SYSTEM STRATEGY FOR GUARANTEED SAFETY OF COMPLEX ENGINEERING SYSTEMS

N. D. Pankratova

A system strategy of guaranteed safe operation of complex engineering systems 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.

Keywords: *system strategy, multifactorial risks, abnormal mode, diagnostics, survivability, serviceability, safety.*

INTRODUCTION

The analysis of failures and accidents reveals their most important causes and the shortcomings of the existing principles of control of serviceability and safety of modern plant and machinery [1, 2]. One of such causes is the specific operation of diagnostic systems intended to detect failures and malfunctions. Such an approach to safety excludes a priori prevention of abnormal mode, which thus may become an abnormality, accident, or a catastrophe. Therefore, there is a practical need to qualitatively change the diagnostic system to account for the principles and structure of control of serviceability and safety of modern complex engineering systems (CESs) under the real conditions of multifactorial risks.

The purpose of the paper is to propose a system strategy for the guaranteed safety operation of a CES as a unified complex of a methodology of serviceability and safety and its implementation as a toolkit of technical diagnostics of the CES while in service.

1. MAIN PRINCIPLES OF PROBLEM SOLUTION AND REALIZATION STRATEGY

The system strategy to guarantee the safety of a CES is based on the proposed principle of timely detection of causes of abnormal situations, prompt prevention of regular situations from becoming abnormal or emergency, revealing risk factors,

predicting basic survivability parameters of an object during a specified period of its operation as fundamentals of the guaranteed safety in the CES dynamics, eliminating the causes of possible nonserviceability based on systems analysis of multifactorial risks of abnormal situations [3].

The key idea of the strategy is to provide (under actual conditions of the operation of a complex system) timely and reliable detection and estimation of risk factors, prediction of their development during a certain period of operation, and timely elimination of the causes of abnormal situations before failures and other undesirable consequences occur.

Strategy realization is based on the following principles:

- system consistency in purposes, problems, resources, and expected results as to the measures of providing safety operation of the complex system;
- timely detection, guaranteed recognition, and system diagnostics of risk factors and situations;
- prompt forecasting, reliable assessment of abnormal situations;
- formation and realization of a rational solution in a practicable time within an unremovable time constraint.

Let us formulate the mathematical problem of recognizing an abnormal situation in the dynamics of a dangerous industrial object.

For each situation $S_k^\tau \in S_\tau$, the set $M_k^\tau \in M_\tau$ of risk factors is known to be formed as $M_k^\tau = \{\rho_{q_k}^\tau \mid q_k = \overline{1, n_k^\tau}\}$. For each risk factor $\rho_{q_k}^\tau \in M_k^\tau$, given are a fuzzy information vector $I_q^\tau = \{I_{q_k}^\tau \mid q_k = \overline{1, n_k^\tau}; k = \overline{1, K_\tau}\}$ and its components:

$$I_{q_k}^\tau = \{\tilde{x}_{q_k j_k p_k}^\tau \mid q_k = \overline{1, n_k^\tau}; j_k = \overline{1, n_{q_k}^\tau}; p_k = \overline{1, n_{q_k j_k}^\tau}\};$$

$$\tilde{x}_{q_k j_k p_k}^\tau = \left\langle x_{q_k j_k p_k}^\tau, \mu_{H_{q_k j_k p_k}}\left(x_{q_k j_k p_k}^\tau\right)\right\rangle; x_{q_k j_k p_k}^\tau \in H_{q_k j_k p_k}^\tau; \mu_{H_{q_k j_k p_k}} \in [0,1];$$

$$H_{q_k j_k p_k}^\tau = \left\langle x_{q_k j_k p_k}^\tau \mid x_{q_k j_k p_k}^- \le x_{q_k j_k p_k}^\tau \le x_{q_k j_k p_k}^+ \right\rangle.$$

For each situation $S_k^\tau \in S_\tau$ and each risk factor $\rho_{q_k}^\tau \in M_k^\tau, M_k^\tau \in M_\tau$, it is

necessary to recognize an abnormal situation in the dynamics of a dangerous industrial object and ensure the survivability of the complex system during its operation.

