MANAGEMENT OF CRITICAL INFRASTRUCTURES BASED ON TECHNICAL MEGASTATE

Oleg IVANCHENKO, Vyacheslav KHARCHENKO,
and Aleksandr SKATKOV

Abstract: The provision for effective operation of critical infrastructures (CI) is approached by taking into account priorities for their safety and reliability. This paper substantiates practical aspects of introducing CI management based on technical megastate. It presents relevant mathematical models based on the principles of analysis and assessment of infrastructure systems safety.

Keywords: Critical infrastructures, megastate, centralized management, decentralized management, safety.

Introduction

Nowadays the problem of providing safe and effective use for purpose critical infrastructures (CI) acquired an international format. This is evidenced by the consequences of accidents: Sayano-Shushenskaya Dam (Russia, 2009); energetic system of the USA and Canada (August 2003); energetic system of Italy and Switzerland (September 2003), etc.

Some aspects of the safety problems in complex technical systems (CTS) and infrastructures [1] require clarification and detailed studying. One such study, performed by the U.S. National Academy of Sciences, looks into the problem of identification, reducing frequency of appearance and elimination of cascading failures in critical infrastructures.[2] After analyzing threats and vulnerability of artificial and natural origin (the hurricane season), the authors estimate CI stability and develop recommendations to ensure the safety of the infrastructure sectors for different U.S. regions.

Issues of infrastructure management in context of ensuring the reliability of production systems are also treated in scientific literature.[3] The problem of risk minimizing in the operation of assets of the company is considered. It is proposed to link the performance of maintenance and repair of particular company equipment with objectives of company in the reliability, safety, environment, quality areas. Other sources report

© ProCon Ltd. This article cannot be reprinted, published on-line or sold without written permission by ProCon.

on analysis of accidents, incidents, energy infrastructure and their impact on resilience, reliability operations of other controlled trials.[4] Of special interest in such cases is the probabilistic assessment of the impact of electric power grid on survivability of public data networks in natural disaster or malicious attacks.

The research results indicate the need for a full analysis of CI safety and reliability problems in terms of prevailing conflict. Essence of conflict is expressed in effort to maximize CI performance due to reallocation of resources between infrastructure's elements (CTS), with full (or partial) neglect of the requirements for centralized (decentralized) management of their readiness for intended use of these elements.

Striking manifestation of formulated conflict, which resulted in human victims (74 people), is accident at Sayano-Shushenskaya (S-Sh) Dam (Russia). This and other examples [5] indicate the need for basic research in this field. To overcome this conflict is offered in the transition to management CI based on *technical megastate*. Purpose of work is to develop principles of analysis of safety, reliability and management of critical infrastructures, based on technical megastate.

Maintenance CI in readiness for its intended use largely depends on the ability to manage their TMS. This fact determines the degree of importance and relevance of the problem. Comparative analysis of accidents at critical energy infrastructures (EI) of USA, Canada, some European countries and Russia should be done before proceeding to the consideration of certain aspects of this problem.

Principle of Management Based on Megastate

Initial Assumptions

Analysis of accidents at the United States, Canada, The European Union states, Russia power systems,[6] demonstrates the absence of a clear concept CI management, focused on risk minimizing in the context of limited resources and the deterioration of the infrastructure components.

An autonomous, independent control of technical state of CTS doesn't contribute to safe and reliable infrastructure functioning. Formally, this means that we have a complex hierarchical structure, that's work is described by multilayer (multi-factor) model, and we consider only states of separately taken layers. Therefore, it's important to develop an approach that operates not only the technical condition of CTS, but also takes into account the reliability, safety of infrastructure in general, providing multi-organization control system.

Using the basic principles of system analysis, we conclude the feasibility of introducing concept of 'CI technical megastate.' This fact causes: need of transition to critical infrastructure management based on technical megastate (TMS); application

of formal methods of assessment based on potential dangers identifying and risk assessment of their occurrence is relevant. Our purpose is to maintain required level of operational readiness by appropriation of CI readiness management strategies based on TMS. Let's define technical megastate and CI readiness management strategies.

As CI technical megastate is a vector-function of states:

$$MS = F(L,S,Q,R,U,Z), \tag{1}$$

where $L = \{L_i\}_{i=1}^{I}$ – set of solved by CI problems; $S = \{S_w\}_{w=1}^{W}$ – set of technical states in which CI can be; $Q = \{Q_j\}_{j=1}^{J}$ – set of structures of CI (with options for reforming (restructuring), modifications, upgrades, etc.); $R = \{R_d\}_{d=1}^{D}$ – set of nodes of CI operating; $U = \{U_b\}_{b=1}^{B}$ – set of CI readiness management strategies; $Z = \{Z_y\}_{y=1}^{Y}$ – set of relations (links) between the components $\{L,S,Q,R,U\}$.

