

# MULTI-FRAGMENTAL AVAILABILITY MODELS OF CRITICAL INFRASTRUCTURES WITH VARIABLE PARAMETERS OF SYSTEM DEPENDABILITY

Vyacheslav KHARCHENKO, Oleg ODARUSHCHENKO,  
and Valentina ODARUSHCHENKO

**Abstract:** This paper presents the development of the MFMC-based methodology and technique for modelling and quantitative availability assessment of critical IT-infrastructure consisting of maintained and partially unmanned systems. It takes into consideration a variation of system and component parameters and, in particular, variation of failure rates caused by detection and elimination of design faults.

**Keywords:** IT-infrastructure, modelling, dependability indicators, defects, evolution of software, fault-tolerant architectures, business-critical infrastructure, safety block diagrams, Markov and semi-Markov chains, variable parameter, macrograph.

## Introduction

### *Motivation*

Critical infrastructures are the range of interacting systems. Failures of such systems can cause partial or total loss of one or few functions, emergency and prior to emergency situations, quick recovery necessity and also redistribution of all system and infrastructure resources. Failures of IT-infrastructure and software-based systems may be caused by different kinds of faults (physical faults of hardware, design faults of software and hardware, interaction faults of software, hardware and system as a whole.<sup>1</sup>

System parameters forming infrastructure and system components can vary in operation. Those variable parameters are dependability and availability parameters, in particular, failure and recovery rates. The variation can be produced by: (1) elimination or importation of new (secondary) design faults, (2) software rejuvenation usage of patches for critical vulnerabilities reduction, (3) upgrade of functionality and evolution of system, (4) variation of recovery time due to change of the number and list of various components faults, etc.

Given condition leads to multiplicative increasing the number of system states and exponential rise of the number of infrastructures states. For instance, if infrastructure consists of  $n$ -systems, each system has  $r$ -states and is described by  $m$ -parameters,  $m_{\text{var}}$  are variable parameters with  $e$  increasing or reducing values, then total number of infrastructure states is  $(r \times m_{\text{var}} \times e)^n$ .

Taking into account variation of dependability and other parameters both systems and infrastructures totally, it is necessary to develop the special analysis methods and application of mathematical apparatus allowing to solve the dimension problem.

### ***Related analysis***

Known works, related to the current problem, are divided into few groups: (i) modeling and quantitative estimation of system and software dependability indicators by use of SW reliability growth models (SRGMs)<sup>2</sup> and models which take into account secondary design faults (defects)<sup>3</sup> and evolution of software,<sup>4</sup> (ii) assessment of SW-based system dependability with different fault-tolerant architectures for critical and business-critical infrastructure,<sup>5</sup> modelling and assessment of availability taking into account features of operation and maintainability aspects, including variation of failure rate.<sup>6</sup> Analysis of these and other works allow to make the following conclusions.

Firstly, the existed SRGMs allow estimating reliability indicators (fault or failure rates, fault probability as function of time, etc.), if sufficiently complete and representative information about testing results is acceptable. It is unknown how these indicators during operation can be estimated taking into consideration detecting and eliminating of design faults. Besides, these changes may occur owing to rejuvenation of SW. Thus, there is problem of taking into account variation of component and system dependability parameters.

Secondly, dependability assessment of fault- and intrusion-tolerant systems and IT-infrastructures is based on application of reliability and safety block diagrams, Markov and semi-Markov chains, FMECA-FTA techniques or Monte-Carlo simulation. Main problems are receiving quantitative indicators of component reliability and system dependability for complex architectures. Markov chains are the most convenient methodological and mathematical apparatus; however, there is problem of the model dimension and regularization of such models for complex systems and infrastructures. Besides, this problem becomes more complex in case of the infrastructures consisting of systems and components with variable parameters.

Our earlier works described an approach to availability assessment of systems with variable failures and recovery rates based on multi-fragmental Markov chains (MFMC).<sup>7</sup> This approach may be adapted to infrastructure analysis but it is necessary

to develop methodology and technique of infrastructure modelling and availability assessment.

The goal of this paper is development of the MFMC-based methodology and technique for modelling and quantitative availability assessment of critical IT-infrastructure consisting of maintained and partially unmanned systems taking into consideration a variation of system and component parameters (in particular, variation of failure rates caused by detection and elimination of design faults). The paper has the following structure. The general approach, initial concepts and examples of infrastructure based on systems with constant and variable parameters analysis are described in the second section. The third section is dedicated to development of MFMC-based infrastructure availability model development technique and its illustration for two-system infrastructure. Example of modelling simplest space IT-infrastructure based on on-board and ground computer systems is described and analyzed in the fourth section. In the last section of the chapter some aspects and practical results of implementation of the proposed technique and directions are discussed.

## Analysis and modelling infrastructures consisting of systems with variable parameters: General approach

### Initial concepts

Let's consider infrastructure I consisting of two interacting systems A and B:  $I = \{A, B\}$ . Each of them is described by functional-and-reliable architecture  $D_a$   $D_b$  in proportion to systems A and B with failure rates  $\lambda_p, \lambda_d$  and failure recovery rate  $\mu_p, \mu_d$  parameters caused by physical  $f_p$  and design  $f_d$  faults.

$$A = \{\lambda_{pa}, \mu_{pa}, \lambda_{da}, \mu_{da}, D_A\};$$

$$B = \{\lambda_{pb}, \mu_{pb}, \lambda_{db}, \mu_{db}, D_B\}.$$

In addition, let's consider that failure rate  $\lambda_{da}$  ( $\lambda_{db}$ ) reduces on constant  $\Delta_{da}$  ( $\Delta_{db}$ ) after design fault  $f_d$  elimination and forms value series:  $\lambda_d, \lambda_d - \Delta_d, \lambda_d - 2\Delta_d, \dots, 0..$  This assumption is based in the number of papers, for instance, on Jelinsky-Moranda model.<sup>8</sup> According to this model failure rate is analogical to the number of remained faults.

