DEVELOPMENT OF SCIENTIFIC PRINCIPLES FOR ENGINEERING SAFETY

Konstantin V.FROLOV,
Academician,
Vice-President
of Russian Academy of Sciences (RAS)

Nikolay A.MAKHUTOV
Corr.-memb. of RAS, Professor,
Mechanical Engineering Research
Institute of RAS (MERI RAS)
4, Griboedov St.,
101830 Moscow, Russia
Voice: (095) 135-7771
Fax: (095) 135-3097
E-mail: makhutov@iies.msk.su

Evgeniy V.GRATZIANSKY
Ph. D., Dipl.Eng.

KEYWORDS: safety, technical systems, disasters, life time, strength, fracture mechanics.

ABSTRACT

The analysis of technogenic and natural catastrophes that occurred over the last decades shows that further scientific and technological civilization development has become impossible without a comprehensive approach to engineering safety.

On the basis of this research in addition to existing norms and standards, special problems of safety and catastrophe analysis are worked out. This experience is primarily accumulated in the atomic, space and aircraft industries.

Further development of science & technology progress, implementation of large-scale projects and preservation of an ecologically sound environment will entail a risk of origination of technogenic, natural and natural-technogenic catastrophes causing regional, national and global consequences. Due to present tendencies in the development of Russia such a risk will exist even in case of military threat reduction. These problems are a main subject of the Russian state scientific and technical program, "The Engineering Safety."

Major accidents and catastrophes occurring in Russia and abroad (in the USA, FRG, Great Britain, Italy, Japan, Norway, India, Mexico) in the last decade have caused thousands of human losses. According to UNO data, about 2,8 mln. people perished and 280 mln. were injured due to natural calamities in the last 20 years. Serious damage has been caused to the environment. Direct economic losses and expenditures for liquidation of natural calamities' consequences have reached tens of billions of dollars.

Nowadays many thousands of potentially hazardous facilities are still in operation in all the continents of earth, which contain radioactive substances, toxic agents, and explosives, which are enough to cause grave damage to the environment and even to completely annihilate life on earth in case of accidents and catastrophes. There are about 50 nuclear and hydrogen combat charges and about 10 nuclear reactors at the bottom of world oceans as a consequence of accidents and catastrophes happening at military sites. The actual probability of grave accident generation (with core melting) at NPPs (the quantity of reactors is about 400 now) is more than 10^{-4} per reactor per year instead of the required and acceptable 10^{-6} - 10^{-7}.

Substantial risk increase in Russia and abroad is related to the fact that the most hazardous technical systems have been located, as a rule, within areas with a dense concentration of population.

As has been revealed by analysis of reasons and consequences of major accidents and catastrophes in Russia and abroad, complex technical systems which present a real danger to people and environment are designed and manufactured, in most cases, using traditional design rules and simple engineering calculation/test methods. Unfortunately, in Russian and foreign practice there are no fundamental scientific principles thoroughfully formed for promoting safety of technical systems, people and the environment according to risk/survivability criteria under badly damaged conditions; national and international guidelines with norms and regulations on accidents' classification (predicted/unpredicted/hypothetical accidents) and their consequences (regional/national/global consequences) aren't compiled yet; general requirements for hazardous operating processes, technologies, materials and technical sites aren't developed either; there are no worked out unified basic provisions on rigid and functional protection systems and emergency monitoring using mobile ground, aerial and space systems; and state technical complexes for liquidation of accidents/catastrophes' consequences have not been created.

Further development of complex technical systems within a lifetime ranging from seconds (rocket-space vehicles) to 50-100 years (nuclear reactors, engineering facilities), without regard for new safety criteria which characterise these systems' transition to final conditions threatening people and the environment, should be considered unacceptable. Quantitative substantiation for conditions of emergency origination should be calculated not only for normal operating conditions, but also for extremal ones which are caused by fractures, explosions, fires, leakages of radioactive and toxic substances, earthquakes, hurricanes, tsunami, aircraft and space vehicle crashes, or subversive actions.

