Classification and Research of the Reactor Protection Instrumentation and Control System Functional Safety Markov Models in a Normal Operation Mode

Yevgeniy Bulba[1,3], Yurij Ponochovny[2], Vladimir Sklyar[1], Aleksandr Ivasiuk[3]

[1] National Aerospace University KhAI, Kharkiv, Ukraine

evhenb@gmail.com, vvsklyar@ukr.net

[2] Poltava National Technical University named after Yurij Kondratyuk, Poltava, Ukraine

pnch1@rambler.ru

[3] RPC Radiy, Kirovograd, Ukraine

ivasiuk.radiks@gmail.com

Abstract. This article presents the basic phases of the development and research instrumentation and control system (ICS) functional safety Markov models on the basis of the self-diagnosing programmable platform. The set of the models sets is obtained on the basis of the failure tree development and analysis, which includes the ICS hardware channels detected and undetected failures. There the classification of ICS in a normal operation mode, considering the different majority body modes and diagnostics levels is presented. The application of the models has allowed determining the boundaries of the ICS safety integrity level 3 (SIL3) in two-dimensional space of the input parameters and system operational time.

Keywords: instrumentation and control system, functional safety, Markov model, safety integrity level

Key terms. MathematicalModeling, MathematicalModel, SoftwareSystems

1 Introduction

Instrumentation and control systems (ICS) of the critical objects, which perform the safety-relevant functions, are estimated from the functional safety positions. The functional safety depends on the right operation of the electric, electronic and programmable electronic (E/E/PE) systems, integrated with the technological systems

ICTERI 2016, Kyiv, Ukraine, June 21-24, 2016

and equipment safety to reduce the external risk [1]. Functional safety analysis principles are interpreted in [2].

The estimation of the functional safety is a definition of risk level in the field of safety. Its value is the composition of probability of dangerous situations on production and gravity of all consequences which can arise during operation. The estimation of the functional safety for the reactor protection systems (RPS) takes the specific place.

The functional safety estimation models are considered in 6 parts of the IEC-61508 [3] standard in details. This document presents the examples of models: reliability block diagrams, failure trees, Markov and multiphase, Petri nets and Monte-Carlo, the formal languages models. Also, as noted in this standard, the given models are examples for creation of models of real systems only. So, in the papers [4, 5] the models of the functional safety of control systems of nuclear reactors and sensor systems of protection taking into account their constraints and operating conditions are analyzed.

The purpose of this article is the classification and creation of ICS RPS Markov safety models in the mode of normal operation and influence of input parameters of model on a measure value of the functional safety is probed.

The article consists of 7 sections. The actual part is an introduction. The second part represents the analysis of the abnormal protection systems operating conditions in the mode of normal operation. The flowchart of reliability and a complete tree of system failures are constructed on the basis of the carried-out analysis. The third section represents the justifications of the main assumptions allowing using of Markov simulation. The fourth section gives us the signs of classification of Markov models of the functional safety of ICS RPS and also the 6 main models considering the hardware failures are selected here. The fifth section presents the Markov graphs and the description of three models: MSaf1, MSaf2 and MSaf6. The sixth section gives the justification of models input parameters values and the ranges of their change.

The last section presents the simulation results of Markov's models.

2 The analysis of reactor protection system operating conditions in the mode of normal operation

The analysis of the abnormal protection system functional safety is mandatory in case of design of the unit. The RPS of the reactor is one of the most important security arrangements and safety of reactor installation in general in many respects depends on its reliability.

The Abnormal Protection Systems can be realized on the basis of platforms with using of the Field Programmable Gates Arrays (FPGA). The main attention in such platforms shall be paid to self-diagnosing for determination of dangerous and safe system failures.

We will consider the operation of ICS which is part of RPS in the mode of normal operation. Normal operation (normal operation) is understood as operation in the set operational limits and conditions. ICS turns on three independent hardware channels, each of which is diagnosed on existence of dangerous failures by the diagnostic system. The considered system functions in the mode with low frequency of requests to safety features. Respectively, for an assessment of the functional safety it is necessary to use Average Probability of Failures on Demand (PFD_{avg}) for each of the safety function.