There are the following types of relationships: $z_1(L,S)$ – the ratio of "problem-technical conditions," each tuple of relations z_1 defines the mapping of tasks to be solved by the CI, the technical condition in which they may be; $z_2(L,Q)$ – the ratio of "problem structure," each tuple of relations z_2 defines the mapping of CI structures solved problems functional purpose; $z_3(L,R)$– the ratio of "problem-modes of operation," each tuple of relations z_3 defines the mapping of tasks and CI modes of operation; $z_4(L,U)$– the ratio of "problem-management strategies," each tuple of relations z_4 defines the mapping of tasks and trials of management strategies for their technical readiness; $z_5(S,Q)$– The ratio of "technical state structure," each tuple of relations z_5 defines the mapping of CI structures and technical conditions in which they may be; $z_6(S,R)$– the ratio of "technical-state modes of operation," each tuple of relations z_6 determines that the technical conditions and modes of operation of CI; $z_7(S,U)$ – the ratio of "technical state-management strategy," each tuple of relations z_7 determines that the technical conditions and management strategies and technical readiness of CI; $z_8(Q,R)$– the ratio of "structure, operation modes," each tuple of relations z_8 determine the compliance structure of the CI and the modes of operation; $z_9(Q,U)$– the ratio "of the structure, management strategy," each tuple of relations z_9 determine the compliance structure of the CI and management strategies for their technical readiness.

For CI, which was originally created as an evolving system, we have $T_{l.c}^{CTS} \subseteq T_{l.c}^{CI}$, where $T_{l.c}^{CI}, T_{l.c}^{CTS} = \{T_i^{CTS}\}_i^N$, $i \in \{1,2,...,N\}$ – duration of life cycle of CI and CTS (from the CI) respectively. If CI is created on basis of existing CTS (for example, as a result of reforming, etc.), then $T_{l.c}^{CI} = max T_{l.c}^{CTS}$.

Maintenance of CI in readiness for its intended use is accordance with the chosen strategy U. Let's define readiness management strategy U as a set of decision-makes rules on intended use of infrastructure at fixed times t_i, where $i = \overline{1,v}$, $t_i \in T$,

$T \le T_{жс.ц}^{ки}$, $T \le T_{l.c}^{CTI}$, taking into account its condition, operating modes, importance of the task and structural construction, that is taking into account its technical megastate. Strategies are distinguished on the degree of centralization: (1) with centralized CI readiness management (RM) U_{cm}; (2) with decentralized CI readiness management U_{dcu}. CI management organizes using of strategies $U_{cm}\left(U_{dcm}\right)$ at all possible levels of hierarchy with the influence of many factors, including functional and information content of security. It needs performing of danger analysis and risk assessment, results of which are currently represented in quantitative, qualitative, or combined form of representation. The results of qualitative analysis are presented in form of textual descriptions, tables, chart, expert assessments, etc. However, this approach doesn't always give a positive result.

In our opinion, one of the major reasons of this problem is lack of grounded CI safety analysis theory and lack of providing of various infrastructures safe operating. In general CI can be constructed by the scheme (Figure 1), "Consumer (C) – a management system (MS) –decision support system (DSS) – controlled objects (CO)." As the CO stands IC CTS. The management system includes two supporting subsystems: the intended use management system (IU MS) and readiness by technical megastate management system (RTMS MS). Structural hierarchy in such scheme is determined by the principles of self-organization, taking into account the dynamic response to external influences (R-factor) and process that characterize intra-system (infrastructure) changes. To do this in early stages of the life cycle (phases of research, development) system from the infrastructure designs according to their evolution and adaptation to changing intended use conditions. Increasing of complexity and scale of problems to be solved with use of CI indicates the need for managing their operational readiness for its intended use. The evidence of this conclusion is confirmed by preceded the accident at S-Sh Dam events.

Let's formulate and describe general principles of CI analysis based on set detailing of types, effects of failures or other events affecting the safety elements (systems) of infrastructure in view of capabilities of their condition management at the appropriate hierarchy level.

