SAFETY OPERATIONS OF THE COMPLEX ENGINEERING OBJECTS

Nataliya Pankratova

***Abstract**: The safety operations of the complex engineering objects on the basis of system control is realized. The essence of such control is systemically coordinated evaluation and adjustment of the operational survivability and safety during the functioning process of an object. The diagnostic unit, which is the basis of a safety control algorithm for complex objects in abnormal situations, is developed as an information platform of engineering diagnostics. By force of systematic and continuous evaluation of critical parameters of object's functioning in the real time mode, the reasons, which could potentially cause the object' tolerance failure of the functioning in the normal mode, are timely revealed.*

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

***ACM Classification Keywords**: H.4.2. INFORMATION SYSTEM APPLICATION: type of system strategy*
***Conference topic**: Applied Program Systems*

Introduction

The practice of the last decades of the last century suggests that the risks of man-made and natural disasters with the consequences of regional, national and global scale are continuously increasing [1], that is due to various objective and subjective conditions and factors [2]. Analysis of accidents and catastrophes can identify the most important causes and weaknesses of control principles for survivability and safety of complex engineering objects (CEO). One of such reasons is the peculiarities of the functioning of the diagnostic systems aimed to identify failures and malfunctions. This approach to safety precludes a possibility of a priori prevention of abnormal modes and as a consequence, there is the possibility of its subsequent transition into an accident and catastrophe.

Therefore, it is necessary to develop a new strategy to solve safety problems of modern CEO for various purposes. Here we propose a strategy that is based on the conceptual foundations of systems analysis, multicriteria estimation and risk forecasting [3]. The essence of the proposed concept is the replacement of a standard principle of identifying the transition from operational state of the object into inoperable one on the basis of detection of failures, malfunctions, defects, and forecasting the reliability of an object by a qualitatively new principle. The essence of this principle is the timely detection and elimination of the causes of an eventual transition from operational state of the object into inoperable one on the basis of systems analysis of multifactorial risk of abnormal situations, a reliable estimation of margin of permissible risk of different modes of complex engineering objects operation, and forecast the key indicators of the object survivability in a given period of its operation.

The processes of CEO functioning and processes of ensuring their safety are principally different. The first is focused on achieving the main production target of complex engineering systems, so they are focused on at all stages of a product's life cycle. The second is regarded as secondary by the defined category of specialists, because in their view, all the major issues of efficiency and reliability and, consequently, the safety of the products are resolved at the stages of its development, refinement, handling, testing. As a result, there are precedents when the developments of goals, objectives and requirements for safety and, above all, for a engineering diagnostics system have not proper justification. As a consequence, it turns out that the figures and properties of the created safety system do not correspond to real necessities of complex objects, which they must satisfy.

Thus, there is a practical necessity to qualitatively change the principles and the structure of operational-capability controls and the safety of modern engineering systems in real conditions of multifactor risk influence. First of all, the control of complex objects should be systemized which means that there should be system coordination of operability control and safety control not merely by the corresponding goals, tasks, resources, and expected results but also, importantly, by the immediacy and effectiveness of interaction in real conditions of abnormal situations. Such coordination should provide immediate and effective interaction between the mentioned control systems. On the one hand, an effectiveness of the safety system should be provided for timely detection of abnormal situations, evaluation of risk degree and level, and the definition of an permissible risk margin during the process of forming recommendations about immediate actions given to the decision maker. On the other hand, the system of operational capability control after receiving a signal about abnormal situations should, in an effective and operative manner, make a complex object ready for an emergency transition to an offline state and should make it possible to effect this transition within the limits of permissible risk. This can be achieved only under the condition that the system of engineering diagnostics fully complies with the timeliness and efficiency of personnel actions in case of emergencies. Namely: Diagnosis should provide such level of completeness, accuracy and timeliness of information about the state and changing of technologically hazardous processes, which will allow staff to prevent the transition of abnormal situation to an accident and catastrophe in time.

It must be noted that the requirement of timeliness is a priority, as the most accurate, most reliable information becomes unnecessary when it comes to staff after an accident or catastrophe. So there is a practical need of systemic coherence of diagnostic rates with the pace of work processes in different modes of complex engineering systems operation. Such coherence can be one of the most important conditions for ensuring the guaranteed safety for the objects with increasing the risk [4].

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

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

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

$$Y_k = \hat{Y}\ [T_k]; TX_k = \hat{X}[T_k];\ TU_k = \hat{U}[\ _k];\ \Xi_k = \hat{\Xi}[\ _k];$$

$$T_k = \{t_k \mid t_k > t_{k-1}\}; T_k \in T^{\pm}; T^{\pm} = \{t \mid t^{-} \le t \le t^{+}\}; Y = (Y_i \mid i = \overline{1,m}); X = (X_j \mid j = \overline{1,n});$$