Then A(B) system is defined by six parameters. In case of  $\lambda_d \neq 0$  the symbols  $\tilde{A}$  ( $\tilde{B}$ ) further denoted, i.e.:

$$\tilde{A} = \{\lambda_{pa}, \mu_{pa}, \lambda_{da}, \mu_{da}, \Delta_{da}, D_A\};$$

$$\tilde{B} = \{\lambda_{pb}, \mu_{pb}, \lambda_{db}, \mu_{db}, \Delta_{db}, D_B\}.$$

The A and B systems are described with set of states subject to failure and recovery process and to state graph  $G_{\tilde{A}}$  and  $G_{\tilde{B}}$ . For  $\tilde{A}$  and  $\tilde{B}$  systems, state graphs are multi-fragment ( $G_{\tilde{A}}$  и  $G_{\tilde{B}}$ ) in the result of parameter  $\lambda_d$  variation (Figure 1.).

Each of  $F_i$  fragments are describes by value parameter  $\lambda_d - (i - 1)\Delta_d$ . Let's consider  $\lambda_d = (n-1)\Delta_d$  is a state between fragments of given situation when design fault is detected and eliminated. Conversion from  $F_i$  fragment state into the same  $F_{i+1}$ . fragment state.

Let's develop the model of infrastructure I (state graph) for different versions of systems A and B.

### **Infrastructure I={A,B}**

*Simple case.* Let's develop infrastructure I={A,B} model. Let's consider the simple case when each system operates in two states (serviceability state, failure state and recovery) and parameters  $\lambda_d$  are constant. In Figure 2 serviceability states are signed as open circle and non serviceability states are half-hatched. Each system states are signed with different colours. The result of system models combination is shown with graphs of state which are the state combination of two initial systems. There are four states of combined graphs, each of states are received by the means of searching system initial state versions.

*Partly general case.* Combination process for two state systems and for system with the set of states and constant parameters is shown in Figure 3. In state graph of infrastructure, the state subset are given as combination the first system two states and possible states (serviceable and non serviceable) of the second system, more complex system.

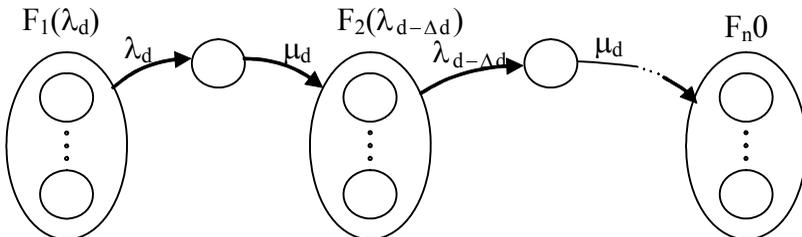


Figure 1: Multi-fragment state graph.

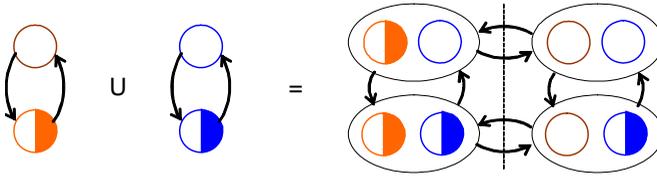


Figure 2: Combination process of systems with two states for infrastructure  $I=\{A,B\}$ .

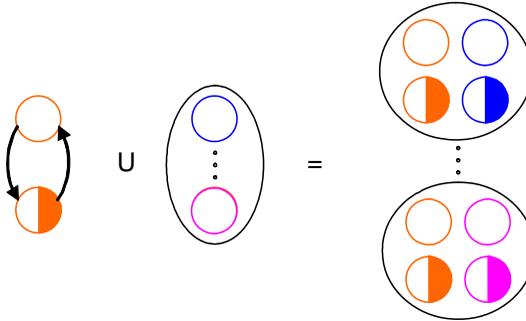


Figure 3: Combination process of systems with two or with set of states for infrastructure  $I=\{A,B\}$ .

*General case.* System combination with the set of states and constant parameters is shown in Figure 4. In this case every set of states is formed as combination of the first and the second system states pair (serviceability and non serviceability).

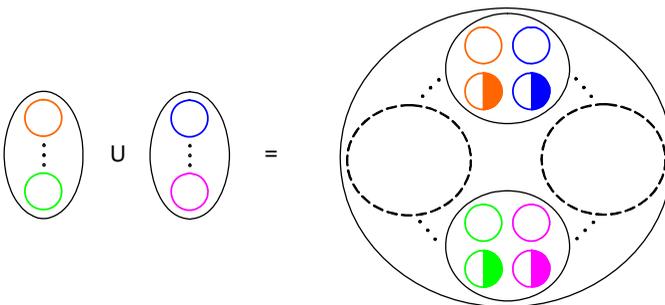


Figure 4: Combination process of system with the set of states for infrastructure  $I=\{A,B\}$ .

**Infrastructure  $I = \{ \tilde{A}, B \}$**

Let's consider combination process of system state graph in case when one system is a variable-parameters system.

*Special case.* Combination process, for two-state system with constant parameters and system with one variable parameter, described with multi-version graph, every fragment in turn has two states, is shown in Figure 5. In initial graph of the second system, except fragments, there are states of transition between fragments caused by event of parameters variation (for instance, design fault detection and elimination) is recording. The final state graph of infrastructure (macrograph) is described by set of fragments which are the result of first and second system states combination. In other words, fragment structure is formed as shown in Figure 2.

$$F_1(\lambda_{da}=\text{var}, \lambda_{db}) \cup F_1(\lambda_{da}=\Delta_{da}, \lambda_{db}) \cup F_{na}(\lambda_{da}=0, \lambda_{db})$$

*General case.* Graphs combination process of system with the set of states, when one of them operates with variable parameters is shown in Figure 6. Final macrograph is shown schematically and fragments set of states in macrograph is a result of state combination as shown in Figure 4. It should be stressed that the number of delta transition states between fragments is determined by the number of fragment states which allow transition. In general case the number of those states is equal to number of initial fragment states. Transition through such states implement into the identical state of follow fragment. The number of delta transitions states will reduce if taking into account assumptions that states with failure overlap set aside of system (infrastructure).