We will consider the safety of a system as its ability to timely prevent the normal operation mode from becoming an abnormal one, an accident, or a catastrophe based on prompt detection of significant risk and to prevent it from becoming a catastrophic risk. The safety is characterized by the following parameters: the degree of risk η_i which is the probability of undesirable consequences; risk level W_i, which is the damage because of undesirable consequences of any risk factors at any instant of time $T_i \in T^{\pm}$ during the operation of the complex system; resource of the admissible risk of abnormal mode T_{pr}, which is the period of operation of the complex system in a certain mode during which the degree and level of risk do not exceed a priori specified admissible values. The safety parameters are evaluated by solving the general problem of analysis of multifactorial risks [4, 5].

The system consistency of the rates of diagnostics and the rates of processes in various operation modes of CES is provided by a unified algorithm for safety control in abnormal situations [6]. This algorithm implements procedures of diagnostics and assessment of abnormal situations during the transition from the normal mode into a sequence of abnormal situations. Based on this, a database and a scenario of a sequence of abnormal situations are formed, and the possibility whereby the complex object passes from abnormal situations to the normal mode is determined.

The strategy of system control of CES serviceability and safety is realized based of a diagnostic unit as an information platform of engineering diagnostics of the CES.

2. 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 that contains the following modules:

(i) acquisition and processing of the initial information during the CES operation;

(ii) estimation of functional dependences (FDs) and revealing patterns from empirical discrete samples;

(iii) quantization of the initial variables;

(iv) forecast of nonstationary processes;

(v) 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 CES Operation. By a CES 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. To this end, groups of sensors are connected to each subsystem, each having different parameters (time sampling, resolution, etc.), depending on what is its nature.

The engineering diagnostics during the CES operation requires samples of size N_{01} and N_{02}, where $N_{01}(N_{01} >> 200)$ is the total sample size during the CES 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 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].

Estimation of Functional Dependences based on Discrete Samples. In the general case, the initial information is specified as a discrete array [7]

$$M_0 = \langle Y_0, X_1, X_2, X_3 \rangle,$$

$$Y_0 = (Y_i \mid i = \overline{1,m}), Y_i = (Y_i[q_0] \mid q_0 = \overline{1,k_0});$$

$$X_1 = (X_{1j_1} \mid j_1 = \overline{1,n_1}), X_{1j_1} = (X_{1j_1}[q_1] \mid q_1 = \overline{1,k_1});$$

$$X_2 = (X_{2j_2} \mid j_2 = \overline{1,n_2}), X_{2j_2} = (X_{2j_2}[q_2] \mid q_2 = \overline{1,k_2});$$

$$X_3 = (X_{3j_3} \mid j_3 = \overline{1,n_3}), X_{3j_3} = (X_{3j_3}[q_3] \mid q_3 = \overline{1,k_3}),$$

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 $q_0 \in [1,k_0]$ there corresponds a certain set $q_0 \Rightarrow \langle q_1, q_2, q_3 \rangle$ of values $q_1 \in [1,k], q_2 \in [1,k_2], q_3 \in [1,k_3]$. 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 $\langle X_{1j_1}[q_1], X_{2j_2}[q_2], X_{3j_3}[q_3] \rangle$ for different $q_0 \in [1,k_0]$. We have also $n_1 + n_2 + n_3 = n_0, n_0 \le k_0$.

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

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

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. To this end, the approximating functions are formed as a hierarchical multilevel system of models. At the upper level, the model determining the dependence of the approximating functions 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:

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

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

$$\Phi_{i1}(x_1) = \sum_{j_1=1}^{n_1} a_{ij_1}^{(1)} \Psi_{1j_1}(x_{1j_1}), \Phi_{i2}(x_2) = \sum_{j_2=1}^{n_2} a_{ij_2}^{(2)} \Psi_{2j_2}(x_{2j_2}),$$
$$\Phi_{i3}(x_3) = \sum_{j_3=1}^{n_3} a_{ij_3}^{(3)} \Psi_{3j_3}(x_{3j_3}). \quad (2)$$

are formed.