$$U = (U_q \mid q = \overline{1,Q}); \Xi = (\Xi_p \mid p = \overline{1,P}) .$$

Here Y is a set of external parameters Y_i that includes technical, economic, and other indicators of system-function 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 $\Xi_p ; \hat{Y}[T_k]$, $\hat{X}[T_k]$, $\hat{U}[T_k]$ 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 provides, during the abnormal mode, the possibility of transition from the mode $\bar{\tilde{R}}_{tr}^{+}$ during the period $\breve{T}_{tr}^{\pm}$ to the normal mode till the critical moment T_{cr} of transition of abnormal mode becomes an accident or catastrophe. Here, the mode $\bar{\tilde{R}}_{tr}^{+}$ is controlled functioning mode conditioned by the control influence U_{tr} of a safety control system. During the time period $\breve{T}_{tr}^{\pm}$ this mode leads to the reduction of the abnormal mode R_{an} to the normal mode R_{nm} . The Mode $\bar{\tilde{R}}_{tr}^{+}$ is characterized by the following functional:

$$\breve{R}_{tr}^{+} : R_{an} \xrightarrow{U_{tr}} R_{nm}$$

which defines the process of the reduction 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 given quality indicators defined by the set Y . 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_i , 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, with mathematical definition is described in [4].

2. 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 of 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 period of operation 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 should be formed on the basis of the following principles [5]:

– 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 diagnosis 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 process of prevention 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 [5].

In particular, the consistency of the diagnosis 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.

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 continue for a long time. However, in real objects in view of existing technical diagnosis systems, oriented toward failure and malfunction detection, it is impossible to ensure that a malfunction or a failure will not appear within the next 5–10min. 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.

The general strategy of such an approach is shown in Fig. 1. There is incomplete, fuzzy information about the object functioning state at the moment $T_k \in T^{\pm}$. This information is not enough for decision making. This implies the significant property of such an approach. This property means that the situation analysis and decision making are provided not only in typical conditions of exact recognition of a normal or an abnormal system mode, but also in conditions where there is only fuzzy, incomplete information about a situation. It is significant that this strategy, in conditions of fuzzy information about a situation, allows one, if necessary, to make a timely decision on emergency stop of the system operation. In the following control strategy in blocks 1–3 there are realized procedures of complex object functioning diagnostics and analysis. In block 4, on the basis of the results of the execution of the procedures of blocks 2 and 3, of a normal functioning mode occurs. During this process, three possible variants of a complex object state are analyzed: the normal functioning mode remains (transition of a control to block 5.0); signs of a normal mode violation appears that make it possible to reveal that at time $T_k \in T^{\pm}$ the situation is abnormal (transition of a control to block 5.1); or at time $T_k \in T^{\pm}$ the situation becomes undefined (transition of a control to block 5.2).