Analysis and CI Safety Principles

Of course, to perform assessment of TMS in direct formulation of the problem (1) is almost impossible task. Therefore in view of physical nature of the solving problem to replace the set of TMS $S = \{S_w\}_{w=1}^{k}$ on the values of probabilistic reliability indices o the CI vital elements (CTS). We need to follow next *safety analysis principles* for this purpose*:*

1. An infrastructure is a set of interacting complex technical systems S_i, $i = 1,...,n$. Each of the systems can be described by the FMECA table (or a hierarchy of tables), TF_i, or its generalization EMECA table, TE_i. Level of detailing a variety of types and consequences of failures (events) of each system is determined by the level of its state management. Each row of table $TF_i(TE_i)$ is associated with state F_{ij}, $j = 1,...,m_j$. Consequently, the set of system states S_i includes a workable state (states) F_{io}, states with single failures (events) F_{ij} and, if it's necessary, the states with multiple failures (events) $F_{ij}^{(h)}$ (the general case $h = 2,...,m_j$):

$$MF_i = \left\{F_{io}, F_{ij}, F_{ij}^{(h)}\right\}. \quad (2)$$

2. On the rules of FMECA (EMECA) technique each state F_{ij} (as well as $F_{ij}^{(h)}$) is paced in corresponding probability P_{ij} and rejection (event) severity W_{ij}. Their multiplication determines degree of states criticality

$$R_{ij} = P_{ij} \cdot W_{ij}. \quad (3)$$

Results of the FMECA (EMECA) analysis (relevant table) are transformed into two-dimensional (or taking into account recovery time – three-dimensional) critical matrix with dimension – a x b, where a and b – number of rows and columns, assigning values to determine the scale of probability P_{ij} (p) and severity W_{ij} (w):

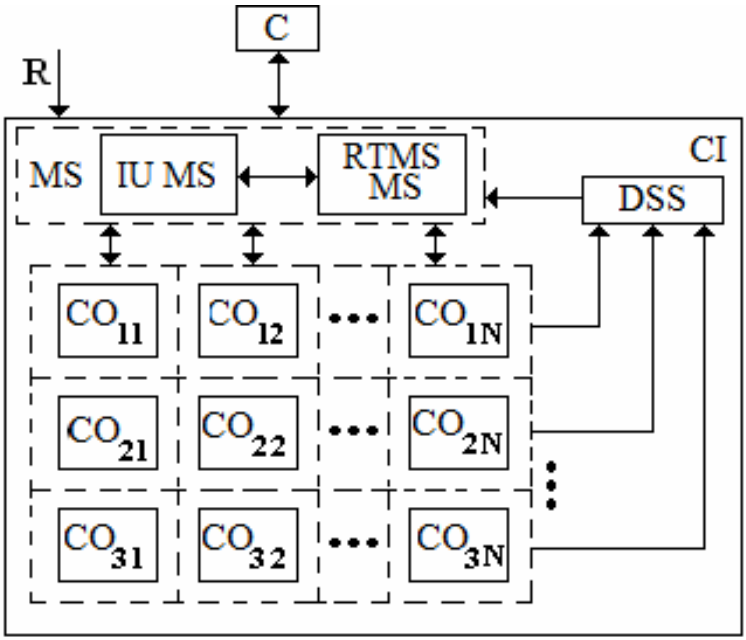

Figure 1: General constructing scheme of CI.

$$MR_i = \left\| R_{ij}(p, w) \right\|. \quad (4)$$

The diagonal of criticality is given in matrix MR_i. If there are elements that are above the diagonal (unacceptable risk $R_{ij} > R_{i_{unac}}$), then corrective actions C_{ij} that ensure reduction of risk to an acceptable level are necessary. The problem of local composition and corrective actions C_{ij} (methods and means of risks reducing) volume optimization by the criterion "acceptable risks – low cost" can be posed at the system S_i level.

3. For each row FMECAi (EMECAi) system S_i table is determined degree (probability) of influence of corresponding failures (events) and transfer of state F_{ij} on the state F_{kg} of other CI systems S_k ($k = 1,...,n, k \neq i, g = 1,...,m_g$).

This effect on state F_{kg} could be as follows: (1) failure (event) F_{ij} leads to change (increase or decrease) in probability P_{kg}; (2) failure (event) F_{ij} leads to change (increase or decrease) in severity W_{kg}; (3) failure (event) F_{ij} causes appearance of new (previously unspecified) failure (event) F_{kmg+1}; (4) failure (event) F_{ij} leads to combination of events 1-3; (5) failure (event) F_{ij} doesn't influence on state F_{kg}.

