INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2024, VOL. 70, NO. 1, PP. 211-218
Manuscript received November 14, 2023; revised March, 2024. doi: 10.24425/ijet.2024.149533

Multi-fragmental and multi-phase availability models of the safety-critical I&C systems with two-cascade redundancy

Vyacheslav Kharchenko, Yuriy Ponochovnyi, and Ievgen Babeshko

Abstract—**Traditional availability, reliability, and safety models face the dimension problem due to a huge number of components in modern systems, motivating further research in this field. This paper focuses on multi-fragmental and multi-phase models for availability and functional safety assessment of the information and control (I&C) systems with two-cascade redundancy considering design faults manifestation during operation. The methodology of the research is based on Markov and semi-Markov chains with the utilization of multi-phase modeling. Several multi-phase models are developed and investigated considering different conditions of operation and failures caused by version faults. The case study of the research is based on the analysis of safety-critical nuclear power plant I&C systems such as the reactor trip systems developed using the programmable platform RadICS.**

Keywords—**safety; availability; reliability; I&C modeling; multi-fragmental models; multi-phase models**

I. Introduction

A. Motivation

THE topical requirements to the industrial systems necessitate from devices implementing safety functions the mandatory usage of specialized information and control (I&C) systems. Such systems are usually implemented using the FPGA- or microprocessor-based programmable platforms.

An example of a programmable platform is RadICS developed by RPC Radiy, which provides a flexible and modular approach of creating fault-tolerant architectures [1]. Such flexibility allows I&C systems based on this platform to meet the strict requirements for guaranteed performance, reliability, and functional safety in different critical industries. However, in the nuclear field, these requirements are controlled by a large number of national and international standards and regulations (for example, [2]) and therefore even are stricter to fulfil. This necessitates the development of appropriate and complete models for evaluating the parameters of reactor protection systems in the nuclear field both at the design stage and during operation. Today, failure scenarios in hardware and software channels of redundant and diverse systems have become extremely of different types. This was a consequence of new threats associated with malicious interference in the operation of these systems, threats of a military nature, sabotage, and cyberattacks. It is also worth noting that when evaluating a traditional two-channel system, it is often assumed that the supervision and diagnostic units for both subsystems have absolute reliability without failures.

Due to the development of the Industry 4.0 concept and the use of Internet of Things technologies in industrial systems, the requirements for the safety integrity level (SIL2-SIL3) have increased significantly. Taking into account all these aspects, there is a need to create an adequate and comprehensive model that will allow determining the safety indicators with high accuracy during the entire system lifecycle. However, on the other hand, the use of a complete system model taking into account all factors becomes more complicated by its dimensionality. Also, such a model is difficult to reconfigure when external influences change and new security challenges appear.

B. Related works

There are many publications dedicated to the development and modeling of various safety- and security-critical redundant systems. The use of mathematical models for systems with functions important for safety in normative documents is recommendatory. The following classes of models can be distinguished: risk-oriented [3], Bayesian [4], fault trees [5], FMECA [6], Markov and semi-Markov [7],[8], multi-phase [9], control flow graph analysis [10], etc.

Among these models, special attention must be given to the Markov and semi-Markov models describing a behavior of complex redundant systems considering different kinds of failures caused by physical, design, and interaction faults [11] including cyberattacks on vulnerabilities. Work [12] summarizes state-of-the-art knowledge on continuous-time Markov chain availability and reliability models, semi-Markov and Markov regenerative models. It is mentioned that such models could be utilized during the safety analysis of critical systems like chemical, nuclear, or power plants.

In [13] the comprehensive model in the form of a state transition diagram is proposed, defining both reliability and

This work was supported by the Ministry of Education and Science of Ukraine, state grant registration number 0123U102106, project title “Methods and case technologies of evidence-based cybersecurity assessment of programmable systems to ensure the protection of critical IT infrastructure”. This publication reflects the views of the authors only, and the Ministry of Education and Science of Ukraine cannot be held responsible for any use of the information contained therein.

Vyacheslav Kharchenko is with the National Aerospace University “Kharkiv Aviation Institute” (e-mail: v.kharchenko@csn.khai.edu).

Yuriy Ponochovnyi is with the Poltava State Agrarian University (e-mail: yuriy.ponch@gmail.com)

Ievgen Babeshko is with the National Aerospace University “Kharkiv Aviation Institute” (e-mail: e.babeshko@csn.khai.edu) and the Istituto di Scienza e Tecnologie dell’Informazione Alessandro Faedo-CNR (e-mail: ievgen.babeshko@isti.cnr.it)

functional safety indicators by a new classification of inoperable states. In [14] functional safety Markov models of cyber-physical system operation are formalized with the assumption that vulnerabilities leading to failures are independent.

In [15] a review of the literature on reliability focusing on Markov and semi-Markov models is performed. It is concluded that due to the exponential explosion in the size of the model, the method may be limited in solving complex problems. The following ways are suggested to reduce the number of states: model simplification or a combination of different modes.

This work considers a macro model for analyzing the operation of the reactor trip system (RTS) of nuclear power plants (NPP) and other safety-critical systems taking into account various types of failures, in particular errors in the diagnostic units of the main and diverse subsystems. This paper is a continuation of scientific research that was described in studies [16],[17],[18]. Publications [16],[17] have been dedicated to the research of multi-cascade redundant control systems considering failures of supervision units, software versions, and recovery processes. An approach based on combining Markov and semi-Markov modeling for assessing the availability and safety of IoT and cloud-based systems considering changes in requirements and environment parameters was researched in [18].

However, in these and other studies, no efforts were put into the development and research of models that consider changes during system operation and incorporate events that occur and influence initial system description models. This circumstance becomes challenging when the model is very complex, and the system behavior is described by hundreds or thousands of states during a long time of operation.