**Infrastructure I = {  $\tilde{A}$ ,  $\tilde{B}$  }**

The process of combination is shown in Figure 7.

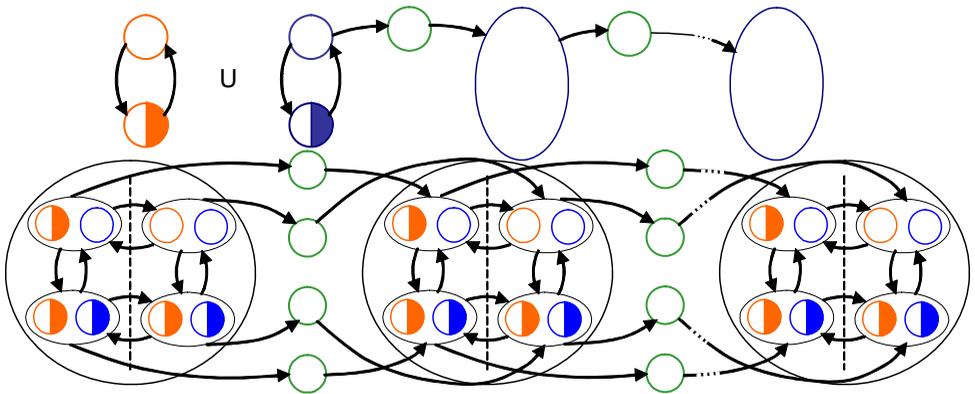


Figure 5: Combination process of two-state system with constant parameters and one-state system with variable parameter and final macrograph.

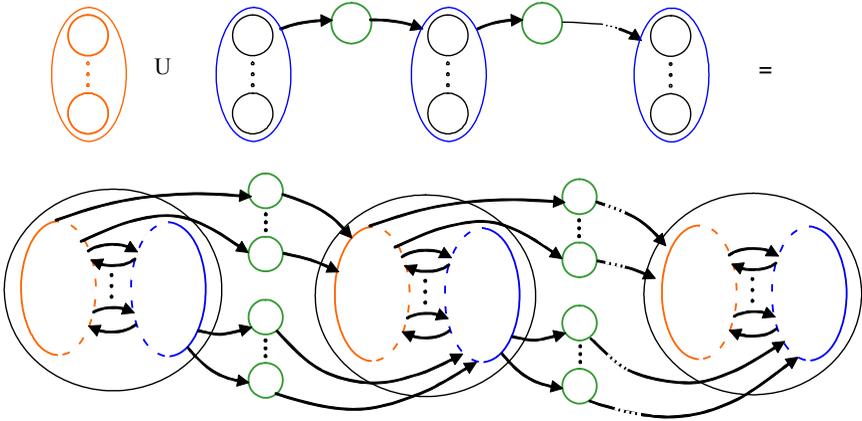


Figure 6: Graphs combination process of system with the set of states, when one of them operate with variable parameters and final macrograph.

### Infrastructure $I = \{ \tilde{A}(\lambda_d, \mu_d), B \}$

Let's analyze infrastructure model versions that consist of systems with two or more variable parameters of one or both systems. Infrastructure  $I = \{ \tilde{A}(\lambda_d, \mu_d), B \}$  is the most simple version of such infrastructures. This infrastructure consists of two systems: system  $\tilde{A}$  with two variable parameters (for instance,  $\lambda_d$  and  $\mu_d$ ) and system  $B$  with constant parameters. Three variant of system  $\tilde{A}$  parameters variation for this infrastructure can be possible:

1. Synchronous parameters variation (by the same reason). In this case state macrograph is similar to graph in Figure 6, or one (horizontal or vertical) of macrograph part which is shown in Figure 7. The chain of macrograph fragments is described as:

$$L = \{ F_1(\lambda_{da0}, \mu_{da0}; \mu_{db}, \lambda_{db}), \dots, F_i((\lambda_{da} - \Delta\lambda_{daj}), (\mu_{da} - \Delta\mu_{daj}); \mu_{db}, \lambda_{db}), \dots, F_{na}(\lambda_{da} = 0, \mu_{dae}; \mu_{db}, \lambda_{db}) \},$$

if,  $\lambda_{da0}, \mu_{da0}$  and  $\lambda_{da} = 0, \mu_{dae}$  - are initial and final parameters  $\lambda_{da}$  and  $\mu_{da}$  values.

2. Parameters vary step-by-step and one-by-one (by different causes). In this case state macrograph is similar to previous case. The difference is in the number of macrograph fragments and their parameter variation value:

$$L = \{ F_1(\lambda_{da0}, \mu_{da0}; \mu_{db}, \lambda_{db}), \dots, F_i((\lambda_{da} - \Delta\lambda_{daj}), \mu_{da}; \mu_{db}, \lambda_{db}), \dots, F_{na}(\lambda_{da} = 0, \mu_{dae}; \mu_{db}, \lambda_{db}) \}.$$

