Multifragmentary models of functional safety of information and control system considering manifestation and elimination of hardware-software defects

Vyacheslav Kharchenko[1,3] [0000-0001-5352-077X], Yuriy Ponochovnyi[1,2] [0000-0002-6856-2013], Artem Boyarchuk[1][0000-0001-7349-1371], Anton Andrashov[3][0000-0003-2238-0449]

[1] National Aerospace University KhAI, Kharkiv, Ukraine

V.Kharchenko@khai.edu, a.boyarchuk@csn.khai.edu

[2] Poltava State Agrarian Academy PSAA, Poltava, Ukraine

pnch1@rambler.ru

[3] Research and Production Company Radiy, Kirovograd, Ukraine

a.andrashov@radiy.com

Abstract. The information and control system (I&CS) of Nuclear Power Plant (NPP) is considered as a set of three independent hardware channels including on-line testing system. NPP I&C system's design on programmable platforms is rigidly tied to the V-model of the life cycle. Functional safety and availability during its life cycle are assessed using Markov and Multifragmentary models. Multifragmentary models are used to assess availability function and proof test period. The multifragment model MICS31 contains an absorbing state in case of hidden faults and allows to evaluate risks of "hidden" unavailability. The MICS41 model simulates "migration" of states with undetected failures into states with detected faults. The results of Multifragmentary modeling (models MICS31 and MICS42) are compared to evaluate proof test period taking into account requirements for SIL3 level and limiting values of hidden fault probabilities.

Keywords: Multifragmentary models, Functional Safety Modeling, Information & Control System, Undetected Software Failure

Key terms. Mathematical Modeling, Mathematical Model, Software Systems

1 Introduction

For different classes of critical systems (medical equipment, banking systems, road, air, railway transport and nuclear power plants (NPP)) very strict requirements have been developed. These requirements determine both the system characteristics from the group of non-functional requirements (availability, reliability, safety, etc.) and the

content of the life cycle phases. During the development cycle, it is possible to change the architecture of the information and control system of NPP project and correct the parameters of its elements. Such actions require justification, which uses special mathematical models to confirm the fulfillment of design requirements.

This paper discusses the class of the information and control systems on programmable platforms, which are used in reactor protection system of NPP in normal operation. This class of information and control system is based on the 2oo3 architecture without versioning with the control system and is described in detail in [1,2]. Expansion of the previously reviewed model consists of detailing the diagnostic procedures. This paper discusses the separate diagnosis of hardware and software with DC_{HW} and DC_{SW} parameters. As a separate process, regular proof tests are highlighted, during which latent HW and SW defects, that are not detected by the integrated control system, are detected.

Studies carried out in [3] have shown that achievement of the requirements of industrial systems on proof test $T_{Areq} \geq 3$ years' period can be by influencing parameters of the functional safety of SW (reducing intensity of dangerous SW $\lambda_{D\ S}$ failure or increasing the completeness of control of dangerous SW DC_S failure). For information and control systems on programmable platforms, SW defects (architectural project defects) are entered into the system of bug tracking after their detection and eliminated within a certain time interval. The elimination of the software defect (assuming no new defects are introduced) causes a decrease in SW failure rate, as shown in [4,5]. To adequately display the elimination of SW defects and reduce the failure rate in studies [6,7], it was suggested to use the mathematical apparatus of multi-fragmentary modeling.

At first glance, the elimination of software defects may cause a desire to use the information and control system project with the initial high intensity of dangerous SW failures, because defects will be identified and eliminated over the time. But this decision should be justified by the results of the study of the corresponding models of the information and control system with the elimination of defects causing dangerous SW failures.

In this paper, multi-fragmentary models of functioning of the information and control system under the conditions of manifestation of dangerous HW and SW failures and elimination of identified SW defects are studied. For each model, graduated and oriented graphs are constructed; using the Matlab functions, systems of Kolmogorov-Chapman differential equations are constructed and solved. As a result, the values of the proof test T_{Areq} period for the SIL3 level and input parameters are obtained, at which the condition $T_{Areq} \geq 3$ years for industrial systems is satisfied.