Safety assurance problem will be of vital importance for the nearest decades in Russia due to expiration of the lifetime of a large number of power units (including atomic ones), chemical and transportation apparatuses, complete replacement or modernization of which requires significant financial and intellectual expenditures.

A great diversity of approaches to complex technical systems' safety is first of all conditioned by the distinctive features of various systems and, naturally, by a statement of local problems for such systems' safety. The absence of a general concept for complex technical systems' safety, which would allow us to carry out unified analysis and to develop scientific criteria for safety assurance standards, can be explained by the aforementioned facts. That's why the main objective is the generalization of fundamental research development and creation of unified scientific principles of safety analysis and safety assurance standards. The following classification of these objects is offered to your attention, which takes into account their design structural peculiarities and the level of potential hazard to people and the environment in case of technogenic and natural catastrophe generation:

- nuclear power engineering sites;
- chemical plants;
- special equipment (rockets, space vehicles, computer-aided systems);

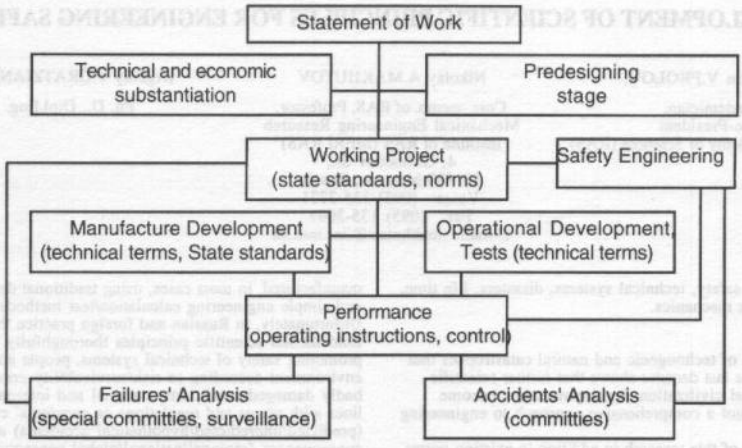

Fig. 1. Structural scheme of technical facilities' development

- unique engineering structures;
- civil engineering sites;
- traditional and non-traditional power engineering sites;
- objects of machine building and metallurgy industries;
- transport systems;
- main pipelines;
- equipment for operation in low temperature conditions (Arctic equipment).

While establishing these unified research principles one should take into account the potential hazard level of this or that object, types of catastrophes and emergencies (regular operational conditions, deviations from normal operating conditions, predicted/unpredicted accidents, hypothetical accidents), affecting factors' assessment, and comprehensive safety criteria systems.

The main goals of fundamental and applied development should be multicriteria safety substantiation (using relevant assessments, modelling, stand simulation, and full-scale tests) for complex technical facilities both of civil and military destination at the design/manufacture/ operation stages. It turns out that modern safety requirements raise the cost of a project and the complexity of its realization to such an extent that it would be expedient to cancel it; though in this case acting traditional norms and requirements can be fully satisfied.

Safety assurance problems are solved according to the most frequent principle within the frames of present design norms and regulations for the majority of complex technical sites—it is assumed in projects that provided acting norms are met, then there is no need to carry out special safety analysis (Fig. 1).

Development of a statement of work, feasibility study, and predesigning are performed, as a rule, without regard for safety requirements, or taking them into indirect account. There is no special consideration for the question of accidents and catastrophes in the statement of work. At the working project stage principal structural schematics and working drawings are developed using basic requirements for standards, norms and other technical documentation as well as safety engineering norms for operators under normal operating conditions; or, deviations from them are foreseen. Manufacture, operational development, adjustment and tests are carried out in accordance with technical terms and standards; additional safety analysis is not conducted at this stage.

