Chapter 22
Guaranteed Safety Operation of Complex Engineering Systems

Nataliya D. Pankratova and Andrii M. Raduk

Abstract A system strategy to estimation of guaranteed survivability and safety operation of complex engineering systems (CES) is proposed. The strategy is based on timely and reliable detection, estimation, and forecast of risk factors and, on this basis, on timely elimination of the causes of abnormal situations before failures and other undesirable consequences occur. The principles that underlie the strategy of the guaranteed safety operation of CES provide a flexible approach to timely detection, recognition, forecast, and system diagnostic of risk factors and situations, to formulation and implementation of a rational decision in a practicable time within an irremovable time constraint. The system control of complex objects is realized. The essence of such control is a 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.

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 security precludes a possibility of a priori prevention

N. D. Pankratova (✉) · A. M. Raduk
Institute for Applied System Analysis National Technical University of Ukraine "Kyiv Polytechnic Institute", Peremogy ave., 37, build, 35,
Kyiv 03056, Ukraine
e-mail: natalidmp@gmail.com

M. Z. Zgurovsky and V. A. Sadovnichiy (eds.), *Continuous and Distributed Systems*, Solid Mechanics and Its Applications 211, DOI: 10.1007/978-3-319-03146-0_22,

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 security 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 forecasting of risk [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 operation of complex technical objects, and forecast the key indicators of the object survivability in a given period of its operation.

22.1 Introduction

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 CES, so they are focused on 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 security 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 security and, above all, for a technical diagnostics system have not proper justification. As a consequence, it turns out that the figures and properties of the created security 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, the 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 when the system of technical 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 security for the objects with increasing the risk [4].

22.2 Information Platform of Engineering Diagnostics of the Complex Object Operation

The strategy of system control of complex objects survivability and safety is realized as an information platform of engineering diagnostics (IPED) of the complex objects The diagnostic unit, which is the basis of a safety control algorithm for complex

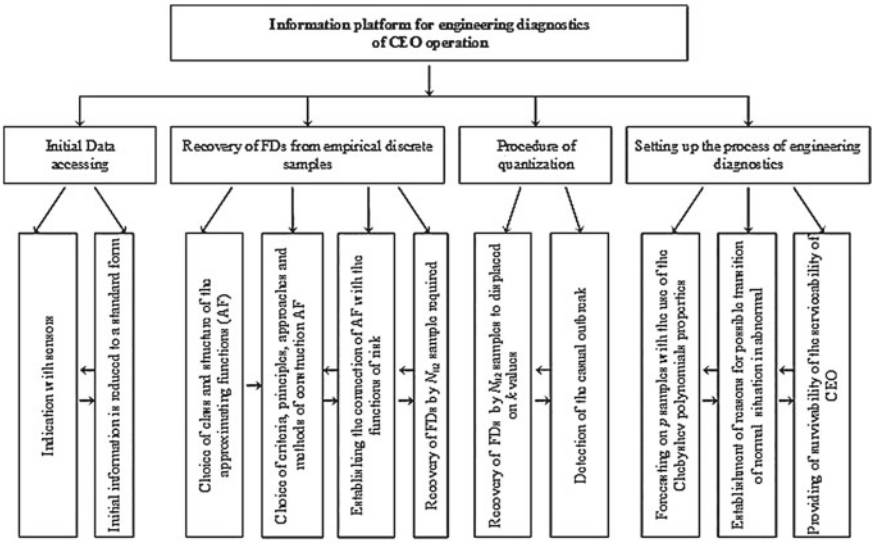


Fig. 22.1 Structural diagram of information platform for engineering diagnostics

objects in abnormal situations, is developed as an IPED (Fig. 22.1). Let us detail some of these modules of the IPED.

Data accessing of the Initial Information during CEO operation. By a CEO we mean an 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. With this purpose, groups of sensors are connected to each subsystem, which different parameters (time sampling, resolution, etc.), depending on what there 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 to estimate the functional dependences (FD's). The initial information is reduced to a standard form, which makes it possible to form FD's from discrete samples. In view of the proposed methodology, Chebyshev polynomials are taken as basic approximating functions, which normalize all the initial information to the interval [0, 1].

