Vadim Ermolayev · Frédéric Mallet ·
Vitaliy Yakovyna · Heinrich C. Mayr ·
Aleksander Spivakovsky (Eds.)

Communications in Computer and Information Science 1175

Information and Communication Technologies in Education, Research, and Industrial Applications

15th International Conference, ICTERI 2019
Kherson, Ukraine, June 12–15, 2019
Revised Selected Papers

Springer

ICTERI

Contents

Multi-fragmental Markov's Models for Safety Assessment of NPP I&C System Considering Migration of Hidden Failures

Vyacheslav Kharchenko[1,3], Yuriy Ponochovnyi[1,2(✉)], Artem Boyarchuk[1], Anton Andrashov[3], and Ihor Rudenko[4]

[1] National Aerospace University KhAI, Kharkiv, Ukraine
{V.Kharchenko, a.boyarchuk}@csn.khai.edu,
yuriy.ponch@gmail.com
[2] Poltava State Agrarian Academy PSAA, Poltava, Ukraine
[3] Research and Production Company Radiy, Kirovograd, Ukraine
a.andrashov@radiy.com
[4] Poltava Oil and Gas College of National Technical University PKNG, Poltava, Ukraine
rudenko_ihor@ukr.net

Abstract. The information and control systems of Nuclear Power Plant and other safety critical systems are considered as a set of three independent hardware channels including online testing system. Nuclear Power Plant information and control systems design on programmable platforms is rigidly tied to the V-model of the life cycle. Safety and availability during its life cycle are assessed using Markov and multi-fragmental models. The multi-fragmental model MICS32 contains an absorbing state in case of hidden faults and allows evaluating risks of "hidden" unavailability. The MICS42 model simulates the "migration" of states with undetected failures into states with detected faults. These models describe the functioning of the system and the complete elimination of software faults. Results of multi-fragmental modeling are compared to evaluate proof test period taking into account requirements for SIL3 level and limiting values of hidden fault probabilities. Multi-fragment models are included in the assessing method of implementation safety requirements of ICS on programmable platforms. The information technology of decision support in assessing and managing the implementation of the requirements for ICS safety is also considered.

Keywords: Multi-fragmental models · Safety modeling · Information technologies · Assessment method of requirements fulfillment

1 Introduction

1.1 Motivation

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

V. Ermolayev et al. (Eds.): ICTERI 2019, CCIS 1175, pp. 302–326, 2020.
https://doi.org/10.1007/978-3-030-39459-2_14

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 (ICS) of the Nuclear Power Plant (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 the 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 (DC is diagnostic coverage). As a separate process, regular proof tests are highlighted, during which latent hardware (HW) and software (SW) faults, that are not detected by the integrated control system, are detected.

1.2 State of the Art

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 safety of SW (reducing an intensity of dangerous SW $\lambda_{D\,SW}$ failure or increasing the completeness of control of dangerous SW DC_{SW} failure). For information and control systems on programmable platforms, SW faults (architectural project faults) are entered into the system of bug tracking after their detection and eliminated within a certain time interval. The elimination of the software fault (assuming no new faults are introduced) causes a decrease in SW failure rate, as shown in [4, 5]. To adequately display the elimination of SW faults and reduce the failure rate in studies [6], it was suggested to use the mathematical apparatus of multi-fragmental modeling.

In work [7], accounting for changes in the intensity of software failures is carried out using the apparatus of regular multi-fragment Markov' models. In articles multi-fragment ICS models have been studied, which allow one to take into account software updates [8], conduct operational verification, and then limit system functions [9].

Analysis of the mathematical apparatus of Markov' modeling critical systems with variable parameters [10], information and cybersecurity of web applications [11], high-availability systems [12] allows highlighting its advantages compared with Bayesian' analysis [13] and simulation modeling [14].

At first glance, the elimination of software faults may cause a desire to use the information and control system project with the initial high intensity of dangerous SW failures, because faults 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 faults causing dangerous SW failures.

Goal of the paper is the following:

- to investigate multi-fragmental 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 faults;

- get 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;
- to develop an appropriate method for evaluation the requirement fulfillment for ICS safety,
- introduce the developed models and method into information technology for decision support in assessing and managing the implementation of the requirements for ICS safety.

The paper is structured by the following way. The first section reveals the relevance and purpose of research, state of the art and the structure of the article. The second section shows the models linking of the safety ICS to the V-model life cycle; The main assumptions of the models, their classifier, and the two models MICS32 and MICS42 in the form of marked-up graphs are disclosed. The third section analyzes results of multi-fragment models study. The fourth section presents the algorithm of the assessing method requirement fulfillment for safety of ICS on programmable platforms. The fifth section shows the IDEF diagram of information technology for decision support and its blocks are disclosed for assessing and managing the implementation of the requirements for the safety of ICS. Section 6 concludes and describe direction of future research.

2 Approach and Modeling Technique

2.1 Principles for the Development and Correction of Markov' Models for Assessing Safety at Different Stages of the V-model Life Cycle

The process of designing an ICS using the V model is being considered as set stages (SetST). At the end of each stage, in order to reduce the effect of accumulation of the number faults and the severity design errors, an assessment is made of compliance with the requirements, in particular, with respect to safety requirements. Early identification of non-compliance with requirements allows to quickly make changes to the design, review architectural decisions or adjust system parameters (perform corrective actions). However, the implementation of corrective actions can change the project in such a way that the developed mathematical model will lose its adequacy and itself will require correction. Consequently, in the multidimensional V-model, it is necessary to introduce a new layer of stages associated with a change in Markov' models for assessing safety, as shown in Fig. 1.

The stage of the V-model is determined by the combination of the following actions:

1. At each stage of the ST_i of V-model, the S_i structure and P_i parameters of the Markov' model are determined or refined (Fig. 1). In the case of consideration alternative architectural design options, a parallel consideration of several Markov' models is possible.
2. Correction of the model (models) and the calculation of the availability function $A_i(t)$ are carried out.

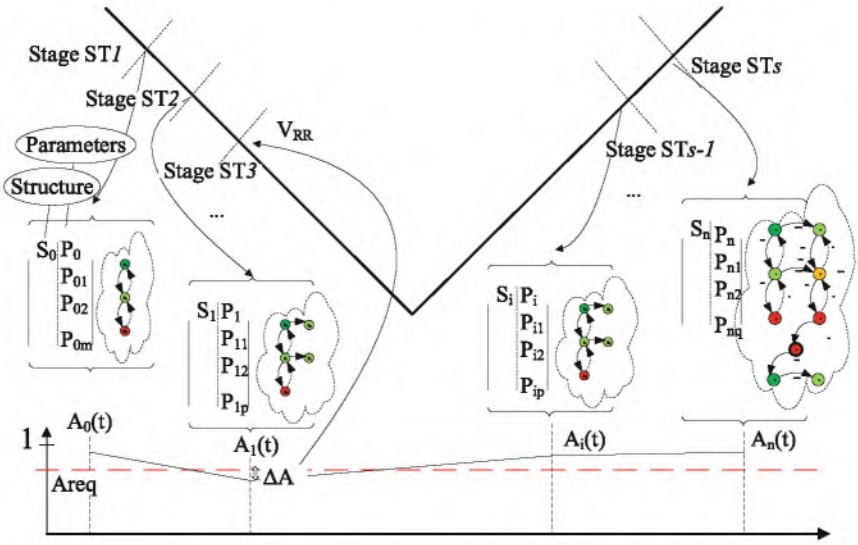

Fig. 1. Stages of the V model ICS design with reference to the change in Markov models for assessing safety

3. To assess the requirements fulfillment, the preparedness function $A_{req}(t)$ is compared and the discrepancy is determined.
4. Corrective actions (CAct) are carried out:

   – determined by set CAct;
   – the selection of CAct is carried out according to the criterion of minimizing costs and guaranteed provision of requirements;
   – CAct implementation is in progress.