Based on the above, the impact of the system S_i on system S_k can be described using the matrix

$$MD_{ik} = \left\| d_{jg}^{ik} \right\|, \quad (5)$$

where d_{jg}^{ik} – vector, taking into account the impact F_{ij} on F_{kg}; this vector could be shown next way:

$$d_{jg}^{ik} = \left\langle \left(x_{jg1}^{ik}, L_{jg1}^{ik}\right), \left(x_{jg2}^{ik}, L_{jg2}^{ik}\right), \left(x_{jg3}^{ik}, L_{jg3}^{ik}\right), \left(x_{jg4}^{ik}, L_{jg4}^{ik}\right), \ldots \right\rangle, \quad (6)$$

and, $x_{jgz}^{ik} = 1(0)$, if corresponding effect type z of impact F_{ij} on F_{kg}, z = 1,…,5 (only one variable x_{jgz}^{ik} can be equal to 1) is implemented (not implemented); L_{jgz}^{ik} – operator characterizing probability and degree of influence (if $x_{jgz}^{ik} = 0$, than $L_{jgz}^{ik} = \varnothing$).

4. Description of the behavior and mutual systems influence can be linked to time. Over time parameters and values of the risk function R_{ij} and elements of the influence matrix D_{ik} may be changed. Final risk matrix for the infrastructure can be obtained on the basis of a system risk matrix MR_i. Elements of MR also are changed over time.

Summary of Safety Principles

1. It's necessary for stable and secure infrastructure functioning: (a) each of systems acted as a risk "filter," where risks are associated with failures (events) of other systems; in this case principle of separation protection is realized; (b) or risk reduction

for each failures (events) to acceptable level on the whole set of system is provided, there the problem of coverage for all path (chains) of influence may be posed and solved; (c) or special system of infrastructure safety SS, controlling the level of risk and ensuring its reducing to acceptable levels, should be. This system should consist of safety subsystems of each system SS_i, or their groups, that manage respective systems risk levels, and either reduce them to acceptable values, or inform the safety system of the upper level. Options for designing distributed adaptive safety systems are possible. These systems are built on principle of separation of protection, protection "in deep."

2. Binding principle that should be implemented with the establishment and modernization of critical infrastructures is the diversity principle. It's realized in systems S_i (local diversity) and on infrastructure level (global diversity). Types, methods, tools for implementing diversity of processes and products at different levels of infrastructure must be rationally allocated and combined, optimizing applying technologies for development of management information systems by the criterion of "reliability-safety-cost."

3. Task of providing safety of CI is solved in complex with tasks of providing responsibility maintain of desired (maximum) level of performance on the other properties (reliability, availability, survivability). Taking into account fact, that critical infrastructures are maintained and, as rule, related to objects of high readiness (or just parts of CI), it is useful as a general optimization criterion use the criterion "required safety (acceptable risk) – the maximum readiness."

4. It is possible to apply the principle of technical cannibalism for infrastructures allowing degradation. This principle involves resources using of the failed CI systems for other systems with a purpose to minimize general functionality or safety reducing level. This principle can be applied in the context of transformation of critical infrastructure.

Implementation Principles of Management Based on Technical Megastate

The foregoing indicates the emergence of an important scientific and technical sphere, which merged the following methodological problems: (1) development of the scientific base for the technical CI readiness based on TMS (calls assessment in the modern world; current CI state analysis; CI framework methodology; CI monitoring principles; models and methods of CI management based on TMS etc.); (2) program's development for CI management based on TMS (models, methods of CI control (monitoring) and management based on TMS; indicators and criteria for performance management etc.); (3) program's development for designing of CI readiness control and management based on TMS (methods of CI readiness control and management synthesis; information technologies for RTMS MS etc.).

Direction of training shall be elected such a way as to best reduce the negative impact of human factors. The reference model is created in view of the provisions. This model is based on the optimization criterion "cost-effectiveness." In mathematical form expression for the proposed criterion can be written as follows:

$$\xi = \begin{cases} \max\limits_{\psi} E(MS), \\ C_{min_{mp}} \le C_{mp} \le C_{max_{mp}}, \\ \psi = \{l,s,g,u,q\}, \end{cases} \quad (7)$$

where E – generalized CI intended use efficiency index; $l \in L, L$ – set of tasks, which are solving by CI; $s \in S, S$ – set of technical states, in which CI can be; $r \in R, R$ – set of CI operation modes; $u \in U, U$ – set of CI readiness strategies; $q \in Q, Q$ – set of CI structures; $C_{min_{mp}}, C_{max_{mp}}$ – minimum and maximum allowed operating costs.