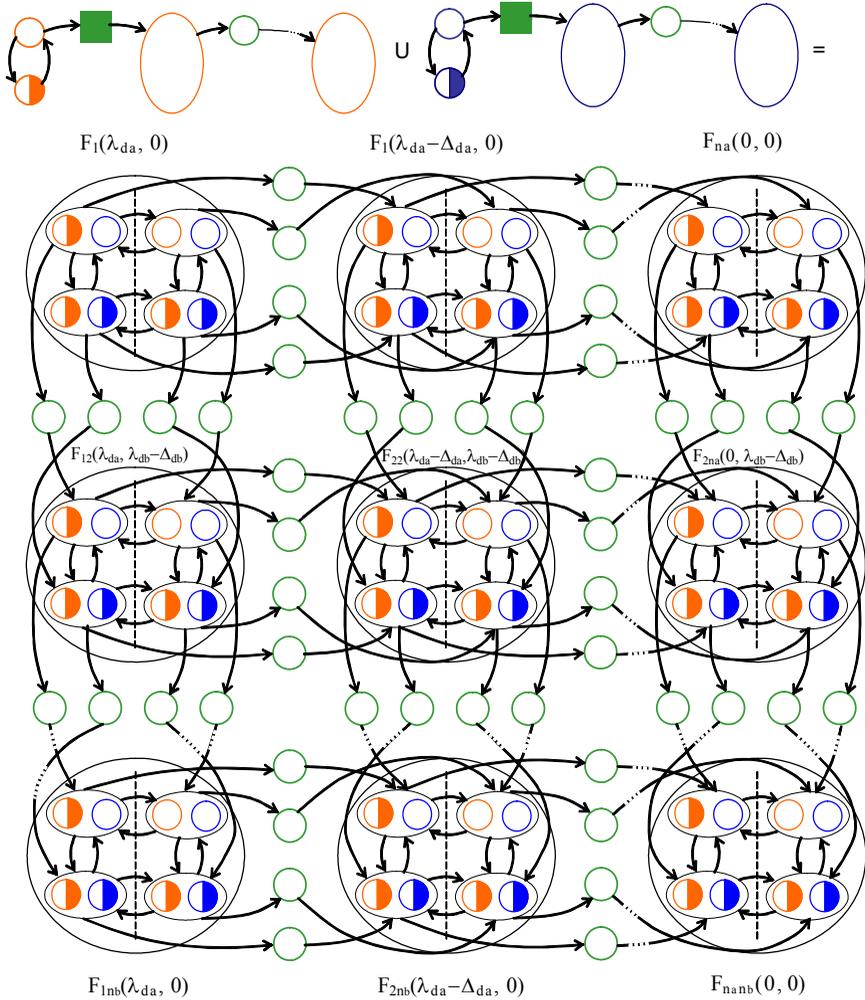


Figure 7: Graphs combination process of system with the set of states and one variable parameters, final macrograph.

- Parameters vary one-by-one and in any sequence. In this case state macrograph is similar to Figure 7. Horizontal  $L_{hq}$  and vertical  $L_{vs}$  chain is described by:

$$L_{hq} = \{F_{q1}(\lambda_{da0}, \mu_{da} - \Delta_{\mu daq}; \mu_{db}, \lambda_{db}), \dots, F_{qi}((\lambda_{da} - \Delta\lambda_{daj}), \mu_{da} - \Delta_{\mu daq}); \mu_{db}, \lambda_{db}), \dots, F_{naq}(\lambda_{da} = 0, \mu_{da} - \Delta_{\mu daq}; \mu_{db}, \lambda_{db})\};$$

$$L_{vs} = \{F_{1s}(\lambda_{da} - \Delta\lambda_{das}), \mu_{da0}; \mu_{db}, \lambda_{db}), \dots, F_{is}((\lambda_{da} - \Delta\lambda_{das}), \mu_{da} - \Delta\mu_{das}); \mu_{db}, \lambda_{db}), \dots, F_{nas}((\lambda_{da} - \Delta\lambda_{das}), \mu_{dae}; \mu_{db}, \lambda_{db})\}.$$

More complex infrastructure models can be received based on all version combination which are described in this section.

### Availability model development and analysis technique of infrastructure based on systems with variable dependability parameters

A sequence of model infrastructure development is the following. Let's note that this sequence is described for example of infrastructure consisting of two systems  $I = \{\tilde{A}, \tilde{B}\}$  and each system is characterized one variable parameter (failure rate  $\lambda_d$  caused by design faults) but it may be generalized for more complex case. The appropriate remarks concerning possible technique generalization are given for each stages.

*Stage 1.* Models (state graphs) of each system  $A(\tilde{A})$  and  $B(\tilde{B})$  forming infrastructures are developed. Model specification degree depends on component count and states which are important for the assessment. For the infrastructure analysis one should be chosen the minimum acceptable state level of detail permitting to decompose set of states of each system according to a criterion "components with constant and variable parameters."

*Stage 2.* Sets of variables  $\pi_j$  are refined by each system  $A_j$  (systems  $A(\tilde{A})$  and  $B(\tilde{B})$ ), forming infrastructure, and also change at various events. For the parameters "failure rate"  $\lambda_d$  change occurs as a result of detection and elimination of design fault, i.e. due to changes in the number of faults. The variation function for the parameter  $\lambda_d$  is specified by reliability model (for example, SRGM). In the special case this function can be changed (decrement) discretely by the value  $\Delta\lambda_{di}$ , though  $\Delta\lambda_{di}$  is the function of the remaining number of design faults,  $N_i$  and can be calculated subject to the initial model (SRGM<sup>9</sup>). The number of levels of change for the parameter  $\lambda_d$  can be calculated if  $\Delta\lambda_{di} = \Delta\lambda_d$  according to the formula:

$$e(\lambda_d) = \lambda_d / \Delta\lambda_d.$$

Let's call this indicator as a depth of parameter variation. Thus, depth of parameter variation  $e_{jk}$  should be calculated for each variable parameter of each system.

*Stage 3.* Common for infrastructure scripts of value variable change of systems  $\tilde{A}$  and  $\tilde{B}$  are determined, on the basis of possible parameter combinations. Combination count  $w$  specifies dimension of multi-fragment state graph of infrastructure  $G_I$ .

