System Coordination of Survivability and Safety of Complex Engineering Objects Operation

N.D. Pankratova

Abstract

A system strategy to estimation the guaranteed survivability and safety of complex engineering objects (CEO) operation is proposed. The principles that underlie the strategy of the guaranteed safety of CEO operation provide a flexible approach to timely detection, recognition, forecast, and system diagnostics of risk factors and situations, to formulation and implementation of a rational decision in a practicable time within an unremovable time constraint. Implementation of the proposed strategy is shown on example of diagnostics of electromobile-refrigerator functioning in real mode.

Keywords: risks, abnormal mode, safety, information platform for engineering diagnostics.

1 Introduction

Creation of modern technology defines a new requirement to ensure technological and environmental safety of CEO operation. This need is caused not only by the fact that the losses of the partial or complete destruction of machines or structures may be ten times higher than the cost of their creation, but also the fact that the disaster may have national or global scale of the impact on the population and the environment. Moreover, the disaster with multimillion losses and billions of victims which during last two or three decades of the last century and the first decade (including the earthquake in Japan) of the XXI century, occurred in all industrialized countries, argue that the existing principles and mechanisms for complex security facilities control do not meet modern requirements. Hence there is a strong need for a fundamental change in the practical approaches and principles of safety of complex objects control, particularly, the objects of modern technology. To improve the control quality of complex objects one should find out the reasons and the factors that cannot provide the agreed level of survivability and safety of complex engineering objects operation. One of these reasons is the peculiarities of diagnostic systems, focused on identifying failures and malfunctions. This approach to security eliminates the possibility of a priori prevention of abnormal regime and, as a consequence, the possibility of its subsequent transition into an accident or disaster.

In this article the system strategy for estimation of guarantee of survivability and safety of complex engineering objects operation on the basis of multifactor risks and principle of timely detection of reasons of abnormal situations and prevention of transition of normal situations into abnormal ones is proposed.

2 Mathematical Formulation of Complex Object System Control Problem

Let us show the mathematical formulation of this problem with a priori set variation intervals of main indicators of the system in the normal mode and predefined permissible bounds of the influence of external factors [1].

It is known that the system functioning is characterized by the following sequence of complex system states: $E_1, E_2, ..., E_k$. Every state E_k is characterized by the specified indicators of the system functioning processes (Y_k, X_k, U_k), the specified indicators of external environmental influence and risk factors Ξ:

$$E_k = \{(Y_k \in Y) \wedge (X_k \in X) \wedge (U_k \in U) \wedge (\Xi_k \in \Xi)\},$$

where the meaning of indicators at the moment $T_k \in T^{\pm}$ is defined by the following relations:

$$Y_k = \hat{Y}[T_k];\ X_k = \hat{X}[T_k];\ U_k = \hat{U}[T_k];\ \Xi_k = \hat{\Xi}[T_k];$$
$$T_k = \{t_k | t_k > t_{k-1}\};\ T_k \in T^{\pm};\ T^{\pm} = \{t | t^{-} \leq t \leq t^{+}\};$$
$$Y = (Y_i | i = \overline{1,m});\ X = (X_j | j = \overline{1,n});$$
$$U = (U_q | q = \overline{1,Q});\ \Xi = (\Xi_p | p = \overline{1,P}).$$

Here Y is a set of external parameters Y_i that includes technical, economic, and other indicators of the system functioning quality; X is a set of internal parameters X_j that includes constructional, technological, and other indicators; U is a set of control parameters U_q; Ξ is a set of external environmental influence parameters and parameters of risk factor influence Ξ_p; $\hat{Y}[T_k], \hat{X}[T_k], \hat{U}[T_k]$ and $\hat{\Xi}[T_k]$ are sets of meanings of appropriate parameters at the moment T_k; and $T^{\pm}$ is a specified or predicted complex object functioning period.