The reliability block diagram of ICS RPS considering the majority voting component and diagnostic system is shown on Fig.1. This work presents the one-version part of ICS which operates in the mode of normal operation is considered (in emergency case two such ICS parts are involved, and each has the separate software version).

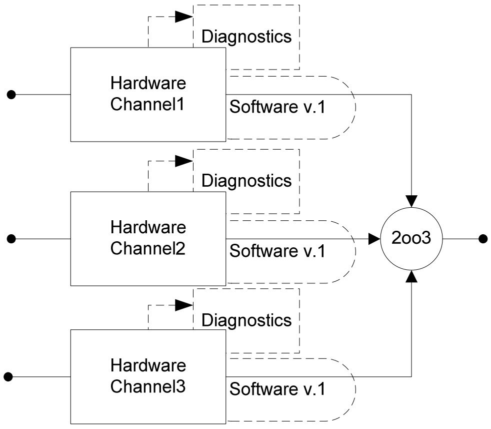


Fig. 1. The reliability block diagram of ICS RPS in the normal operation mode

The analysis of failures is made by the methods of collection and research of information on system failures in general, or elements of system. The majority of methods are based on carrying out inquiries of experts, application of numerical methods, the pilot studies, methods of probability theory and mathematical statistics [6].

The RPS failure tree creation and, as a result, Markov model of the system states can be result of such analysis.

Fig.2 shows the ICS tree of failures and at the same time the graphic notation (+, – ×, *, #) for display of corresponding states is used:

(+) – up state of hardware channel;

(*) – up state of software;

(–) – reveal of the dangerous failure in hardware channel revealed by the diagnostic system (the detected dangerous failure);

(×) – reveal of a dangerous failure in hardware channel, undetected by the diagnostic system (the undetected dangerous failure);

(#) – reveal of a software failure, a software failure is considered as a failure for the general reason.

Note: as in this system repair is made at once after reveal of an explicit failure, the repair state isn't considered, and return to run state with a repairing rate μ is modeled.

For display of change of states (transitions in between) the following notation is used:

- the solid line shows the transitions which will happen in system aren't dependent on operation modes of its elements;

- the dotted line shows the possible transitions which existence depends on a specific operation mode of elements of system.