*Stage 4.* State graphs of systems  $G_{A_j}$  (graphs  $G_A$  and  $G_B$ ) are designed at fixed (initial) value variables. Method of graph design is standard for systems describing in Markov and semi-Markov chains.

*Stage 5.* Multi-fragment state graphs  $MG_{A_j}$  (graphs  $MG_A$  and  $MG_B$ ) are designed subject to change of variable set  $\pi_j$  ( $\lambda_{da}$ ,  $\lambda_{db}$ ). Each graph contains initial fragment, e-1 of one-type internal and final fragments.

*Stage 6.* Combined state graph of infrastructure  $MG_I$  is designed by means of graph composition  $MG_{A_j}$  (graphs  $MG_A$  and  $MG_B$ ). Set of states in the general case is determined as Cartesian product of states  $M_A \times M_B$ .

## **Case-study: an example of availability model development for space computer-based infrastructure**

### *Description of study infrastructure*

As a case-study let's consider the block diagram of infrastructure on the base of a space complex (Figure 8).<sup>10</sup> In fact such a structure consists of two interacting systems: on-board information-management system (IMS) of a spacecraft (system A, Figure 9a) and earth information-management system (system B). Develop and research the availability model of this infrastructure under the assumption that majorizing is used for the on-board information-management system (IMS) and replacement redundancy is used for earth information-management system. Reliability block diagrams (RBD) of systems A и B are shown in Figures 9b and 9c respectively.

Let's consider that each system has one variable parameter ( $\lambda_{d1}$  и  $\lambda_{d2}$ ), in this infrastructure, i.e. the research infrastructure is related to the class  $\mathbf{I} = \{\tilde{\mathbf{A}}(\lambda_{d1}), \tilde{\mathbf{B}}(\lambda_{d2})\}$ . Such assumption is close to practice since some cases are known, when design faults are detected under application in on-board and earth systems. Elimination of design faults and recovery of systems can be implemented by the means of special hardware and software tools built-in on-board systems allowing the correction of performing algorithms and programs.

### *Development and research of the system $\tilde{\mathbf{A}}$ model*

The system  $\tilde{\mathbf{A}}$  is described by six parameters:

$$\tilde{\mathbf{A}} = \{\lambda_{p1}, \mu_{p1}, \lambda_{d1}, \mu_{d1}, \Delta_{d1}, D_A\}.$$

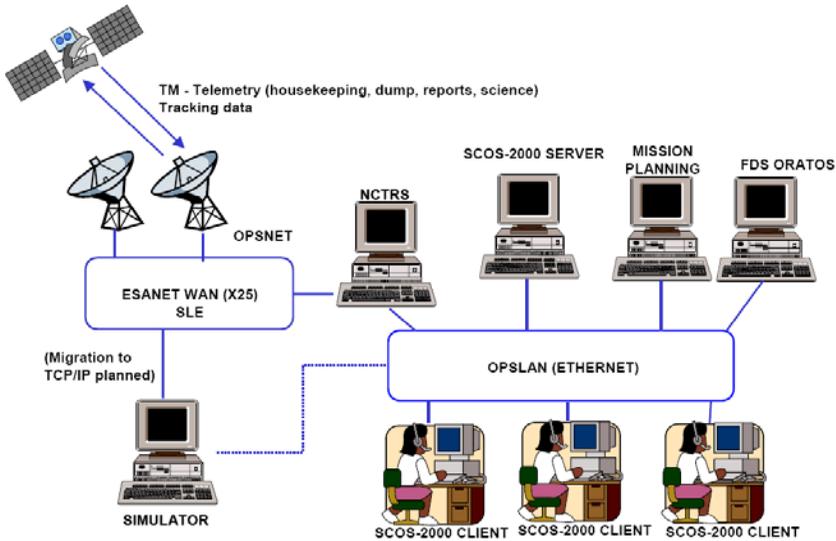


Figure 8: Block diagram of space infrastructure.

Multi-fragment graph  $MG_A$  of the system subject to parameter  $\lambda_{d1}$  change is shown in the fig. 10. After fault demonstration  $f_d$ , failure rate  $\lambda_{d1}$  reduces on certain value  $\Delta_{d1}$  and forms values  $\lambda_{d1}, \lambda_{d1} - \Delta_{d1}, \dots, \lambda_{d1} - i\Delta_{d1}, \dots, \lambda_{d1} - (e_1-1)\Delta_{d1}, 0$ . Graph contains the initial fragment  $F_1, F_{e_1-1}$  one-type internal and final fragment  $F_n$ . Research results of this system is shown in Figure 11. In this figure dependencies of availability function based on the following parameters value ( $\lambda_{p1}= 1e-5; \mu_{p1}= 0,1; \lambda_{d1}= 1e-4; \Delta_{d1}=5e-5; \mu_{d1}= 0,02$ ) are shown.

**Model development and research of system  $\tilde{B}$**

System  $\tilde{B}$  is also characterized by six parameters:

$$\tilde{B} = \{ \lambda_{p2}, \mu_{p2}, \lambda_{d2}, \mu_{d2}, \Delta_{d2}, D_B \}.$$

Multi-fragment graph  $MG_B$  system subject to parameter  $\lambda_{d2}$  change is shown in the Figure 12. After fault detection  $f_d$  failure rate  $\lambda_{d2}$  decreases by a constant  $\Delta_{d2}$  and forms the series of values:  $\lambda_{d2}, \lambda_{d2} - \Delta_{d2}, \dots, \lambda_{d2} - i\Delta_{d2}, \dots, \Delta_{d2}, \dots, \lambda_{d2} - (e_2-1)\Delta_{d2}, 0$ . By analogy with the system  $\tilde{A}$  graph contains an initial fragment  $e_2-1$ , one-type internal and final fragments.