2 Approach and modeling technique

2.1. Model specification

In this work we develop six models using Markov process theory as show in Table 1. Models MICS01 and MICS02 were studied at the papers [1,8] with the assumption of manifestation of only dangerous HW failures.

Table 1. Functional safety models of the information and control system NPP

General characteristics of the model	Model specification	Conventional notions
A) Markov model for evaluating the functional safety of the information and control system with an absorbing state	- three groups of states (without manifestation of SW defect, with detected SW failure and with undetected SW failure) - there is one absorbing state (output only after the proof test)	$M_{ICS}01$
B) Markov model for evaluating the functional safety of the information and control system with the migration of hidden failures	- three groups of states (without manifestation of SW defect, with detected SW failure and with undetected SW failure) - there is no absorbing state (after the manifestation of the undetected failure, its "migration" is possible before the proof test)	$M_{ICS}02$
C) Multifragmentary models for evaluating functional safety of the information and control system with incomplete elimination of design defects	- several fragments, in each fragment there are three groups of states - there is the absorbing state in each fragment (output only after the proof test)	$M_{ICS}31$
	- several fragments, in each fragment there are three groups of states - there is no absorbing states (after the manifestation of the undetected failure, its "migration" is possible before the proof test)	$M_{ICS}41$
D) Multifragmentary models for evaluating functional safety of the information and control system with incomplete elimination of design defects	- several fragments, in the first fragments there are three groups of states - in the last fragment, there are two groups of states, since all SW defects are eliminated - there is the absorbing state in each fragment (output only after the proof test)	$M_{ICS}32$
	- several fragments, in the first fragments there are three groups of states - in the last fragment, there are two groups of states, since all SW defects are eliminated - there is no absorbing states (after the manifestation of the undetected failure, its "migration" is possible before the proof test)	$M_{ICS}42$

The assumptions during models building are as follows:

- the events of failures and restoration of hardware channels and software (until the defect is eliminated) constitute of the simplest flows (stationary, ordinary and without aftereffect), with the corresponding constant λ_{HW}, λ_{SW} (failure rate) and μ_{HW}, μ_{SW} (recovery intensity) parameters;
- the system uses identical hardware channels with the same failure rates;
- the failure rate of the majority body and the control system is negligibly small and these systems are assumed to be absolutely reliable in the considered model;
- the model considers only dangerous failures of hardware channels of the information and control system and SW information and control system, the intensity of the dangerous failures is estimated according to the method [2] and data obtained for similar systems [9] as $\lambda_{D\,HW} = 0.497 * \lambda_{HW}$; $\lambda_{D\,SW} = 0.476 * \lambda_{SW}$;

- when diagnosing a part of dangerous failures, the intensity of detected dangerous failures is $\lambda_{DD\,HW} = \lambda_{D\,HW} * DC_{HW}$, and the intensity of undetected dangerous failures.

2.2. Multifragmentary model for evaluating the functional safety of the information and control system with the absorbing states

MICS31 multifragmentary model is improved in comparison with MICS01 and contains absorbing states in each fragment. The application of the principle of multifragmentation [7] allows us to adequately make the model of the elimination of design defects with the subsequent decrease in the intensity of dangerous SW failures. The graduated graph of the model is presented in Fig.1. The two-fragmentary model describing the operation of the information and control system, in the course of which one design defect is eliminated, is considered. Each fragment of the model contains 25 states: S0 ... S24 in the initial F0 fragment and S25 ... S49 in the final F1 fragment. The initial operation of the system is described by the change of states, as in MICS01 model, but after detecting the dangerous SW failure, which manifests itself with λD S 0 intensity, the mechanism for its elimination is initiated, after which the system goes into the new fragment of F1 states, which is modeled by the corresponding S18 → S25, S19 → S26, S20 → S28, S21 → S29, S22 → S31, S23 → S32, S24 → S33 transitions with μSR>μS intensity.