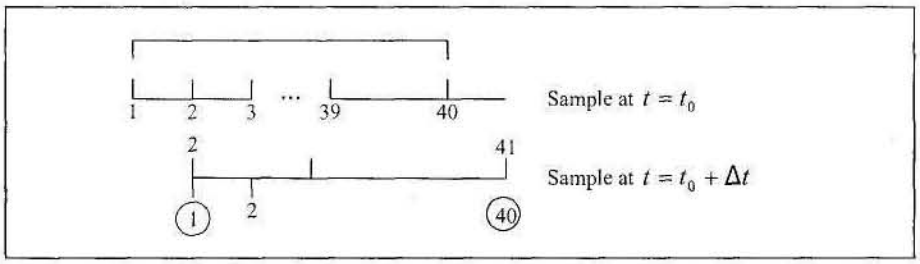

Fig. 1. Sample at $t = t_0$ and $t = t_0 + \Delta t$

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 (2) and can be represented as the following generalized polynomials:

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

In some cases, in forming the structure of the models, one should take 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 (1)-(3) as a hierarchical multilevel system of models

$$[1+\Phi_i(x)] = \prod_{s=1}^{S_0}[1+\Phi_{is}(x_s)]^{c_{is}}; [1+\Phi_{is}(x_s)] = \prod_{j_s=1}^{n_s}[1+\Psi_{sj_s}(x_{sj_s})]^{a^s_{ij_s}};$$
$$[1+\Psi_{sj_s}(x_{sj_s})] = \prod_{p=1}^{P_{j_s}}[1+\varphi_{j_sp}(x_{sj_s})]^{\lambda_{j_sp}}. \quad (4)$$

We will use the Chebyshev criterion and for the functions φ_{j_sp}, we will use biased Chebyshev polynomials $T_{j_sp}(x_{j_sp}) \in [0,1]$. Then the approximating functions are found 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. Such an approach reduces the procedure of forming the approximating functions to a sequence of Chebyshev approximation problems for inconsistent systems of linear equations [8, 9].

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 $[d^-_{j_s}, d^+_{j_s}]$, 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.

1.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.

2.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 1 schematizes the sample for the instant of time $t=t_0, N_{02}=40$ and $t=t_0+\Delta t(t=1,2,3,...,t_k,...,T)$.

3.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}.

4. Processing of each sample in each variable should involve the following procedures:

— evaluating $\Phi_i^k(x_1^k,...,x_j^k,...,x_n^k), i=\overline{1,m}, j=\overline{1,n}$, in the form (2) or (4) for each k th measurement for $t=t_k$;

— setting up a step function of the first level

$$Z_{1j}=\sum_{p=1}^{M_1} d_{jp}U(\hat{x}); U(\hat{x})=\begin{cases}0, \hat{x}<0\\ 1, x\geq 0,\end{cases} \hat{x}=x_j-x_p; d_{jp}=\begin{cases}0{,}15 & \text{if } p=1,\\ 0{,}1 & \text{if } p=\overline{2,9},\\ 1 & \text{if } p=10,\end{cases}$$

$x=0{,}1\cdot p; p=\overline{1,10}; M_1=10;$

—setting up a step function of the second level

$$Z_{2j}=\sum_{p=1}^{M_2} d_{jp}U(\hat{x}); M_2=10; x_p^0=\begin{cases}0{,}5 & \text{if } p=1,\\ 0{,}1 & \text{if } p=\overline{2,9}, d_{jp}=\begin{cases}0{,}1 & \text{if } p=\overline{1,9},\\ 1 & \text{if } p=10.\end{cases}\\ 1{,}15 & \text{if } p=10,\end{cases}$$