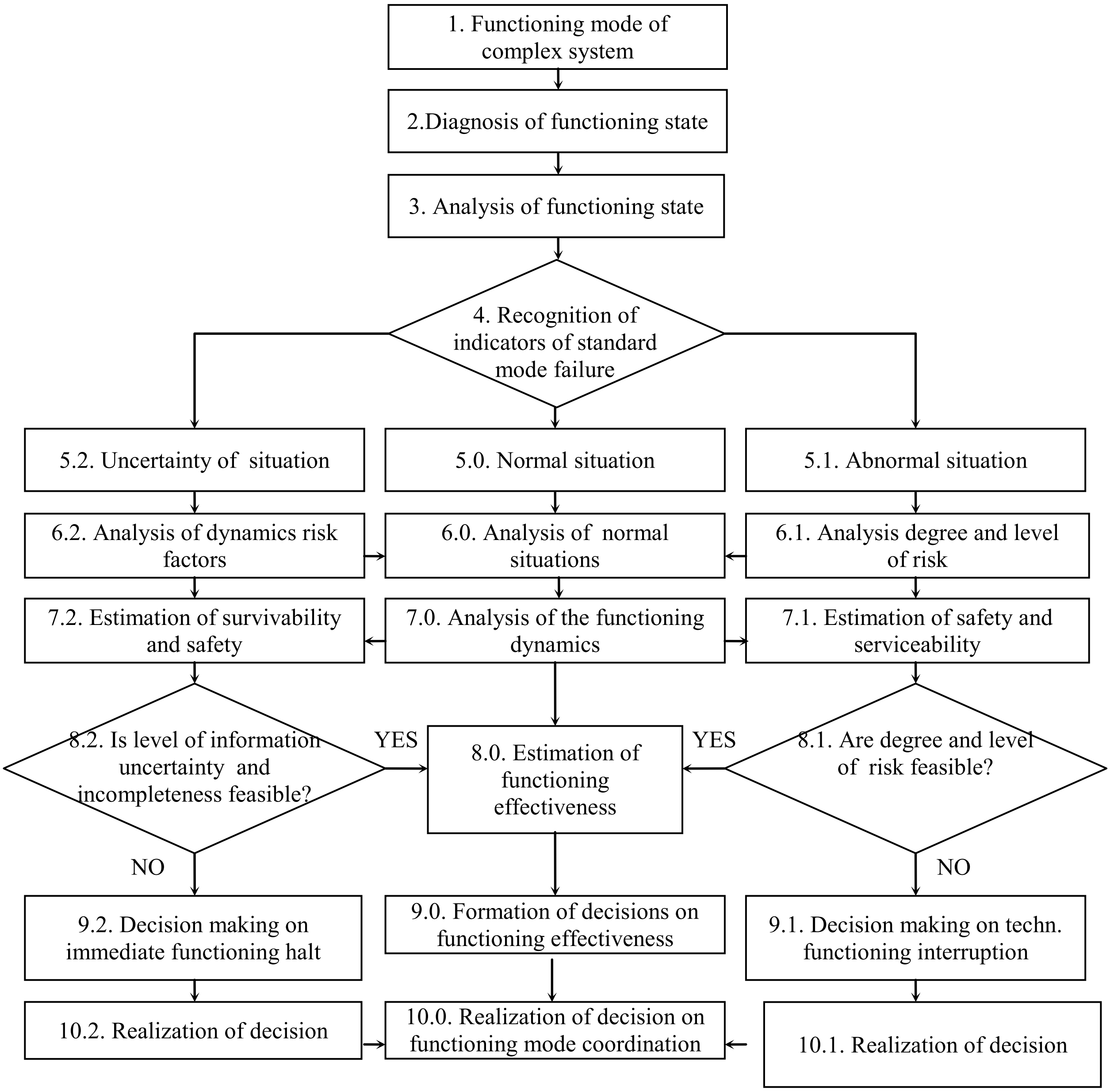

1. Functioning mode of complex system
2.Diagnosis of functioning state
3. Analysis of functioning state
4. Recognition of indicators of standard mode failure
5.2. Uncertainty of situation
5.0. Normal situation
5.1. Abnormal situation
6.2. Analysis of dynamics risk factors
6.0. Analysis of normal situations
6.1. Analysis degree and level of risk
7.2. Estimation of survivability and safety
7.0. Analysis of the functioning dynamics
7.1. Estimation of safety and serviceability
8.2. Is level of information uncertainty and incompleteness feasible?
YES
8.0. Estimation of functioning effectiveness
YES
8.1. Are degree and level of risk feasible?
NO
NO
9.2. Decision making on immediate functioning halt
9.0. Formation of decisions on functioning effectiveness
9.1. Decision making on techn. functioning interruption
10.2. Realization of decision
10.0. Realization of decision on functioning mode coordination
10.1. Realization of decision

Figure 1. Structural scheme of the system control strategy of a complex objects' serviceability and safety

In the first case the system operates in normal mode, and quality control is executed (6.0–10.0 units). In the second variant on the basis of the sequence of abnormal situations the following actions are realized. The risk degree and level of an abnormal situation sequence is analyzed, and the safety and operational capability of complex objects are evaluated (6.1–7.1 units) and a decision is made regarding the scheduled stop of the complex object functioning (transition of the control to the blocks 8.1–10.1) or a decision is made regarding the continuation of the complex object functioning if the values of risk degree and level are acceptable (transition of the control to block 8.0). In the third variant, an evaluation of survivability and safety of the system in conditions of uncertain information about abnormal situations is made. For this, the following sequence of operations is realized. An analysis is made of risk factors sequence of abnormal situations, on the basis of which the complex object survivability and safety are evaluated (6.2–7.2 units). If a certain uncertainty level and incompleteness level are acceptable, then the decision about the continuing functioning of an object is made (transition of the control to block 8.0). Otherwise, the decision on emergency stop of an object functioning is made (transition of the control to the blocks of 9.2, 10.2).

The strategy of system control of complex objects serviceability and safety is realized as an information platform of engineering diagnostics of the complex objects.

3. Information platform for engineering diagnostics of CES 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 [6] 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 diagnosis of abnormal situations;
- forecast of nonstationary processes;
- generation of the process of engineering diagnostics.

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 an 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, biased Chebyshev polynomials are taken as basic approximating functions, which normalizes 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 [6]. We will use the Chebyshev criterion and biased Chebyshev polynomials $T_{j_s p}(x_{j_s p}) \in [0,1]$. Such an approach reduces the procedure of forming the approximating functions to a sequence of Chebyshev approximation problems for inconsistent systems of linear equations [5].

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 $[d_{j_s}^-, d_{j_s}^+]$, 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 $N_{02} + N_2$. Figure 2 schematizes the sample for the instant of time $t = t_0, N_{02} = 40$ and $t = t_0 + \Delta t$ $(t = 1,2,3,...,t_k,...,T)$.

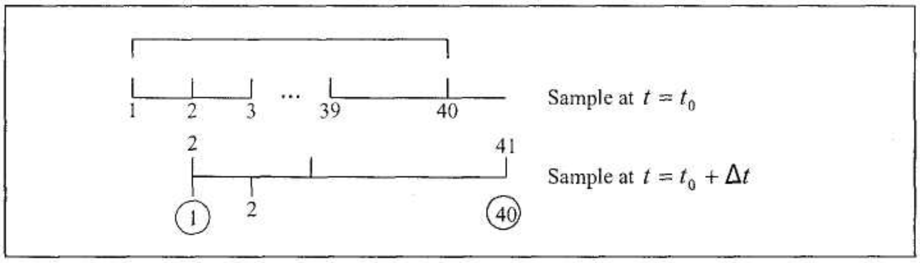


Figure 2. Sample at $t = t_0$ and $t = t_0 + \Delta t$

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.