In the new fragment, the system functions in the same way as described for MICS01 model [1] (taking into account the “shift” of state numbering by 25). At the same time, in F1 fragment, the intensity of the manifestation of dangerous SW failures is equal to $\lambda_{D\,S\,1}$, and is defined as:

$$\lambda_{DSi} = \lambda_{DSi-1} - \Delta\lambda_{DS} \quad (1)$$

Since design defects remain in the system, after manifestation and detection of the dangerous SW failure, the system restarts to eliminate its consequences with μS intensity, which is modeled by S41 → S25, S42 → S26, S44 → S28, S45 → S29, S47 → S31, S48 → S32, S49 → S33 transitions.

In all fragments of MICS31 model, there are absorbing states: S17 in F0 fragment and S42 in F1 fragment.

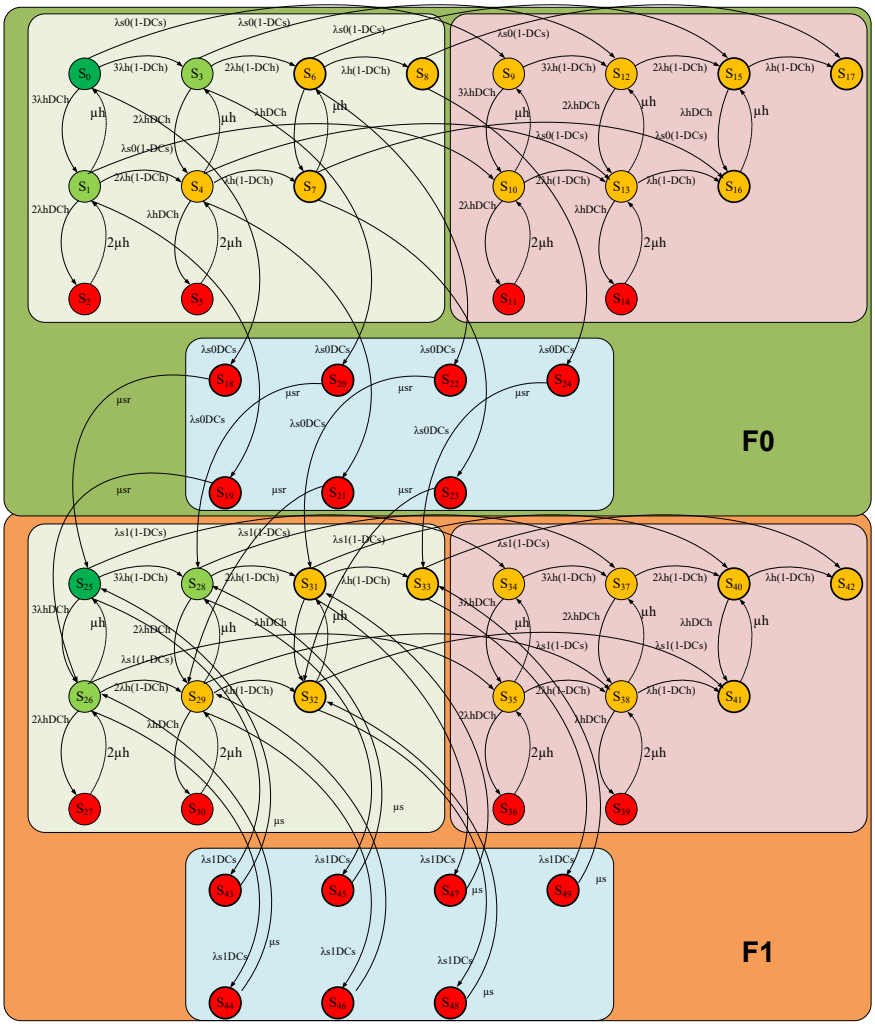

Fig. 1. Marked graph of ICS model with absorbing states and elimination one SW defect

2.3. Multifragmentary model for evaluating the functional safety of the information and control system with the migration of failures

