METHODOLOGICAL RESTRICTIONS OF THE THEORY OF ENSURING SAFETY OF THE ECOLOGICALLY DANGEROUS OBJECTS

Aminaga Sadigov
Institute of Cybernetics of ANAS, F.Agayev str. 9, AZ1141, Baku, Azerbaijan
E-mail: aminaga@box.az

ABSTRACT

Describes the system theory of optimal safety control of ecologically dangerous objects in accordance with the concept of maximum security at minimum total cost for prevention, mitigation and insurance virtual accident. Regularity probability of an accident is excluded. Virtual accident is used. It has no regularities and virtually not required, but theoretically not be excluded because of error prevention and mitigation of the accident. The theory is focused on advanced science intensive technologies for providing maximum safety of ecologically dangerous objects.

Keywords: *accident, environmental security, security management, mathematical model.*

1. INTRODUCTION

The problem of environmental security is rather challenging in the technology associated with energy sources and electrical energy production and waste burial. The negative impact on the environment as the result of energy consumption is considerably increasing. With the lack of protection costs for mitigating possible negative consequences exceed the amount of the produced energy. The problem of managing environmental security is a complex one that's why it can not be formulated [1] in the framework of any theory. Any theory due to its being of axiomatic character allows to formulate only the limited range of tasks comprising a small part of the total amount of the problem tasks.

The solution of scientific-technical problem of environmental safety demands the attraction of experts with different background. In the process of solution different theories are used such as cybernetics, theory of automatic control, diagnostics, reliability, safety and so on. Each of these theories has its axiomatics, methodology and mathematical tools and field of application, different from the fields of application of other theories. Thus, each of the theories of this kind has a local character and solves the certain amount of relevant problems (without taking into consideration the connection with other tasks solution) by means of corresponding local theories. Due to the partial approach to the problem solution no local theory can cope with the inclusion of subproblems into the common algorithm of problem solution. Normally the common algorithm of problem solution is developed by a highly qualified practitioner who integrates local solutions into the system solution at the logic-expert level.

The consequence of the logic-expert approach is the impossibility of building a mathematical model of managing complex objects. This leads to the impossibility of optimization and as a result to the risk of large economic losses.

The above mentioned can equally refer to the classical theory of safety and classical theory of reliability. They do not consider theory of safety and reliability management. They are solely limited by the analyses.

The solution of a complex scientific problem of optimal control of ecologically dangerous objects including nuclear stations can be done on the basis of the system approach. Systemacy must be based on the axiomatic proposition of the impossibility of complex problem solution on the base of one theory. The system theory must contain a methodology of control providing the structural synthesis of local theories as well as the corresponding mathematical tools allowing to work out algorithms of control according to the efficiency criteria and implement control in the form high technology. Naturally, such system theory has all formal restrictions of any theory, based on axiomatics: it is restricted by intuition, philosophy, methodology, mathematical tools and field of application. But unlike any local one the system theory of control of ecological security serves for the solution of a complex problem from the point of view of efficiency and solves it in conjunction with local theories (and not in isolation) on the quantity optimization basis. Whereas it serves as an optimization jointing of these theories into the general algorithm of safety management by the efficiency criterion. In general, this system theory together with local theories allows to obtain new quality and for the first time switch to the optimal control of individual ecological security of ecologically dangerous objects (EDO). The present work the basics of which are given in [2-10] deals with generalization and development of the system theory of individual ecological safety control and reliability of the energy object.

For the implementation of the system approach of ensuring economic and technical efficiency of nuclear power it is necessary to develop methodological provisions of the optimal control of safety and reliability of nuclear power plants (NPP) on condition costs for the safety are minimized. So, it is necessary to take into account methodological restrictions of the experts approach to safety control including operators influence. Analysis and minimization of operator's contribution to the danger of the EDO and unreliability of its safety control systems is of primary importance. This accounts for a great role of human factor in safety ensuring on one hand and low, not corresponding the safety requirements, operator reliability indicator values due to ergonomic restrictions on the other hand. These values do not meet the requirements for the components of modern control systems and technological problems which values of reliability indicators are higher than 0,999. Indeed, according to the statistic data of the failure of energy blocks the values of human reliability indicators do not exceed 0,9 [8]. Due to ergonomic restrictions of the man this value can be considerably increased even by means of the most up to date simulators. So, the solution of the problem of operator's unreliability contribution to the unreliability of the safety control system can be achieved only by choosing the corresponding structure of subsystem control and the place of operator in it (see [5,7]).