At the bottom of Fig. 1, in the form of a graph, the results of verification compliance with the requirements for safety are illustrated. When the safety level falls below a predetermined value, CAct (as V_{RR} in Fig. 1) is promptly introduced. Also, at the last stage, a change in the Markov' model is illustrated for adequate modeling of the system with the elimination of faults (reaction to changes in the operating conditions of the system).

In this paper, we study the ICS design of a nuclear power plant, previously considered [5, 6]. The structural diagram of the ICS reliability is presented in Fig. 2. It includes three independent hardware channels, each of which is diagnosed for dangerous failures by the monitoring system. The hardware channels use the same type of software, so its failure is equivalent to a failure for a common reason.

The monitoring system is characterized by the DC parameter (diagnostic coverage). In the designed system, a distinction is made between the hardware coverage and software diagnostics, respectively, the DC_{HW} and DC_{SW} parameters are entered. Monitoring is carried out continuously and detected failures are eliminated immediately after detection.

The assumptions during models building are as follows:

- the events of failures and restoration of hardware channels and software (until the fault 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 [3, 15] 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 is $\lambda_{DU\,HW} = \lambda_{D\,HW} * (1 - DC_{HW})$; and similarly $\lambda_{DD\,SW} = \lambda_{D\,SW} * DC_{SW}$, $\lambda_{DU\,SW} = \lambda_{D\,SW} * (1 - DC_{SW})$.

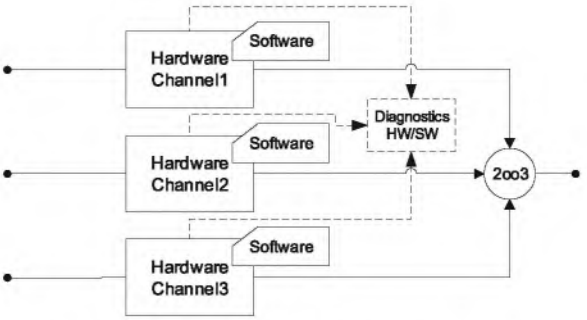

Fig. 2. Reliability block diagram of the ICS

Each hardware channel of the model can be in one of three states:

- workable;
- the manifestation of a dangerous failure detected by the control system (detected dangerous failure);
- manifestation of a dangerous failure not detected by the control system (undetected dangerous failure).

Figure 3 shows the tree of system failures, using the graphical notation (+, –, ×) [1, 18] to display the corresponding states: a working, detected dangerous failure and undetected dangerous failure. Also, the HW/SW notation was used for display to highlight the place of failure identification (hardware channel/software).

When compiling the fault tree in Fig. 3, the logic of the majority body functioning (2 out of 3 voting systems) was taken into account. If faults are detected in two failures or in the SW, the system stops until the fault is eliminated; as a result, there are no states in the fault tree that include the combination (–hw, –hw, –hw).

To simplify the presentation, the tree is divided into three sectors on the basis of the SW operability – in the first sector, the SW is operational, in the second and third – it is inoperative due to an explicit and hidden failure, respectively.

The basic Markov' ICS models considered in this paper are built on the basis of set states from the failure tree (includes at least 25 states).

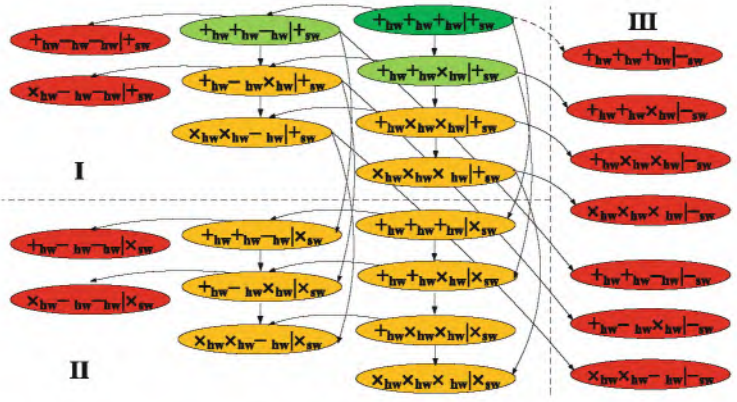

Fig. 3. ICS failure tree

Table 1. Safety models of the information and control system NPP

General characteristics of the model	Model specification	Conventional notions
(A) Markov model for evaluating the safety of the information and control system with an absorbing state	– three groups of states (without manifestation of SW fault, with detected SW failure and with undetected SW failure) – there is one absorbing state (output only after the proof test)	MICS01
(B) Markov model for evaluating the safety of the information and control system with the migration of hidden failures	– three groups of states (without manifestation of SW fault, 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)	MICS02

(*continued*)

Table 1. (*continued*)

General characteristics of the model	Model specification	Conventional notions
(C) Multi-fragmental models for evaluating safety of the information and control system with incomplete elimination of design faults	– 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)	MICS31
	– several fragments, in each fragment there are three groups of states – there are no absorbing states (after the manifestation of the undetected failure, its "migration" is possible before the proof test)	MICS41
(D) Multi-fragmental models for evaluating safety of the information and control system with incomplete elimination of design faults	– 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 faults are eliminated – there is the absorbing state in each fragment (output only after the proof test)	MICS32
	– 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 faults are eliminated – there are no absorbing states (after the manifestation of the undetected failure, its "migration" is possible before the proof test)	MICS42

In this paper we develop six models using Markov process theory as shown in Table 1. Models MICS01 and MICS02 were studied at the papers [1, 18] with the assumption of manifestation of only dangerous HW failures and only DC_{HW} parameter. Models MICS31 and MICS42 were studied at the papers [19]. We discuss in this work the separate diagnosis of hardware and software with DC_{HW} and DC_{SW} parameters.

2.2 Development and Research of Model MICS32 for Assessing the ICS Safety with the Complete Elimination of Design Faults

The MICS32 multi-fragment model, in comparison with the MICS31 [19], describes the operation of the ICS with the gradual elimination of all identified design faults. The marked graph of the model is shown in Fig. 4.