C. *Objectives and structure*

Objectives of this research are:

- to develop multi-fragmental and multi-phase functional safety assessment models of the recoverable systems with two-cascade redundancy;
- to investigate mechanisms for reducing software failure rates and their impact on system safety;
- to formulate recommendations for safety assessment model construction.

The methodology of the research is based on Markov and semi-Markov chains with the utilization of multi-phase modeling. The main focus of the research is the development and research of models for availability assessment of the safety-critical NPP I&C systems, first of all, reactor trip systems.

The structure of the paper is the following: Section 2 describes the system under research and the initial model. In Section 3 conceptual approach is presented. Section 4 is devoted to the development and research of the multi-phase models. In Section 5 we provide a discussion and directions for future research.

II. Researched System and Initial Model

A. Block diagram of a two-cascade redundant structure

In the reliability block diagram of the NPP reactor trip system shown in Fig. 1, a modified redundant one-out-of-two (1oo2) architecture is used [16],[17]. In this architecture, each channel is additionally provided with two-out-of-three (2oo3) redundancy and built-in diagnostic units. Reactor trip subsystems generate priority one-bit signals for the shutdown signal. If the output channels maintain the same states when errors occur in the versions, i.e. main and diverse software subsystems, these errors are detected using built-in diagnostics. Such a redundant architecture includes a certain margin of reliability, which allows responding to failures accordingly.

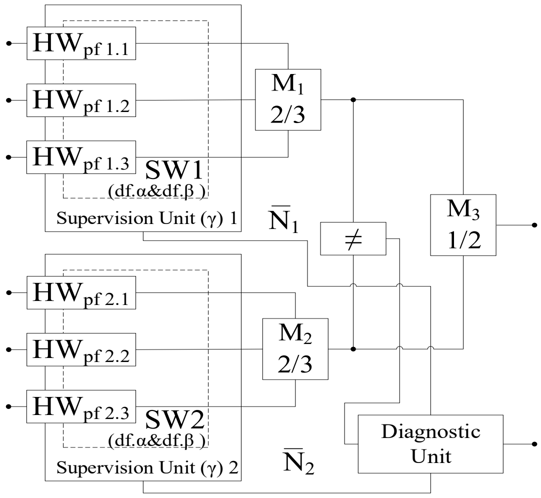


Fig. 1. Block diagram of RTS I&C system for modeling the manifestation of physical defects (pf), design defects (df, absolute α, and relative β), and faults of the supervision and diagnostic units (γ)

The application of a modular platform like RadICS [1] allows the use of a central diagnostic module together with built-in means to check the correctness of signals coming from other modules. An additional output signal comparison module (marked as the "≠") contributes to increasing the level of reliability and safety. But this increases the number of possible diagnostic states, as well as the general number of states of the reactor trip system.

B. *Macro model of recoverable two-version control system with two-cascade 2oo3/1oo2 redundancy considering supervision means faults*

In work [16], a case study was presented with marked graph-based model containing 619 states built to describe the RTS operation. The model describes the manifestation of 6 types of failures, the elimination of design defects of software channels, and the recovery of system operational states. The modeling of changes in the manifestation rate of design defects (after their detection and elimination) is carried out using the principle of multi-fragmentation [17].

The macrograph shown in Fig.2 is divided into 24 fragments. Within each fragment, the manifestation rate of defects remains constant (that is, the property of Markov processes is preserved). When the system transitions from one fragment to another, there is a jump-like change in the manifestation rate of the design defect (this is illustrated by the appropriate transition arrow).

It should be emphasized that the investigation of models of such size is a challenging task. In studies [16],[17],[18], the generalization of individual blocks was performed, as well as the detailing of the system operation within specific fragments.

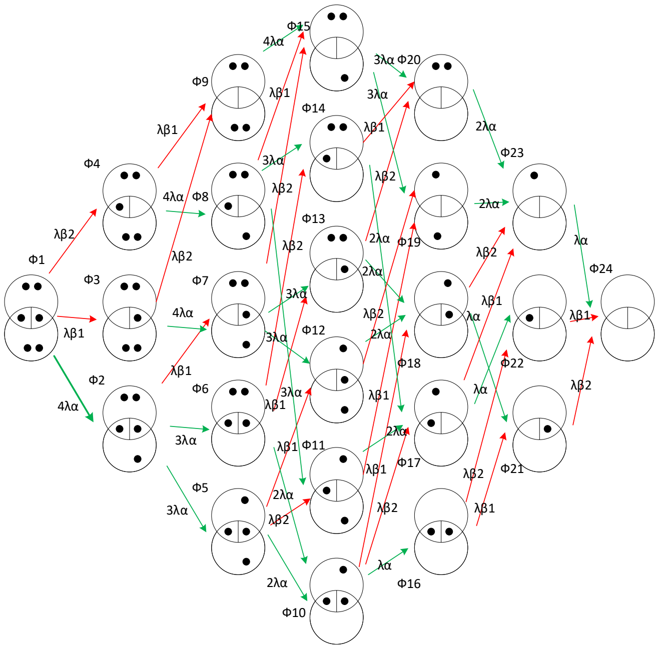


Fig.2. Macrograph describing the functioning of the RTS I&C system with the configuration {nα1=2, nα2=2, nβ1=1, nβ2=1}

The developed macro model provides the following advantages:

- the macro model combines all known types of failures, making modeling more accurate;
- the use of the macro model allows to analyze the impact of individual failure types on system safety by setting zero parameters for "unnecessary" system components during failure analysis;
- good extensibility for typical failure types: with an increase in the number of typical failures (for example, an increase in the number of undetected design defects in one of the software versions), the number of fragments in the macro model will increase;

On the other hand, the model also has its disadvantages, namely:

- the macro model has a large dimension, which complicates its understanding, reduces its visibility, and requires significant computing resources for modeling;
- the macro model has poor extensibility for atypical (not taken into account) types of failures: for their simulation, the macro model needs to be rebuilt at the level of states in fragments and connections between fragments;
- the macro model is focused on modeling Markov processes of failures and recoveries, it cannot be used for non-Markov distributions.