Performance of new and acting facilities is executed according to pertinent operating instructions with arrangement, if necessary, of technical control and certification procedures. Operating failures are registered by special departmental committees or surveillance services. Major accidents and catastrophes are investigated by special interdepartmental committees and surveillance bodies. According to the results of investigation accomplished by these bodies design and technology solutions are adopted which are directed to avoiding new failures and accidents. As well, changes are introduced into safety engineering instructions. Practically all branches of machine building, construction and power engineering, and the transport industry are operating according to this scheme.

While developing a general structure of basic safety norms for complex technical systems it is necessary to consider:

- hazard level of a complex technical system;
- types of emergencies;
- comprehensive set of affecting factors;
- safety criteria system.

Project and design requirements of the upper level are developed based on fundamental provisions of development of complex technical systems which in the majority are common to all types of structures for all countries. Fundamental provisions of the complex technical systems' concept are stated in different documents of design offices, firms, institutes, and state associations.

As regards the aforementioned facts, the structure of safety norms and regulations for complex technical systems should be compatible with the present structure of norms and regulatory rules for design, manufacture, operational development and tests of sites and systems. As compared to theconventional practice of complex technical systems development, new stages of work on safety issues should be introduced (Fig. 2).

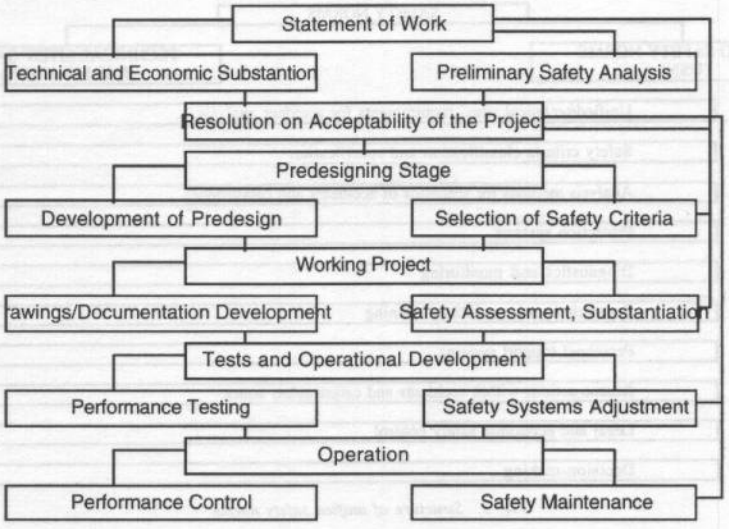

Fig. 2. Structural scheme for complex technical systems' development

Relevant safety requirements for a designed system should be included in the Statement of Work for the project. These requirements will be further developed in the course of safety works, transferring to their direct quantitative wording. At the initial stage of work while compiling the statement of work, preliminary safety analysis has been done.

A resolution on acceptability of a project from the point of view of safety is of exclusive importance. Adoption of such a resolution should be exercised at all further stages of complex technical systems' development. As Russian and foreign experience confirms, in the case of absence of adoption of a resolution on acceptability of a project on safety norms and criteria, it could be possible to implement any project, provided it met all other norms in force.

At the predesigning stage one should include the formation and specification of criteria and methods for providing safety into the documentation of this stage.

At the working design stage safety substantiation should be conducted including mathematics and physical emergencies' modelling together with working drawing preparation.

At the operational development and tests stage, there will be comprehensive elaboration of systems to ensure safety together with experimental performance tests which reveal whether the real system's characteristics meet the requirements of the statement of work.

As regards the operation stage, operating control over the state of complex engineering facilities has been foreseen using pertinent diagnostic methods within the framework of conventional development of complex technical systems. In compliance with the developed safety concept, possibilities for efficient emergency response to catastrophes' origination, using monitoring and diagnostic means, should be included in the concepts of operation of complex technical sites which may cause potential hazards. Support of the designed safety level should be based on both deterministic approaches and on probabilistic ones.

Thus, the right-hand branch of the structural scheme of complex technical systems' development depicts the necessity of considering safety assurance issues at all the stages of project development. Regulatory and surveillance bodies should have the right to participate in adoption of resolutions on project acceptability from a safety point of view.