In MICS41 multifragmentary model, the assumption of the "migration" of hidden failures into decisive ones, described earlier for MICS02 model, was adopted. There are no absorbing states on the graduated graph of the model (Fig. 2). Transitions from the undetected dangerous failure state are simulated without additional measures (proof test). This model also deals with the elimination of the decisive DC SW after its manifestation. This is modeled as in MICS31 model by S18 → S25, S19 → S26, S20 → S28, S21 → S29, S22 → S31, S23 → S32, S24 → S33 transitions with μSR

intensity. In the last F1 fragment, system recovery after the dangerous SW failure is performed by restarting with μs intensity without its elimination.

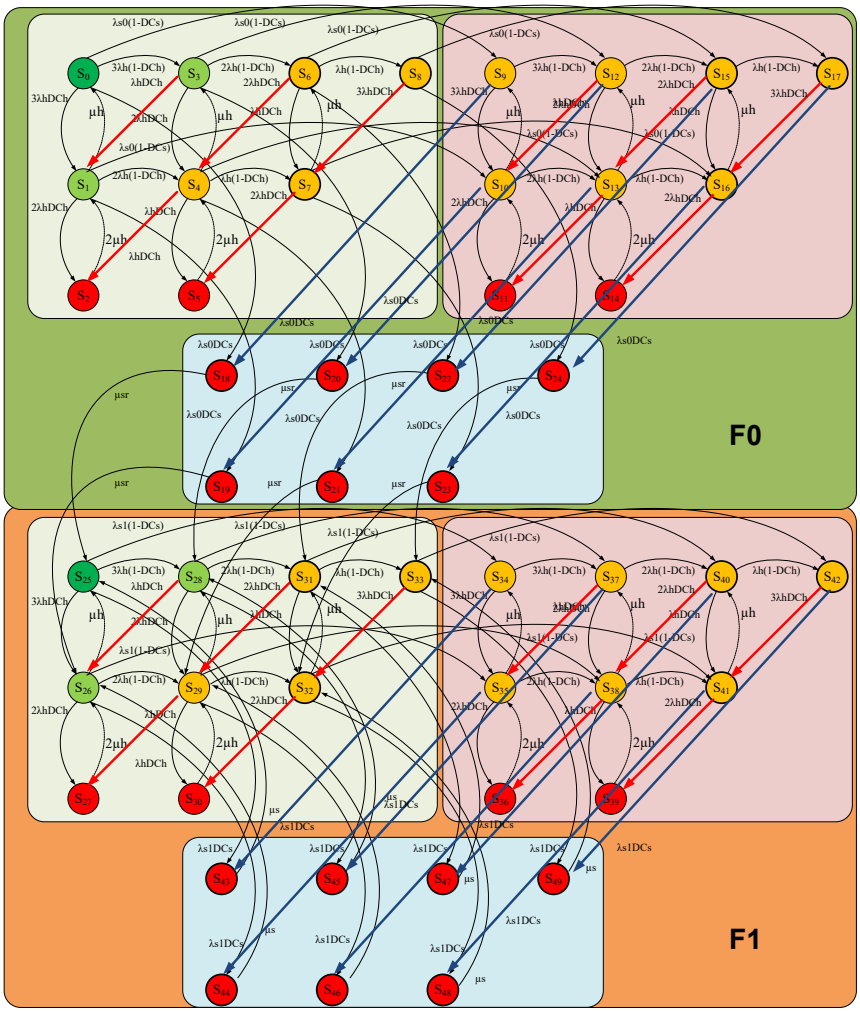

Fig. 2. Marked graph of multi fragmentary ICS model with migration of hidden failures MICS41

The number and nature of the states of the MICS41 model graph is identical to the previous MICS31 model. In addition to the MICS31 model, transitions have been added that simulate the migration of hidden HW failures: S3→S1, S4→S2, S6→S4, S7→S5, S8→S7, S12→S10, S13→S11, S15→S13, S16→S14, S17→S6; transitions that simulate the migration of hidden SW failures: S9→S18, S10→S19, S12→S20, S13→S21, S15→S22, S16→S23, S17→S24 (for initial fragment F0). For F1 fragment migration of hidden HW failures is presented in transitions S28→S26, S29→S27, S31→S29, S32→S30, S33→S32, S37→S35, S38→S36, S40→S38, S41→S39, S42→S41; migration of hidden SW failures is presented in transitions S34→S43,

S35→S44, S37→S45, S38→S46, S40→S47, S41→S48, S42→S49.