Recovery of Functional Dependences based on Discrete Samples. In the general case, the initial information is specified as a discrete array [5].

$$
\begin{gathered}
M_0 = \langle Y_0, X_1, X_2, X_3 \rangle, \\
Y_0 = (Y_i | i = \overline{1, m}), \;\; Y_i = (Y_i[q_0] | q_0 = \overline{1, k_0}), \\
X_1 = (X_{1j_1} | j_1 = \overline{1, n_1}), \;\; X_{1j_1} = (X_{1j_1}[q_1] | q_1 = \overline{1, k_1}), \\
X_2 = (X_{2j_2} | j_2 = \overline{1, n_2}), \;\; X_{2j_2} = (X_{2j_2}[q_2] | q_2 = \overline{1, k_2}), \\
X_3 = (X_{3j_3} | j_3 = \overline{1, n_3}), \;\; X_{3j_3} = (X_{3j_3}[q_3] | q_3 = \overline{1, k_3})
\end{gathered}
$$

where the set Y_0 determines the numerical values

$$
Y_i[q_0] \Rightarrow \langle X_{1j_1}[q_1], X_{2j_2}[q_2], X_{3j_3}[q_3] \rangle
$$

of the unknown continuous functions $y_i = f_i(x_1, x_2, x_3)$, $i = \overline{1, m}$, $x_1 = (x_{1j_1} \mid j_1 = \overline{1, n_1})$, $x_2 = (x_{2j_2} \mid j_2 = \overline{1, n_2})$, $x_3 = (x_{3j_3} \mid j_3 = \overline{1, n_3})$. To each value of $q_0 \in [1, k_0]$ corresponds a certain set $q_0 \Leftrightarrow (q_1, q_2, q_3)$ of values $q_1 \in [1, k_1]$, $q_2 \in [1, k_2]$, $q_3 \in [1, k_3]$. The set Y_0 consists of k_0 different values $Y_i\,[q_0]$. In the sets X_1, X_2, X_3 a certain part of values $X_{1j_1}\,[q_1]$, $X_{2j_2}\,[q_2]$, $X_{3j_3}\,[q_3]$, for some values $q_1 = \hat{q}_1 \in \hat{Q}_1 \subset [1, k_1]$, $q_2 = \hat{q}_2 \in \hat{Q}_2 \subset [1, k_2]$, $q_3 = \hat{q}_3 \in \hat{Q}_3 \subset [1, k_3]$, repeats each, but there are no completely coinciding sets $\left\langle X_{1j_1}\,[q_1]\,,\; X_{2j_2}\,[q_2]\,,\; X_{3j_3}\,[q_3] \right\rangle$ for different $q_0 \in [1, k_0]$. We have also $n_1 + n_2 + n_3 = n_0, n_0 \leq k_0$. It is known that $x_1 \in D_1$, $x_2 \in D_2$, $x_3 \in D_3, X_1 \in \hat{D}_1$, $X_2 \in \hat{D}_2, X_3 \in \hat{D}_3$, where

$$
D_s = \langle x_{s\,j_s} | d^-_{sj_s} \leq x_{sj_s} \leq d^+_{sj_s}, \;\; j_s = \overline{1, n_s} \rangle, \; s = \overline{1, 3};
$$

$$\hat{D}_s = \langle X_{sj_s} | \hat{d}^-_{sj_s} \le X_{sj_s} \le \hat{d}^+_{sj_s},\ j_s = \overline{1, n_s} \rangle,\ s = \overline{1, 3};$$

$$d^-_{sj_s} \le \hat{d}^-_{sj_s},\ d^+_{sj_s} \ge \hat{d}^+_{sj_s}.$$

It is required to find approximating functions $\Phi_i(x_1, x_2, x_3), i = \overline{1, m}$, that characterize the true functional dependences $y_i = f_i(x_1, x_2, x_3),\ i = \overline{1, m}$, on the set D_s with a practicable error.

