacts includes both normal and abnormal operation events (components failures, human errors, extreme environmental loads, intentional unauthorized impacts on CES) that are expected to occur or might occur at least once during the lifetime of the CES.

In this approach a number of low probability impacts of extreme intensity are neglected as being practically incredible. Other impacts or impact combinations are not identified and, consequently, not analyzed. Such impacts and impact combinations of different types 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. Such disasters are referred to as beyond design-bases accidents.

A typical example of a beyond design-basis accident is the recent accident at the Fukushima NPP where the height of the Tsunami wave exceeded the designed level. Another example is the Chernobil catastrophe that was caused by a combination of technical failures, operator’s errors and organizational violations.

It should be noted that the efforts on protection of CESs have been traditionally focused on technical issues. All this allows one to substantially increase reliability of the technical components of CESs. This approach however is close to its exhaustion. This is due to the fact that CESs are no longer predominantly technical but socio-technical systems. The performance of CES is becoming more and more dependable on human and organizations factors. The statistics of accidents at CES reads that from 70 to 90% of accidents at complex engineering systems are caused by human errors made at the stage of design, construction, maintenance and operation of complex engineering systems. It means that these accidents can not be prevented by technical measures only. Some of the emergencies are typical and predictable but others are not. The latter are classified as beyond design-basis events. Some of human errors should also be classified as beyond design-basis impacts on CES.

The traditional approach to modeling socio-technical systems implies decomposition the system into technical, human and organizational subsystems (levels) that are then studied within different disciplines. The interdependencies between subsystems and their influences on the system’s safety are not considered properly.

It should be noted that design, construction and operation of complex engineering systems are being done in competitive environment. There is always a temptation to increase effectiveness by means of reducing investments in safety related activity. In order to justify such reduction organizations operating CESs may intentionally underestimate safety and security risks. The easiest way to do it is to unfoundly reduce the set of design-basis impacts and design-basis accidents or in other words to extend the list of beyond design-basis impacts in order not to consider them. The question “How to assess risks resulted from beyond design-basis events?” requires a special detailed investigation.

Currently available methodologies of risk assessment and CESs design codes have been developed without accounting for risks of beyond design-basis accidents. It means that these methodologies and codes should be revised to include into consideration risks of beyond design-basis impacts on complex engineering systems.

Complex engineering systems are becoming global networks. Protection of complex engineering systems requires pulling the efforts of specialist from different countries. Traditional risk assessment methodologies were developed for complicated technological systems with fixed boundaries, well-specified targets of hazards and for systems for which exists historical and/or actuarial data on accidents initiation events, components failure rates and accidents’ consequences which allow one to quantify and verify models taking into account uncertainties deriving from both natural variations of the systems parameters (and performance conditions) as well as from lack of knowledge about the system itself.

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. The performance of complex engineering systems (as socio-technical systems) depends on the interaction between technical, human and organizational factors. Due to rapid technological and societal developments of the recent decades complex engineering systems are becoming steadily more complex. It means that (1) in safety assessments for CES there are too many details to be considered and (2) some modes of CES’s operation may be incompletely known due to complex nonlinear interactions between components of CES, tight couplings among different systems and because CES and its environment may change faster than they can be described. As a result complex engineering systems are becoming underspecified and therefore intractable [7]. Thus for CES it is not possible to describe its performance in every detail, and their performance must therefore be flexible and adaptive rather than rigid. The
distinction between tractable and intractable systems is very important in development safety management systems for CESs. Intractable systems cannot be completely described or specified. In other words for complex engineering systems it is practically impossible to define a bounding set of design-basis impacts that are expected to occur or might occur at least once during the lifetime of the CES.

Most current safety methods however have been developed on the assumption that systems are tractable. As this assumption is not valid for CESs, there is a need to develop methods to deal with intractable systems. This could be done based on Resilience and Robustness Engineering. The proposed approach should not be considered as a substitute 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 new approach will be based on such concepts as robustness and resilience to provide more comprehensive explanations of accidents as well as identify ways to reduce risks caused by beyond design-basis impacts. In other words the new safety paradigm for complex engineering systems and other complex socio technical 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 robustness and resilience towards beyond design-basis impacts.

Traditionally, accidents at CES have been viewed as resulting from a chain of failure events, each related to its “causal” event or events. It means that currently available risk assessment techniques are based on this linear notion of causality, which have severe limitations in the modeling and analysis of modern complex socio-technical systems that include nonlinear interactions between components, feedback loops, multiple source of failure, etc. Thus traditional accident modeling approaches are not adequate to analyze accidents that occur in complex engineering systems where accidents do not occur due to a single technical failure or human error; rather they arise from the interconnection of several causal factors originating at many levels in a system: hardware failures, human errors (mistakes and/or procedural violations committed by CES operators), latent conditions (arising from such aspects as management decision practices, or cultural influences), local triggering events (such as extreme weather conditions).