III. Conceptual Approach Based on the Evolution of the Macro Model

A. *Transformation of macro model*

In the work [16], within the framework of the general methodology, various aspects and cases of construction of mathematical models of the information systems operation are considered. It is also emphasized that in some cases there is a need to change the already existing model for new requirements/parameters/environment of I&C system. However, this situation/case is partially illustrated.

So, for example, if in the macro model shown in Fig. 2, it is known that the event of the manifestation of an absolute defect according to the parameter λβ1 has occurred, then after this event the use of the full graph of the model is no longer appropriate (because it models the manifestation of only one software defect according to the specified parameter). Therefore, after this event, the graph can be modified, as shown in Fig. 3.

Fig. 3 illustrates the model dimensionality reduction from 24 fragments to 12 fragments. However, to use the shown "gluing" of models, it is necessary to answer two questions:

- at what point in time will this absolute defect manifest itself, so as it will be possible to change the macro model;

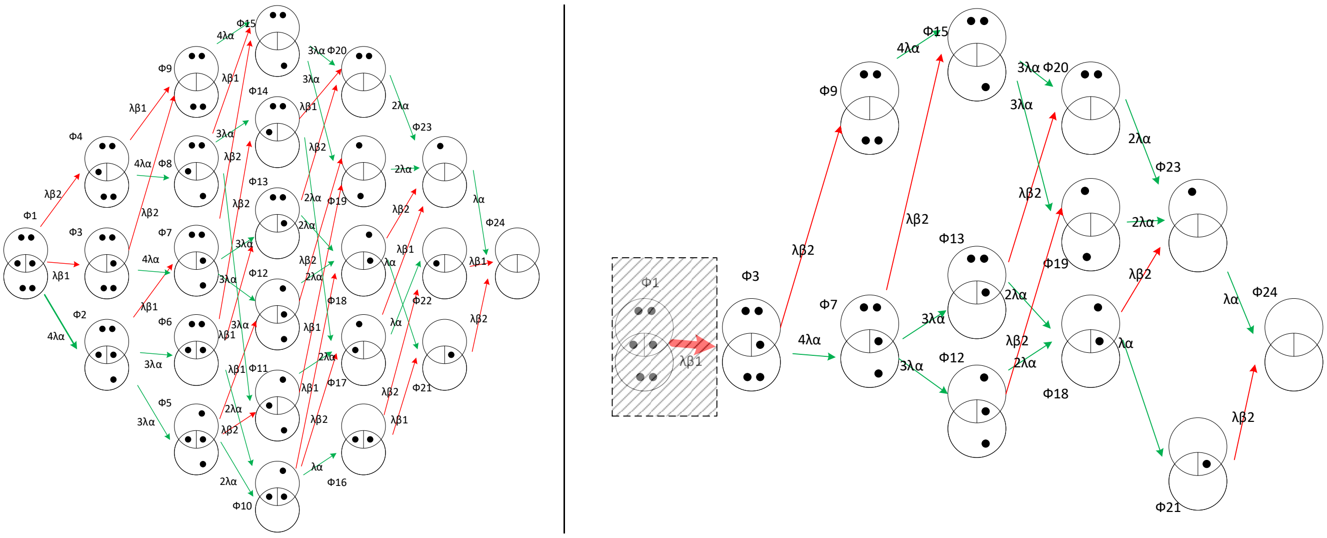


Fig. 3. Illustration of the macro model dimensionality reduction after the absolute software defect manifestation according to the parameter λβ1

- which modeling technique can be used to "glue" / merge two separate Markov models.

The answer to the first question is difficult to obtain at the design stage (a priori, the defect manifestation is a probabilistic event). But at the system operation stage, the moment of absolute software defect manifestation can be recorded after its detection by the diagnostic system. In some cases, if diagnostic tests are performed at regular intervals, it can be predicted that the absolute software defect manifestation will be detected precisely during such an interval.

The technique of "gluing" the simulation results of separate Markov models in time is better known as the technique of "multi-phase" simulation [9]. The features of its application will be considered further.

The use of the macro model in this case is complicated by its dimensionality. Therefore, the part of the macro model that describes the absolute software defects manifestation in both versions, marked as β, will be considered next.

A multi-fragmental model that describes the manifestation of absolute software defects is considered in [17]. Its feature is the condition of eliminating such a defect after its manifestation. This causes the transition of the system to a new fragment (Fig. 4).

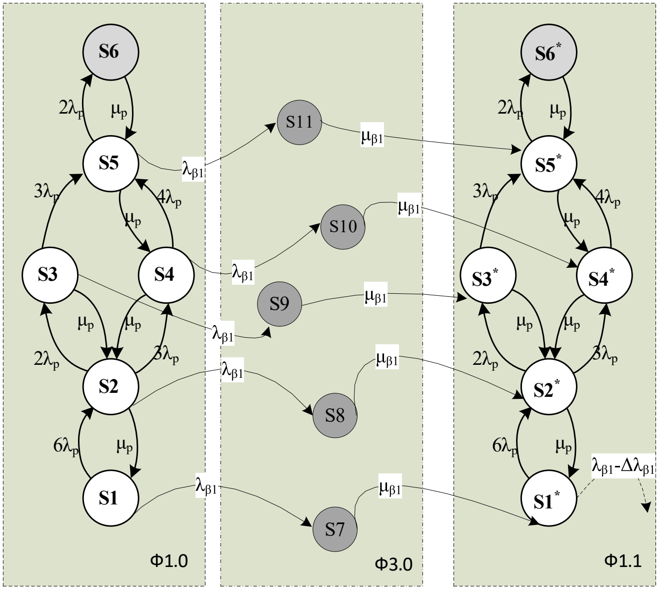


Fig. 4. Transitions between fragments due to the manifestation of the absolute design faults of the software versions according to the λ_β parameter.