The influence of the human factor in the technology of safety control of the man-machine system is not limited by the operator's assessment. As was pointed out, this influence should be considered as one of the factors, but not the most important one, of efficiency problem of the technological process of the control of man-machine system safety, such as NPP. In general, this is the problem of correlation of creative and axiomatic components of man's work as well their efficient use in technological processes of control. So it is necessary to consider the efficiency of the expert method used by the man in the technology of safety control in general.

As any scientific approach, the expert method inevitably has methodological restrictions. They are the result of natural restrictions of the human factor both in the implementation of separate operations of the technological process control and in the process control in general. The above considered analysis of the influence of operator's unreliability on the unreliability of control system can serve as an example of these two kinds of restrictions.

The classical theories of safety and reliability used in the current technology of ensuring security of EDO are closely related with the methodological ones. They mainly use the probability mathematical tools and mathematical statistics. The analysis of accidents developed in these theories is closely connected with the analysis of reasons of the object unreliability according to the event tree analysis [11-15]. Let's dwell upon the most significant methodological restrictions of classical theories reliability and safety.

2. METHODOLOGICAL PECULIARITIES OF THE PROBLEM OF SAFETY CONTROL

Restrictions of the expert approach in general are due to the methodological peculiarities of the problem of safety control as a science. The problem of ecological safety control is a complex one. That's why it can not be formulated [1] in the framework of one theory. Any theory due to its being of axiomatic character allows formulate only the limited range of tasks comprising a small part of the total amount of the problem tasks.

Normally fundamental researches are carried out in the framework of local theories each of which is different from the others in terms of intuition, axiomatics, mathematical tools and field of application. Due to these restrictions only local tasks of the safety control problem are fulfilled, whereas the problem of the optimal control in general has not been set and the ways of its solution have not been identified which leads to a greater methodological alienation from each other. One of the most negative results is the atomism of science due to the lack of science intensive technology of interrelation of local theories in the framework of which the complex problem could be set and solved and in particular the problem of ecological safety control. As the result of methodological independence the practical use of local theories inevitably ends up with qualitative rough estimates due to the fact that local theories are included into the common science intensive technology of control on the quality base of the logic-expert methods. This practically excludes the uniqueness of safety control models, their adequacy to the technological processes. The possibility of optimization of the whole control process is excluded. In particular, theory of the safety analysis and reliability theory as well as local ones. The risk analysis itself can not be considered independently from the control as it is its constituent part and can have a positive practical importance only in interconnection with other control procedures provided they correspond to the required validity.

The efficiency of the current processes of safety control depends to a greater extent on the expert who performs system functions (for example, a person in charge of the programme, project, chief designer, chief engineer etc.). It depends on the subjectivity of the human factor and can not provide the optimal control in terms of technical and economic efficiency as a whole. Methodological restrictions of the expert approach used by the man are of global character. Below we shall dwell upon some of them which, to our mind, are of great interest..