A procedure of identification possible failure of sensors is based on the following thoughts. If the sensor functions are normal, each of his indications is not out of the threshold level. Any indication can be confirmed by previous and subsequent values. This is firstly connected with the nature of monitored processes: the majority of changes in the status process are not instantaneous. Therefore, the abrupt change in the sensor readings can be taken as evidence of failure of measuring devices. This approach is realized in the following way. At each step the arithmetic mean P of previous y_{i-1} and subsequent y_{i+1} measurements is calculated. Then we compare this value P with current value $y_i : \Delta = P - y_i$. If deviation Δ exceed of threshold level, then operator displays a message about a possible sensor's failure.

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.

Timely Diagnosis of Abnormal Situations. Timely diagnosis of abnormal situation is an important aspect of complex system. The possibility of prevention not only the result of abnormal situation, but also abnormal situation may reduce risk of disruption to a minimum. Therefore, several ways of work with abnormal situation was provided.

First, each value is obtained in a result of the recovery of functional dependence, compared with the threshold level of abnormal and emergency situation. In this case, having reached any of the indicators of such a boundary, a warning about the occurrence of the abnormal situation is appeared on the operator scoreboard. The reason of this situation and the current level of risk in the system are also indicated.

Also the reason of this situation and the current level of risk in the system are indicated. This approach allows us to monitor the immediate developments in the monitored system. From the standpoint of the algorithm it is described as fig. 3:

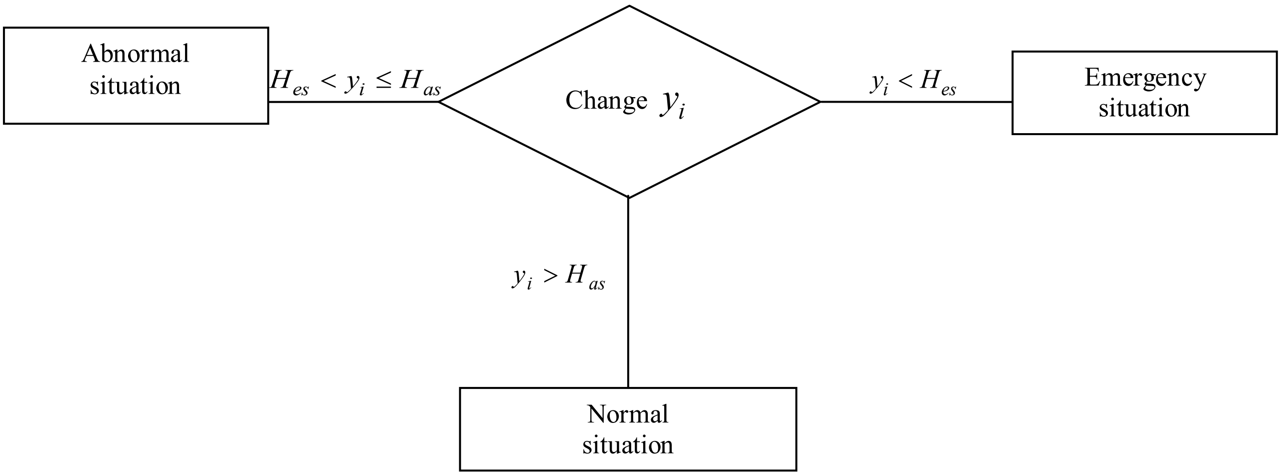


Fig. 3. Structural algorithm of timely diagnosis of abnormal situations

Secondly, for early detection of the possibility of the abnormal situation becoming a similar approach is used for the forecasted results. That is, after each step of forecasting, the obtained values are compared with the boundary values of the abnormal or emergency situation. The operator also receives all the information on the scoreboard. This allows to pass ahead of the abnormal situation for a few steps, and if possible to prevent it.

Thirdly, the operator can monitor the development of the system and to respond to negative trends in the process. For it the operator scoreboard displays the level of danger in the system and the current and predicted risk. The level of danger 7 means an emergency situation, levels 4, 5 and 6 indicates the abnormal one. Accordingly, levels 0–3 mean the normal functioning. In this case, as can be seen, the higher the risk, the closer the system to the emergency situation. If it is at danger level 3, the operator must be prepared for a possible deterioration of the process development and the transition to abnormal mode of operation. Using this approach operator gets several points of monitoring the system state. He can determine in advance the approximation of the emergency, he receives a warning when it is directly approaching, and he will be warned when the abnormal situation is happened, if it is not able to avoid it in time.

Forecast of Nonstationary Processes. Forecast of the critical parameters is done by using the method of coordinate descent and the degree of approximation to the sensors indicators according the algorithm:

- based on a number of values of input parameters currently using alternating-variable descent method, their predictive value in the future was calculated, system of equations has been solved

$$\begin{pmatrix} t^p & t^{p-1} & \dots & t^0 \\ t^p & t^{p-1} & \dots & t^0 \\ t^p & t^{p-1} & \dots & t^0 \\ t^p & t^{p-1} & \dots & t^0 \end{pmatrix} \cdot \begin{pmatrix} x_{1pr}^0 \\ x_{1pr}^1 \\ \dots \\ x_{1pr}^p \end{pmatrix} = \begin{pmatrix} x_1^0 \\ x_1^1 \\ \dots \\ x_1^p \end{pmatrix};$$

- with the found vector $\left(x_{1pr}^0 \quad x_{1pr}^1 \quad \dots \quad x_{1pr}^p\right)^T$ predicted value index of the k-th sensor at time t_{i+1} is given by $x_{kpr}(t_{i+1}) = \left(t^p \quad t^{p-1} \quad \dots \quad t^0\right) \cdot \begin{pmatrix} x_{1pr}^0 \\ x_{1pr}^1 \\ \dots \\ x_{1pr}^p \end{pmatrix} = \sum_{j=0}^{p} t^j x_{1pr}^{p-j}$;

- the functional dependences were recovered, which was the desired predicted values of objective functions.