Since the initial information is heterogeneous as well as the properties of the groups of factors under study, which are determined, respectively, by the vectors x_1, x_2, x_3, the degree of the influence of each group of factors on the properties of approximating functions should be evaluated independently. With this purpose, the approximating functions are formed as a hierarchical multilevel system of models. At the upper level, the model of determination of the approximating functions dependence on the variables x_1, x_2, x_3 is realized. Such a model in the class of additive functions, where the vectors x_1, x_2, x_3 are independent, is represented as the superposition of functions of the variables x_1, x_2, x_3:

$$\Phi_i(x_1, x_2, x_3) = c_{i1}\Phi_{i1}(x_1) + c_{i2}\Phi_{i2}(x_2) + c_{i3}\Phi_{i3}(x_3), i = \overline{1, m}. \tag{22.1}$$

At the second hierarchical level, models that determine the dependence $\Phi_{is}(s = 1, 2, 3)$ on the components of the variables x_1, x_2, x_3, respectively, and represented as

$$\begin{gathered}\Phi_{i1}(x_1) = \sum_{j_1=1}^{n_1} a^{(1)}_{ij_1}\Psi_{1j_1}(x_{1j_1}),\ \Phi_{i2}(x_2) = \sum_{j_2=1}^{n_2} a^{(2)}_{ij_2}\Psi_{2j_2}(x_{2j_2}),\\ \Phi_{i3}(x_3) = \sum_{j_3=1}^{n_3} a^{(3)}_{ij_3}\Psi_{3j_3}(x_{3j_3}).\end{gathered} \tag{22.2}$$

are formed.

At the third hierarchical level, models that determine the functions $\Psi_{1j_1}, \Psi_{2j_2}, \Psi_{3j_3}$ are formed, choosing the structure and components of the functions $\Psi_{1j_1}, \Psi_{2j_2}, \Psi_{3j_3}$ being the major problem. The structures of these functions are similar to (22.2) and can be represented as the following generalized polynomials:

$$\Psi_{sj_s}(x_{j_s}) = \sum_{p=0}^{P_{j_s}} \lambda_{j_s p}\varphi_{j_s p}(x_{sj_s}), \quad s = 1, 2, 3. \tag{22.3}$$

In some cases, forming the structure of the models, it should be taken into account that the properties of the unknown functions $\Phi_i(x_1, x_2, x_3), i = \overline{1, m}$, are influenced not only by a group of components of each vector x_1, x_2, x_3 but also by the interaction of their components. In such a case, it is expedient to form the dependence of the approximating functions on the variables x_1, x_2, x_3 in a class of multiplicative functions, where the approximating functions are formed by analogy with (22.1)–(22.3) as a hierarchical multilevel system of models

$$[1+\Phi_i(x)]=\prod_{s=1}^{S_0}[1+\Phi_{is}(x_s)]^{c_{is}};\quad [1+\Phi_{is}(x_s)]=\prod_{j_s=1}^{n_s}[1+\Psi_{sj_s}(x_{sj_s})]^{a^s_{ij_s}};$$
$$[1+\Psi_{sj_s}(x_{sj_s})]=\prod_{p=1}^{P_{j_s}}[1+\varphi_{j_sp}(x_{sj_s})]^{\lambda_{j_sp}}. \tag{22.4}$$

The Chebyshev criterion will be used and for the functions φ_{j_sp}, biased Chebyshev polynomials $T_{j_sp}(x_{j_sp})\in[0,1]$ will be used. Then the approximating functions based on the sequence $\Psi_1,\Psi_2,\Psi_3\to\Phi_{i1},\Phi_{i2},\Phi_{i3}\to\Phi_i$ which will allow obtaining the final result by aggregating the corresponding solutions are found. 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 to forming 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 allow 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 formed solution. The procedure of quantization of discrete numerical values is implemented as follows.

As the base reference statistic for each variable $x_1,\dots,x_n,y_1,\dots,y_m$, 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 22.2 schematizes the sample for the instant of time $t=t_0$, $N_{02}=40$ and $t=t_0+\Delta t\,(t=1,2,3,\dots,t_k,\dots,T)$.

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}.

Forecasting Nonstationary Processes. The models for forecasting nonstationary processes are based on the original sample of the time series for the initial interval D_0 and base dynamic model of processes (22.1)–(22.3). To this end, we will use the well-known property of Chebyshev polynomials that functions are uniformly approximated on the interval [0, 1]. The essence of the approach is as follows. The initial data are normalized for the interval $D=\{t|t_0^-\leq t\leq t^+\}$, $D=D_0\cup D_0^+$, which includes the initial observation interval $D_0=\{t|t_0^-\leq t\leq t^+\}$ and the prediction interval $D_0^+=\{t|t_0^+<t\leq t^+\}$. Then, to determine the dynamic model of the processes as the estimated approximating functions (22.1) or (22.4), based on the initial data, the system of equations is formed for the interval D_0. The dynamic