3. ERRORS OF METHODOLOGY OF LOCAL APPROACHES

Main, principle inaccuracy of local approaches used for ensuring safety of EDO can be revealed by comparing methodology of engineering-technological approach with the methodology of the logic-mathematical one. The engineering-technological approach is based on the concepts of the observed consistency of the connection of components of technical control subsystems and physical, technological, energy, information and other processes occurring in them. Their specifics are determined by practical needs for concrete and unequivocal decisions taken separately according to different local theories (theory of automatic control, energy systems, measurement system etc.). These decisions are combined into the technology of safety control on the basis of qualitative (information-logic) models excluding optimization. The logic-mathematical approach is aimed at building a safety analysis model on the basis of algebra of logic, the theory of probability and mathematical statistics. The used mathematical concept (for example, of probability, passage to the limit etc.) bears an abstract character excluding practical illustration and uniqueness (for example, connection of probability with statistics). Methods of analysis based on them are isolated from the methodology of engineering methods. In particular, they lack record keeping of information laws of components connection in the control subsystems which leads to the problem of dimension of models. Such an approach to the model building is more clearly illustrated in the event tree method which has long been the basic in the modern theory of NPP safety [11-16]. As the result, the models offered according to this model do not contain the feedback circuit and information flows necessary for the control theory. That's why, these models do not allow to adequately describe the technological process of safety control of EDO, solve the problem of dimension and work out the theory of the optimal safety control.

In general, for the theory of the optimal safety control of EDO it is necessary to combine the methodology of engineering approach allowing to provide illustration and correctness of the safety control models with the methodology of mathematical approach allowing to optimize the structu.re of EDO safety control.

4. ERRORS OF THE CHOICE OF MATHEMATICAL MODEL OF THE TIME OF ACCIDENT OCCURRENCE OF THE ECOLOGICALLY DANGEROUS OBJECT

The principle concept of the safety control theory is the choice of the mathematical model of the time of accident occurrence at the NPP [11-16]. The concept of the unlimited random continuous variable of the time of occurrence of a severe accident η belongs to semiinfinite interval: $y \in [0;\infty]$. As is known, the probability

$$P\{\eta \in [0;\infty]\} = \int_0^\infty \psi(y)dy = 1 \qquad (1)$$

The probability of a severe accident at the interval of the operation life $[0,\tau]$ equals

$$P\{\eta \in [0,\tau]\} = \int_0^\tau \psi(y)dy = 1 - \int_\tau^\infty \psi(y)dy \qquad (2)$$

With the generally normalized assumed value of severe accident risk probability 10^{-7} reactor/year and operation life $\tau = 30$ лет, the probability of the accident during the period of the operation life

$$P\{\eta \in [0.\tau]\} = \int_0^\tau \psi(y)dy \cong 3.10^{-6} \quad \text{reactor /operation life} \qquad (3)$$

is insignificant. This, according to rate setters, it makes it impossible for any severe accident with the emission of radio active substances materials to happen. However, error of approximation of the limited operation life of the object is not taken into account by the unlimited random value which leads to the next incorrectness of the mathematic model. Indeed, for the unlimited random value of the time of the severe accident η, the value of the accident probability at the interval after removing NPP from service $[\tau;\infty]$ equals

$$P\{\eta \in [\tau;\infty]\} = \int_\tau^\infty \psi(y)dy = 0{,}999997 \qquad (4)$$

From the expression (4) it is clear that the greatest (almost one hundred percent) accident probability, for example, melting of the active zone, will come after removing NPP from service. It is natural that such a conclusion contradicts the main concepts of the NPP properties. It is obvious that after removing from service (provided there is no nuclear fuel in the reactor) melting of the active zone is impossible.

Error of the model of the unlimited random value of the time of severe accident occurrence (for example melting of

the active zone) η can be seen according to the following analysis. Let's assume that probability of the time of melting of active zone $P\{\eta > t\}$ is subordinated to the exponential law $P\{\eta > t\} = 1 - e^{-\lambda t}$. This analysis is well suited for a priori analysis. For small values of accident probability $P\{\eta > t\} = \lambda t$ equation is more suitable**.** Intensity of the occurrence of the active zone melting $\lambda = 1/T^0$**,** where T^0 – the average value of the time of the active zone melting. Accordingly, for $t = 1$ year, probability $P\{\eta > 1\} = \lambda 1 = 10^{-7}$. Then, the average value of the time of active zone melting is $T^0 = 10^7$ year. According to the technology of the NPP operation active zone melting is only possible provided there is nuclear fuel in the reactor. It is clear that active zone melting can happen during the NPP operation. Due to it the statistical average value of the melting time $\grave{O}^0_{\hat{N}\grave{O}}$ can not be more than the operation life of the NPP τ even in case if active zone melting happened in the last operation year of the NPP. The NPP operation life τ is measured by decades and is significantly less than the value of 10^2 years. So, there is always an inequation $T^0_{CT} \le \tau << T^0$**.** Consequently, the value $T^0 = 10^7$ does not have common sense. On the other hand, the rated value of the risk indicator of the active zone melting $P\{\eta > t\} \le 10^{-7}$ reactor/year can not be proved. It is the result of the incorrect application of mathematical methods for the solution of practical tasks.