The forecast was realised on 10 steps ahead, as forecasts for more of them are not appropriate since it is accumulated the error of solving method of equations system. Functional dependences for the values of incoming parameters recovered at each step to ensure the most accurate forecast in order not to miss a moment of possible becoming abnormal situation.

Setting up the Process of Engineering Diagnostics. We will use the system of CES operation models to describe the normal operation mode of the object under the following assumptions and statements.

- Each stage of CEO operation is characterized by the duration and by the initial and final values of each parameter y_i determined at the beginning and the end of the stage, respectively. The variations of y_i within the stage are determined by the corresponding model.
- All the parameters y_i are dynamically synchronous and in phase in the sense that they are simultaneously (without a time delay) increased or decreased under risk factors.

- The control $U = (U_j \mid j = \overline{1,m})$ is inertialess, i.e., there is no time delay between the control action and the object's response.
- The risk factors $\rho^{\tau}_{q_k} \mid q_k = \overline{1, n^{\tau}_k}$ change the effect on the object in time; the risk increases or decreases with time.
- The control can slow down the influences of risk factors or stop their negative influence on the controlled object if the rate of control exceeds the rate of increase in the influence of risk factors. The negative influence of risk factors is terminated if the decision is made and is implemented prior to the critical time T_{cr}. At this moment the risk factors cause negative consequences such as an accident or a catastrophe.

To analyze an abnormal mode, let us introduce additional assumptions as to the formation of the model and conditions of recognition of an abnormal situation.

- The risk factors $\rho^{\tau}_{q_k} \mid q_k = \overline{1, n^{\tau}_k}$ are independent and randomly vary in time with a priori unknown distribution.
- The risk factors can influence several or all of the parameters y_i simultaneously. A situation of the influence of risk factors is abnormal if at least two parameters y_i simultaneously change, without a control, their values synchronously and in phase during several measurements (in time).
- The influence of risk factors will be described as a relative change of the level of control. The values of each risk factor vary discretely and randomly.

We will recognize risk situations by successively comparing $\tilde{y}_i[t_k]$ for $\tilde{y}_i[t_k]$ several successive values of $t_k, k = \overline{1, k_0}$, where $k_0 = 3 \div 7$. As follows of the assumptions, the condition of a normal situation is synchronous and in phase changes of $\tilde{y}_i$ for several (in the general case, for all) parameters, whence follows a formula for different instants of time t_k for all of the values of i and for the same instants of time t_k for different values of i (different parameters):

$$\mathrm{sign}\Delta\tilde{y}_i[t_1, t_2] = \ldots = \mathrm{sign}\Delta\tilde{y}_i[t_k, t_{k+1}] = \ldots = \mathrm{sign}\Delta\tilde{y}_i[t_{k_0-1}, t_{k_0}], \tag{1}$$

$$\mathrm{sign}\Delta\tilde{y}_1[t_k, t_{k+1}] = \ldots = \mathrm{sign}\Delta\tilde{y}_i[t_k, t_{k+1}] = \ldots = \mathrm{sign}\Delta\tilde{y}_n[t_k, t_{k+1}], i = \overline{1,n}. \tag{2}$$

As follows from (1) and (2), given an abnormal situation on the interval $[t_1, t_{k_0}]$, the following inequalities hold simultaneously:

- the inequality of the signs of increment $\Delta\tilde{y}_i$ for all the adjacent intervals $[t_k, t_{k+1}]$ for $k = \overline{1, k_0}$ for each parameter $\tilde{y}_i, i = \overline{1,n}$;
- the inequality of the signs of increment $\tilde{y}_i, i = \overline{1,n}$, for all of the parameters $\tilde{y}_i$ for each interval $[t_k, t_{k+1}]$, $k = \overline{1, k_0}$.

4. Diagnostic of reanimobile's functioning

Contensive Statement of a Problem. The work of reanimobile, which moves in the operational mode, i.e. with the patient on board, is considered. Patient's life is provided with medical equipment, which is powered from the reanimobile's onboard electrical.

Basic equipment includes:

- ICE1 — basic internal combustion engine (ICE), which causes the car to move and rotate the main generator of G1;
- G1 — the main generator, with the capacity of 1.1KW that generates electricity when the angular velocity of crankshaft rotation is above 220 rad/sec (when the speed is above 220 rad/sec generator is switched on, when falls down 210 rad / s is off);
- TGB — transmission — gearbox (gear ratio: 1 — 4.05; 2 — 2.34; 3 — 1.39; 4 — 1; 5 — 0.85; main transmission — 5.125);
- ICE2 and T2 — auxiliary engine with a generator power of 1.1kW, which is used in emergency situations to provide power (standby ICE2 consumes fuel ICE2 0.5liters / hour);
- RB — rechargeable battery that provides power to the equipment when the generators do not generate electricity;
- PD — power distribution unit, which provides: battery charge, users' power from one of the generators, or from the battery, or the combination mode.