Required: determine in the moment $T_i \in T^{\pm}$ such values of degrees η_i and levels W_i of risk, as well as a margin of permissible risk T_{ar}, which provide, during the abnormal mode, the possibility of transition from the mode $\overline{\tilde{R}}^{+}_{tr}$ during the period $\check{T}^{\pm}_{tr}$ to the normal mode, till the critical moment T_{cr} of transition of abnormal mode becomes an accident or catastrophe. Here, the mode $\overline{\tilde{R}}^{+}_{tr}$ is the controlled mode of functioning conditioned by the influence U_{tr} of a safety control system. During the time period $\check{T}^{\pm}_{tr}$ this mode leads to the reduction of the abnormal mode R_{an} to the normal mode R_{nm}. The mode $\overline{\tilde{R}}^{+}_{tr}$ is characterized by the following functional:

$$\check{R}^{+}_{tr} : R_{an} \overset{U_{tr}}{\to} R_{nm},$$

which defines the process of the transition of the abnormal mode R_{an} to the normal mode R_{nm} under the influence of the control system. The main system property is an operational capability characterized by the given quality indicators defined by the set Y. The system safety will be considered as an ability to timely prevent a consecutive transfer from a normal mode to an accident or a catastrophe on the basis of timely detection of essential risk factors and elimination of the possibility of their conversion into catastrophic risk factors. Safety is characterized by the following indicators: degree of risk η_t, level of risk W_i and the margin of permissible risk T_{pr} of an abnormal mode; the margin of permissible risk T_{as} of an accident; and the margin of permissible risk T_{cr} of a catastrophe. The quantitative values of safety indicators are defined on the basis of the general problem of multifactor risk analysis, the mathematical definition of which is described in [2].

3 Strategy for Solving the Problem of System Control of Complex Objects

The main goal of the proposed strategy is to guarantee a rationally justified reserve of survivability for a complex system in real conditions of fundamentally irremovable information and time restrictions.

The main idea of the strategy is to ensure the timely and credible detection, recognition, and estimation of risk factors, forecasting their development during a definite operation period in real conditions of a complex objects operation, and on this basis ensuring timely elimination of risk causes before the occurrence of failures and other undesirable consequences.

The main approaches and principles of the strategy for providing guaranteed safety of complex systems will be formed on the basis of the following principles [3]:

- system coordination according to the goals, tasks, resources, and expected results of measures aimed at ensuring the safety of a complex system;

- mutual coordination of goals, tasks, resources, and expected results of control of serviceability and safety of a complex system;

- timely detection, guaranteed recognition, and system diagnostics of factors and situations of risk;

- efficient forecasting and credible estimation of abnormal and critical situations;
- timely formation and efficient realization of decisions of safety control in the prevention process of abnormal and critical situations.

Therefore, the most important and obligatory requirement of the strategy is system coordination of decisions and actions at all stages of a product's life cycle according to its goals, tasks, terms, resources, and expected results. The coordination must be provided simultaneously from the position of guaranteeing both the required indicators of safety and survivability and the required indicators of serviceability during the given period of operation [1].

In particular, the consistency of diagnostics and control are especially important for transport systems, where there principally cannot be an emergency stop in conditions of unexpected effect of catastrophic risk factors. Such systems include all categories and all types of aircraft.

At first, note the principal differences between the given problem and typical control problems. The main difference is that the initial information about a complex object contains only a small part of information about its state, properties, functioning processes, and operational capability characteristics. This information represents only the state and work characteristics of such objects in normal mode. Undoubtedly, this information is enough for decision making during the complex object control only on the condition that the normal mode continues for a long time. However, in real objects in view of existing technical diagnostics systems, oriented toward failure and malfunction detection, it is impossible to ensure that a malfunction or a failure will not appear within the next 5–10 min. It is a priori unknown how much time it will take to repair a malfunction. It may take from a few minutes up to several hours or even days and months. And, consequently, the possible damage is a priori unknown, and thus the safety control system is, essentially, a recorder of information about facts and damage. A fundamentally different approach can be realized on the basis of the system control of complex objects. The essence of such control is systemically coordinated evaluation and adjustment of the operational capability and safety during the functioning process of an object.

4 Information platform for engineering diagnostics of CEO operation

The diagnostic unit, which is the basis of a safety control algorithm for complex objects in abnormal situations, is developed as an information platform [4] that contains the following modules:

- acquisition and processing of the initial information during the CEO operation;
- recovery of functional dependences (FDs) from empirical discrete samples;
- quantization of the discrete numerical values;
- identification of sensors failure;
- timely diagnostics of abnormal situations;
- predicting of the process of engineering diagnostics;
- forecast of nonstationary processes.