The given example shows the negation of the statistical stability of the model of the casual event of the accident as well as necessity for the virtual accident model. That's why the model of the unlimited random value of the time of the severe accident can not be accepted for the correct assessment of probability of accident risk.

Let's dwell upon the correctness of the model of the limited random value of severe accident ξ with the probability density $\phi(x)$, when the value x of the random value ξ belongs to the final interval: $x \in [0;\tau]$**.** According to the theory, probability of the severe accident occurrence during the operation life

$$P\{\xi \in [0;\tau]\} = \int_0^\tau \psi(y)dy = 1 \qquad (5)$$

Consequently, according to the model of the limited random value ξ, severe accident at the NPP during the operation life is inevitable. According to the above mentioned, postulation of the model both as unlimited η**,** and limited ξ of random values of time of the severe accident occurrence is not suited for the optimal safety management of the NPP with the aim of preventing the accident as with such postulation accidents become statistically regular (theoretically inevitable) and, thus, any protection is theoretically impossible.

5. ERRORS OF POSTULATION OF THE PROBABILITY NATURE OF THE POTENTIALLY PROBABLE SEVERE ACCIDENTS OF THE ECOLOGICALLY DANGEROUS OBJECTS

The main principle of the expert analysis is the development of scenarios in the form of symptom-oriented instructions of a possible severe accident at the potentially dangerous object due to the failure (initiating event) of this or that component of the safety management system. The scenario is the combination of events of operability and non-operability (failures) of the components of the subsystem of the object protection together with the initiating event which, according to the experts' opinion can lead to accidents. Whereas, a priori stochastic regularity of accidents is postulated. The example of such an approach is the analysis of "highly improbable events" which were practically not observed [11-15]. The sequence of "more probable events" connected with improbable event of the postulated causative-consecutive chain [12]. Based on this idea the combination of the initiating event with different combinations of events of operability and non-operability of components of accident protection subsystems chosen by the expert is considered. These events are assumed as independent, probability of combination equals the product of event probability, forming combination. Probability of accidents equals the probability of the initiating event multiplied by the sum of probabilities of those combinations which, according to the expert's opinion are "more probable events" and can together with the initiating event lead to an accident. For example, probability of hazardous substances emissions due to the reactor active zone melting is considered [11, 13].

The methodological error of such analysis is the acceptance of the probabilistic hypothesis of accidents on one hand and postulation of independence of events forming a combination of events on the other hand. Indeed, if the accident event was not observed and is, thus, statistically unstable its frequency of occurrence equals zero. Consequently, its probability (as theoretical representation of frequency) also equals zero. Then, "more probable events" are incompatible and, thus, dependent. That's why hypothesis of their independence can not be accepted. It is not known that the event of active zone melting is not stable (only two severe accidents not bound by common statistical

regularities are known).
Consequently, if there are no grounds for the hypothesis of the persistence of accident frequency (statistical stability of its regularities), so there are grounds for its probabilistic hypothesis. Such accident is hypothetically possible but it is not statistically regular.
Hypothetic probability differs from the statistical regularity (inevitability).Such probability can not be denied in principle but it is not regular as the probabilistic accident model. Thus, proceeding from the hypothetical (not probabilistic) probability of accident an approach to the safety management vitally different from the probabilistic approach should be used.
Methodologically important case, requiring to take into account improbable events like earthquake or plane crash. For example, periodicity of earthquakes is assumed to be 10^6 years. If the operation life of the object is $\tau << 10^6$ years (for NPP $\tau < 100$ years), then persistence of frequency of earthquakes at the limited interval τ can not be stated in terms of safety management. Otherwise, events of such kind, in terms of optimal management, should be considered as statistically unstable to the accident event at the potentially dangerous object and NPP in particular.