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 and base dynamic model of processes (1)-(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 $D=\{t \mid t_0^- \leq t \leq t^+\}, D=D_0\cup D_0^+$, which includes the initial

observation interval $D_0 = \{t \mid t_0^- \le t \le t^+\}$ and the prediction interval $D_0^+ = \{t \mid t_0^+ < t \le t^+\}$. Then, to determine the dynamic model of the processes as the estimated approximating functions (1) or (4) based on the initial data, the system of equations is formed for the interval D_0 as follows:

$$0,5a_0 + \sum_{n=n_1}^{N} a_n T_n^*(\tau_{k_1}) - \hat{y}_{k_1} = 0; k_1 = \overline{1, K_0}; \quad (5)$$

$$\hat{y}_{k_1} = y(\tau_{k_1}), \tau_{k_1} \in [0, \tau_{k_1}^+], \tau_{k_1}^+ = \frac{t_k^+ - t_0^-}{t^+ - t_0^-} < 1, t_k \in D_{K_0}, D_{K_0} \subset D_0$$

The dynamic model of the process within the observation interval D_0 is determined by solving system (5) and is described by

$$\Phi_1(\tau_1) = 0,5a_0^0 + \sum_{n=n_1}^{N} a_n^0 T_n^*(\tau_1); \tau_1 \in D_0 \quad (6)$$

The dynamic forecasting model is based on the extrapolation of function (6) to the interval D_0^+ and is expressed by the formula

$$\Phi_2(\tau_2) = 0,5a_0^0 + \sum_{n=n_1}^{N} a_n^0 T_n^*(\tau_2); \tau_2 \in D_0^+. \quad (7)$$

The dynamic model of the process within the given interval $D = D_0 \cup D_0^+$ based on (6) and (7) is described by the

$$\Phi_0(\tau) = \begin{cases} \Phi_1(\tau_1) \text{ if } \tau_1 \in D_0, \\ \Phi_2(\tau_2) \text{ if } \tau_2 \in D_0^+, \end{cases}.$$

Models for long-term and short-term forecast differ by both the ratio of observation and forecast intervals and the order of the Chebyshev polynomials used in the model.

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.

1.Each stage of CES 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.

2.All the parameters y_i are dynamically synchronous and inphase in the sense that they simultaneously (without a time delay) increase or decrease under risk factors.

3.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'sresponse.

4.The risk factors $\overline{\rho_{q_k}^{\tau}} \mid q_k = \overline{1,n_k^{\tau}}$ change the effect on the object in time; the risk increases or decreases with time.

5.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 provided that 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.

6.The risk factors $\rho_{q_k}^{\tau} \mid q_k = \overline{1,n_k^{\tau}}$ are independent and randomly vary in time with a priori unknown distribution.

7.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).

8.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.

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 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 th parameter y_i; ρ_{q_k} is the value of the q th risk factor at the instant of time t_k.

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

$$\tilde{y}_i[t_k] = \frac{1}{m}\sum_{j=1}^{m}\tilde{b}_{ij}\sum_{r=0}^{R_j}a_{jr}T_r^*(U_j); \tilde{b}_{ij} = b_{ij}\cdot F_i(\rho_{q_k}), \quad (8)$$

where the function $F_i(\rho_{q_k})$ should correspond to the condition whereby $\tilde{y}_i = y_i$ 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

(9)

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 change abruptly at the cyclone-anticyclone interface). The most complex is the case where one risk factors vary continuously and others abruptly.

We will recognize risk situations by successively comparing $\tilde{y}_i[t_k]$ for $\tilde{y}_i[t_k]$ for 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 inphase 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):

$$\operatorname{sign}\Delta\tilde{y}_i[t_1,t_2] = \ldots = \operatorname{sign}\Delta\tilde{y}_i[t_k,t_{k+1}] = \ldots = \operatorname{sign}\Delta\tilde{y}_i[t_{k_0-1},t_{k_0}], \quad (10)$$

$$\text{sign}\Delta\tilde{y}_1[t_k,t_{k+1}]=...=\text{sign}\Delta\tilde{y}_i[t_k,t_{k+1}]=...=\text{sign}\Delta\tilde{y}_n[t_k,t_{k+1}], i=\overline{1,n}. \quad (11)$$

As follows from (10) and (11), 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 $[t_k,t_{k+1}]$, $k=\overline{1,k_0}$.