Let us detail these modules of the information platform of engineering diagnostics (IPED).

Acquisition and processing of the initial information during the CEO operation. By a CEO we mean a complex engineering object consisting of several multi-type subsystems that are system-consistent in tasks, problems, resources, and expected results. Each subsystem has functionally interdependent parameters measured with sensors. To this end, groups of sensors are connected to each subsystem, each having different parameters (time sampling, resolution, etc.), depending on what its nature is.

The engineering diagnostics during the CEO operation requires samples of size N_{01} and N_{02}, where $N_{01}(N_{01} >> 200)$ is the total sample size during the CEO real-mode operation; $N_{02}(N_{02} << N_{01};\ N_{02} = 40 \div 70)$ is the size of the basic sample required for estimation the FDs. The initial information is reduced to a standard form, which makes it possible to form FDs from discrete samples. In view of the proposed methodology, the biased Chebyshev polynomials are taken as basic approximating functions, which normalize all the initial information to the interval $[0,1]$.

Recovery of FDs based on Discrete Samples. The approximating functions are formed as a hierarchical multilevel system of models [5]. We will use the Chebyshev criterion and biased Chebyshev polynomials $T_{jsp}(x_{jsp}) \in [0,1]$. Such an approach reduces the procedure of forming the approximating functions to a sequence of Chebyshev approximation problems for inconsistent systems of linear equations.

Due to the properties of Chebyshev polynomials, the approach of formation the functional dependences makes it possible to extrapolate the approximating functions set up for the intervals $[\hat{d}_{j_s}^{-},\ \hat{d}_{j_s}^{+}]$ to wider intervals $[\hat{d}_{j_s}^{-},\ \hat{d}_{j_s}^{+}]$, which allows forecasting the analyzed properties of a product outside the test intervals.

Quantization of Discrete Numerical Values. The quantization is applied in order to reduce the influence of the measurement error of various parameters on the reliability of the solution being formed. The procedure of quantization of discrete numerical values is implemented as follows. As the base reference statistic for each variable $x_1, ..., x_n, y_1, ..., y_m$, the statistic of random samples in these variables of size $N_{01} \geq 200$ is taken. As the base dynamic statistic in the same variables, the statistic of the sample of the dynamics of the object for the last N_{02} measurements is taken. Therefore, the very first measurement of the original sample should be rejected and measurements should be renumbered in the next measurement $N_{02} + N_2$.

For the current dynamic parameters, we take the statistics of samples of size $N_{02} + N_2$ biased by N_2 with respect to the statistics of samples of size N_{02}.

Identification of sensors failure. Functioning of CEO involves monitoring the state of this system using various equipments, sensors, measuring devices. In this case, the recorded figures are not checked for validity in most cases. Often indicators of the transition system in abnormal or emergency mode of operation may be false. Thus, in this situation it is expedient to introduce procedures of identification possible failure of sensors.

To guarantee the sensor functioning reliability and exclude random malfunctions, the input readings of the sensors are filtered by a median filter. Inside the filter window the reading values are sorted in ascending (descending) order; the value that is strictly in the middle of the sorted list is directed to the filter output. In case the number of readings is even, the output value equals the mean of two readings in the middle of the sorted list. The window moves along the filtered signal and the calculations repeat.

$$x_i = \begin{cases} \mathrm{sort}(x_{i-1}, x_{i+1})[2], & i = 2, ..., n-1 \\ \frac{x_i + x_{i+1}}{2}, & i = 1 \\ \frac{x_{i-1} - x_i}{2}, & i = n \end{cases}$$

This technique allows to avoid random malfunctions and provides for stable functioning of complex technical systems.

Also failure of the sensors operation can be monitored by comparing the forecasted and actual results of measurements. Since the forecast follows the general behavior of the system, based on recent measurements, the deviation of the actual one may indicate the failure of sensors. Therefore, in operation of CEO a regular comparison of forecasts and their corresponding recovered values are implemented. As in the previous case, the deviation, which is greater than a threshold level, gives the message about the possible failure of the sensor.