Research results of this system is shown in Figure 13. In this figure dependencies of availability function based on the following parameters value ( $\lambda_{p2}= 1e-4$  1 per hour;  $\mu_{p2}= 0,1; \lambda_{d2}= 1e-4; \Delta_{d2}=5e-5; \mu_{d2}= 0,04$ ) are shown .

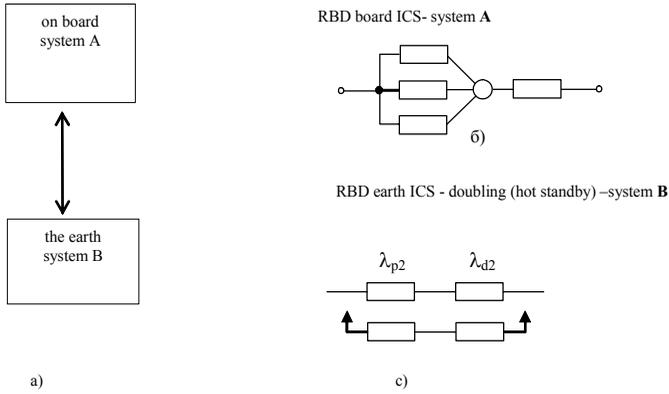


Figure 9: Simplified infrastructure block-diagram (a) and RBDs of systems A (b) and B (c).

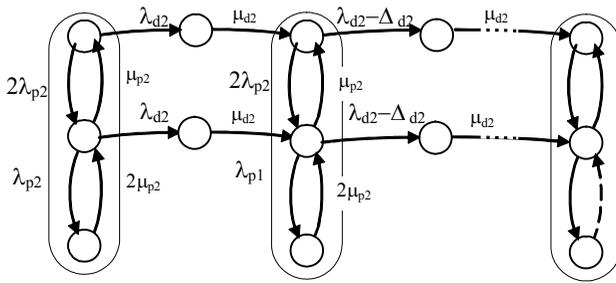


Figure 10: Graph of system  $\tilde{A}$ .

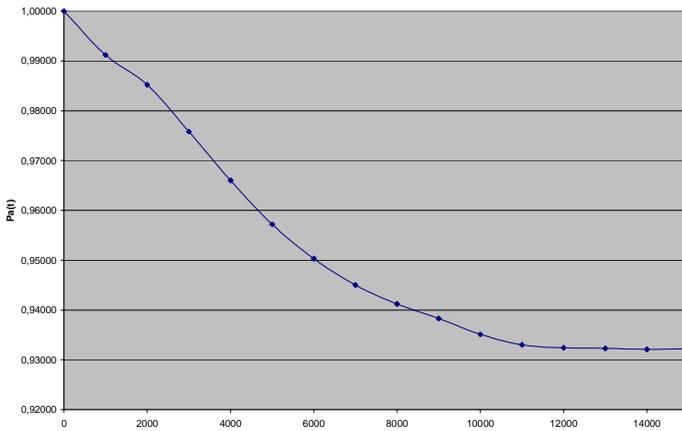


Figure 11: Dependency diagram of  $P_a(t)$  (availability function) of system  $\tilde{A}$ .

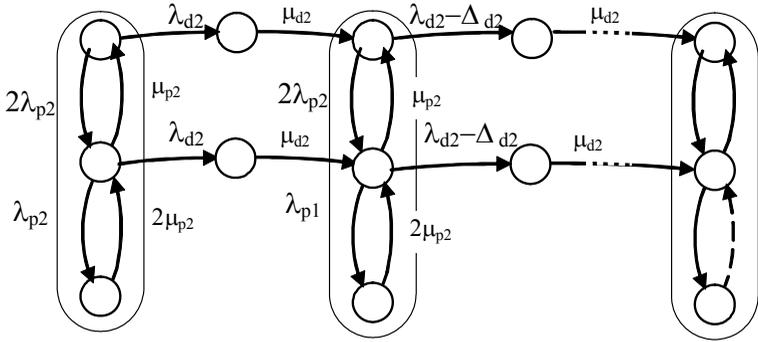


Figure 12: Graph of system  $\tilde{B}$ .

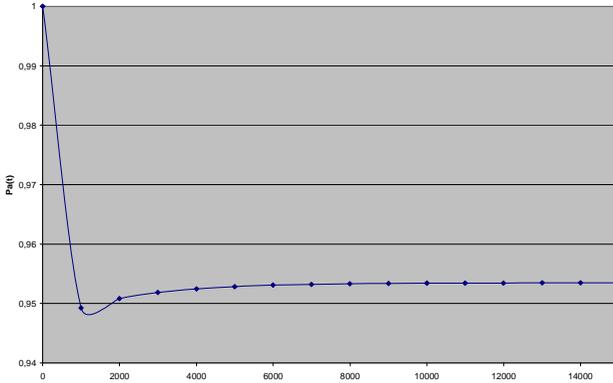


Figure 13: Dependency diagram of  $P_a(t)$  (availability function) of system  $\tilde{B}$ .

**Model development and research of infrastructure**

In developing the infrastructure of the state graph the following symbols are used:

-  SW and HW components of infrastructure I up-state;
-  HW component failure ( $f_p$ ) of system  $\tilde{B}$ ;
-  HW component failures of two channels of system  $\tilde{B}$ ;
-  HW component failure of system  $\tilde{A}$ ;
-  HW component failures of systems  $\tilde{A}$  and  $\tilde{B}$ ;

-  HW component failure of system  $\tilde{\mathbf{A}}$  and failures of two channels of system  $\tilde{\mathbf{B}}$  caused by HW failures;
-  failures of two channels of system  $\tilde{\mathbf{A}}$  caused by HW failures;
-  failures of two channels of system  $\tilde{\mathbf{A}}$  caused by HW failures and failure of one channel of system  $\tilde{\mathbf{B}}$  caused by HW;
-  failure of infrastructure  $\mathbf{I} = \{ \tilde{\mathbf{A}}, \tilde{\mathbf{B}} \}$  caused by HW failures;
-  failures of systems  $\tilde{\mathbf{A}}$  and  $\tilde{\mathbf{B}}$  caused by SW failures ( $f_d$ ).