4 Simulation and comparative analysis

The calculation of the availability indicators is performed for the input data from Table 2. To construct the matrix of the Kolmogorov-Chapman system of differential equations, we use the matrixA function [4]. The Kolmogorov solution was performed in the Matlab system using the ode15s method for the time interval of [0 ... 50000] hours. The results of the solution are presented in the graphical form in Fig. 3.

Table 2. Values of input parameters of simulation processing

#	**Parameter**	**Base value**
1	λ_{Dh}	46.04622e-6 (1/hour)
2	DCh	0.9989
3	μ_h=1/MRTh	1/8 = 0.125 (1/hour)
4	λ_{Ds}	6.27903e-6 (1/hour)
5	DCs	0.9902
6	μ_s=1/MRTs	10 (1/hour)
7	μ_{sr}	1/24=0.04167 (1/hour)
8	$\Delta\lambda_{Ds}$	1.5697575e-06 (1/hour)

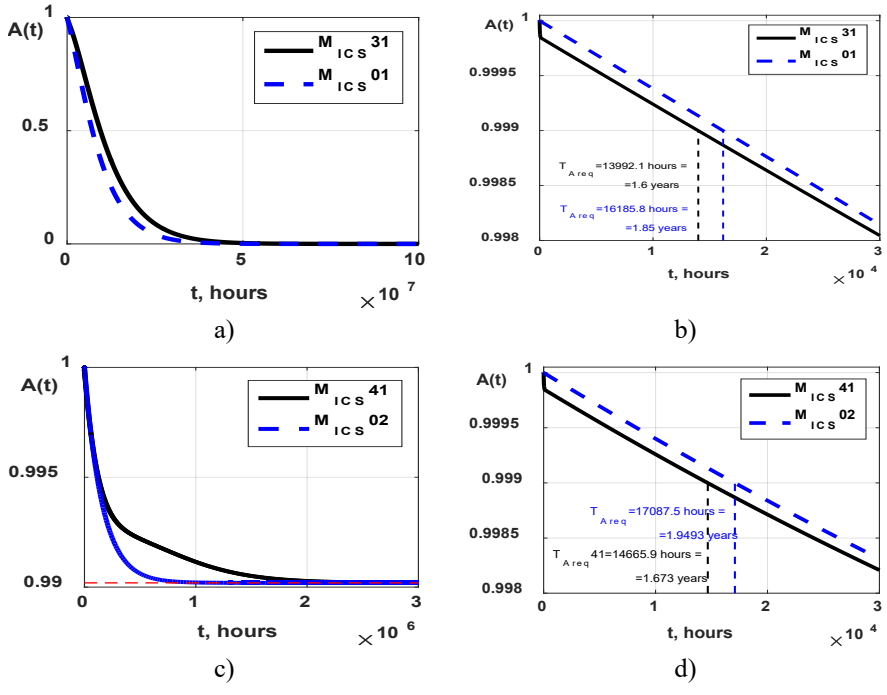

Fig. 3. The results of modelling of availability function of models $M_{ICS}31$ (a), $M_{ICS}41$ (c) and determining T_{Areq} interval with an error ξ=1e-6 (b,d)

The presence of absorbing states in MICS31 model causes the availability function behavior similar to MICS01 model - its striving to zero. But it is obvious that the elimination of design defects slows the decrease in availability to zero. The decrease in the level of availability below 0.999 occurs after 13992 hours, or 1.6 years. This value is worse than in MICS01 model, and does not meet the standard for industrial systems in 3 years or 26298 hours.