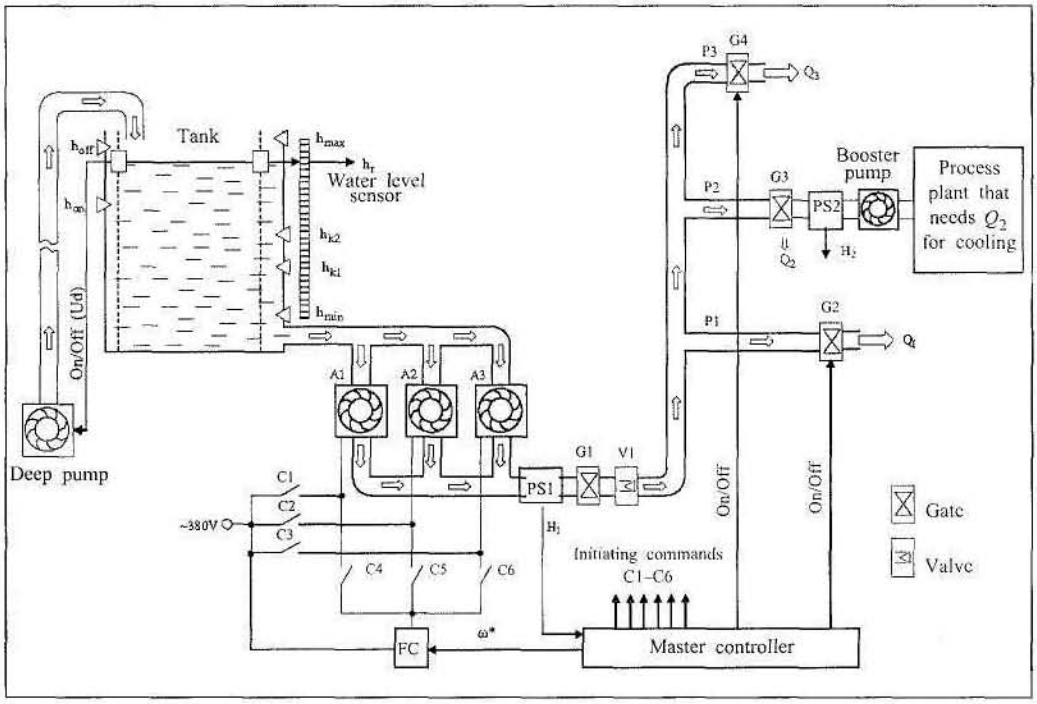

Fig. 2. A function chart of a deep water supply system

Conditions (10) and (11) are rigid; for practical purposes, it will suffice to satisfy the conditions for the representative number (3-5), which determine the parameters $\tilde{y}_i$ but not for all parameters i. The corresponding quantities in (10) and (11) are defined by

$$\Delta\tilde{y}_i[t_k,t_{k+1}]=\tilde{y}_i[t_{k+1}]-\tilde{y}_i[t_k], \quad (12)$$

where $\tilde{y}_i[t_k]$ are defined by (8); we assume 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 (10) and (11) 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 (10) and (11) rather than the value defined by (12). 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 (10) or for individual $[t_k, t_{k+1}]$ according to (11).

3. DIAGNOSTIC OF A DEEP WATER SUPPLY SYSTEM

As an example of the realization of a system strategy of guaranteed CES safety, we will consider a real deep water supply system (Fig. 2). The main purpose of the system is to supply a specified volume Q_n of water to consumers, of which cooling of an ecologically dangerous process plant is of priority.

There are three groups of consumers with maximum normal water consumption $Q_1 \le 0,3Q_n, Q_2 \le 0,4Q_n$ and $Q_3 \le 0,3Q_n$, respectively. Water delivery to consumers PI and P3 is not a critical factor and can be cut off with controlled gates G2 and G4, respectively. Water delivery to the process plant P2 is obligatory, and should not be interrupted not to cause an inadmissible accident.

Normally, one or two pumps operate depending on water consumption. The output pressure is stabilized by a master controller that sets the speed of the controlled pump and connects (or disconnects) noncontrolled pumps. Transients in an abnormal mode may be due to both insufficient (half or quarter) nominal output of the deep pump and possible water loss at consumers PI and P3.