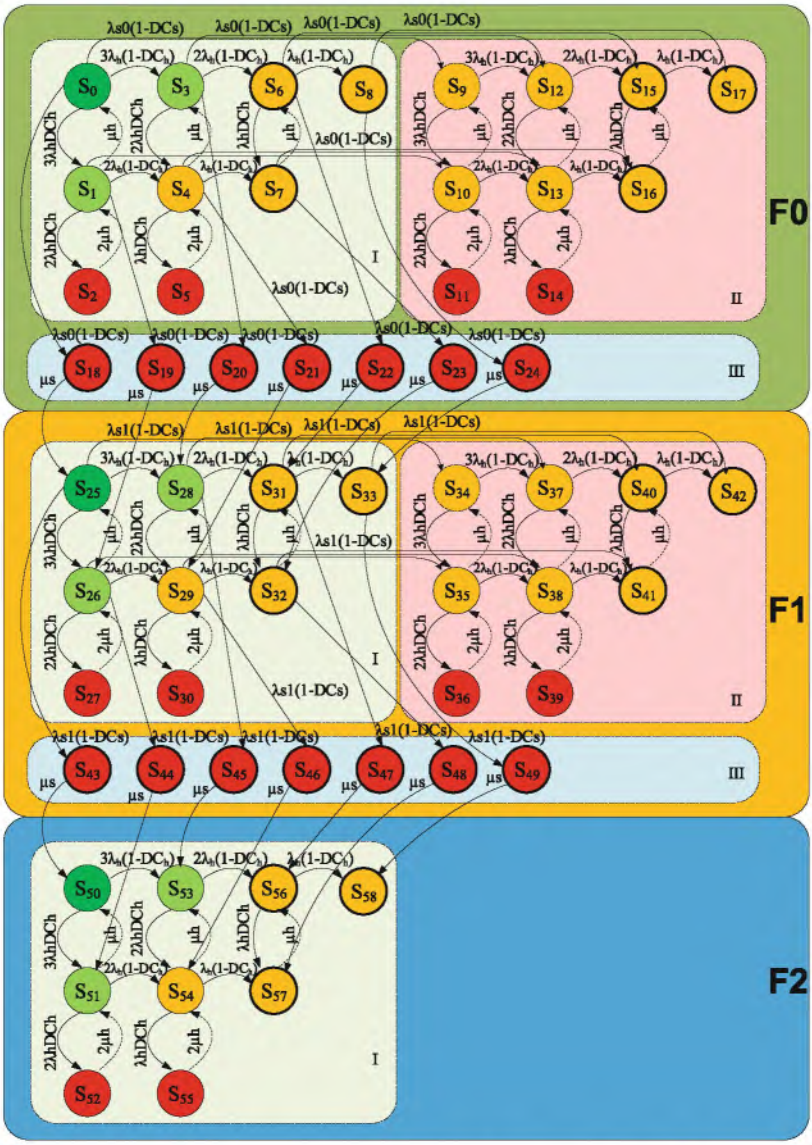

Fig. 4. Marked graph of the ICS functioning model with absorbing states and elimination of all design faults

A three-fragment model (fragments F0, F1 and F2) is described, which describes the functioning of the ICS, during which two (of two) design faults are eliminated. Fragments F0 and F1 of the model contain 25 states: S0 … S24 in the initial fragment F0 and S25 … S49 in the fragment F1. The last fragment of F2 contains 9 states S50 … S58. Fragments F0 and F1 according to the logic of functioning are identical to the initial fragment F0 of the MICS31 model (in fragment F1, taking into account the "shift" of state numbering by 25).

After the detection of a dangerous SW failure, which manifests itself with an intensity of $\lambda_{D\,SWi}$, a mechanism for its elimination is initiated, after which the system goes into a new fragment of states. In the new fragment, the intensity of the occurrence of dangerous SW failures is $\lambda_{D\,SWi} + 1$, and is determined by

$$\lambda_{D\,SWi} = \lambda_{D\,SWi-1} - \Delta\lambda_{D\,SW} \tag{1}$$

After the manifestation and detection of the second dangerous SW failure, the system goes to the last F2 fragment, in which only dangerous HW failures appear.

Absorbing states are present in all fragments of the MICS32 model: S17 in the fragment F0, S42 in the fragment F1 and S58 in the fragment F2.

The availability function taking into account dangerous failures is defined as (2):

$$\begin{aligned} A(t) = {} & P_0(t) + P_1(t) + P_3(t) \\ & + P_{25}(t) + P_{26}(t) + P_{28}(t). \end{aligned} \tag{2}$$

Baseline conditions: $t = 0$, $P_0(0) = 1$, $P_1(0) \ldots P_{49}(0) = 0$.

2.3 Model MICS42 for Evaluating the Safety of the Information and Control System with the Migration of Failures

In the MICS42 multi-fragment model, the assumption is made of the "migration" of latent failures into explicit ones, and the gradual elimination of all design faults.

After the transition of the system to an absorbing state, a new failure is likely to occur over time, which will be detected by the diagnostic system. Once identified, a failure response procedure will be initiated, during which previously hidden failures are detected.

There are no absorbing states on the marked column of the model (Fig. 5) and the elimination of two (out of two) design faults is described. In the last F2 fragment, the system operation is modeled without dangerous SW failures.

The number and character of the MICS42 model graph states are identical to the previous model MICS32 [19]. In addition to the MICS32 model, transitions have been added that simulate the migration of hidden HW and SW faults.

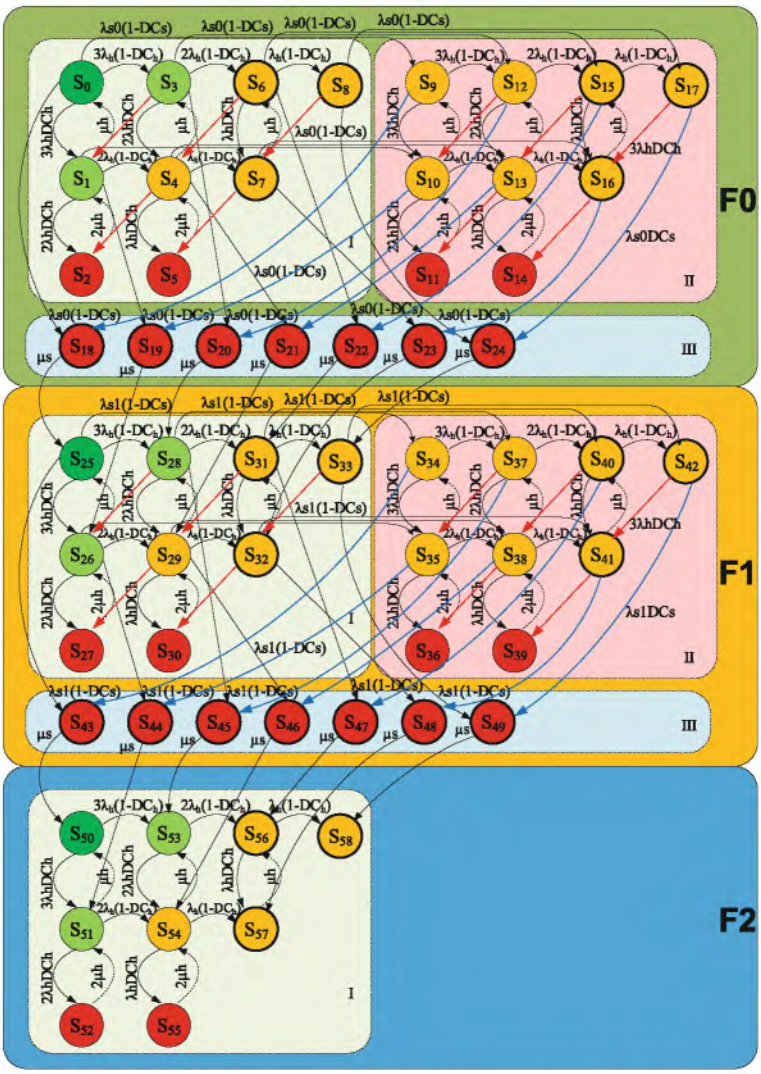

Fig. 5. Marked graph of a multi-fragment model of the ICS functioning with migration of latent failures MICS42

3 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 matrix A function [16]. The solution was performed in the Matlab system using the ode15s method [17] for the time interval of [0 … 50000] h. The simulation results for the five-fragment model (Nf = 5) are shown in Fig. 6 and for clarity, are compared with the results of MICS01 and MICS31 previous models [18, 19].