In such a case, the event - the absolute software defect manifestation - is accidental. Accordingly, the time of transition of the system to a new fragment is also random. This condition allows us to use the transformation of the non-Markov model with a variable absolute software defects manifestation rate λ_β to the quasi-Markov multi-fragmental model. The use of a multi-phase model to simplify the considered multi-fragmental model is somewhat inappropriate (since, in fact, such a simplification does not occur). But in real life, another case is possible, when the elimination of design defects occurs at a clearly defined (deterministic) time of releasing a software update. For this type of development, it is necessary to build and apply a multi-phase mathematical model.

B. Parameterization and research of macro model

Next, the construction and research (comparison) of various I&C system models was carried out. For all models, the same values of input parameters are adopted in Table I.

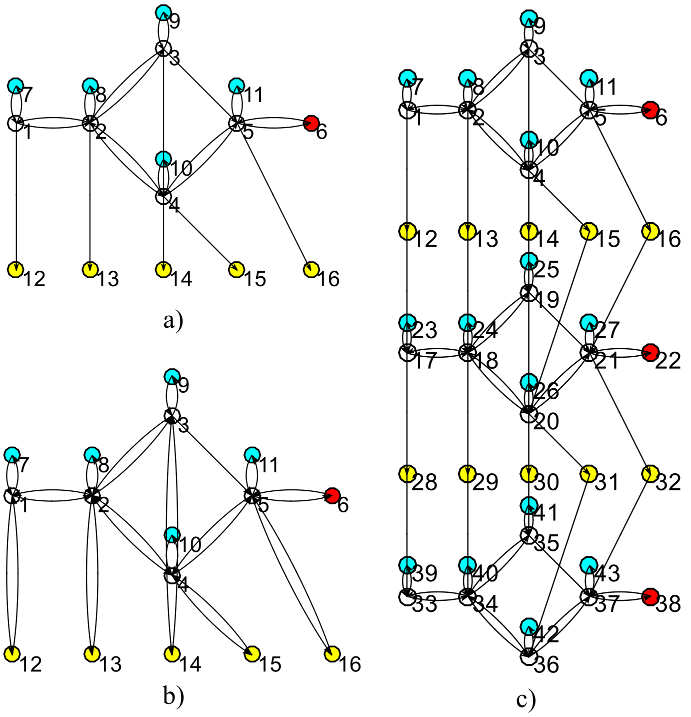
TABLE I
VALUES OF MODEL INPUT PARAMETERS

#	Symbol	Parameter	Value
1	λp	RTS failure rate due to physical faults	1e-4 (1/h)
2	λγ	Supervision means failure rate	1e-6 (1/h)
3	μp	RTS recovery failure rate	1 (1/h)
4	μγ	Supervision means recovery rate	0.25 (1/h)
5	λβ	Software failure rate due to absolute design defects causing different signals	2e-6 (1/h)
6	μβ	Software recovery rate	0.0714 (1/h)
7	Nβ	Estimated number of absolute design defects of the second type	3..5

In a single-fragmental model with absorbing states, after the absolute software defect manifestation, the system goes into absorbing states (marked in yellow in Fig.5, a).

In a single-fragmental model without absorbing states, the system is restarted at some rate after the absolute software defect manifestation (Fig.5, b).

The multi-fragmental model with the elimination of defects immediately after their appearance is shown in Fig.5, c.



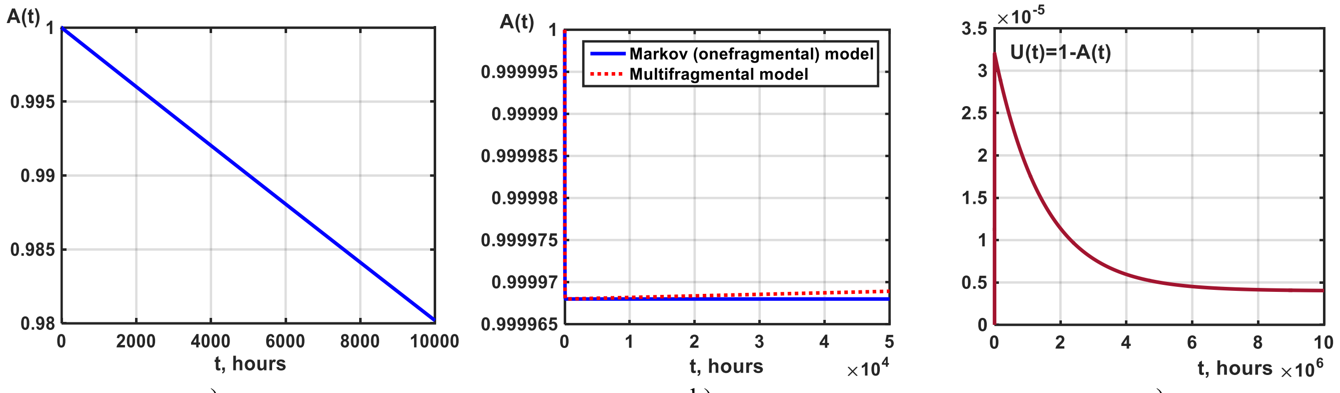
a)

b)

c)