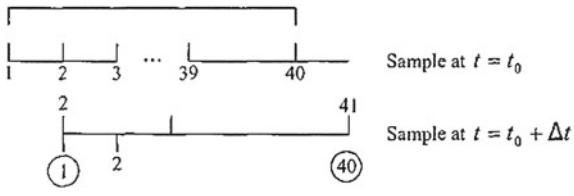


Fig. 22.2 Sample at $t=t_0$ and $t=t_0+\Delta t$

forecasting model is based on the extrapolation of approximating functions for the interval D_0 to the interval D_0^+ [5].

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 simultaneously (without a time delay) increase or decrease under risk factors.
- The control $U = (U_j | j = \overline{1, m})$ is inertialless, i.e., there is no time delay between the control action and the object's response.
- The risk factors $\rho_{q_k}^{\tau} | q_k = \overline{1, n_k^{\tau}}$ 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 provides the decision making prior implementation 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 according to the formation of the model and conditions of recognition of an abnormal situation.

- The risk factors $\rho_{q_k}^{\tau} | q_k = \overline{1, n_k^{\tau}}$ are independent and randomly vary in time with a priori unknown distribution.
- The risk factors can influence on 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 are simultaneously changed, without a control, their values are synchronous and are 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 are varied discretely and randomly.

Based on acceptable assumptions, let us present additional models and conditions to detect an abnormal situation. Denote by $\tilde{y}_i$ the value of the parameter y_i is influenced by the risk factors; $F_i(\rho_{q_k})$ is the function that takes into account the level of influence of the risk factors on the i parameter y_i; ρ_{q_k} is the value of the q risk factor at the instant of time t_k.

According to item 8, it is assumed that the value of $\tilde{y}_i[t_k]$ at the instant of time t_k is determined by

$$\tilde{y}_i[t_k] = \frac{1}{m} \sum_{j=1}^{m} \tilde{b}_{ij} \sum_{r=0}^{R_j} a_{jr} T_r^*(U_j); \quad \tilde{b}_{ij} = b_{ij} \cdot F_i(\rho_{q_k}), \tag{22.5}$$

where the function $F_i(\rho_{q_k})$ should correspond to the condition where $\tilde{y}_i = y_i$ in the absence of the influence of risk factors (i.e., for $\rho_{q_k} = 0$). Therefore, one of the elementary forms of the function $F_i(\rho_{q_k})$ is

$$F_i(\rho_{q_k}) = 1 - \prod_{q_k=1}^{n_{q_k}} (1 - c_{iq_k}\rho_{q_k}).$$

Note that risk factors can vary in time continuously (for example, pressure continuously changes as an aircraft lifts) or abruptly (for example, during cruise flight at a certain height, pressure may be changed abruptly at the cyclone-anticyclone interface). The most complex is the case where one risk factor varies continuously and others vary abruptly.

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 from item 2 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):

$$\operatorname{sign}\Delta\tilde{y}_i[t_1, t_2] = \ldots = \operatorname{sign}\Delta\tilde{y}_i[t_k, t_{k+1}] = \ldots = \operatorname{sign}\Delta\tilde{y}_i[t_{k_0-1}, t_{k_0}], \tag{22.6}$$

$$\operatorname{sign}\Delta\tilde{y}_1[t_k, t_{k+1}] = \ldots = \operatorname{sign}\Delta\tilde{y}_i[t_k, t_{k+1}] = \ldots = \operatorname{sign}\Delta\tilde{y}_n[t_k, t_{k+1}], i = \overline{1, n}. \tag{22.7}$$

As follows from (22.6) and (22.7), 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 $[t_k, t_{k+1}]$, $k = \overline{1, k_0}$.

Conditions (22.6) and (22.7) are rigid; for practical purposes, it will enough to satisfy the conditions for the representative number (22.3)–(22.5), which determine the parameters $\tilde{y}_i$ but not for all parameters i. The corresponding quantities in (22.6) and (22.7) are defined by

$$\Delta\tilde{y}_i[t_k, t_{k+1}] = \tilde{y}_i[t_{k+1}] - \tilde{y}_i[t_k], \tag{22.8}$$

where $\tilde{y}_i[t_k]$ are defined by (22.5); it is assumed that $\rho_{q_k}[t_{k+1}] > \rho_{q_k}[t_k]$ i.e., the dependence of each risk factor is a function of time, which increases, or $\rho_{q_k}[t_{k+1}] < \rho_{q_k}[t_k]$ i.e., the dependence is a decreasing function.