Table 2. Values of input parameters of simulation processing

#	Parameter	Base value
1	λ_{Dhw}	46.04622e−6 (1/h)
2	DChw	0.9989
3	$\mu_{hw} = 1/MRT_{hw}$	1/8 = 0.125 (1/h)
4	λ_{Dsw}	6.27903e−6 (1/h)
5	DCsw	0.9902
6	$\mu_{sw} = 1/MRTs$	10 (1/h)
7	μ_{sr}	1/24 = 0.04167 (1/h)
8	$\Delta\lambda_{Dsw}$	1.5697575e−06 (1/h)

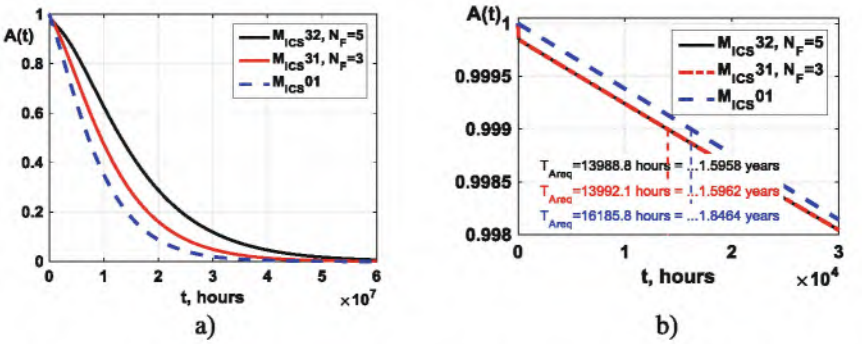

Fig. 6. The results of modeling of availability function of models MICS32 (a) and determining T_{Areq} interval with an error ξ =1e−6 (b)

On a long time interval (6 * 10^7 h, Fig. 6a), the difference between the results of the three-fragment MICS31 and five-fragment MICS32 models is visible. But this difference is almost leveled at a short interval of 3 years, characteristic of prooftest industrial systems and this is clearly seen in Fig. 6b.

The simulation results of the multi-fragment model MICS42 are shown in Fig. 7 and for clarity, are compared with the results of the MICS02 and MICS41 previous models [18, 19].

The MICS42 availability function seeks a fixed value of 0.999992. At the same time, it has a minimum with a value of 0.993 and two points of requirement level intersection of SIL3 at 0.999. The first intersection corresponds to T_{Areq} = 1.7 years and matches the result of the MICS41 model. The second intersection corresponds to T_{Areq} = 348 years (Fig. 7c) and is unacceptable from a practical point of view.

For MICS32 and MICS42 models, the additional studies were conducted to determine the values of the input parameters at which $T_{Areq} \geq$ 26298 h. The intervals for changing the input parameters are the same as for MICS31 and MICS41model and are shown in Table 3.

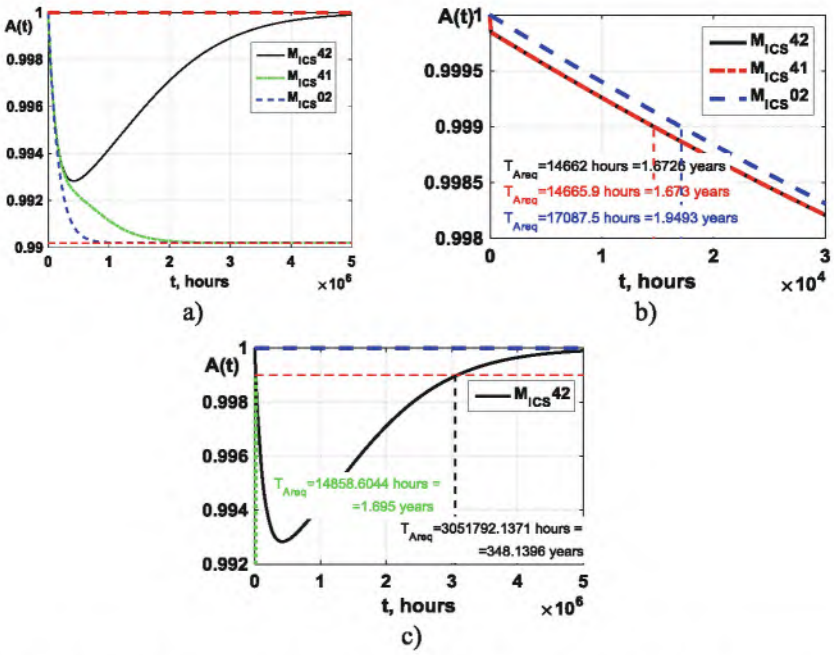

Fig. 7. The result of modeling the availability MICS41 model function (a) and determining the TAreq interval with an error of $\xi = 1e{-}6$ (b, c)

Table 3. Variable input parameters of the ICS model

#	Variable parameter	Designation	Values series
1	Diagnosing dangerous hardware failures control completeness	DC_{HW}	[0..1]
2	Diagnosing dangerous software failures control completeness	DC_{SW}	[0..1]

Studies of the MICS32 model on the influence of changes in input parameters from Table 3 showed results identical to the MICS31 model (difference in 4...5 decimal places). An exception can be considered the simulation result, illustrated in Fig. 8. Firstly, as in the MICS31 model, starting from $DC_{SW} = 0.9947$, the condition T_{Areq} 26298 h is provided. Secondly, on the $DC_{SW} = [0.9994...0.9997]$ interval, the MICS31 model shows better T_{Areq} results in comparison with the single-fragment model MICS01 (shown in Fig. 8b). The five-fragment model MICS32, despite the complete elimination of design faults, loses in terms of T_{Areq} in comparison with the models MICS01 and MICS31.

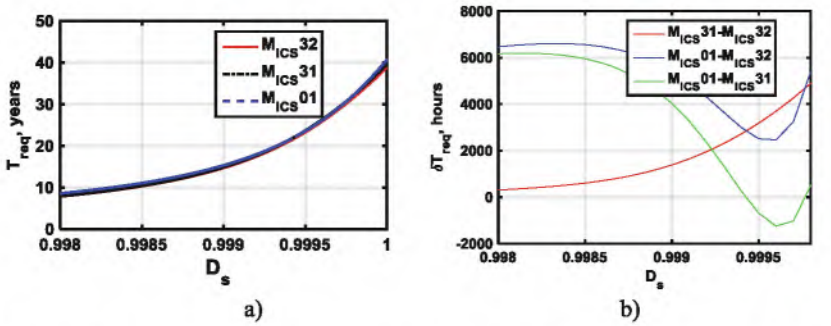

Fig. 8. Graphs of changes in the resulting T_{Areq} interval of the MICS32 model (a) and the difference in the T_{Areq} intervals of the MICS01, MICS31, MICS32 models (b) for different values of the DC_{SW} input parameter

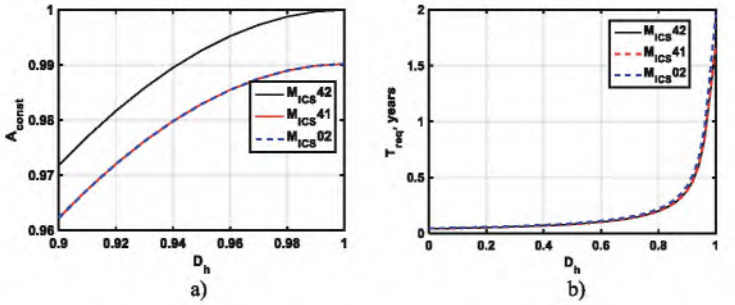

Fig. 9. Graphs of the settled value of the MICS42 model availability function (a), determination of the TAreq interval (b) for different values of the DCH input parameter

Thus, the MICS32 multi-fragment model with absorbing states is characterized by a decrease in the availability function to zero. For typical values of input parameters (Table 2), the implementation of SIL3 requirements is guaranteed over the interval [0 … 1.6 years]. An increase in the Tprooftest test interval to 3 years is possible with an increase in the completeness of monitoring to detect dangerous SW failures to $DC_{SW} = 0.9947$ and higher.