Tension in the on-board network depends on the generators and the level of battery charge. In the normal mode all equipment power is provided from the main generator and RB.

The main consumers, which are considered during the simulation:

- medical equipment, which consumes about 500 watts;
- illumination of the main cabin — 120 W;
- outdoor lighting (lights) — 110 W;
- car's own needs — 100 W.

Charge current is limited at the level that corresponds to the power extracted from the generator, equal to 200 watts. Reanimobile must travel a distance of 70 km. with a specific schedule of speed, which is formed by road situation.

It is required to ensure electric power for medical equipment, which is located in the main cabin. Since the motion is carried out at night, it is needed to provide additional coverage of the inner and outer. Kinematics parameters approximately correspond to the ambulances, based on GAZ.

Depending on the speed transmission, ratio is changed, therefore, the frequency of crankshaft rotation of the main internal combustion engine (ICE1) is changed. At the beginning of the way there are 47liters of fuel in the tank. Nutrition ICE1and ICE 2 are from the same tank. In normal situation, the car safely drives patient for 11,700 seconds (3 hours and 15 minutes). In this case, the battery voltage does not decrease less than 11.85V. At the end of the way there are 4.1liters of fuel in the tank.

Transition into abnormal mode is caused by malfunction of the charger, voltage sensor RB. It is assumed that the sensor gives out false information that the battery is fully charged. Since recharging RB is not done, then with the lapse of time the battery is discharged, and, consequently, the voltage on-board network on the intervals of generator outages (when switching gears, ICE1 idling) will also be decreased. Due to deep discharge the mode is occurred when the output voltage RB is not enough to maintain the medical equipment operability and this is an emergency situation.

The Recognition of an Abnormal Situation. The recognition of an abnormal situation occurs in accordance with prescribed critical values.

1) For stress in the on-board network: abnormal is 11.7V, emergency is10.5V

2) For the amount of fuel: abnormal is 21, and emergency is 11.

3) For the voltage at the rechargeable battery: an abnormal situation is 11.5V. Thus, while reducing the value of the function below one of the set values, the operation of reanomobile goes to an abnormal mode of functioning.

In other words, if Y_t < H critical exists, at the moment of time t CES functioning goes to an abnormal mode. Where Y_t is a predicted value for the recovered functional dependence. On the diagrams, this process can be observed in the form of decreasing a prediction level (pink curve) below the threshold of the abnormal mode (blue line).

Critical variables:

- Board voltage (depending on the parameters of the RB, the generators condition, the load current). This option could lead directly to an emergency, if the board voltage drops below trip level of medical equipment.
- Fuel level. Depends on the power, which is taken off from the main engine (made in proportion to rotation speed). Decline below a certain point can lead to abnormal (when you can call another car or refueling, and catering equipment from RB) or emergency mode (when the car made a stop for a long time without charging).
- Voltage RB (depending on the generators condition, the total electricity consumption).

Real-time monitoring of the technical diagnostics is conducted in the reanimobile operation process with the purpose of timely exposure of potentially possible abnormal situations and guaranteeing the survivability of the system's functioning. In compliance with the developed methodology of the guaranteed CTO functioning safety at the starting phase $t = t_0$, functional recovery $y_i = f_i(x_1,...,x_j,...)$ is performed using $N_{02} = 50$ given discrete samples of values y_1, y_2, y_3 and their arguments. Here $y_1 = Y_1(x_{11}, x_{12}, x_{13}, x_{14}), y_2 = Y_2(x_{21}, x_{22})$, and $y_3 = Y_3(x_{31}, x_{32}, x_{33})$, where x_{11} is the measured voltage RB; x_{12} is the velocity of crankshaft rotation; x_{13} is power, which is provided by auxiliary generator; x_{14} is the total power consumption; x_{21} is the velocity of crankshaft rotation; x_{22} is power, which is provided by auxiliary generator; x_{31} is the velocity of crankshaft rotation; x_{32} is power, which is provided by auxiliary generator; x_{33} is the total power consumption. All data on the variables $Y_i, i=1,2,3$ and their arguments $x_i, i=1,2,3$ are given as samples during the reanimobile's motion within 50000 seconds.

In this case, the voltage sensor gives false information about the voltage RB. When the voltage drops below 11.7V the diagnostic system provides a driver with the signal about an abnormal situation which can be developed into an emergency. The driver stops the car ($t=7323s$), switches on a standby generator ($t=7414s$) and eliminates the failure ($t=7863s$). Having recharged the battery from a standby generator when $t=8533s$, the driver turns off the standby generator and resumes the motion ($t=8623s$). Due to low battery, voltage at its terminals starts to decrease rapidly. The diagnostic system warns about abnormal situation again, to solve the problem the driver forcefully supports ICE1 speed at 250 rad/s, thus ensuring continued operation of the main generator.

As a result, fuel consumption is increased, which leads to the abnormal situation ($t=13000s$) when the amount of fuel is reduced to 1liter. At this moment of time the car is forcibly stopped by the signal of the diagnostics system (before reaching their destination) and a standby generator is switched on to provide the electric power supply (one liter of fuel is enough for 2 hours operation of standby generator that allows refuel the car or call for help).