In accordance with FMECA methodology [7] for solving tasks of CI management, development of alternative models for assessment probability indexes of reliability, that are included in (3),(4), is proposed. Actually, complex approach to solving of this problem by using mathematical models of two levels is implemented. The first level involves the development and construction of macro-models described by (1),…,(4). Formalizing solution of the problem, we proceed to the second modeling level – micro-models designing. On the second level micro-models of CTS are designed. For this variant alternative semi-Markov models are proposed as a reference models. In this case, the assessment of the reliability level, with sequential determination of the functional safety index value, can be done by calculating the values of pointwise readiness indexes (PRI) and operating readiness indexes (ORI). At the same time as the base model is recommended to use mathematical ones of two types: (1) PRI assessment models (micro-models of first type) are used for CTS (infrastructures) of constant readiness; (2) ORI assessment models (micro-models of second type) are used for CTS (infrastructures), which a certain time period may be in standby mode until the intended using.

First type models should be used to assess PRI of CTS with an autonomous technical state control (TSC) system (and mandatory autonomous power supply) which is running in monitor mode. As example for implementation of TSC system is a vibration control system hydro turbine generator. In this case, monitoring mode is regarded as an organization form of constant control (vibration control) of the vital parameters that the determinate not only the CTS efficiency, but also affect infrastructure readiness to make effective intended use in accordance with (7). And, the flow of information to video control systems is provided at specified intervals (at frequent intervals)

as a result of monitoring. One can be note that for analogue of such infrastructures (energy systems, maritime mobile objects, etc.) the most critical hidden mechanical failures of nodes or sub-components (CTS) of infrastructures. On this basis, we construct a semi-Markov CTS model and perform PRI assessment. As a monitoring object we mean CTS.

Semi-Markov Models

Multifactorial and multi-layer model (1) allows considering infrastructure aspects of its construction. But the link between infrastructure elements will transform already complex model to extremely complex, and the problem (7) – to unsolvable. Therefore it is proposed to consider various options of interdependence of infrastructures at micro-model level. Let's consider the example of functioning between technical state control and CTS with accumulation of infrastructure mechanic damage, which leads to hidden failures. Transmission graph for example is shown in Figure 2.

Assume that CTS is operated during a time interval, which lasts t . We assume that at the initial moment of using on readiness (RS) and ready for using CTS (state E_0) periodic technical state control (TSC) are conducted, this reviews lasts τ_c. The transformation from state E_0 to E_1 occurs in a fixed nonrandom time τ_c. Sudden and false failures may occur during the TSC and random times exponentially distributed. After it recovery of CTS RS is made, which takes random time τ_γ, distributes according to Erlang. After it CTS goes to state E_0. State E_2 corresponds to the reduction of monitoring object's RS after a sudden failure and identify of hidden failures.

During further operation at random times, corresponding to the gamma distribution with parameters (α,η), where $\alpha = 2$, $\eta = \lambda_4 = 1 \ \ h^{-1}$, hidden failures appear, in which CTS becomes inoperable (IS) state E_3, corresponding to hidden failures. Moreover, we assume that hidden failures occur only when damage number r of me-

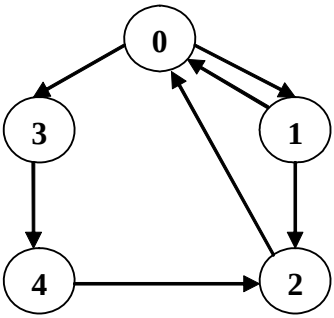

Figure 2: States graph for semi-Markov CTS model for hidden failures.

chanical components of CTS accumulates. We assume that the sequence of events "damage-hidden failure-recovery" in results CTS develops as follows:

1) $r-1$ undetected failure occurs on $k-1$ interval of control;

2) failure with number r occurs on interval of control with number k, which transforms to hidden failure (state E_3);

3) failure is detected authentically on $k+1$ interval of control (state E_4) and CTS goes to state E_2.

Applying methods described by Volkov,[8] PRI can be calculated in the following manner:

$$K_г(t)=\frac{\overline{t_1}}{Q}, \tag{8}$$

$$\overline{t_1}=\frac{2-\lambda_4 t P_э-2P_э}{\lambda_4}, \tag{9}$$

$$Q=\overline{t_1}+\frac{\alpha P_э}{\gamma}\left(1-P_{кmc}\right)+\tau_в(1-P_{кmc}P_э)+(1-\alpha P_э)\beta, \tag{10}$$

$$\beta=\frac{2P_э+(1-\alpha)(1+P_э)-2}{\lambda_4(1-P_{кmc}(1-\alpha)-P_э)}+\tau_к, \tag{11}$$

$$\alpha=1-\lambda_4 t,\ \tau_в=\frac{2}{\lambda_1},\ \gamma=\lambda_2+\lambda_3, \tag{12}$$