Initial fragment of multi-fragment graph of infrastructure  $\mathbf{I} = \{ \tilde{\mathbf{A}}, \tilde{\mathbf{B}} \}$  is shown in Figure 14.

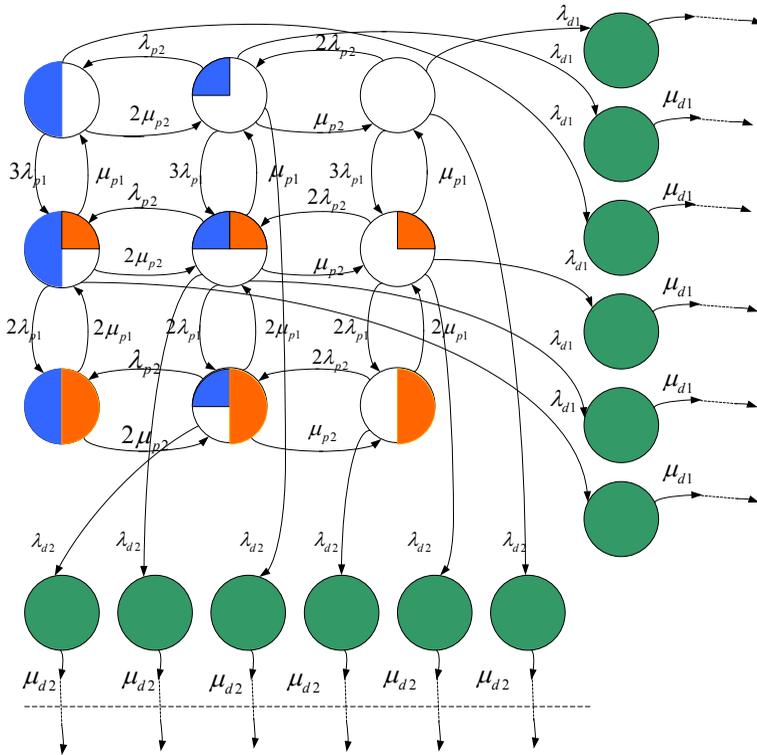


Figure 14: Initial fragment of infrastructure multi-fragment graph.

Internal fragments of the model are analogous to the initial fragment according to the set of states (Figure 15). The main difference is in values of  $\lambda_{d1}$  and  $\lambda_{d2}$  that are decreased by values of  $\Delta\lambda_{d(1,2)}$  after removing next shown design fault of systems  $\tilde{\mathbf{A}}$  and  $\tilde{\mathbf{B}}$ .

The model contains final fragments (Figure 16), The main difference of these fragments is removing software design faults of systems  $\tilde{\mathbf{A}}$  and  $\tilde{\mathbf{B}}$ .

Research results of this system are shown in the Figure 17.

**Conclusion**

Main problem of critical infrastructures availability assessment is high complexity of models which increases if an infrastructure consists of systems and components with variable dependability parameters. A set of infrastructure states, in fact, is defined as Cartesian product of system states sets taking into account variation of system and component parameters. The proposed methodology and technique of availability infrastructure analysis and modelling are based on apparatus of multi-fragmental Markov chains. It is reached through discretisation of rates and presentation Markov chain as a set of repetitive regular fragments.

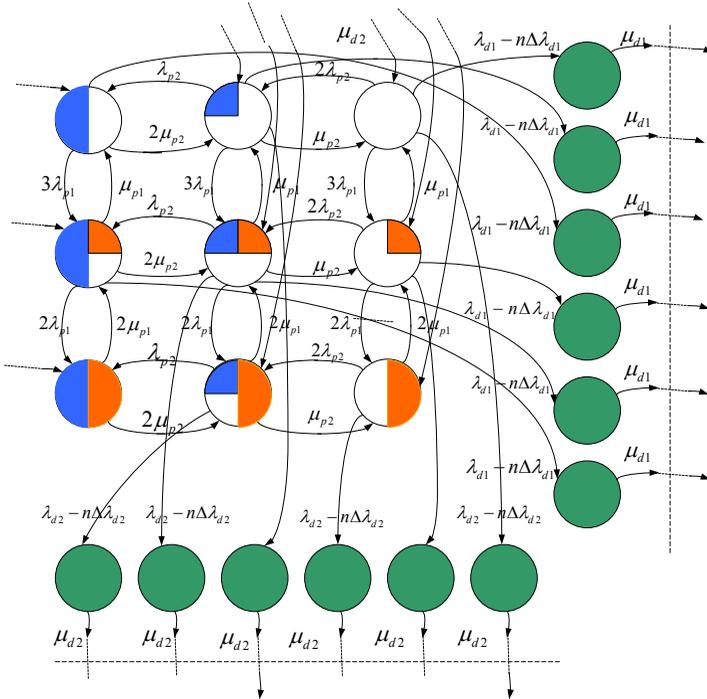


Figure 15: Internal fragment of multi-fragment graph of infrastructure.