For the MICS42 model, additional studies were also conducted to determine the values of the input parameters at which $T_{Areq} \geq 26298$ h. The intervals for changing the input parameters are shown in Table 3. The results of the study were obtained for a model with five fragments (Nf = 5).

The results of the influence values of input parameter DC_{HW} on the availability function of the MICS42 model are shown in Fig. 9. As the graph in Fig. 9a show, when $DC_{HW} \rightarrow 1$, A_{const} also tends to 1. But at the same time, the interval of transition of the function to the stationary state does not allow the condition $T_{Areq} \geq 3$ years (Fig. 9b).

The results of the influence DC_{SW} input parameter values on the behavior of the MICS42 model availability function are shown in Fig. 10a. The dependence of Aconst

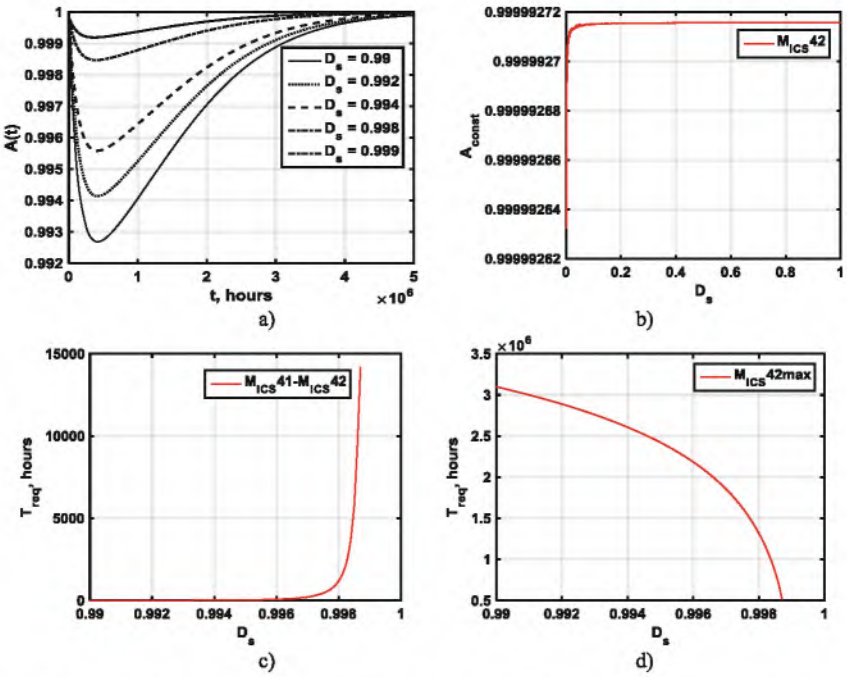

Fig. 10. Graphs of the availability function MICS42 model (a), the stationary value availability function (b), the difference T_{Areq} for MICS41 and MICS42 models (c) determining the T_{Areq} interval (d) for different values of the DC_{SW} input parameter

on DC_{SW} for the MICS42 model is nonlinear: for $D_{SW} = 0 = > A_{const} = 0$, but already for the smallest $D_{SW} > 0$, $A_{const} = > 0.9999927$ (Fig. 10b). But, although the value $A_{const} = 0.9999927$ satisfies the requirements of SIL3, it is not achieved immediately, and at the same time, the availability function is significantly reduced to a minimum at the initial stage.

The result shown in Fig. 10c illustrates the difference between the MICS41 and MICS42 models in terms of T_{Areq} (for the MICS42 model, the first, left point of intersection level of 0.999 is considered). Ensuring a $T_{Areq} \geq 3$ years condition for the five-fragment model MICS42 starts with $DC_{SW} = 0.9942$. For $DC_{SW} > 0.996$, the difference in T_{Areq} between MICS41 and MICS42 exponentially increases.

The question arises: is it possible to shift to the left the second intersection point by the function of availability level 0.999. The answer is illustrated in Fig. 10d – yes it is possible up to $T_{Areq} = 5 * 10^5$ h at $DC_{SW} \rightarrow 0.9987$. A further increase in $DC_{SW} \rightarrow 0.999$ causes the entire chart to rise above the border A = 0.999 (seen in Fig. 10a), which eliminates the need for prooftest.

Thus, the MICS42 multi-fragment model is characterized by a decrease in the availability function to a minimum, and then an increase to the stationary value A_{const}. For typical values of input parameters (Table 2), the implementation of SIL3 requirements is guaranteed over the interval [0 … 1.69 years]. An increase in the

$T_{proof\ test}$ interval to 3 years is possible with an increase in the completeness of monitoring to detect dangerous SW failures to the level of $DC_{SW} = 0.9942$. Starting at $DC_{SW} = 0.999$, SIL3 requirements are guaranteed to be met without additional test checks.

4 Method for Assessing the Requirements Implementation for ICS Safety on Programmable Platforms

The developed mathematical models make it possible to evaluate the fulfillment of the safety requirements of the designed ICS. In accordance with Fig. 1, the application of the developed models is advisable in specific time frames tied to the stages of the V-model of the project life cycle (and possibly to a separate layer of the V-model). In connection with the need to select one of several models for a particular design stage, tight timing to the beginning/end of the life cycle phase, substantiation of assumptions, changes in the structure and parameters of models, it is necessary to streamline and regulate these operations in the framework of one method.

At a certain stage of the V model life cycle of the ICS project on programmable platforms, the expert group forms an idea of the project architecture, the components used and their operating modes, planned test intervals, etc. This information is generated based on the personal experience of experts, operating experience and certification of such systems, from analysis of system requirements. Based on the work of the expert group, a task is formed to develop and study a mathematical model ICS functioning, which allows assessing the fulfillment of safety requirements. The input data for the model development are the project architecture (allow to create the structure of the Si model as the basis for constructing a labeled graph of states and transitions), reliability parameters of components (HW, SW, majority element and diagnostic system) for dangerous failures (distinguish the values of the input parameters of Markov models for estimating safety and permissible ranges of their change), proof test parameters and quantitative requirements for safety based on SIL (safety integrity levels). Based on the developed mathematical model are determined:

- compliance with safety requirements ($A \geq A_{req}$) in general and at time intervals;
- compliance with T_{Areq} requirements (for industrial systems $T_{Areq} \geq 3$ years);
- the values of the input parameters from the permissible change intervals at which the requirement $T_{Areq} \geq 3$ years is provided.