The availability function of MICS41 model is approaching to the stationary value of 0.9901, at that it goes into the established mode on 10^6 hours later than the result of the single-fragment MICS02 model. The decrease in the level of availability below 0.999 occurs after 14666 hours, or 1.67 years. This value is worse than in MICS02 model, and does not meet the standard for industrial systems in 3 years or 26298 hours.

For MICS31 and MICS41 models, the additional studies were conducted to determine the values of the input parameters at which $T_{Areq} \geq 26298$ hours. The intervals for changing the input parameters are the same as for MICS01 model and are shown in Table 3.

Table 3. Variable input parameters of the ICS model

#	Variable parameter	Designation	Values series
1	The rate of dangerous hardware failures	λ_{DH}	[0.05…5]e-5 (1/hour)
2	Diagnosing dangerous hardware failures control completeness	DC_H	[0..1]
3	Diagnosing dangerous software failures control completeness	DC_S	[0..1]

Cyclic scripts for Matlab were built to calculate the models. The results of the research are shown as graphical dependences in Fig. 4 – Fig. 6.

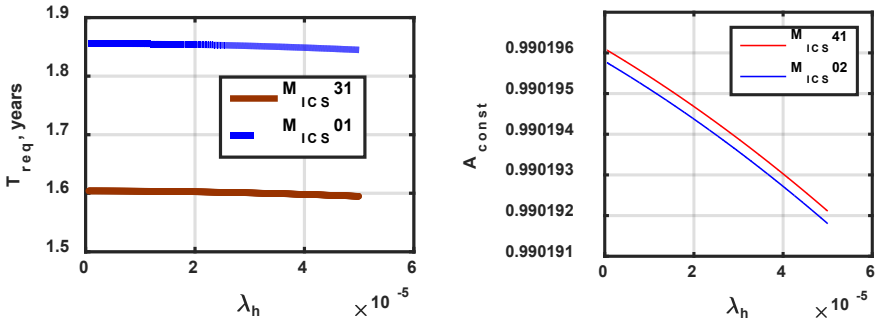

Fig. 4. Graphs for determining the T_{Areq} interval of M_{ICS} 31 models (a) and the established value of the availability function of MICS41 model (b) for different values of the input λ_{DH} parameter

The results of the influence of values of the input λ_{DH} parameter on the behavior of

availability function of M ICS 31 model are shown in Fig. 4 (a). With the decrease in the intensity of dangerous failures of HW, the reduction in availability to zero slows down. But taking into account the scale on the horizontal axis (10^8 hours), this result is not applicable in practice.

The results of the influence of values of the input λ_{DH} parameter on the established value of the function of M ICS 02 model are shown in Fig. 4 (b). With the decrease in the intensity of dangerous HW failures, A_{const} increases insignificantly (6 decimal places), which cannot be used for practical application. The result presented in Fig. 4(b) is also practically not interesting, since a change of λ_{DH} by two orders of magnitude does not allow to assure $T_{Areq} \geq 26298$ hours' condition.

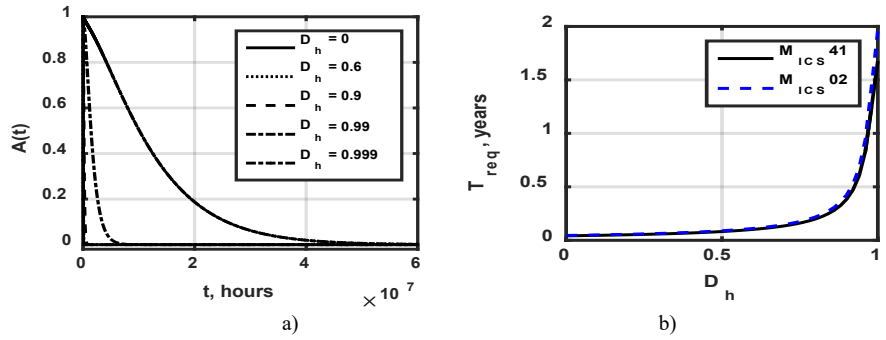

Fig. 5. Charts of the availability function of $M_{ICS}31$ model (a), interval T_{Areq} of $M_{ICS}41$ model (b) for different values of input parameter DC_H