$$P_э=e^{-\lambda_4 t},\ P_{кmc}=e^{-\gamma\tau_к}, \tag{13}$$

where λ_1 – intensity of reduction (Erlang distribution parameter); λ_2 – intensity of sudden failures; λ_3 – intensity of false failures. In (12) γ parameter will be determined taking into account CTS (CI element) aging time τ under the influence of electrical and thermal stresses, using known empirical model:[9]

$$\gamma=\lambda_2+\lambda_3=\frac{1}{\tau}, \tag{14}$$

$$\tau=\tau_0\left(\frac{E}{E_0}\right)^{-n}\cdot e^{-BT}, \tag{15}$$

where $T=\frac{1}{t_0}-\frac{1}{t}$ – conventional thermal stress; t_o – a reference temperature; t – an absolute temperature; τ_o – corresponding lifetime at the electrical stress E_o and temperature t_o; E – electrical stress; E_o – the lower limit of the electrical stress, below

which the electrical aging can be neglected; n – the voltage endurance coefficient; B – proportional to the activation energy of the main thermal degradation reaction.

Plot of lifetime of the critical elements of PI from electrical stress and temperature is shown in Figure 3. In such a way, we using a mathematical model of aging (15) take into account "located" elements (CTS) "located" interdependence,[10] and we can assume the probability of multiple CI components failures.

There is plot of $K_г(t,\lambda)$ for model described by (9),…,(14). Result is taken for following parameters: hidden failures intensity, that appears by CTS mechanical damage accumulating, $\lambda_4 = 1\ h^{-1}$; CTS sudden and false failures intensity $10^{-4} \le \gamma \le 10^{-3}\ h^{-1}$; various CTS recovery of working condition intensity $\mu = \lambda_1 = 1\ h^{-1}$; duration of TSC intervals in monitoring state $\tau_c = 6$ min.

In Tab1e 1 assessments of PRI for first type model (average recovery time $T_r = 30$ h) are given. Those results are gotten for instant parameter values, given above. PRI assessments are gotten taking into account sudden and hidden failures. Accumulation of mechanical damages leads to appearance of hidden failures. Plot of $K_г(t,\lambda)$ presented on Figure 4. The value of PRI and duration of using significantly increases by reduction of hidden failures intensity.

Performed research and analysis of obtained data indicates, that at constant values of recovery intensity and hidden failures intensity significant increase of PRI values is provided not only by reducing of duration of PRI (in 5-10 times), but by reducing of using time of CTS (in 6 times).

The transition graph for a similar semi-Markov model for the case of floating failures distributed exponentially and the recovery time, and recovery time, distributed according to Erlang, are presented in Figure 5. Plot of $K_г(t,\lambda)$ presented on Figure 6.

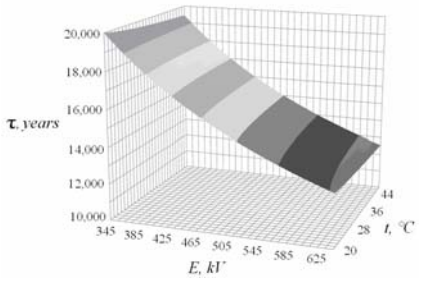

Figure 3: The dependence PI element's lifetime on ambient temperature electrical stress value for parameters: n=0,8; B=1.

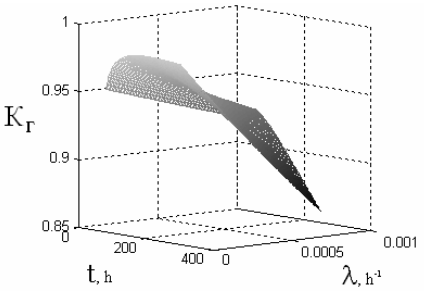

Figure 4: $K_г(t,\lambda)$ for hidden failures.

Table1. PRI Assumes for first type model.

#	τ_k, h	CTS using duration, month		
		6	3	1
1	10	0,97 / 0,31	0,98 / 0,47	0,99 / 0,725
2	2	0,97 / 0,31	0,985 / 0,47	0,99 / 0,727
3	0,1	0,973 / 0,31	0,985 / 0,47	0,99 / 0,728

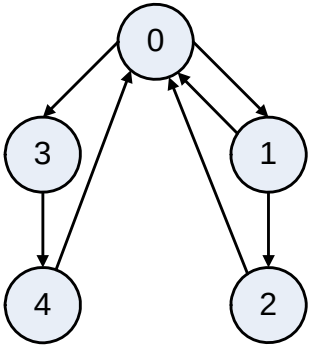

Figure 5: Semi-Markov state graph for CTS model for the case of floating failures.