The algorithm of the assessing method for requirements fulfillment of ICS safety on programmable platforms is presented in Fig. 11. It contains 23 blocks and is based on the use of Markov models by correcting their structure and parameters according to the stages of the life cycle described by the V-model.

At the beginning (block 2), from the general set of design requirements, quantitative requirements for the safety ICS are identified (in the example considered: for SIL3 $A \geq 0.999$).

Further, on the basis of the initial architecture design, a reliability block diagram (RBD) of the system is built, on the basis of which a tree of dangerous failures and a marked graph will be built (block 3).

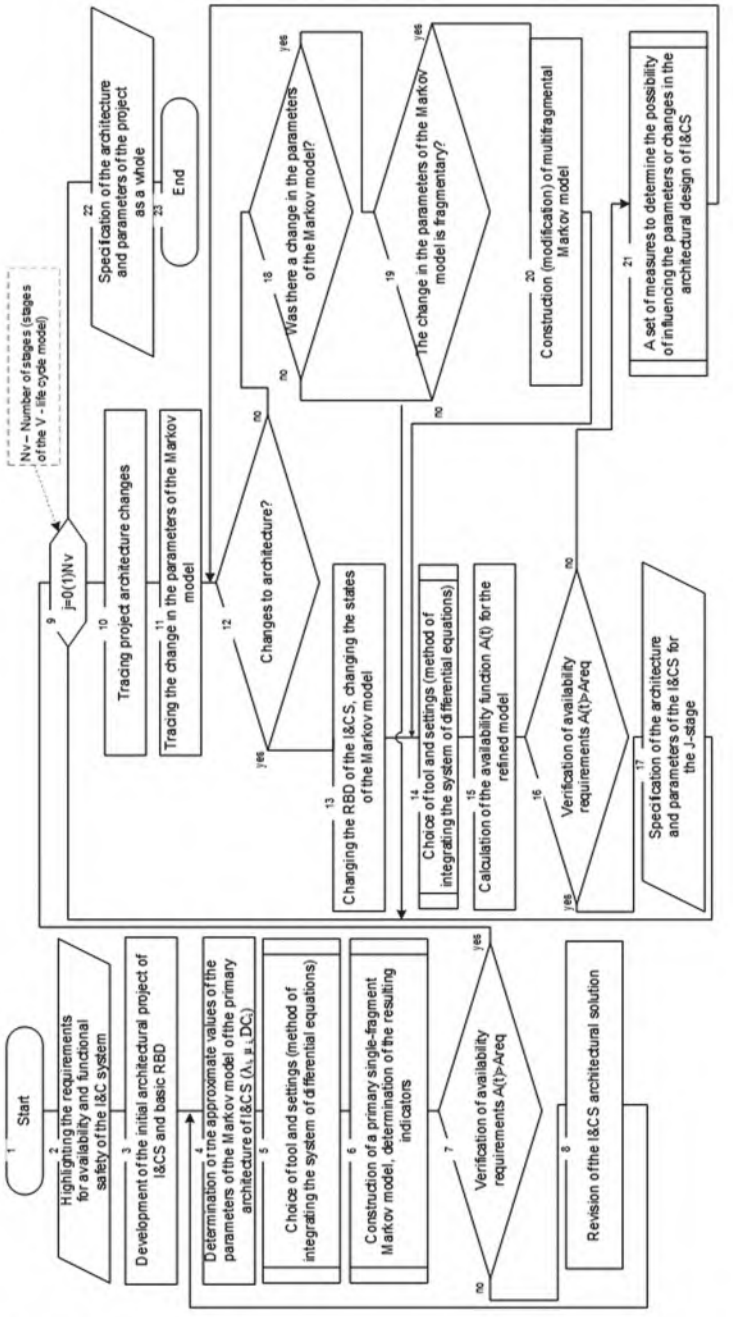

Fig. 11. Algorithm for the assessing method the implementation of the requirements for ICS safety on programmable platforms

In block 4, the input parameters of the Markov' model of safety estimation are determined based on the experience of experts and the operation of such systems.

Block 5 describes the selection of tools for Markov' modeling. This block is constituted, but its contents are considered in detail [7] and are not considered in this paper.

Compound block 6 describes the construction of the primary Markov' model (as a rule, single-fragment). Its sequence is illustrated in detail [6].

In block 7, a procedure for checking requirements is illustrated. If the result is positive, the ICS project is approved and a new stage of the V-model life cycle begins. A negative result requires a review of architectural design (block 8).

Blocks 9–21 illustrate the iterative process of ICS designing (from the point of view of layer V-model related to Markov' modeling). Throughout the life cycle, tracking is made of changes to the project architecture (block 10), or changes in its components or their operating modes (block 11), affecting the safety parameters, which are displayed as input parameters to the Markov' model.

Changing the project architecture, as a rule, will entail a change in the labeled graph of the model (blocks 12, 13). Changing the parameters may not be so radically reflected in the contents of the digraph (blocks 18, 13), but if the change causes the elimination of faults, then it is necessary to use a multi-fragment modeling apparatus (blocks 19, 20).

In case of changes in the project that entailed the modification of the Markov' model, blocks 14–16 are repeated, describing the choice of tool, construction and research of the Markov' model for assessing safety. If the requirements check is positive, the specification of the architecture and project parameters for the subsequent life cycle stage is approved (block 17), if negative, the composite block 21 is executed with a set of appropriate measures.

After completing all the stages of the life cycle, the architecture and parameters of the project as a whole are finally specified (block 22).

In the course of the research, the ICS was linked to the ICS project for the implementation of the emergency protection system of the NPP reactor in normal operation.

Previous versions of the project were certified according to the SIL3 level, which allowed us to calculate the typical values of the input parameters presented in Table 2. Initially, to evaluate the safety requirements, a single-fragment model MICS01 was developed, as a result of the study of which the conformity of SIL3 was confirmed on the interval of intertest checks $T_{\text{proof test}} = 16186$ h. At the next stage, the life cycle during the analysis of the operation and maintenance of previous versions of the system revealed and confirmed the fact of the migration of latent failures. This led to the development and study of a single-fragment model MICS02, for which $T_{\text{proof test}} = 17087$ h.

Studies of the MICS01 and MICS02 models showed that increasing test intervals to $T_{\text{Areq}} \geq 3$ years can be achieved by reducing the intensity of dangerous SW failures. Since the terms of the project are limited, and the elimination of identified design faults is possible at the operational stage, it was decided to consider the possibility of putting into operation a system with an acceptable residual level of SW faults, on condition that the requirements for safety are met.

To verify compliance with the requirements, four multi-fragment models MICS31, MICS32, MICS41 and MICS42 were sequentially developed and investigated. The research results showed that in spite of the elimination of design faults and a decrease in the intensity of dangerous SW failures, it is not possible to increase the test intervals Tprooftest for typical values of the input parameters of the models. This is due to the increase in system downtime during the elimination of the design fault in comparison with the duration of the SW restart to restore the system.

Figure 12 summarizes the simulation results for all six models. Over a limited time interval [0 … 30000 h], multi-fragment models with incomplete and complete elimination of design faults MICS31 and MICS32, MICS41 and MICS42 showed almost identical results.