The value of the input DC H parameter of MICS31 model affects the speed of the transition of the availability function to the established value: with the increase in DC H from 0.99 to 0.999, the descent of availability to zero slows down by $4 * 10^7$ hours. The value of the input DC_H parameter of MICS41 model practically does not affect the speed of the transition of the availability function to the established value. On the other hand, the change in DC_H from 0 to 1 also causes the change in Aconst within [0...0.9902]. The result presented in Fig.5 (b) is also important for practice, since after modeling it becomes obvious that the increase in DC_H to 1 does not allow to ensure $T_{Areq} \geq 26298$ hours' condition (as in M ICS 31 model).

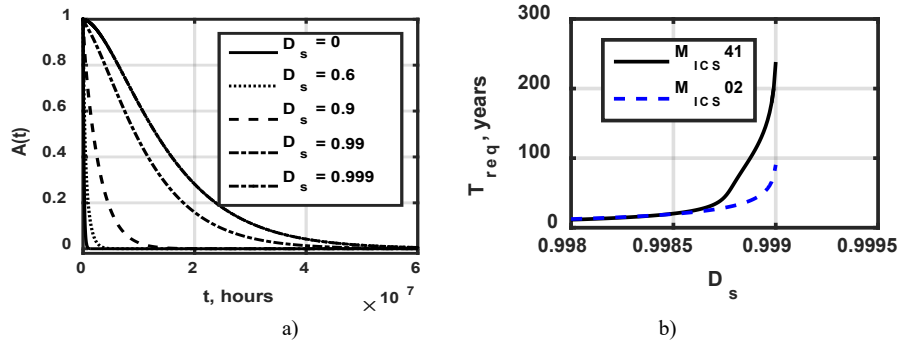

Fig. 6. Charts of availability function of $M_{ICS}31$ model (a), interval determination T_{Areq} $M_{ICS}41$ model (b) for different values of the input parameter DC_s

The results of the influence of values of the input DC_S parameter on the behavior of availability function of $M_{ICS}31$ model are shown in Fig. 6 (a). With the increase in the test coverage of dangerous SW failures by the order of magnitude (from $DC_S = 0.99$ to $DC_S = 0.999$, etc.), the availability function goes to zero level several times slower (from $5 * 10^7$ to $6 * 10^7$ hours). The following result is important for practice: starting from $DC_S = 0.9947$ value, $T_{Areq} \geq 26298$ hours' condition is provided.

The results of the influence of values of the input DC_S parameter on the behavior of availability function of model are shown in Fig. 6 (b). The dependence of A_{const} on DC_S for $M_{ICS}41$ model is linear and is not shown in the graph. With $DC_S = 1 \rightarrow A_{const} = 0.9999924$. The value satisfying the requirements of SIL3 ($A_{const} = 0.99909$) is achieved at $DC_S = 0.9991$. Theoretically, this allows us to talk about systems without proof test, but from the practical point of view, it is very difficult and costly to achieve such level of control completeness.

The results shown in Fig. 6 (b) illustrate the maintenance of $T_{Areq} \geq 3$ years' condition starting from $DC_S = 0.9942$ value. And what is more interesting, in Fig. 6(b) it is shown that in $DC_S = [0.998 ... 0.9991]$ interval the multi-fragmentary $M_{ICS}41$ model over the proof test period significantly benefits the single-fragmentary $M_{ICS}02$ model.

5 Conclusions

In the article, the multifragmentary model architecture for information and control systems of NPP 2oo3 is presented with occurred HW and SW faults and eliminating of hidden defects.