Fig. 5. The single-fragmental models (a,b) and multi-fragmental model (c) of the RTS I&C system

The modeling results of the basic single-fragmental models and multi-fragmental RTS I&C system model for input data from Table I are shown in Fig. 6. The result of the simulation of single-fragmental model with absorbing states (Fig.6, a) is that availability decreases over time and goes to 0. The availability function of the single-fragmental model without absorbing states (Fig.6, b) decreases to a constant level Aconst=0.999967989787930 (1- Aconst=3.2010e-05).



a) b) c)

Fig. 6. Modeling results of the basic single-fragmental models and multi-fragmental RTS I&C system model

In a multi-fragmental model, the availability function initially decreases to the level of Amin=0.999968 (Fig.6,b), and then goes to the stable level of the system without software defects Aconst=0.9999959 (U=1 - Aconst= 4.04e-06; Fig.6, c).

IV. Multi-phase models

A. The description of the classical multi-phase model

To build a multi-phase reliability model, the NPP I&C system was considered, the reliability block diagram of which is presented in Fig. 1. Manifestation of the supervision unit defects is not shown on the graph to reduce its dimension and simplify understanding, but such defects are considered in calculations performed later. The marked graph simulating the system behavior o during the one phase has 11 states: – operational (S1...S5 - with a detected failure from one to two RTS), – inoperable (S6 – with detected three hardware failures, S7...S11 – with detected software failure caused by the manifestation of an absolute design defect). In the time intervals between software updates, the behavior of the system is modeled by the Markov process in the left part of Fig.7: RTS defects are manifested in I&C system - hardware failures (transitions S1 → S2, S2 → S3, S2 → S4, S3 → S5, S4 → S5 and S5 → S6), the manifestation of software failures is simulated by transitions S1 → S7 ... S5 → S11), RTS recovery is shown as a change of states S2 → S1, S3 → S2, S4 → S2, S5 → S4 and S6 → S5. A software restart is not simulated because the manifestation of an absolute defect in both software versions is an event that puts the system in a failsafe state.

Software update procedures are carried out at certain points in time (in Fig. 7 - moments of putting the connection matrix into effect). The logic of constructing the transitions of this matrix is as follows. If a software defect appeared during the previous phase, the procedure for eliminating it is initiated when the software is updated (transitions S7 → S12 ... S11 → S16). If during the previous phase the I&C system component was operational, then it remains in the corresponding operational state (S1 → S1 ... S5 → S5), if the I&C system entered an inoperable state, then it remains in it (S6 → S6).

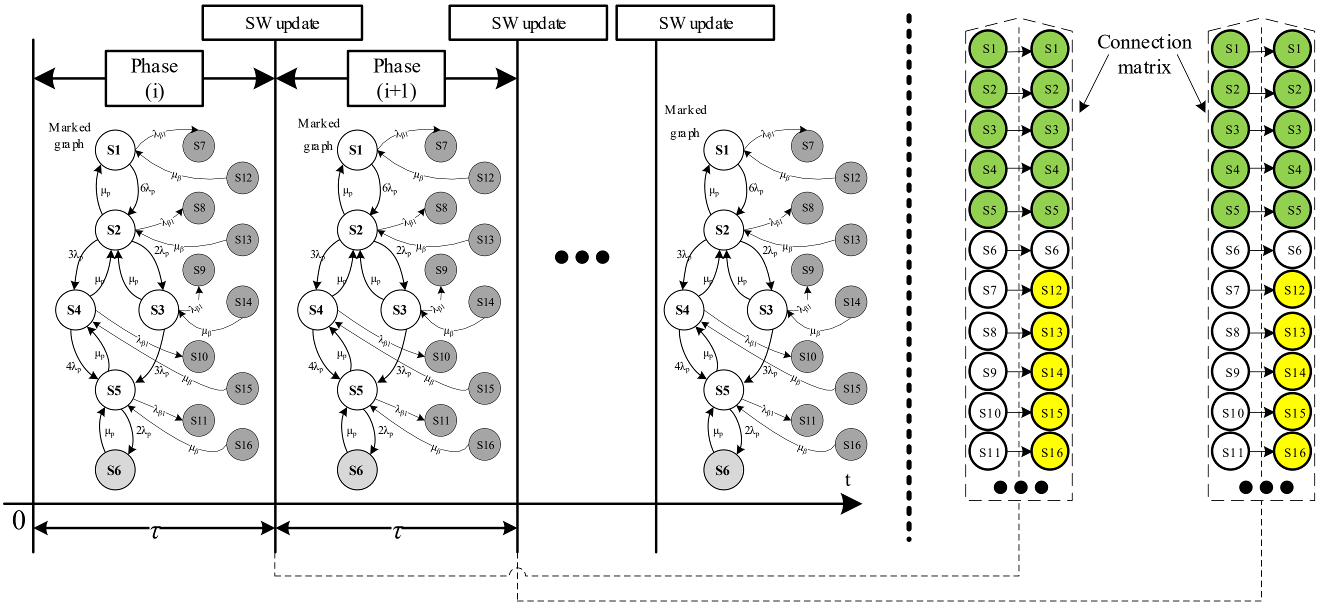


Fig. 7. The multi-phase model of the RTS I&C system built using the classical approach

If the system went into failsafe states and started updating (states S12...S16) but did not have time to eliminate the software defect during the phase duration, then it remains in these states (transitions S12 → S12 ... S16 → S16).