A generalization of the obtained simulation results made it possible to form the following observations:

- a change in $\lambda_{D\ HW}$ (in the range [0.05e−5 … 5e−5]) and DC_{HW} cannot achieve $T_{proof\ test} = 3$ years;
- SIL3 with $T_{proof\ test} = 3$ years is achieved with $DC_{SW} = 0.9947$ (MICS31, MICS32) or $DC_{SW} = 0.9942$ (MICS41, MICS42);
- for MICS41, MICS42 with $DC_{SW} = 0.9991 => A_{const} = 0.99909$), that is, the requirements of SIL3 are met without proof test.

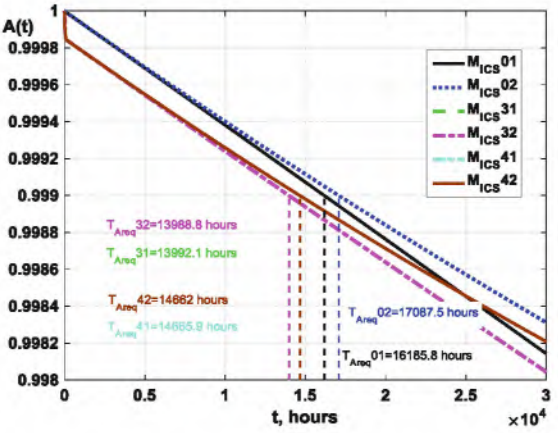

Fig. 12. Combined study results from six models to T_{Areq}

A generalization of the obtained quantitative values at which the level of safety integrity SIL3 is achieved for three-year test intervals is performed in Table 4.

Table 4. The result of applying the method of estimating safety requirements in the form of input parameter values to fulfill the condition $T_{proof\ test}$ = 3 years at SIL3

M_{ICS}	λ_{DSW}	DCsw
Base	6.23e−6	0.9902
01	3,9e−06	0,9939
02	4,11e−06	0,9934
31,32	–	0,9947
41,42	–	0,9942

After studying all the results obtained, the expert group decided to use a project with increased requirements for the completeness of the control occurrence of dangerous failures of the DC_{SW} = 0.9934 substation.

5 Information Technology for Decision Support in Assessing and Managing the Implementation of Requirements for ICS Safety

5.1 Streams and Processes

Information technology (IT) is based on the procedures for constructing and researching V-models to assess the completeness, consistency, and other characteristics of project requirements. Compliance management technologies are also categorized according to the V-model project stages and are based on the models application and methods discussed in this paper.

Figure 13 shows IT in the form of a sequence information flows, their processing and decision support tools.

Input information streams:

- Requirements of normative documents – standards, norms, rules, guidelines and other documents containing requirements for availability and safety information and control systems of nuclear power plants;
- Customer requirements – unformalized and inconsistent descriptions of the ICS functions of NPPs and other characteristics from the point of view of the customer, including the design cost limit;
- Certification data from previous versions of ICS – the results of the parameters evaluation (the rates of dangerous and safe failures, diagnostic coverage, test intervals between tests, as well as the average recovery time of components after failure detection.

Output information streams:

- specification of ICS requirements, their architecture and component parameters.

Intermediate information streams:

- a fixed set of unsorted requirements;

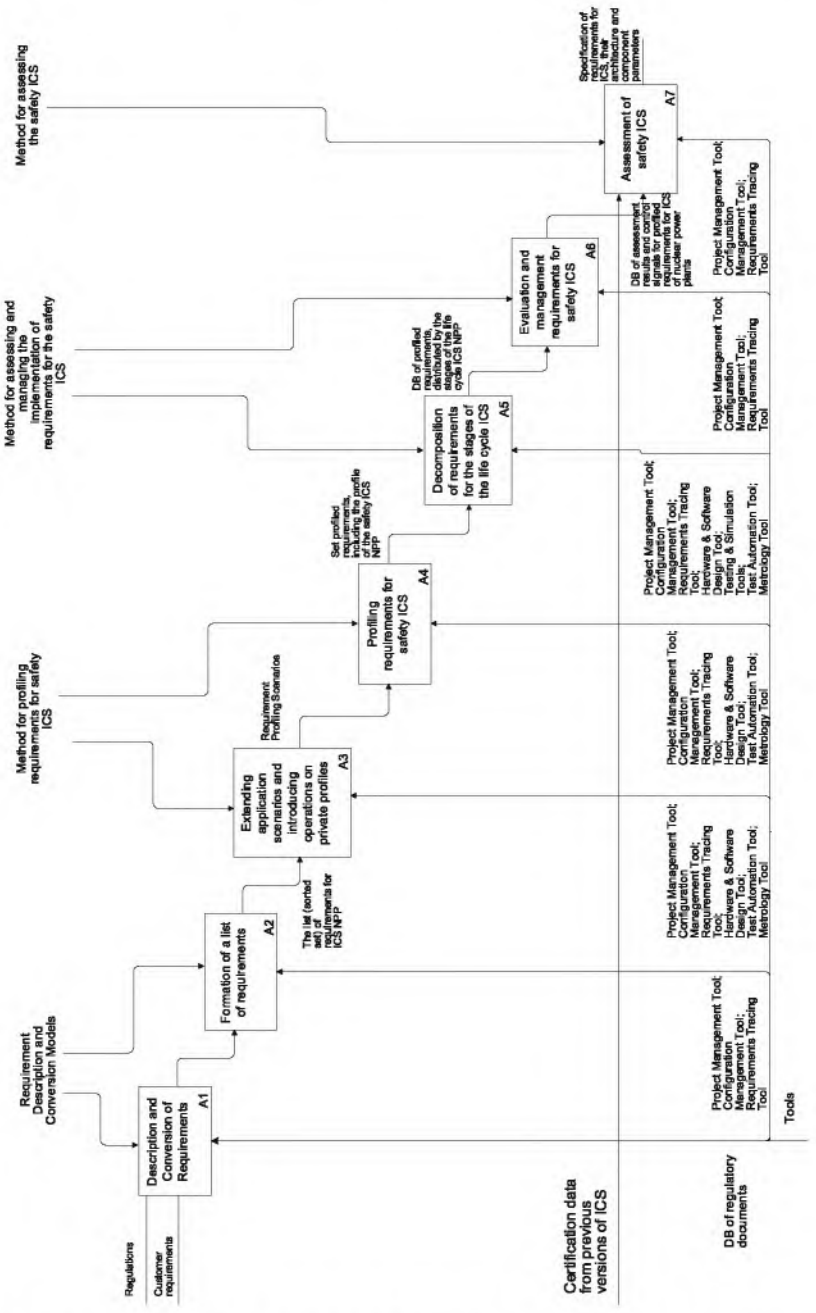

Fig. 13. Decision support IT in assessing and managing the implementation of requirements at the stages of the V-model for designing information and control systems for NPP

- the list (sorted set) of ICS requirements of nuclear power plants;
- scenarios for profiling requirements;
- many profiled requirements, including the profile of the safety ICS NPP;
- a database of profiled requirements distributed by the stages of the life cycle ICS of the NPP;
- a database of assessment results and control signals for profiled requirements for the IMS of nuclear power plants.