Predicting Nonstationary Processes. The models for predicting nonstationary processes are based on the original sample of the time series for the initial interval D_0. Different prediction models are applied to forecast the sensor readings. The choice of a model is based on the general shape of provided graphs for each sensor, taking into account the meaning of each sensor. In particular, if the figure behavior adheres to an average value or linearly and monotonously decreases (increases), linear regression can be applied, or autoregression in other cases.

It is advisable to forecast 5–10 values ahead, and to take the window of 40–50 values for FD_s restoration. The forecasted values are substituted into the recovered FD_s, thus giving a prediction for goal function values.

Setting up the Process of Engineering Diagnostics. We will use the system of CEO operation models to describe the normal operation mode of the object. Algorithm of technical diagnostics in detail is described [1]. One important issue is the formalization of risk factors with recovered functional dependency. Let's propose the following requirements for defining the risk function:

1. The risk function equals one when at least one estimated parameter reaches acciden value.
2. The intermediate risk function values lie within $[0;1]$ interval.
3. The risk degree grows nonlinearly, considerably rising after exceeding a specific risk factor value.
4. The transition to abnormal situation should characterize to some extent the risk degree.

The following formalization of risk function is proposed. Let's consider the events $\{F_i\}$ – the failure by i-th factor, $i =\overrightarrow{1,3}$.

$F = \underset{i=\overrightarrow{1,3}}{\cup} F_i = \overline{\overline{\cup F_i}} = \overline{\cap \overline{F_i}}$ – the failure by any of the factors. The probability of the emergency situation is represented as

$$P(F) = P(\overline{\cap \overline{F_i}}) = 1 - P(\cap \overline{F_i}) = 1 - \prod_{i=1}^{3} (1 - P(F_i)). \qquad (1)$$

To satisfy the requirements 1–4 $P(F_i)$ is defined as a sigmoid: $P(F_i) = (th(\hat{x}_i) + 1)/2$, where $\hat{x}_i$ are factor values normalized to the interval $[-3;3]$.

It is considered that $\hat{x}_i = 0$ at the moment when the situation factor crosses the abnormal mode bound, i.e. the risk growth starts even before the situation transitions into abnormal mode.

The application of the given accident probability formula (1) results in increased sensitivity of the system when approaching the emergency situation and permits to avoid crossing the border limit. The risk function should be defined by the probability of an accident caused by a specific factor, and damage amount from the respective accident. At the same time the higher amount of damage should correspond to the higher accident weight in calculation of the risk function.

5 Diagnostics of electromobile-refrigerator functioning in real mode

Electromobile-refrigerator needs to deliver perishable cargo within a city. The cargo is distributed in equal parts among four points, that have different distance between them. The electromobile has 800 kg carrying capacity. Each consumer is unloaded an equal amount of the cargo, weighing 200 kg.

In regular mode, taking into account the relief of the area, the electromobile can execute this work only if powered by a fully charged storage cell (SC). The movements of the electromobile are supervised by a control centre operator, who has a system of predicting abnormal situations for timely decision-making regarding the alteration of possible route to the next consumer.

Under the terms of the contract between the carrier and the consumer of cargo, the carrier has to pay a penalty for a delay in delivery, proportional to the delay time.

The profit can be determined by the formula:

$$Q = Q_{in} - W_{AB}C_{kW_h} - V_B C_B - k_{n_1}\tilde{t}_1 - k_{n_2}\tilde{t}_2 - k_{n_3}\tilde{t}_3 - k_{n_4}\tilde{t}_4 - Q_a,$$

where Q is profit, Q_{in} – payment received from the customer, W_{AB} – amount of electric power from the power circuit for SC charging,

C_{kW_h} – electric power cost (for K.W.H.), V_B – amount of consumed gas during the delivery (liters), C_B – gas price for a liter, k_{n_j} – rate of penalty, specific for each destination point, $j = 1, 2, 3, 4, \tilde{t}_1, \tilde{t}_2, \tilde{t}_3, \tilde{t}_4$ – delay times for cargo delivery in respective points, Q_a – fixed costs of equipment amortization, salaries etc.