The Risk Detection Procedure. Taking into account the specifics of operation of the system, following risk detection procedures were constructed. When reanimobile is functioning, possibility of abnormal situation is calculated with the formula

$$F(\rho_k)=1-(1-\rho_{Gv})(1-\rho_{Av})(1-\rho_F),$$

where ρ_{Gv} is the probability that the board voltage drops below the emergency level; ρ_{Av} is the probability that the battery voltage drops below the emergency level; ρ_F is a probability that the fuel level drops below the emergency level. ρ_{Gv}, ρ_{Av} and ρ_F are calculated in the following way:

$$\rho_{Gv}=1-\left|(H_{1an}-y_{1pr})\right|/\left|1{,}75*(H_{1an}-H_{1e})\right|; \quad H_{1an}\neq H_{1e},$$

$$\rho_F=1-\left|(H_{2an}-y_{2pr})\right|/\left|1{,}75*(H_{2an}-H_{2e})\right|; \quad H_{2an}\neq H_{2e},$$

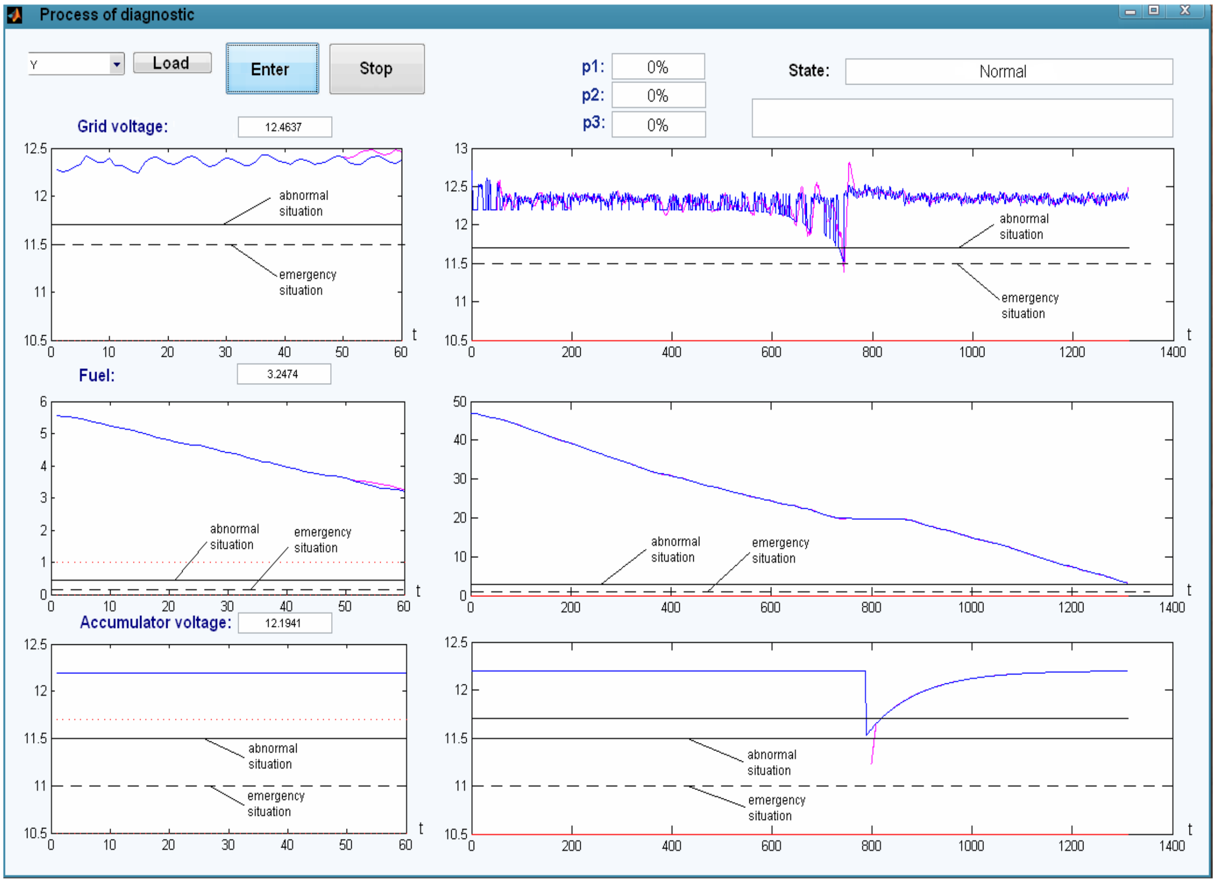
$$\rho_{Av}=1-\left|(H_{3an}-y_{3pr})\right|/\left|1{,}75*(H_{3an}-H_{3e})\right|; \quad H_{3an}\neq H_{3e},$$

where H_{1an} is board voltage in abnormal situations ($Y_{1r} \Leftarrow 11.7\text{V}$); y_{1pr} is the current board voltage (recovery functional dependence using forecast); H_{1e} is board voltage in an emergency ($Y_{1r} \Leftarrow 10.5\text{V}$); H_{2an} is the level of fuel in abnormal situations ($Y_{2r} \Leftarrow 1\text{L}$); y_{2pr} is the current value of the fuel (recovery functional dependence using forecast);

H_{2e} is the level of fuel in an emergency ($Y_{2r} = 0$); H_{3an} is a battery voltage in the abnormal mode ($Y_{3r} \Leftarrow 11.7\text{B}$); y_{3pr} is the current battery voltage ((recovery functional dependence using forecast); H_{3e} is a board voltage in an emergency ($Y_{3r} \Leftarrow 10.5\text{V}$).