Analysis of the obtained results of modeling the availability of the for information and control systems of NPP architecture with partially eliminating of design defects has shown that:

a) for the multifragmentary M_{ICS} 31 model with absorbing the decrease in the availability function to zero is significant. For typical values of input parameters (Table 2), the fulfillment of SIL3 requirements is guaranteed in [0 ... 1.6 years] interval. The increase in the interest $T_{proof\ test}$ interval of up to 3 years is possible with the increase in the control completeness to detect dangerous SW failures to $DC_S = 0.9947$ level and higher;

b) the multifragmentary M_{ICS} 41 model is characterized by the decrease in the availability function to the stationary A_{const} value. For typical values of input parameters (Table 2), the fulfillment of SIL3 requirements is guaranteed in [0 ... 1.67 years] interval. The increase in the interest $T_{proof\ test}$ interval of up to 3 years is possible with the increase in the control completeness to detect dangerous SW failures to $DC_S = 0.9942$ level. Starting from $DC_S = 0.9991$, SIL3 requirements are guaranteed to be fulfilled without additional proof tests.

The developed mathematical models make it possible to assess the fulfillment of the requirements for the functional safety of the designed information and control system. Application of the developed models is advisable in specific time counts tied to the phases of the V-model of the project life cycle (and possibly to the separate layer of the V-model).

Future steps include:

- it is necessary to put in order and regulate the operations of choosing one of several models for the specific design phase, tight time reference to the beginning/end of the life cycle phase, substantiation of assumptions, changes in the structure and parameters of models in one method.

References

1. Bulba, Y., Ponochovny, Y., Sklyar, V., Ivasiuk, A. Classification and research of the reactor protection instrumentation and control system functional safety Markov models in a normal operation mode. CEUR Workshop Proceedings, 1614, 308-321 (2016).
2. IEC 61508-6:2010. Functional safety of electrical/electronic/programmable electronic safety related systems, Part 6: Guidelines on the application of IEC 61508-2,3 (2010).
3. Langeron, Y. Barros, A. Grall, A. Berenguer, C. Combination of safety integrity levels (SILs): A study of IEC61508 merging rules. Journal of Loss Prevention in the Process Industries 21(4), 437-449 (2008)
4. Kharchenko, V., Ponochovnyi, Y., Boyarchuk, A.: Availability Assessment of Information and Control Systems with Online Software Update and Verification. In: Ermolayev V., Mayr H., Nikitchenko M., Spivakovsky A., Zholtkevych G. (eds) Information and Communication Technologies in Education, Research, and Industrial Applications. ICTERI 2014. Communications in Computer and Information Science, vol 469, 300-324 (2014).
5. Kharchenko, V., Ponochovnyi, Y., Abdulmunem, A., Andrashov, A.: Availability Models and Maintenance Strategies for Smart Building Automation Systems Considering Attacks on Component Vulnerabilities. In: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds) Advances in Dependability Engineering of Complex Systems. DepCoS-RELCOMEX 2017. Advances in Intelligent Systems and Computing, vol 582, 186-195 (2017).
6. Kharchenko, V., Ponochovnyi, Y., Boyarchuk, A., Brezhnev, E.: Resilience Assurance for Software-Based Space Systems with Online Patching: Two Cases. In: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds) Dependability Engineering and Complex Systems. DepCoS-RELCOMEX 2016. Advances in Intelligent Systems and Computing, vol 470, 267-278 (2016).
7. Kharchenko, V.; Butenko, V.; Odarushchenko, O., Sklyar, V.: Multifragmentation Markov Modeling of a Reactor Trip System. ASME Journal of Nuclear Engineering and Radiation Science, vol. 1 (3), 031005-031005-10 (2015).
8. Ponochovniy, Y., Bulba, E., Yanko, A., Hozbenko, E.: Influence of diagnostics errors on safety: Indicators and requirements. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 54-58 (2018).
9. D7.24-FSC(P3)-FMEDA-V6R0. Exida FMEDA Report of Project: Radiy FPGA-based Safety Controller (FSC) (2018).