The situation becomes abnormal, when traffic conditions or other factors lead to untimely delivery of cargo, or the gas consumption is exceeding. This leads to drastic decrease in profitability due to payments of penalties or gas prices.

Situation also becomes abnormal, if an estimated movement reserve is substantially lower than necessary to complete the route, or the energy reserve in SC is lower than admissible either over a long time, or at the start of route.

Critical functions and respective variables are presented in Table 1.

Implementation of the system diagnostics process. In real mode of electromobile-refrigerator operation the correction of the recovered FD_s is performed with taking into account the risk factors influence. At the initial time moment the first 40 elements of the sample are taken and normalized to the $[0, 1]$ interval. From the normalized sample of 40 elements the functional dependence is restored using the conjugate directions method and gradient method. Shifted Chebyshev polynomials are used as basis polynomials. The recovered FD_s are corrected considering the risk function and the forecast procedure. The FD_s received in this manner is a forecast for the next 10 steps. Then a shift for 10 steps is performed. The next 40 elements of the sample are taken (10–50). The described procedure is implemented for them etc. Thus a dynamic forecast is received. At each time moment the probability of reaching the accident state is also calculated by the parameters of SC charge and calculated movement reserve. The probability of accident situation is calculated as $P = 1 - (1 - P_{PZX})(1 - P_{SC})$, where P_{SC} is a probability that the SC charge will be lower than the accident level, $P_{SC} = 1 - (SC_{abs} - SC_r)/(SC_{abs} - SC_a)$, where SC_{abs} is SC charge for abnormal situation; SC_r is current SC charge; SC_a is SC charge for accident situation; P_{PZX} is probability that the difference between movement reserve and the remaining route length is less than

Table 1. Critical functions and their defining variables

Critical functions	**Arguments**	**Substantial description of variable**
Y_1 transportation profit	x_{11}	Average movement speed
	x_{12}	Current movement speed
	x_{13}	Route remainder to point 4
	x_{14}	Movement reserve
	x_{15}	Consumed gas amount
	x_{16}	Expenses value $(-W_{AB}C_{kWh} - Q_a)$
	x_{17}	Payment received from the customer for transportation
Y_2 estimated movement reserve	x_{21}	Average movement speed
	x_{22}	Average SC power consumption rate
	x_{23}	Energy amount stored in SC
	x_{24}	Total car weight
	x_{25}	Current speed
	x_{26}	Current power, consumed/recuperated in the battery
Y_3 energy amount in SC	x_{31}	Mechanical power at the shaft of the drive engines
	x_{32}	Generator charge power
	x_{33}	Power consumed by the refrigerator
	x_{34}	Power consumed by other systems
	x_{35}	Drive engine voltage

the accident level, $P_{PZX} = 1-(PZX_{2abs}-PZX_2)/(PZX_{2abs}-PZX_a)$, where PZX_{2abs} is difference of movement reserve for abnormal situation; PZX_2 is current movement reserve difference; PZX_a is difference of movement reserve for accident situation.

During the system operation process the information panel is displaying the information regarding the diagnostics process that allows the operator to receive timely information about the transition of functions SC_r and PZX_2 to the abnormal mode and to make well-timed decisions to suppress the reasons that lead to abnormal situations, accidents and catastrophes.

The danger level classification was done with 7 levels and is shown in Table 2.

Table 2. Danger level classification

Danger level	*Values*	*Description*
0	$[0;17]$	Safe situation
1	$[1/7;2/7)$	Abnormal situation by one parameter
2	$[2/7;3/7)$	Abnormal situation by several parameters
3	$[3/7;4/7)$	Accident threat observed
4	$[4/7;5/7)$	High accident threat
5	$[5/7;6/7)$	Critical situation
6	$[6/7;1)$	The chance to avoid accident is exceptionally small
7	1	Accident

A check is performed each step by comparing values forecasted p steps ahead with the maximum permissible values.

In this example the maximum permissible values were considered as:

1. Transportation profit: abnormal – 0,94, accident – 0,5.
2. Calculated movement reserve: abnormal – 1, accident – 0,4.
3. Voltage in storage cell: abnormal situation – 5 MJ, accident – 0.