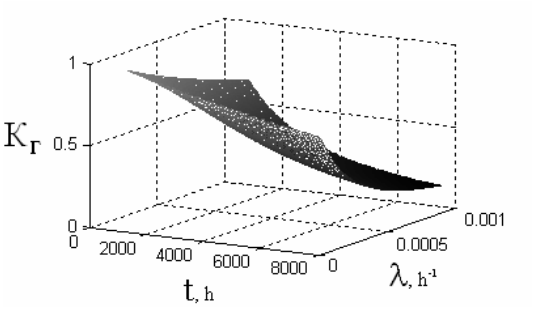

Figure 6: $K_г(t,\lambda)$ for the case of floating failures

Cyclomatic complexity of the component models of critical infrastructure

Many factors and "layering" of macromodel (1) allows to take into account infrastructural aspect of the construction of CI. But applying this model because of its bulkiness and complexity of the representation of initial data is difficult. Therefore, in some cases, it is proposed to describe the CI model at a lower level of the hierarchy - at the "microscopic" (the model) that takes into account the interdependence of the various versions of components (elements) infrastructure for to simplify it. These models can be considered as models for monitoring the components of CI. Functioning of complex technical systems (STS) as components of the CI can be described by a broad class of well-known mathematical models. In our view, in the first place the semi-Markov models should be allocated to, because they allow to adequately reflect

the most significant features of ITS-related: (1) the emergence of cascading failures in clinical trials, (2) the need to use the CI to a high degree of readiness for use.

Different versions of STS will describe operation with the relevant semi-state graphs of models shown in Figure 7,8. To estimate the complexity of the graphs we introduce a measure cyclomatic complexity (CC), defined as

$$\vartheta = H - (N_1 + N_2 / N_1) + 2 , \quad (16)$$

where H – the total number of transitions (edges) of the graph N_1 – the number of reversible (non-absorbing) states N_2 – the number of absorbing states.

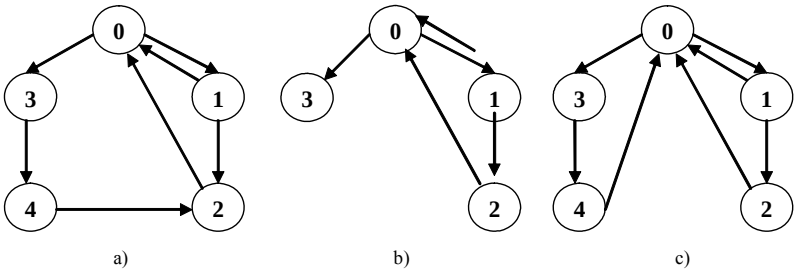

Figure 7: Graph of states of semi-Markov models operating at STS unreliable control of technical condition for the cases of the hidden faults and floating.

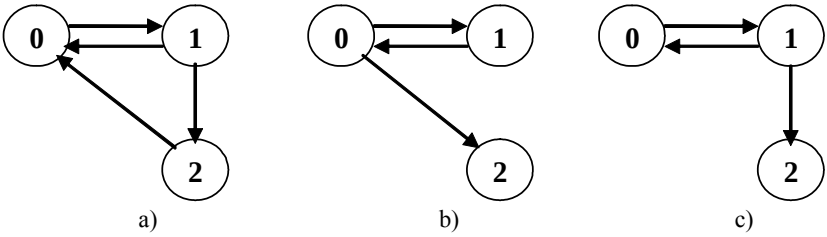

Figure 8: Graph of states of semi-Markov models operating at STS authentic control of technical condition for the cases of catastrophic failure.

On Figures 7, 8 it is shown that the worst-case situations occur for variants use STS, described the state graph containing the absorbing states (Figure 7b, 8b, 8c). The situations described by these graphs the most critical, since the restoration of an efficient condition STS excluded. We put them in compliance with the unacceptable risk values $R_j > R_{np}$, where $j = \overline{1,m}$. All other columns describe the situation with

acceptable values of risk. Consequently, in the formalized form STS can be described by a system of constraints

$$\Im = \begin{cases} \theta \subset \Theta, \vartheta_k = \varnothing, k \notin i, i = \overline{1,n} \\ \varphi \subset \Theta, \vartheta_l \neq \varnothing, l \in j, j = \overline{1,m}, \\ K_{\varepsilon i}(t) \geq K_{\varepsilon mp}, \\ K_{\varepsilon j}(t) < K_{\varepsilon mp}, \\ R_i \leq R_{ac}, \\ R_j > R_{ac}, \\ C_{min_{mp}} \leq C_{mp} \leq C_{max_{mp}}, \end{cases} \quad (17)$$

where $\Theta = \theta \cup \varphi$ – majority of values of the CA for the well-known set of state graphs; $\theta = \{\vartheta_i\}_{i=1}^{n}$ – majority of values of the CA for graphs, which do not contain absorbing states; $\varphi = \{\vartheta_j\}_{j=1}^{m}$ – majority of values of the CA for graphs containing absorbing states; ϑ_k, ϑ_l – CA values of the index for graphs that contain absorbing states; $K_{\varepsilon mp}$ – limit value SAG; R_{ac} – acceptable risk value, given in the form of peer review using comparative approach, implemented in the form of cross-sectional analysis of information on safety and security components of CI.