In those cases when a complex technical system project is prepared on the whole, or only some part of it is prepared, but the project itself hasn't been commerciallized yet, safety factors should be considered in the same volume as the statement of work, predesigning, and working design development stages for a new project development.

Owing to the comparative stability of general mechanisms of emergency propagation at various types of facilities, it would be advisable to foresee two levels of safety norms and standards, while forming a structure of general safety norms (Fig. 3):

- unified safety norms - USN (for main types of objects) ;
- technical sites' safety norms - TSSN (for the given type of object).

The first chapter of materials on USN should contain the following:

- general requirements for safety analysis of objects;
- determination of potential hazard level for objects;
- classification of emergencies according to their technological, economic, social, political, and ecological basic consequences;
- classification of accident types according to the reasons of their initiation;
- classification of accident types according to probability level of their outburst;
- classification of accidents' character according to relevant groups of affecting factors.

As regards the second chapter of materials on USN, it should contain classification and specifications of both qualitative and quantitative safety criteria. Quantity and

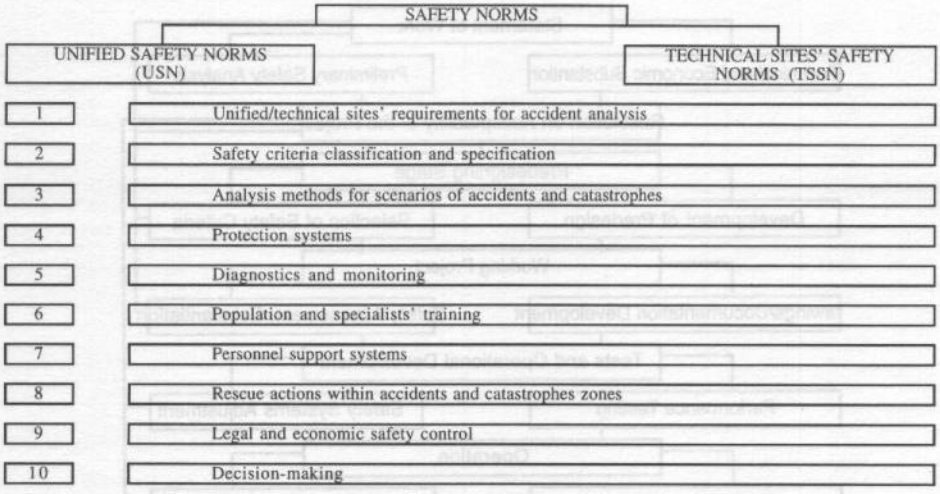

Fig. 3. Structure of unified safety norms

combinations of required criteria values should be related to classes, types and character of accidents and catastrophes.

As regards the third chapter of materials on USN, it should contain analysis methods of initiation and propagation terms for emergency scenarios from the point of view of modern fundamental science. The major attention should be paid to mathematics and physical modelling for emergency propagation and pertinent response to it.

As regards the fourth chapter of materials on USN, it should contain general information on selection of emergency protection systems for the population, the environment and technical sites.

As regards the fifth chapter of materials on USN, it should contain general requirements for objects' diagnostics and monitoring, not only in regular situations but also in emergencies. The diagnostics should cover technical facilities, their personnel, the population and the environment.

As regards the sixth chapter of materials on USN, it should contain general requirements for training methods for the population and specialists' response in emergencies (at accidents' initiation and propagation stages).

As regards the seventh chapter of materials on USN, it should contain systems and means of support, training and retraining of operators at potentially hazardous facilities.

As regards the eighth chapter of materials on USN, it should contain emergency response measures for personnel, the population, and search-and-rescue services for localization of accidents and liquidation of their consequences.

As regards the ninth chapter of materials on USN, it should contain requirements on legal and economic safety control.

As regards the final chapter of materials on USN, it should contain general recommendations on decision-making at local, governmental and international levels in emergencies and in the course of liquidation of their consequences.