Several results during an emerged abnormal situation are given in figure (see Fig.1) as a graphical distribution of time dependent functional dependencies Y_1 – transportation profit, Y_2 – calculated movement reserve, Y_3 – amount of energy in SC and respective risk levels $W_{yi}, i = 1, 2, 3$.

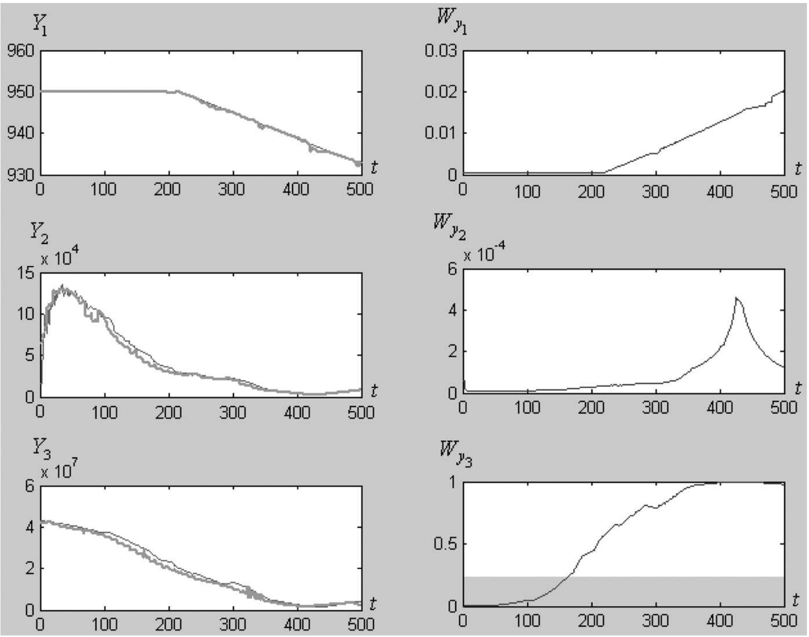

Figure 1. Distribution of time dependent functional dependencies Y_1 – transportation profit, Y_2 – calculated movement reserve, Y_3 – amount of energy in CEO and respective risk levels

6 Conclusion

A system strategy to estimation the guaranteed survivability and safety of CEO operation allows preventing the inoperativeness and abnormal situations. The real-time complex, system, and continuous estimation of the parameters of object operation detects situations that can bring the object out of the normal-mode operation. The simultaneous monitoring and integrated estimation of the parameters of a finite number of functionally dynamic parameters allow detailing the processes of object operation of any order of complexity. For situations that may cause deviations of the parameters from the normal mode of object operation, a timely decision can be made to change the mode of operation or to artificially correct some parameters getting the operation survivable. The principles that underlie the strategy of the guaranteed safety of CEO operation provide a flexible approach to timely detection, recognition, prediction, and system diagnostics of risk factors and situations, to formulation and implementation of a rational decision in a practicable time within an unremovable time constraint.

References

[1] N.D. Pankratova. *System strategy for guaranteed safety of complex engineering systems.* Journal Cybernetics and Systems Analysis, vol.46, no.2(2010), pp. 243–251.

[2] N.D. Pankratova, B.I. Kurilin. *Conceptual foundations of the system analysis of risks in dynamics of control of complex system safety.* P.2: The general problem of the system analysis of risks and the strategy of its solving. Journal Autom. Inform. Sci. vol.33, no.2(2001), pp. 1–14.

[3] N.D. Pankratova. *Safety operations of the complex engineering objects.* International Journal. "Information technologies & knowledge." ITHEA. SOFIA, V.5, N.2, 2011, pp. 152–167.

[4] N.D. Pankratova, A.N. Radjuk. *Guaranteed safety operation of complex engineering systems.* Continuous and Distributed Systems. Theory and Application. Springer, 2014, pp. 313–326.

[5] N.D. Pankratova. A*rational compromise in the system problem of disclosure of conceptual uncertainty.* Journal Cybernetics and Systems Analysis, vol.38, no.4(2002), pp. 618–631.

Nataliya Pankratova

Institute for Applied System Analysis of National Technical University of Ukraine
"Kiev Polytechnical Institute"
E–mail: *natalidmp@gmail.com*