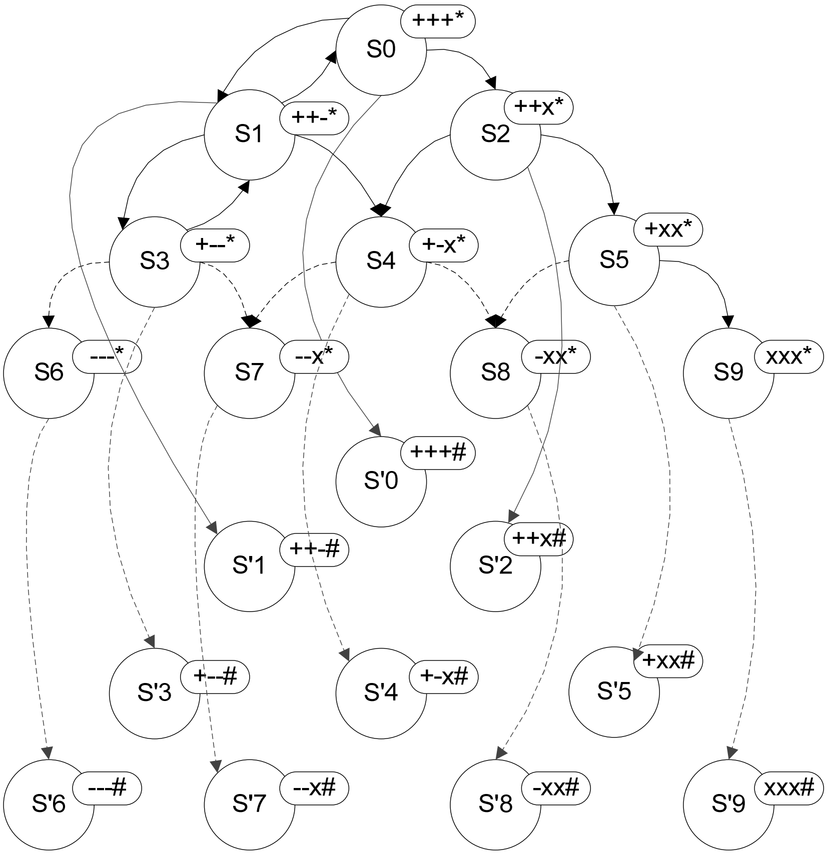


Fig. 2. The general failure tree of ICS RPS in the normal operation mode

Not all states, which are shown on the Fig.2, are admissible for the specific mode of functioning of the ICS elements and restrictions accepted in case of creation of model of estimation of the functional safety.

3 Main assumptions of instrumentation and control systems markov models

The ICS is characterized by the parameter of diagnostic coverage (DC). Unlike the models provided in [3,5] in the considered the diagnostic system is executed continuously (not periodically) and the revealed failures are eliminated immediately after detection. The remaining assumptions in case of model creation are the following:

- the failure and repair events of the hardware channels make the elementary flows (stationary, ordinary and without aftereffect), with constant parameters λ (failure rate) and μ (repair rate);
- the identical hardware channels with identical failures rate are used in the system;
- the majority device and the diagnostic system failure rate are scornfully small;
- in this model only the dangerous ICS hardware channels failures, those failure rate is calculated as $\lambda_D = 0.5*\lambda$ [3] is considered;
- the common cause failure rate is scornfully small, so it is not considered in this model [2];
- when diagnosing, the part of the dangerous failures is revealed, consequently, the rate of the found dangerous failures is $\lambda_{DD} = \lambda_D*DC$, and the rate of undetected dangerous failures is $\lambda_{DU} = \lambda_D * (1–DC)$;

  The software failures are not within the scope of this work.

4 ICS RPS functional safety Markov models classification features

Work [3] presents the typical models of systems with diagnosing of dangerous failures and majority vote system. The programmed logic-based implementation of ICS RPS allows using the additional functions and operation modes of the diagnostic system and majority device.

The list of ICS function enhanced modes and the appropriate classification features are shown in Table 1.

Table 1. ICS RPS operation modes classification features

#	Classification feature	Feature meaning
1	Majority voting component response on the reveal of the hardware undetected failures	1.0 – single majority device (without response) 1.1 – majority device with the undetected failure channel switching-off function 1.2 – majority device with the function of the enhanced diagnostics in the case of the unidentified failure
2	Undetected failures countermeasure (warfare) methods	2.0 – without response 2.1 – with «migration» of the undetected failure in detected 2.2 – with the enhanced undetected failures diagnostics
3	Software failure response	3.1 – without software failure repair 3.2 – with software failure repair

From the 18 possible classification features combinations the 12 is permissible. The half of 12 permissible combinations has such feature as the software failures repair, which upsets the condition of markov property in the construction of models [7]. Therefore, the set of markov models according to the proposed classification features will be the following:

M={MSaf1,MSaf2,MSaf3,MSaf4,MSaf5,MSaf6},

where

MSaf1={1.0∪2.0∪3.1} is a typical model with the single majority device, in which the failures, undetected by the diagnostic system, are collected;

MSaf2={1.0∪2.1∪3.1} is a model of the system with the single majority device, in which the hardware channels do not switch off after the reveal of the undetected failure, and the reveal of the detected failure is possible in them (in this paper it is called as the «migration» of the undetected failure in detected);

MSaf3= {1.0∪2.2∪3.1} is a model of the system with the single majority device, in which the enhanced diagnostic of the failures, undetected by the diagnostic system is carried out periodically;