The connection matrix [L] is used to calculate the initial conditions at the beginning of phase (i+1) based on the probabilities of the states at the end of phase (i), which is written mathematically in the form of equation (1). Replacing Pi(τ) with the values obtained at the previous iteration determines the recurrence of equation (1), which makes it possible to calculate the initial conditions at the beginning of each interval (phase of the model).

$$\begin{bmatrix} P_1(0) \\ P_2(0) \\ P_3(0) \\ P_4(0) \\ P_5(0) \\ P_6(0) \\ P_7(0) \\ P_8(0) \\ P_9(0) \\ P_{10}(0) \\ P_{11}(0) \\ P_{12}(0) \\ P_{13}(0) \\ P_{14}(0) \\ P_{15}(0) \\ P_{16}(0) \end{bmatrix}_{i+1} = \begin{bmatrix} 1000000000000000 \\ 0100000000000000 \\ 0010000000000000 \\ 0001000000000000 \\ 0000100000000000 \\ 0000010000000000 \\ 0000000000010000 \\ 0000000000001000 \\ 0000000000000100 \\ 0000000000000010 \\ 0000000000000001 \\ 0000000000010000 \\ 0000000000001000 \\ 0000000000000100 \\ 0000000000000010 \\ 0000000000000001 \end{bmatrix} \cdot \begin{bmatrix} P_1(\tau) \\ P_2(\tau) \\ P_3(\tau) \\ P_4(\tau) \\ P_5(\tau) \\ P_6(\tau) \\ P_7(\tau) \\ P_8(\tau) \\ P_9(\tau) \\ P_{10}(\tau) \\ P_{11}(\tau) \\ P_{12}(\tau) \\ P_{13}(\tau) \\ P_{14}(\tau) \\ P_{15}(\tau) \\ P_{16}(\tau) \end{bmatrix}_i = [L]\vec{P}_i(\tau) \qquad (1)$$

The calculation of the indicator of instantaneous unavailability of the system is carried out according to the equation (2).

$$U(t) = \sum_{k=1}^{n} q_k P_k(t) \qquad (2)$$

where the linear vector q_k takes the value $q_k = 1$ if the system is in an inoperable state and $q_k = 0$ if the I&C system is operational. Within one phase of the model, the unavailability function is calculated as (3).

$$U(t) = 1 - \sum_{i=6}^{16} P_i(t) \qquad (3)$$

The average unavailability indicator U_{avg} is calculated by the method described in [14], using the following definite integral (4).

$$U_{avg}(\tau) = \int_0^{\tau} U(t)dt \qquad (4)$$

During the model construction, it is necessary to take into account the change in the parameter λ_β when eliminating the software defect. The defect is eliminated after the software update. But this event is probabilistic, therefore it is not possible to predict exactly in which time interval λ_β will be decreased by $\Delta\lambda_\beta$. The following technique was used during the construction of the multi-phase model. At the beginning of a new phase, the probability of the software defect manifestation is defined as the sum of the probabilities P7(τ)+...+P11(τ) of the previous phase. Then the change in the software failure rate in the new phase is determined by the equation (5).

$$\Delta\lambda_\beta(\tau+1) = \Delta\lambda_\beta \cdot \sum_{i=7}^{11} P_i(\tau) \qquad (5)$$

B. *Research on modifications of "classic" multi-phase models*

In the "classic" multi-phase model only ones "1" and zeros "0" are present in the matrix L, and in which there are no transitions weighted by the recovery parameter after the absolute software defect manifestation. Then the graph inside the phase contains absorbing states, and the output from them occurs according to the rules described in the connection matrix L.

To check the applicability of the multi-phase model authors used the approach described below. The connection matrix for a system with no interphase transitions at all is an identity matrix (matrix with "1" in the diagonal and "0" in all remaining places). The obtained results for such case are shown in Fig.8.

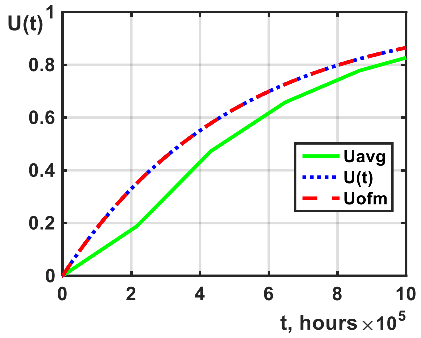


Fig. 8. "Classic" multi-phase model with identity matrix [L]

The result is a blue chart without spikes, "identical" (inverted to 1) to the graph of the "basic" single-fragmental model with absorbing states. The connection matrix in the first multi-phase model, in which the exit from the absorbing states occurs every time with a periodic event (does not correspond to real-life conditions!) see in (1). This model compared to one shown in Fig. 7 doesn't have states S12…S16.

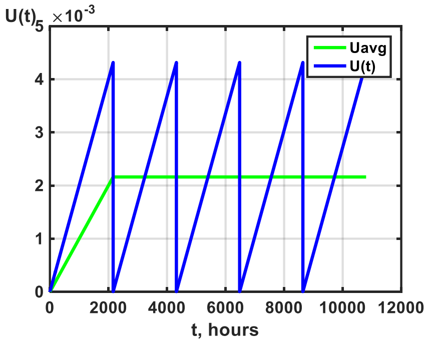


Fig. 9. "Classic" multi-phase model without states S12…S16

The result of the simulation (Fig. 9) is that at each periodic event the unavailability function is “zeroed” - each time it decreases to zero. The average level of unavailability is 2.2e-03. If the model parameters are adjusted so that the periodicity of events is greater than the interval under observation, then the resulting function will correspond to the chart of the “basic” single-fragmental model with absorbing states (Fig. 8).