According to IPED requirements, sensors are installed at different elevations of the tank and at some reference points of the water supply system; the readings are taken every 10 sec. We will use the readings of the water level sensor h_r and water head sensor H_2 at the input of the process plant and their arguments during 5000 sec

(500 samples).

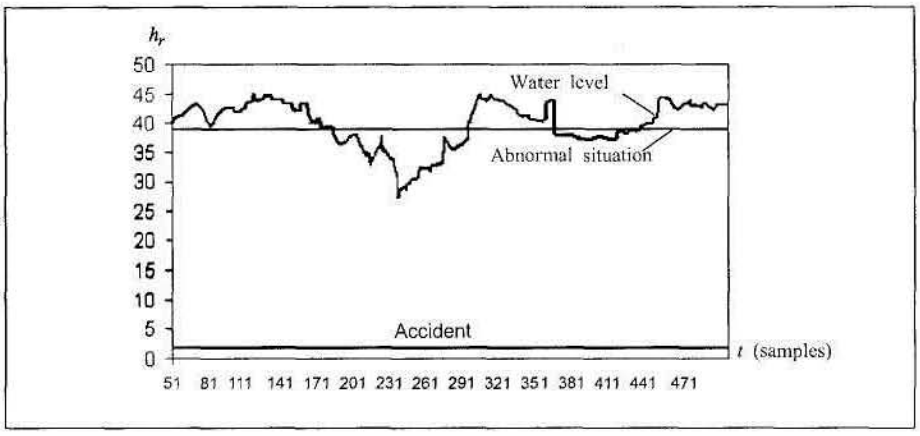

Fig. 3. Time distribution of water level h_r in the tank

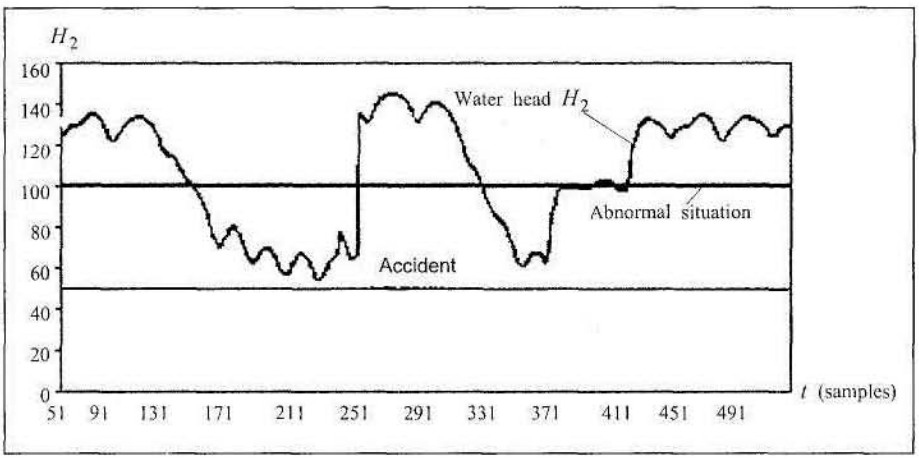

Fig. 4. Time distribution of water head H_2 at the input of the process plant

The deep pump fills the tank of volume $V_r = 25\text{m}^3$. The pump is energized if the water level $h_r < 40\text{m}$ and deenergized $h_r < 45\,\text{m}$. The output of the deep pump is $Q_p = 1,5Q_n$. The water is delivered from the tank to the consumers by a pumping unit that consists of three pumps (A1, A2, and A3), two operating in normal mode and one in emergency. The output of each pump is $Q_{pi} = 0,5Q_n (i = A1, A2, A3)$. To stabilize the pressure for the pumping unit, a PS1 sensor is placed at the output pipe to measure the water head H_1. Water arrives at the water supply system through a noncontrolled gate G1 and valve VI. A monitoring water pressure sensor PS2 and a booster pump (to regulate the amount of consumed water and thus the temperature of the boiler) are installed at the input of the process plant (boiler).