This structure of risk was taken on the basis of the normalization behavior of the process in the interval (0,1). Design formula repelled by conditions: the risk during the emergency must be equal to 1, the risk at the border of abnormal mode should be equal to 0,4. In the result, the risks on all fronts are taken into account. The overall risk is 1 during the damage 0,5–0,6 at the border of the abnormal mode.

Some results of reanimobile's functioning during the first 7000 sec. are shown in Fig. 4 as the diagrams of stress distribution of the on-board network, the amount of fuel in the tank, the rechargeable battery voltage. The transition into abnormal mode happens due to failure of the sensor battery voltage. So far as the battery recharging is not implemented, the battery is discharged with the lapse of time and, consequently, the voltage in the on-board network in the period of 6500-7400 sec. is also decreased and transits into abnormal mode. The fuel level, which depends on the capacity of the internal combustion engine, is also reduced.



Process of diagnostic

Y

p1: 0%

p2: 0%

p3: 0%

State: Normal

Grid voltage: 12.4637

Fuel: 3.2474

Accumulator voltage: 12.1941

Figure 4. Stress distribution of the on-board network, the amount of fuel in the tank, the rechargeable battery voltage in accordance of time t sec.

At any time of the program operation user has the ability to look at the operator scoreboard, which displays a series of indicators that reflects the character of the state of CEO of the reanimobile functioning. This is such indicators as: indicators of sensors accumulator battery voltage, fuel quantity in the tank, the voltage on-board network, the state of the system, the risk of the damage, the causes of the abnormal or emergency mode, as well as the indicator of the danger level of the system operation and possible failure of sensors.

4. Conclusion

System coordination of survivability and safety control by the goals, objectives, resources and expected results, as well as by efficiency and effectiveness of interaction in the real conditions of abnormal situations allows to provide the effective and efficient interaction of these control systems. On the one hand, it is ensured the efficiency and effectiveness of safety systems according to timely detection of abnormal situations, estimation of its degree and level of risk, definition of the margin of permissible risk in the process of forming the recommendations for the prompt actions of the DM. On the other hand, the survivability control system must effectively and efficiently operate after receiving a signal about the abnormal situation to ensure the availability of a complex object for the emergency transition into abnormal mode and provide its realization within a margin of permissible risk.

The proposed strategy of system coordination of survivability and safety engineering objects operation, implemented as a tool of information platform of engineering diagnostics of the complex objects, ensures the prevention of inoperability and the danger of object’s functioning. By force of systematic and continuous evaluation of critical parameters of object’s functioning in the real time mode, the reasons, which could potentially cause the object’ tolerance failure of the functioning in the normal mode, are timely revealed. For situations, development of which leads to possible deviations of parameters from the normal mode of the object’s functioning, it is possible timely to make a decision about the change of the operation mode of the object, or an artificial correction of the parameters to prevent the transition from the normal mode into the abnormal one, accident and catastrophe.

The principles, which are included in the implementation of the guaranteed safety of CEO operation strategy, provide a flexible approach to timely detection, identification, forecasting and system diagnosis of factors and risk situations, formation and implementation of sustainable solutions during the acceptable time within the fatal time limit.

Bibliography

[1] Frolov K. V. (gen. ed.), Catastrophe Mechanics [in Russian], Intern. Inst. for Safety of Complex Eng. Syst., Moscow —1995. —389 p.

[2] Troshchenko V. T. (exec, ed.), Resistance of Materials to Deformation and Fracture: A Reference Book, Pts. 1, 2 [in Russian], Naukova Dumka, Kyiv. —1993, 1994. —702 p.

[3] Pankratova N.and Kurilin B., Conceptual foundations of the system analysis of risks in dynamics of control of complex system safety. P. 1: Basic statements and substantiation of approach // J. Autom. Inform. Sci. —2001. —33, №. 2. —P. 15-31.

[4] Zgurovsky M. Z., Pankratova N. D., System Analysis: Theory and Applications, Springer, Berlin. —2007. —475 p.

[5] Pankratova N.D., “System strategy for guaranteed safety of complex engineering systems”, Cybernetics and Systems Analysis 46, 2 (2010): 243-251.

[6] Pankratova N.D., “System approach to estimation of guaranteed safe operation of complex engineering systems”, International Book Series «Information science&computing». –New Trends in Information Technologies. ITHEA. SOFIA (2010):115-128.

Authors' Information

Nataliya Pankratova *– DTs, Professor, Depute director of Institute for applied system analysis, National Technical University of Ukraine “KPI”, Av. Pobedy 37, Kiev 03056, Ukraine; e-mail: natalidmp@gmail.com*

Major Fields of Scientific Research: System analysis, Theory of risk, Applied mathematics, , Applied mechanics, Foresight, Scenarios, Strategic planning, information technology