Thus, the study of complex engineering systems (being socio-technical systems) requires an understanding of the interactions and interrelationships between the technical, human, social and organizational aspects of systems. These interactions and interrelationships are complex and non-linear, and traditional modeling approaches cannot fully analyze the behaviors and failure modes of such systems. Thus each complex engineering systems should be treated as an integrated whole, and the emphasis will be made on the simultaneous consideration of technical and social aspects of systems, including engineering design and maintenance strategies of CESs as well as social structures and cultures, social interaction processes, and individual factors such as capability and motivation of operators. Interdisciplinary research should be applied to capture the complexity of complex engineering systems from a broad systemic view for understanding the multi-dimensional aspects of safety and modeling accidents in socio-technical systems.

As previously stated due to the complexity of complex engineering systems and their potential to large-scale catastrophes in order to ensure safety of such systems one needs to move beyond traditional design-basis risk assessment framework. Here a new paradigm is needed that is focused on increasing CES’s robustness and resilience (Figure.3). That means that if the beyond design-basis accidents are to be considered the scope of the analysis should be widened. Safety related efforts should be focused not only on development of protection barriers and safeguards from predetermined (postulated) set of maximal credible accidents but also on increasing complex engineering system robustness and resilience that would prevent catastrophic failure and long-term disfunctioning of CESs in case of beyond design-basis accident.
Figure 3. A new paradigm of CES safety: transition from “Protection” to “Protection + Resilience”

Quantitative measures of robustness (based on energy absorption, the ratio between direct and indirect risks and others) and resilience (based on shape of the CES’s recovery curve) should be developed as well as a set of measures to increase CES’s robustness and resilience will be identified.

4. Conclusion

Complex engineering systems should be considered as techno-social systems whose performance depends on tightly coupled technical, human and organizational functions. A new approach to ensuring CES’s safety will be developed to address the new safety concerns that arise from the use of increasingly complex socio-technical systems. This approach should be based on the following premises:

1. Complex engineering systems should be considered as socio-technical systems whose performance is determined by interaction of technical, human and organizational factors.

2. Performance conditions for CES are always underspecified because they are too complex to be described in every detail and because they are not stable and fixed. Thus it is impossible to characterize the CES’s performance by analyzing its response to a bounding set of design-basis impacts.

3. Low probability – high consequences (beyond design-basis) events should be included into the scope of CES risk assessment and management framework. This requires development of additional measures aimed at increasing CES’s robustness and resilience in case of beyond design-basis impacts.

4. Many adverse events in CES can not be attributed to a single failure or malfunctioning of components. They result from unexpected combinations of various adverse factors. Occurrences of accidents in CES may be due to a combination of performance variability, malfunctions, human errors, adverse unauthorized impacts. Safety management must therefore be not only reactive but also proactive as well.

5. Risk assessment and management models for complex engineering systems should include several levels (legislators, managers, system operators, hardware components etc).
6. Impacts of technological and intelligent terrorism should be included in the framework of CES risk assessment. This requires that a number of specific features of terrorist impacts (feedbacks between vulnerability and consequences) be accounted for.

Acknowledgments
This work was financially supported by the Russian Foundation for Basic Research (grant no. 14-19-00776-P).

References
[1] Makhutov N and Reznikov D 2010 Engineering Infrastructures: Problems of Safety and Security in the Russian Federation European Perspectives on Security Research pp 93-106
[2] Makhutov N, Khaziakhmetov R and Reznikov D 2012 Basic Scenarios of Terrorist Attacks at Hydropower Engineering Facilities Proceedings of the 3rd International Forum on Risk Analysis, Dam Safety Dam Security and Critical Infrastructure Management pp 389-394
[3] Makhutov N, Reznikov D and Petrov V 2014 Specific Futures of Ensuring Critical Infrastructures Safety Safety in technosphere 3 No 1(46) pp 3-14
[4] Epstein S 2006 Unexampled events, resilience and PRA Proceedings of the Second Resilience Engineering Symposium pp 105-116
[5] Schintler L A, Gorman S, Kulkarni R and Stough R 2007 Moving from Protection to Resiliency:A Path to Securing Critical Infrastructure Critical Infrastructure pp 291-307
[6] Lundberg J and Johansson B 2006 Resilience, stability and requisite interpretation in accident investigations Proceedings of the Second Resilience Engineering Symposium pp 191-198
[7] Cacciabue P & Hjälmdahl Magnus & Lüdtke Andreas & Riccioli Costanza 2011 Human Modeling in Assisted Transportation: Models, Tools and Risk Methods 10.1007/978-88-470-1821-1