6. CONCLUSION

So, the consequence of methodological error of postulating the probabilistic nature of potentially severe accidents (like active zone melting) is the transfer of hypothetically probable (but practically not inevitable) accidents to the class of statistically regular and, thus, theoretically inevitable. Thus, the concept of defense in depth becomes theoretically useless as, according to the probabilistic hypothesis, an accident is inevitable in spite of presence of any kinds of protection.

7. REFERENCES

[1]. Chernyakhovsky E.R. Managment of environmental safety. (In Russian). Moscow, "Alpha-Press", 2007, 248p.
[2]. Gusev L.B. Ershov G.A. Methodology, theory and practice of modeling and calculation of reliability, survivability, security, complex organizational and technical systems. (In Russian) // Marine Technology, № 1, 1998.
[3]. Pampura V.I. The method of developing of mathematical models of managment of ecological safety of objects. (In Russian) Reports of the National Academy of Sciences of Ukraine, 1999, № 1, p. 197-203.
[4]. Sadigov A.B. Creation of mathematical models and methods for solving of tasks of operational control in emergency situations. (In Russian)//Computer Mathematics. Kiev, 2011, № 1, p. 37-45
[5]. Pampura V.I. Optimal control of NPP safety and probabilistic risk analysis (In Russian) // Reports of the National Academy of Sciences of Ukraine, 2001, № 5, p.185-191.
[6]. Pampura V.I. Optimization of the insurance risk of a virtual severe accident(In Russian) // Reports of the National Academy of Sciences of Ukraine, 2002, № 3, p. 198-204.
[7]. Ostreykovsky V.A., Shviryayev Y. V. Safety of nuclear power plants. The probabilistic analysis. (In Russian). Moscow, Fizmatlit, 2008, 352 p.
[8]. Pampura V.I. Analysis of the effectiveness of the human factor in the technology of optimal control of environmental safety of human-machine systems (In Russian) // Cybernetics and Computer Science, 2002, Issue 136, p. 32-54.
[9]. Pampura V.I. Maximum security with minimum possible cost(In Russian) // Reports of the National Academy of Sciences of Ukraine, 2006, № 5, p. 185-190.
[10]. Lisichenko G.V., Zabulonov Y.L, Khmil G.A. Natural, technological and environmental risks: analysis, evaluation and management (In Russian). Kiev, "Naukova Dumka", 2008, 542 p.
[11]. Henly E.J., Kumato Kh. Reliability of engineering systems and risk assessment. Moscow, Mashinostroenie, 1979, 528 p.
[12]. Ueaver L. The risk of an accident on NPP with light water reactors. / Safety of nuclear power. Moscow, Atomizdat, 1980, p.114-133.
[13]. Probabilistic analysis of safety of nuclear power plants (In Russian). / V.V. Begun, O.V.Gorbunov, I.N.Kadenko and others. Kiev, 2000, 568 p.
[14]. Sadigov A.B. Creation and use of automated control systems for the protection of people and objects in an emergency (In Russian). Proceedings of the International Conference "Twenty five years after the Chernobyl disaster. Secure of the Future", Kiev, 2011, p. 150-154.
[15]. Sadigov A.B. Creating a database of certification of potentially dangerous objects (In Russian). Proceedings of the II Republican Scientific Conference "Modern Problems of Information, Cybernetics and Information Technology". Baku, 2004. Volume I, p. 97-100.
[16]. Hight, F.Kh. Risk. Uncertainty and profit. / Transl. from English, Moscow, Delo, 2003, 360 p.