The processing information flows (functions):

- Description and transformation of requirements – includes the formation of the verbal information presentation in the form of semantic facet-hierarchical structures, the formation of functions requirements, architecture, availability and safety of the ICS of nuclear power plants based on the requirements of regulatory documents and customer requirements;
- Extension of application scenarios and the introduction of operations on private profiles – includes the use of special metrics; as a result of applying the method, the risks of faults associated with loss, insufficient detail and incorrect requirements are reduced;
- Profiling safety requirements for ICS – includes the construction of a set-theoretic model of life cycle, V-models modification and their generalization into multi V-models based on the proposed graph;
- Decomposition of requirements according to the stages of life cycle ICS – includes determining return points in the life cycle for each requirement and options for its non-fulfillment, calculating metrics, determining the types of corrective actions and calculating costs for different return scenarios and options for corrective actions;
- Evaluation and management of the requirements implementation for the safety ICS;
- Allows for the rapid assessment and correction of non-compliance, to ensure the required completeness of inspections and reduce time costs;
- Evaluation of the safety ICS – includes the development and study of Markov' models, the correction of their structure and parameters according to the stages of the life cycle described by the V-model, comparison of the predicted value and the formation of recommendations to ensure the availability function to the specified requirements.

5.2 Tools

Decision support tools for this technology include:

- Data base (DB) of normative documents – a database including texts of standards, norms, rules, manuals and other documents containing requirements for information and control systems of nuclear power plants for availability and safety;
- Certification data for the components of the ICS architecture of a nuclear power plant, as well as its previous versions – values of failure rates, dangerous failures, diagnostics coverage, proof test intervals of components available for use and previous versions of information and control systems of nuclear power plants;

- Tools for assessing availability (MICS models) – tools for calculating the availability function, include software implementation of the developed ICS models using the Matlab calculation package;
- Project Management Tool;
- Configuration Management Tool;
- Requirements Tracing Tool;
- Hardware & Software Design Tool;
- Test Automation Tool;
- Metrology Tool
- Testing & Simulation Tools.

Table 5 shows the distribution of the tools developed application for the main stages of the V-model design life cycle ICS NPP. It should be noted that the need to consolidate the areas of responsibility of individual employees, the distribution of work by time and individual departments at this stage does not allow integrating the developed tools into a single software package. But this circumstance does not prevent the coordinated work of all substations at different stages of the life cycle.

Table 5. IT tool specification

Tools	Requirements specification	Architecture	Design & coding	Verification	Integration & validation
Project management tools & configuration management tools	+	+	+	+	+
Requirements tracing tool	+	+	+	+	+
CAD PCB layout tools & hardware design tools		+	+		
SW design tools & coding tools			+		
Static analysis tool & cyclomatic complexity calculation tool				+	
Automated software testing tool & test coverage analysis tool				+	
Serial port monitor & I/O simulation tool				+	+
Test automation tool				+	+
Metrology tool					+

6 Conclusions

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

The section presents an improved method for assessing the safety of ICS using Markov' models by adjusting their structure and parameters according to the stages of the life cycle described by the V-model, comparing the predicted value and generating recommendations to ensure availability function to the specified requirements, which ensures their implementation and reduces implementation costs.

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

(a) for the multi-fragmental MICS31 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 $DC_{SW} = 0.9947$ level and higher;
(b) the multi-fragmental MICS41 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.

An analysis of the results obtained in the course of modeling the functioning of the ICS on programmable platforms showed that:

- by changing $\lambda_{D\ HW}$ (in the range [0.05e−5 … 5e−5]) and DC_{HW} it is impossible to achieve $T_{proof\ test} = 3$ years;
- SIL3 at $T_{proof\ test} = 3$ years is achieved at $DC_{SW} = 0.9947$ (MICS31, MICS32) or $DC_{SW} = 0.9942$ (MICS41, MICS42);
- for MICS41, MICS42 with $DC_{SW} = 0.9991 => A_{const} = 0.99909$), that is, the requirements of SIL3 are met without prooftest.

The developed mathematical models make it possible to assess the fulfillment of the safety requirements 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).

The future step includes: 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. In: CEUR Workshop Proceedings, vol. 1614, pp. 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. Ournal Loss Prev. Process. Ind. **21**(4), 437–449 (2008)
4. Zhu, M., Pham, H.: A software reliability model with time-dependent fault detection and fault removal. Vietnam J. Comput. Sci. **3**(2), 71–79 (2016)
5. Pham, H.: Loglog fault-detection rate and testing coverage software reliability models subject to random environments. Vietnam J. Comput. Sci. **1**(1), 39–45 (2014)
6. Kharchenko, V., Butenko, V., Odarushchenko, O., Sklyar, V.: Multifragmentation Markov modeling of a reactor trip system. ASME J. Nucl. Eng. Radiat. Sci. **1**(3), 031005–031005-10 (2015)
7. Butenko, V.: Modeling of a reactor trip system using Markov chains: case study. In: Proceedings of the 2014 22nd International Conference on Nuclear Engineering. Volume 5: Innovative Nuclear Power Plant Design and New Technology Application; Student Paper Competition (2014)
8. Vizarreta, P., Trivedi, K., Helvik, B., Heegaard, P., Kellerer, W., Machuca, C.: An empirical study of software reliability in SDN controllers. In: 2017 13th International Conference on Network and Service Management (CNSM) (2017)
9. Trivedi, K., Bobbio, A.: DSN 2016 tutorial: reliability and availability modeling in practice. In: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W) (2016)
10. Matos, R., Dantas, J., Araujo, J., Trivedi, K., Maciel, P.: Redundant eucalyptus private clouds: availability modeling and sensitivity analysis. J. Grid Comput. **15**, 1–22 (2016)
11. Chang, X., Lv, S., Rodriguez, R., Trivedi, K.: Survivability model for security and dependability analysis of a vulnerable critical system. In: 2018 27th International Conference on Computer Communication and Networks (ICCCN) (2018)
12. Ataie, E., Entezari-Maleki, R., Rashidi, L., Trivedi, K., Ardagna, D., Movaghar, A.: Hierarchical stochastic models for performance, availability, and power consumption analysis of IaaS clouds. IEEE Trans. Cloud Comput. (2017)
13. Taylor-Rodríguez, D., Womack, A., Fuentes, C., Bliznyuk, N.: Intrinsic Bayesian analysis for occupancy models. Bayesian Anal. **12**, 855–877 (2017)
14. Sukhwani, H., Alonso, J., Trivedi, K., Mcginnis, I.: Software reliability analysis of NASA space flight software: a practical experience. In: 2016 IEEE International Conference on Software Quality, Reliability and Security (QRS) (2016)
15. D7.24-FSC(P3)-FMEDA-V6R0. Exida FMEDA Report of Project: Radiy FPGA-based Safety Controller (FSC) (2018)
16. 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. AISC, vol. 470, pp. 267–278. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39639-2_23

17. Ode15s: Solve stiff differential equations and DAEs - variable order method. https://www.mathworks.com/help/matlab/ref/ode15s.html. Accessed 27 Sept 2019
18. Kharchenko, V., Ponochovnyi, Y., Andrashov, A., Brezhniev, E., Bulba, E.: Modelling and safety assessment of programmable platform based information and control systems considering hidden physical and design faults. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds.) DepCoS-RELCOMEX 2019. AISC, vol. 987, pp. 264–273. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-19501-4_26
19. Kharchenko, V., Ponochovnyi, Y., Boyarchuk, A., Andrashov, A.: Multi-Fragmental Markov models of information and control systems safety considering elimination of hardware-software faults. In: CEUR Workshop Proceedings, vol. 2393, pp. 738–748 (2019)