The practical importance of recognizing an abnormal situation based on (22.6) and (22.7) is in the minor alteration of $\tilde{y}_i[t_k]$ subject to risk factors since the "indicator" of the change is the sign of the difference in (22.6) and (22.7) rather than the

value defined by (22.8). In other words, such an approach is much more sensitive than typical approaches used in diagnostics. Moreover, it allows "filtering" random changes and random measurement errors $\tilde{y}_i$ for separate i according to (22.8) or for individual $[t_k, t_{k+1}]$ according to (22.7).

22.3 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 [6].

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 1.1 kW that generates electricity when the angular velocity of crankshaft rotation is above 220 rad/s (when the speed is above 220 rad/s 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 1.1 kW, which is used in emergency situations to provide power (standby ICE2 consumes fuel ICE2 0.5 l/h);
- 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 W;
- 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 W. 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 is changed (ICE1). At the beginning of the way there are 471 of fuel in the tank. Nutrition ICE1 and ICE2 are from the same tank. In normal situation, the car safely drives patient for 11,700 s (3 h and 15 min). In this case, the battery voltage does not decrease less than 11.85 V. At the end of the way there are 4.11 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 (while switching gears, ICE1 is 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 11.7 V, emergency is 10.5 V
2) For the amount of fuel: abnormal is 21, and emergency is 11.
3) For the voltage at the rechargeable battery: an abnormal situation −11.5 V. 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 $y_i = f_i(x_1, \ldots, x_j, \ldots)$ 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 50,000 s.

In this case, the voltage sensor gives false information about the voltage RB. When the voltage drops below 11.7 V 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 ($t = 7{,}323$ s), switches on a standby generator ($t = 7{,}414$ s) and eliminates the failure ($t = 7{,}863$ s). Having recharged the battery from a standby generator when $t = 8{,}533$ s, the driver turns off the standby generator and resumes the motion ($t = 8{,}623$ s). 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 ($t = 13{,}000$ s) when the amount of fuel is reduced to 1 l. 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 h 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:

$$\begin{aligned}
\rho_{Gv} &= 1 - \left|(H_{1es} - y_{1pr})\right| / \left|1,75 * (H_{1es} - H_{1a})\right|; H_{1es} \neq H_{1a};\\
\rho_{Av} &= 1 - \left|(H_{3es} - y_{3pr})\right| / \left|1,75 * (H_{3es} - H_{3a})\right|; H_{3es} \neq H_{3a};\\
\rho_F &= 1 - \left|(H_{2es} - y_{2pr})\right| / \left|1,75 * (H_{2es} - H_{2a})\right|; H_{2es} \neq H_{2a},
\end{aligned}$$

where H_{1es} is board voltage in emergency situations ($Y_{1r} \Leftarrow 11.7$ V); y_{1pr} is the current board voltage (recovery functional dependence using forecast); H_{1a} is board voltage in an emergency ($Y_{1r} \Leftarrow 10.5$ V); H_{2es} is the level of fuel in emergency situations ($Y_{2r} \Leftarrow 1$ L); y_{2pr} is the current value of the fuel (recovery functional dependence using forecast); H_{2a} is the level of fuel in an emergency ($Y_{2r} = 0$); H_{3es} is a battery voltage in the abnormal mode ($Y_{3r} \Leftarrow 11.7$ B); y_{3pr} is the current battery

voltage ((recovery functional dependence using forecast); H_{3a} is a board voltage in an emergency ($Y_{3r} \Leftarrow 10.5$ V).

This structure of risk was taken on the basis of the normalization behavior of the process in the interval (0,1). Create the 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 7,000 s. are shown in Fig. 22.3 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 conducted, the battery is discharged with the lapse of time and, consequently, the voltage in the on-board network in the period of 6,500–7,400 s is also decreased and transits into abnormal mode. The fuel level, which depends on the capacity of the ICE, is also reduced.

At any time of the program operation user has the ability to look at the operator scoreboard (Fig. 22.4), which displays a series of indicators that reflects the character of the state of CEO of the reanimobile functioning. These are 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.