C. Modified “classic” multi-phase model

In this model, only ones "1" and zeros "0" are present in the matrix [L], and there are transitions weighted by the recovery parameter after the absolute software defect manifestation. The connection matrix of this model also contains only "1" and "0", it is assumed that at the moment of a periodic event, the system from the absorbing state of the absolute software defect manifestation passes into the recovery state, which is "input" (non-absorbing, starting) in the next phase models.

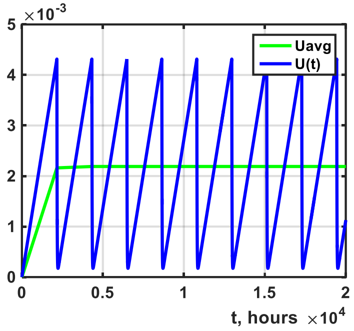


Fig. 10. Modified “classic” multi-phase model

Simulation results (Fig. 10) have shown that the averaged unavailability function increases due to the introduction of new states but does not go to “zero” with each periodic event.

D. A multi-phase model with a modified connection matrix

Looking for a way to “summarize” the results of multi-fragmental and multi-phase models, we concluded that the use of an identity communication matrix (which contains only “1” and “0”) does not allow activating the probabilistic mechanism of reducing the software failure rate, because the system every time goes into states that are weighted “1” in the connection matrix.

The introduction of an additional state with a transition from it, weighted by μ_β, also does not make it possible to activate the mechanism for reducing the software failure rate. Therefore, we tried a different approach – we used μ_β as a parameter of the connection matrix. Then the matrix has the following form (6).

$$[L]=\begin{bmatrix} 1000000000000000 \\ 0100000000000000 \\ 0010000000000000 \\ 0001000000000000 \\ 0000100000000000 \\ 0000010000000000 \end{bmatrix} \tag{6}$$

$$\begin{bmatrix} \mu_\beta 0000000000(1-\mu_\beta)0000 \\ 0\mu_\beta 0000000000(1-\mu_\beta)000 \\ 00\mu_\beta 0000000000(1-\mu_\beta)00 \\ 000\mu_\beta 0000000000(1-\mu_\beta)0 \\ 0000\mu_\beta 0000000000(1-\mu_\beta) \end{bmatrix}$$

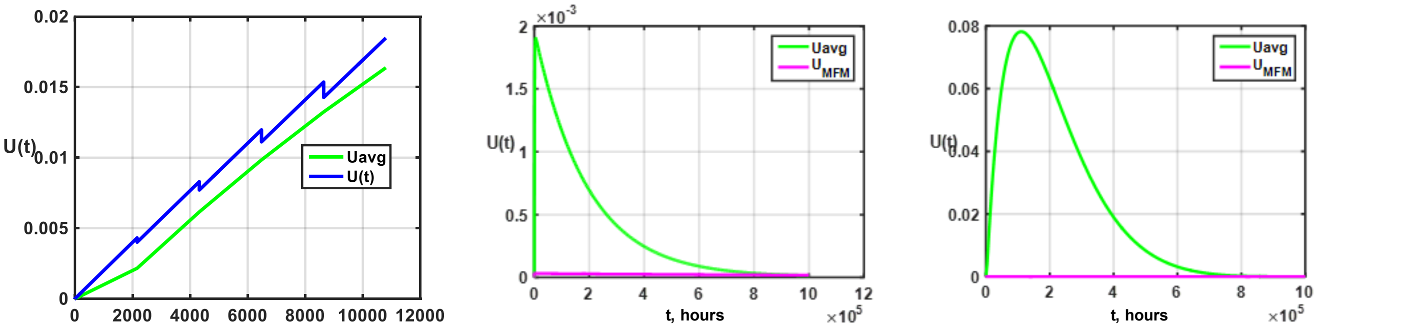
The simulation results show that the mechanism of reducing the software failure rate in this approach works (Fig.11, a). At the same time, the averaged unavailability U_{avg} = 1.4553e-05, which is better than one of the multi-fragmental model (apparently this is related to the averaging mechanism). Comparison with MFM (pink) is shown in Fig. 11,b.

If the interval between phases is increased from 3 days to 180 days, the chart "shifts", as shown in Fig. 11,c.

V. Discussion and Conclusion

Modeling results of different variants of Markov, multi-fragmental, and multi-phase model construction allow concluding normal convergence during defined system operation modes. The expected effect of unavailability function reduction in the case of project defect elimination and classic multi-phase model is not obtained. Although in standard IEC-61508-6 there are charts that illustrate such an effect explicitly, a detailed description of such model construction is missing.

Application of classic multi-phase modeling as a mathematical apparatus for “merging/gluing” different models is possible. But in this case, it is necessary to have determined event characteristics that lead to change in the system model: time of event occurrence and unambiguous (not probable) system reaction for this event (this fact causes the usage of matrix [L] with elements “0” and “1”).



a) b) c)

Fig. 11. Multi-phase model with a modified connection matrix (a) and its comparison with a multi-fragmental model for periodical checks with Δt=3 days (b) and Δt=180 days (c)

For cases when a determinate event leads to random effects on the system, it is necessary to use a modified matrix [L] that includes probabilistic components, but apparently this approach requires more effort to be implemented, as at the moment authors were not able to find a confirmation for it in the available sources.

This paper advances the conceptual approach of RTC I&C system evolutional models with regard to the application of multi-phase modeling for "merging/gluing" system Markov models that describe system operation in different intervals. In comparison to the multi-fragmental approach discussed above, this approach allowed to describe adequately system behavior during the occurrence of determinate events.

Modeling results have shown normal model convergence, i.e. the same behavior of the unavailability function under the condition of the absence of periodical determinate events and utilization of the identity connection matrix [L].