To timely detect the causes of potential abnormal situations and to ensure survivability, the engineering diagnostic is monitored in real time during the system operation. According to the developed methodology of guaranteed safety of CES operation, the functional dependences $y_i = f_i(x_1,...,x_j,...)$ are estimated at the initial stage $t = t_0$ based on $N_{02} = 50$ initial discrete samples of values h_r and H_2 and their arguments; $y_1 = h_r(x_{11},x_{12}); y_2 = H_2(x_{21},x_{22},x_{23},x_{24})$ where x_{11} is total water consumption; x_{12} is the output of the deep pump; x_{21} is water head H_1 at the output of the pumping installation; x_{22} is total water consumption; x_{23} is the number of pumps in operation; x_{24} is the speed of the controlled pump.

Based on the analytic relationships h_r and H_2 estimated within the interval [0; 0.8] (in view of the property of biased Chebyshev polynomials whereby the functions should be approximated uniformly on the interval [0; 1]), a guaranteed forecast for ten values of the samples in the interval (0.8; 1] is carried out. The resultant values are used to make a certain decision: the water supply system operates in the normal mode; the water supply system operates in an abnormal mode, there are certain deviations; the water supply system passes into emergency operation mode; sensors fail.

The normal mode is ensured by synchronous and inphase variations of the parameters of h_r and H_2 and their arguments. An abnormal situation will occur if at least one of the functional dependences h_r or H_2 drops below the admissible level: h_r <39m; H_2 < 100. By an accident we mean a situation where H_2 drops below $H_{2\min} = 50$ m and the water level h_r decreases to $h_{k2} = 2$ m for longer than 60 sec. A failure in sensors is detected when the procedure of "setting up a step function" is used, which makes it possible to detect a random overshoot in one of the sensors.

Some results of the monitoring are presented as a time distribution of the estimated functional dependences of the water level h_r (Fig. 3) and water head H_2 at the input of the process plant (Fig. 4).

During the operation of the water supply system, a data panel displays the diagnostic process quantitatively and qualitatively and the operator obtains the timely

preliminary information on the possible transition of the water level h_r and water head H_2 to an abnormal mode. This allows detecting the cause in due time and making a decision on eliminating the abnormal situation, accident or catastrophe.

The analysis shows that the monitoring of the water supply system operation by using the developed methodology of the guaranteed safety of CES operation allows making a real-time decision to ensure the survivability of the serviceability of the deep water supply system.

CONCLUSIONS

The proposed strategy of the guaranteed safety of CES operation implemented as an 1PED toolkit prevents 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 to make the operation survivable. The principles that underlie the strategy of the guaranteed safety of CES operation provide a flexible approach to timely detection, recognition, prediction, and system diagnostic of risk factors and situations, to formulation and implementation of a rational decision in a practicable time within an unremovable time constraint.

REFERENCES

1. K. V. Frolov (gen. ed.), Catastrophe Mechanics [in Russian], Intern. Inst. for Safety of Complex Eng. Syst., Moscow (1995).
2. V. T. Troshchenko (exec, ed.), Resistance of Materials to Deformation and Fracture: A Reference Book, Pts. 1, 2 [in Russian], Naukova Dumka, Kyiv (1993, 1994).
3. M. Z. Zgurovsky and N. D. Pankratova, System Analysis: Theory and Applications, Springer, Berlin (2007).
4. N. Pankratova and B. Kurilin, "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., 33, No. 2, 15-31 (2001).
5. N. Pankratova and B. 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," J. Autom. Inform. Sci., 33, No. 4, 1-14 (2001).
6. N. D. Pankratova, "System analysis in the dynamics of the diagnostic of complex engineering systems," Syst. Doslidzh. Informats. Tekhnol., No. 1, 33-49 (2008).
7. N. D. Pankratova, "A rational compromise in the system problem of disclosure of conceptual uncertainty," Cybern. Syst. Analysis, 38, No. 4, 618-631 (2002).

8. C. Lanczos, Applied Analysis, Prentice-Hall, Englewood Cliffs, N. J. (1956).
9. E. Ya. Remez, Foundations of Numerical Methods of Chebyshev Approximation [in Russian], Naukova Dumka, Kyiv (1969).