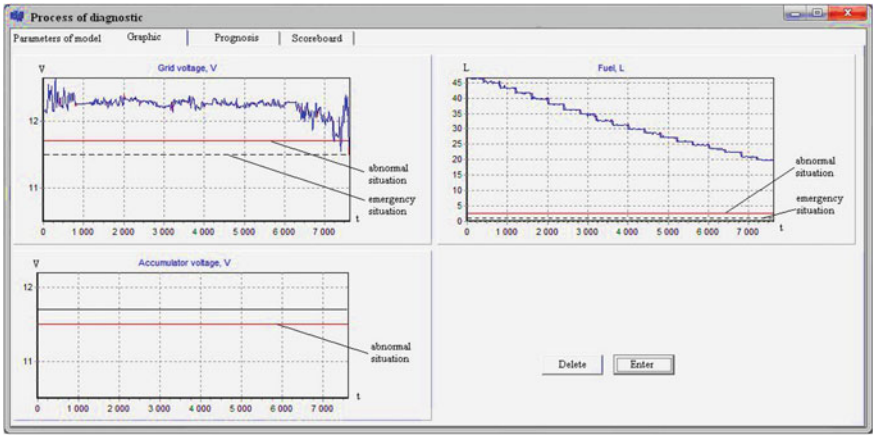
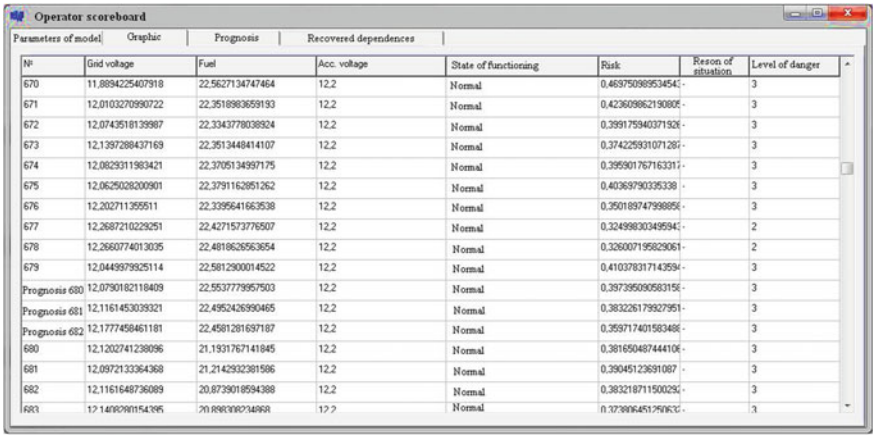
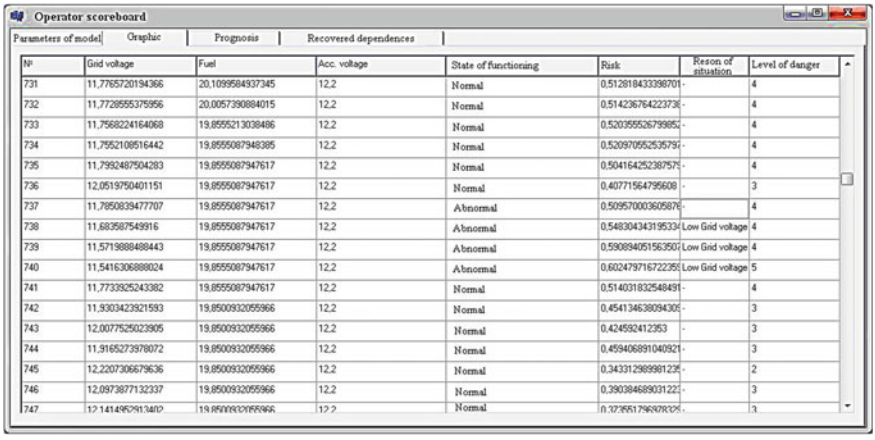


Fig. 22.3 Distribution of the on-board network, the amount of fuel in the tank, the rechargeable battery voltage in accordance of time *t*