Application of the modified connection matrix [L] that includes recovery rates μ_β made it possible to reproduce an effect of unavailability function reduction in the case of design defect elimination. As this takes place, the value of the unavailability function obtained by multi-phase modeling $U_{avg} = 1.4553e\text{-}05$ spans in the range of [4.04e-06…3.2010e-05] this function values, calculated using Markov models under conditions of total defect absence and system operation without their elimination. On the one hand, such obtained result confirms the adequacy of the chosen modeling approach. On the other hand, additional efforts are required to find out the reasons for multi-phase and multi-fragmental modeling divergences. Research in this direction would be one of the possible future steps.

Acknowledgements

We are very grateful to the experts from RPC Radiy and RPC Radics LLC for their appropriate and constructive suggestions that helped to improve this paper.

References

[1] FPGA-Based Safety Platform RadICS https://www.exida.com/SAEL-Safety/rpc-radiy-fpga-based-safety-controller-fsc-radics

[2] IAEA Safety Standards Series No. SSG-2 (Rev. 1). Deterministic Safety Analysis for Nuclear Power Plants. 2019. https://www-pub.iaea.org/MTCD/publications/PDF/PUB1851_web.pdf

[3] S.-M. Shin, S. H. Lee, S. K. Shin, I. Jang, and J. Park, "STPA-based hazard and importance analysis on NPP safety I&C systems focusing on human–system interactions," Reliability Engineering & System Safety, vol. 213, p. 107698, 2021. doi:10.1016/j.ress.2021.107698

[4] S. J. Lee et al., "Bayesian belief network model quantification using distribution-based node probability and experienced data updates for software reliability assessment," IEEE Access, vol. 6, pp. 64556–64568, 2018. doi:10.1109/access.2018.2878376

[5] M. R. Mamdikar, V. Kumar, and P. Singh, "Dynamic Reliability Analysis Framework Using Fault Tree and Dynamic Bayesian Network: A Case Study of NPP," Nuclear Engineering and Technology, vol. 54, no. 4, pp. 1213–1220, 2022. doi:10.1016/j.net.2021.09.038

[6] O. Illiashenko and E. Babeshko, "Choosing FMECA-based techniques and tools for safety analysis of Critical Systems," Information & Security: An International Journal, vol. 28, pp. 275–285, 2012. doi:10.11610/isij.2822

[7] Z. Zeng, Y.-P. Fang, Q. Zhai, and S. Du, "A Markov reward process-based framework for resilience analysis of Multistate Energy Systems under the threat of extreme events," Reliability Engineering & System Safety, vol. 209, p. 107443, 2021. doi:10.1016/j.ress.2021.107443

[8] S. Kaalen, M. Nyberg, and C. Bondesson, "Tool-supported dependability analysis of Semi-Markov processes with application to autonomous driving," 2019 4th International Conference on System Reliability and Safety (ICSRS), 2019. doi:10.1109/icsrs48664.2019.8987701

[9] F. Felgner and G. Frey, "Multi-phase Markov models for functional safety prediction: Efficient simulation of Markov models used for safety engineering and the online integration of individual systems' diagnostic and maintenance history," 2011 3rd International Workshop on Dependable Control of Discrete Systems, 2011. doi:10.1109/dcds.2011.5970331

[10] K. Bobrovnikova, S. Lysenko, B. Savenko, P. Gaj, O. Savenko. Technique for IoT malware detection based on control flow graph analysis, Radioelectron. Comput. Syst. 2022, 1, pp. 141-153, doi:10.32620/reks.2022.1.11

[11] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan.-March 2004, doi:10.1109/TDSC.2004.2. Trivedi 2017

[12] K.S. Trivedi, A. Bobbio, "Reliability and Availability Engineering—Modeling, Analysis, and Applications;" Cambridge University Press: Cambridge, UK, 2017; pp. 1–730

[13] L. Ozirkovskyy, B. Volochiy, O. Shkiliuk, M. Zmysnyi, P. Kazan, "Functional Safety Analysis of Safety-Critical System Using State Transition Diagram", Radioelectron. Comput. Syst. 2022, 1, pp. 145–158, doi:10.32620/reks.2022.2.12

[14] V. Kovtun, I. Izonin, and M. Gregus, "The functional safety assessment of cyber-physical system operation process described by Markov chain", Sci Rep 12, 7089 (2022). doi:10.1038/s41598-022-11193-w

[15] A. Farahani, A. Shoja, and H. Tohidi, "Markov and semi-Markov models in system reliability," in Engineering Reliability and Risk Assessment, Elsevier, 2023, pp. 91-130, doi:10.1016/B978-0-323-91943-2.00010-1

[16] V. Kharchenko, Y. Ponochovnyi, E. Ruchkov, and E. Babeshko, "Safety Assessment of the two-cascade redundant information and control systems considering faults of versions and supervision means," New Advances in Dependability of Networks and Systems, pp. 88–98, 2022. doi:10.1007/978-3-031-06746-4_9

[17] V. Kharchenko, Y. Ponochovnyi, I. Babeshko, E. Ruchkov, and A. Panarin, "Safety assessment of maintained control systems with Cascade Two-version 2oo3/1oo2 structures considering version faults," Lecture Notes in Networks and Systems, pp. 119–129, 2023. doi:10.1007/978-3-031-37720-4_11

[18] V. Kharchenko, Y. Ponochovnyi, O. Ivanchenko, H. Fesenko, and O. Illiashenko, "Combining markov and semi-markov modeling for assessing availability and cybersecurity of Cloud and IOT Systems," Cryptography, vol. 6, no. 3, p. 44, 2022. doi:10.3390/cryptography6030044