Thus, the rate of CA (16) and system constraints (17) are the basis for assessing the effectiveness of different variants of the various components of the CI.

Conclusion

In this study, we formulate the principles of analysis and CI safety. Results of combined (both quantitative and qualitative) analysis of the failures implications or other events, affecting the safety, may be represented in the table-matrix form for suitable processing. Using matrices problem of global optimization of corrective actions is formulated, which may represent a superposition of the problems of local optimization to ensure the safety of critical infrastructure and the transition to managing their technical megastate. Offered alternative models of CTS elements functioning are used to estimate the corresponding reliability indices. Their subsequent use is associated with the opportunity to determine the criticality of failures and assessing the severity of their consequences.

Further investigation may be directed at: development of detailed models of technical infrastructure state; posing and solving of problem of CI safety management based on megastate; development of safety CI architectures and other.

Notes:

[1] Vyachelsav Kharchenko, "Dependability and Dependable Systems: Elements of Methodology," *Radioelectronics and Computer Systems* 5 (2006): 7-19.

[2] *Cascading Infrastructure Failures: Avoidance and Response* (Washington, D.C.: The National Academy of Sciences, May 2007).

[3] V.I. Iorsh, I.E. Kryukov and I.N. Antonenko, "Control of Infrastructure and Safety of Production Systems," *Management Methods and Tools* 1: 11-12 (Moscow, Innovator, 2009): 72-73.

[4] Sean Gorman, "A Methodology for Critical Infrastructure Resiliency," Appendix D in *Report of the Critical Infrastructure Task Force* (Washington, D.C.: Homeland Security Advisory Council, 2006), pp. 23-36, <www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf>; Tom Leonidas Jr., "Restoring Reliability to Emergency Power Systems". Maintenance Solutions (2006). <www.facilitiesnet.com/powercommunication/article/Restoring-Reliability-to-EmergencyPower-Systems--4325#>.

[5] Xiang Zhang, et al., "Determination of the Actual Condition of the Electrical Components in Distribution Systems," *Proceedings of the XIVth International Symposium on High Voltage Engineering* (Beijing, China: Tsinghua University, 25-29 August 2005). 325.

[6] *Processing*, <www.iamik.ru>.

[7] IEC 812, *Analysis Techniques for System Reliability – Procedure for Failure Modes and Effects Analysis (FMEA)* (Geneva: International Electrotechnical Commission, 1985), 41; Hasan Sozer, Bedir Tekinerdogan and Mehmet Aksit, "Extending Failure Modes and Effects Analysis Approach for Reliability Analysis at the Software Architecture Design Level," *Lecture Notes in Computer Science* 4615 (2007), *Architecting Dependable Systems* IV (Springer, 2007), 409-433.

[8] L.I. Volkov, *Control of Air Complexes Operation* (Moscow: Higher Education, 1981), 368.

[9] *Performance-Focused Maintenance for Distribution Substations: Survey and Guide with KPIs and Algorithms for Living and Predictive Maintenance* (Palo Alto, CA: EPRI, 2006).

[10] Cascading Infrastructure Failures: Avoidance and Response.

OLEG IVANCHENKO, PhD, is associate professor at the Computer Systems and Cybernetics Department, Sevastopol National Technical University, Sevastopol, Ukraine.

VYACHESLAV KHARCHENKO was born in Ukraine, 1952. PhD (1981), Professor (1992), Doctor of Science (1995). He is Head of the Computer Systems and Networks Department, National Airspace University "KhAI" and the Centre of Safety Infrastructure-Oriented Research and Analysis, Ukraine. He is a Member of IEEE, ERCIM-SERENE group, IEEE Global Education in Microelectronics Systems (I-GEMS), leader and supervisor of national projects in the area of safety and business critical applications (NPP I&Cs).

ALEKSANDR SKATKOV, PhD, Doctor of Technical Science, is Professor and Head of the Computer Systems and Cybernetics Department, Sevastopol National Technical University, Sevastopol, Ukraine.