№	Grid voltage	Fuel	Acc. voltage	State of functioning	Risk	Reson of situation	Level of danger
670	11,8894225407918	22,5627134747464	12,2	Normal	0,469750989534543		3
671	12,0103270990722	22,3518983659193	12,2	Normal	0,423609862190805		3
672	12,0743518139987	22,3343778038924	12,2	Normal	0,399175940371926		3
673	12,1397288437169	22,3513448414107	12,2	Normal	0,374225931071287		3
674	12,0829311983421	22,3705134997175	12,2	Normal	0,395901767163317		3
675	12,0625028200901	22,3791162851262	12,2	Normal	0,40369790335338		3
676	12,2027113555511	22,3395641663538	12,2	Normal	0,350189747998959		3
677	12,2687210229251	22,4271573776507	12,2	Normal	0,324998303495943		2
678	12,2660774013035	22,4818626563654	12,2	Normal	0,326007195829061		2
679	12,0449979925114	22,5812900014522	12,2	Normal	0,410378317143594		3
Prognosis 680	12,0790182118409	22,5537779957503	12,2	Normal	0,397395090583159		3
Prognosis 681	12,1161453039321	22,4952426990465	12,2	Normal	0,383226179927951		3
Prognosis 682	12,1777458461181	22,4581281697187	12,2	Normal	0,359717401583488		3
680	12,1202741238096	21,1931767141845	12,2	Normal	0,381650487444106		3
681	12,0972133364368	21,2142932381586	12,2	Normal	0,39045123691087		3
682	12,1161648736089	20,8739018594388	12,2	Normal	0,383218711500292		3
683	12,1469891154395	20,8883082344868	12,2	Normal	0,373890451259632		3

Fig. 22.3 (continued)



№	Grid voltage	Fuel	Acc. voltage	State of functioning	Risk	Reson of situation	Level of danger
731	11,7765720194366	20,1099584937345	12,2	Normal	0,512818433398701		4
732	11,7728555375956	20,0057390884015	12,2	Normal	0,514236764223736		4
733	11,7568224164068	19,8555213038486	12,2	Normal	0,520355526799852		4
734	11,7552108516442	19,8555087948385	12,2	Normal	0,520970552535797		4
735	11,7992487504283	19,8555087947617	12,2	Normal	0,504164252387575		4
736	12,0519750401151	19,8555087947617	12,2	Normal	0,40771564795608		3
737	11,7850839477707	19,8555087947617	12,2	Abnormal	0,509570003605876		4
738	11,683587549916	19,8555087947617	12,2	Abnormal	0,548304343195334	Low Grid voltage	4
739	11,5719888488443	19,8555087947617	12,2	Abnormal	0,590894051563507	Low Grid voltage	4
740	11,5416306888024	19,8555087947617	12,2	Abnormal	0,602479716722359	Low Grid voltage	5
741	11,7733925243382	19,8555087947617	12,2	Normal	0,514031832548491		4
742	11,9303423921593	19,8500932055966	12,2	Normal	0,454134638094305		3
743	12,0077525023905	19,8500932055966	12,2	Normal	0,424592412353		3
744	11,9165273978072	19,8500932055966	12,2	Normal	0,459406891040921		3
745	12,2207306679636	19,8500932055966	12,2	Normal	0,343312989981235		2
746	12,0973877132337	19,8500932055966	12,2	Normal	0,390384689031223		3
747	12,1414952913402	19,8500932055966	12,2	Normal	0,373651296878354		3

Fig. 22.4 Scoreboard of diagnostic process

22.4 Conclusion

System coordination of survivability and safety control on 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 security 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 to make a timely 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 CES 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.

References

1. Frolov, K.V.: Catastrophe Mechanics [in Russian]. Internship Institute for Safety of Complex Engineering System, Moscow (1995)
2. Troshchenko, V.T.: Resistance of Materials to Deformation and Fracture: A Reference Book. Pts. 1, 2 [in Russian]. Naukova Dumka, Kyiv (1993, 1994)
3. Pankratova, N., 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. Autom. Inform. Sci. **33**(2), 15–31 (2001)
4. Zgurovsky, M.Z., Pankratova, N.D.: System Analysis: Theory and Applications. Springer, Berlin (2007)
5. Pankratova, N.D.: System strategy for guaranteed safety of complex engineering systems. Cybern. Syst. Anal. **46**(2), 243–251 (2010)
6. Raduk, A.M.: System evaluation of the complex technical systems functioning. Syst. Res. Inf. Technol. **1**, 81–94 (2010)