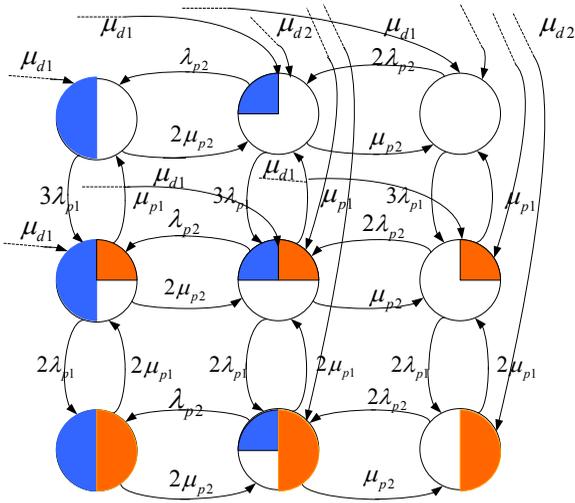


Figure 16: The final fragment of multi-fragment graph of infrastructure

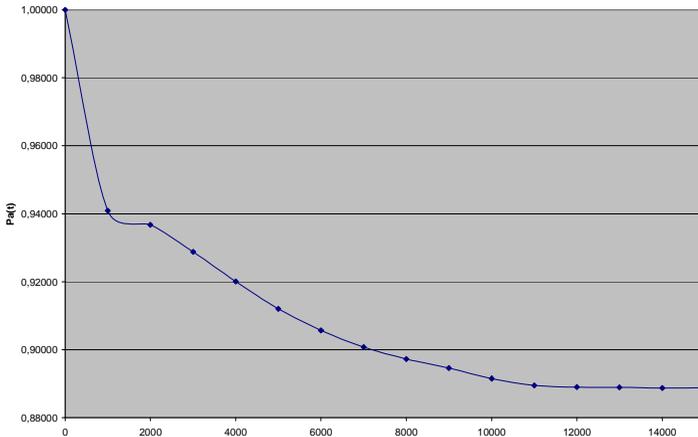


Figure 17: Dependency diagram of  $P_a(t)$  (availability function) of system I.

In the frameworks of the paper this technique was presented for critical IT-infrastructure consisting of two systems with variable failure rate caused by variation of software design faults.

The analysis of research results allows concluding that OFM-based value of availability function is more than MFM-based values on early stage of system operation if processes of detection and elimination of SW design faults are implemented. How-

ever the OFM-based availability function after a certain “crucial” time point becomes less than MFM-based values. So, when OFM selecting increases the risks of false estimation of CS dependability.

Trustworthiness of modelling results and technique as a whole was confirmed by MC-based simulation results for several CSs. Improved Markov models of CS dependability were researched for different applications. It allows to increase accuracy of dependability (availability function) assessment. The developed models permit to research a behaviour of CSs at non-stationary mode and define time of decreasing availability caused by SW fault recovery. Given research results of sub-systems  $\tilde{\mathbf{A}}$  and  $\tilde{\mathbf{B}}$  and infrastructure I confirm the statement.

Further research will likely address:

- development of the MFMC-based technique for semi-Markov chains taking into consideration different distribution laws of time between failures and recoveries for different infrastructure, system and component faults (physical, design, interaction faults) and different kinds of intrusions;
- optimization of the parameters for different procedures of maintainability and state management of systems and infrastructures using planned-prophylactic strategies and flexible strategies, which are found on using data about actual information-technical state;
- improvement of the proposed technique to infrastructure analysis by use of object-oriented modeling approach.

## Notes:

---

<sup>1</sup> Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, “Basic Concepts and Taxonomy of Dependable and Secure Computing,” *IEEE Transactions on Dependable and Secure Computing* 1:1 (2004): 11–33.

<sup>2</sup> Nancy Leveson, “Role of Software in Spacecraft Accidents,” *Journal of Spacecraft and Rockets* 41:4 (2004): 564–75; Michael R. Lyu, *Handbook of Software Reliability Engineering* (McGraw-Hill, 1996); John D. Musa, Anthony Iannino, and Kazuhira Okumoto, *Software Reliability: Measurement, Prediction, Application* (New York, NY: McGraw-Hill, 1990).

- <sup>3</sup> Nazim Madhavji, Juan Fernandez-Ramil, and Dewayne Perry, eds., *Software Evolution and Feedback: Theory and Practice* (Chichester: John Wiley, 2006).
- <sup>4</sup> Michael Butler, Cliff B. Jones, Alexander Romanovsky, and Elena Troubitsyna, eds., *Rigorous Development of Complex Fault-Tolerant Systems*, LNCS 4157 (Berlin: Springer, 2006).
- <sup>5</sup> Mikhail A. Yastrebenetsky, ed., *NPP I&Cs: Problems of Safety* (Kyiv: Technika, 2004), (translated in the U.S. by NPC, 2007); Nestor Peccia, “SCOS-2000 ESA’s Spacecraft Control for the 21<sup>st</sup> Century,” Ground System Architectures Workshop (GSAW 2003), Manhattan Beach, California, 4-6 March 2003.
- <sup>6</sup> Vyacheslav Kharchenko, Oleg Odarushchenko, et al., *Modeling Dependable Systems and Networks* (Kharkiv: National Aerospace University, 2008).
- <sup>7</sup> Kharchenko, Odarushchenko, et al., *Modeling Dependable Systems and Networks*; Vyacheslav Kharchenko and B. Konorev, eds., *High Availability Technologies for Space Systems* (Kharkiv: National Space Agency of Ukraine, 2010).
- <sup>8</sup> Leveson, “Role of Software in Spacecraft Accidents”; Musa, Iannino, and Kazuhira Okumoto, *Software Reliability: Measurement, Prediction, Application*.
- <sup>9</sup> Vyacheslav Kharchenko and B. Konorev, eds., *Space Systems Software Quality Assurance and Assessment* (Kharkiv: National Space Agency of Ukraine, 2007).
- <sup>10</sup> Peccia, “SCOS-2000 ESA’s Spacecraft Control for the 21st Century.”

**VYACHESLAV KHARCHENKO** – see the CV on p. 51 of this volume.

**OLEG ODARUSHCHENKO** – see the CV on p. 145 of this volume.

**VALENTINA ODARUSHCHENKO** – see the CV on p. 145 of this volume.