Concerning materials on technical sites' safety norms (TSSN), they should contain:

- a list of basic distinctive features of potentially hazardous objects;
- chosen class, type and character of accidents and catastrophes;
- quantitative and qualitative safety criteria;
- recommended assessment methods for prediction of probable emergency propagation;
- diagnostics and monitoring methods for objects and the environment in usual situations and in emergencies;
- population and specialists' training for emergency response measures;
- personnel life-support methods and means in emergencies;
- measures on protection of operators, the environment, and technical sites;
- recommendations and requirements for actions to be undertaken in emergency areas;
- legal and economic standards for safety control; and,
- recommendations on decision-making at relevant levels.

Thus, while developing the above unified scientific principles of safety standards, there should be taken into account: the potential hazard level of the objects, types of accidents and emergencies (regular operating conditions, deviations from normal operating terms, predicted/unpredicted/hypothetical accidents), a comprehensive safety criteria system, and affecting factors' assessment.

The International Institute of Engineering Safety (IIES) was organized on the basis of the national program, "The Engineering Safety," by representatives of public and scientific organizations of Russia and some other countries; it is an effective instrument in realizing international cooperation on the above mentioned tasks in ensuring safety in designing and maintaining potentially dangerous facilities.

The IIES is established by representatives and specialists of scientific, industrial and public organizations of Russia, FRG, Bulgaria, Norway, Canada, Sweden, Netherlands,

Kazakhstan, Armenia, Georgia, the Ukraine, Byeloruss, Moldova, and other countries.

The IIES is a non-governmental organization. IIES activity is executed over the territories of Russia and foreign countries under support of international and national public organizations, National Academies of Sciences, governmental institutions, committees and commissions, industrial enterprises, companies and organizations.

The IIES combines efforts and unites activities of scientists on forming a general theory and conception of technical facilities safety, on working out of methods and safety providing means for certain most potentially hazardous structures and manufactures, on implementation and usage of safety technologies, on enlightenment activity, as well as on forming a safety culture and spreading it in society.

The problems solved in the framework of IIES activity consist of the following main elements:

- fundamental scientific developments of accidents and disaster theory (physics, chemistry, disaster mechanics, principles of hard and functional defence, physical and mathematics modelling and monitoring, emergency diagnostics);
- prediction of catastrophic natural phenomena, and parameter definition of their impact on complex technical systems, on towns and population;
- international cooperation on population protection against accidents and disasters (warning, rescue, evacuation, life supply measures, etc.) and on their liquidation of their consequences;

The activity of the IIES is carried out on the following main trends:

- research accomplishment on theory and safety criteria of complex engineering systems;
- applied developments on projects of providing safety for complex engineering facilities;
- personnel training and information services on the problems of safety of complex technical systems.

The principal tasks of the Institute covered by the program of its work are as follows:

- transfer to novel design technological solutions to prevent large-area technical accidents and natural calamities;
- mitigation of accident and disaster consequences in cases when their prevention is impossible;
- execution of combined national and international measures on population protection, as well as on liquidation of accident and disaster consequences;
- development of a unified international conception, criteria and principles of ensuring engineering facilities' safety (for nuclear power facilities, aircraft and aerospace systems, chemical enterprises, transport systems, machinery and metallurgic enterprises, special equipment facilities, pipe lines, etc.);
- development of methods and systems of international warning about major accidents and disasters and coordinated actions in hazardous zones;
- development of principles, technologies and techniques of liquidation of the consequences of accidents and disasters at complex technical systems in emergency areas and in natural calamity zones;
- creation of main principles of emergency monitoring, rescue and emergency diagnostics in technological disaster zones and natural calamity areas; and,
- information exchange and collaboration in the field of methods and means of actual diagnostics of emergency situations and safety.

The IIES is open for the affiliation of other organizations and specialists in Russia and other countries as founding members and participants in its work, sharing the purposes and scope of its activities, and who are interested in realization of joint developments in the field of ensuring engineering safety of complex technical facilities.