MSaf4={1.1∪2.0∪3.1} is a model of the system with the majority device, which switches off the hardware channel, if there is a mismatch with other channels, which are regarded as intact by the diagnostic system;

MSaf5={1.1∪2.2∪3.1} is a model of the system with the majority device, which switches off the hardware channel, if there is a mismatch with other channels, which are regarded as intact by the diagnostic system; also in the ICS the enhanced diagnostic of the failures, undetected by the diagnostic system is carried out periodically;

MSaf6={1.2∪2.2∪3.1} – is a model of the system with the majority device, which initiates the hardware channels enhanced diagnostic in the case of the mismatch, and the diagnostic system acknowledges them as intent.

To lower the dimensionality this paper represents the approach to division on the models of hardware and software features, which is used in work [8]. The software models are not within the scope of this work, they are described in [7, 8]. Further, three ICS RPS function safety estimation Markov models, taking into account the hardware dangerous failures will be considered.

5 ICS RPS functional safety markov models

5.1 ICS RPS functional safety model with the single majority device without the responses on the diagnostic system non-identified failures (MSaf1)

The marked graph (digraph) of the model of ICS operation in the conditions of dangerous failures reveal is shown on Fig.3. This graph is constructed on the classical approach, which is described in [3] and contains the absorbing state S_8 with undetected dangerous failures. The output from a state of an undetected dangerous failure without carrying out additional actions isn't provided in the classical model.

Proceeding from the functioning of the diagnostic system and majority device logic, contains:

a) Operational states (up states): S_0 (all channels are operational), S_1 (in one of channels the dangerous failure appears and is found) and S_3 (in one of channels the dangerous failure appears, but isn't found);

b) non-operation states (down states): S_2 (in two channels dangerous failures appear and are found), S_4 (in one of channels the dangerous failure appears and is found, in another - it appears, but isn't found) and S_5 (in two channels dangerous failures appear and are found, in the third channel it appears, but isn't found);

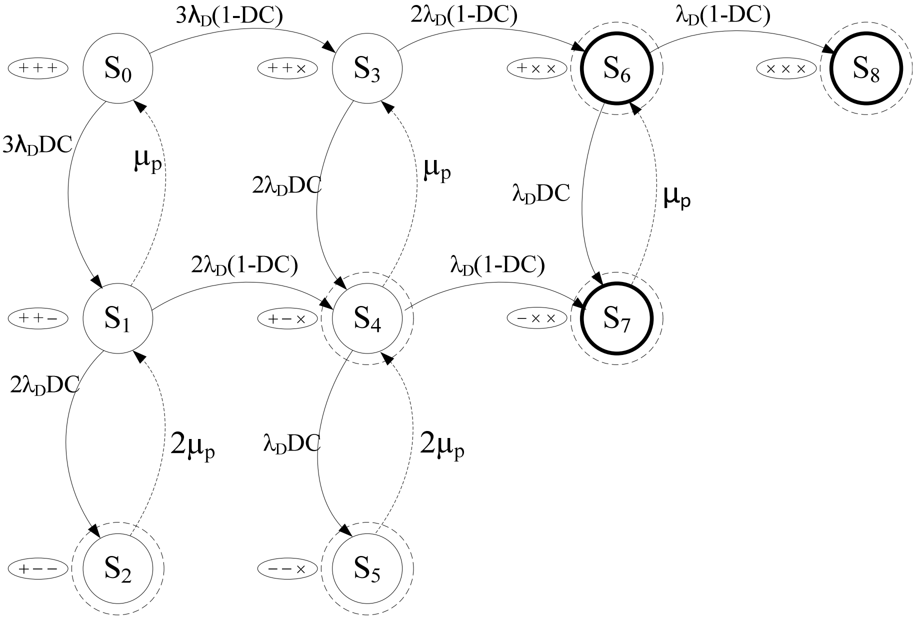


Fig. 3. The marked graph of the model of ICS RPS operation with the absorbing state (MSaf1)

c) states with undetected dangerous failures which majority device is incapable to parry an organ: S_6 (in two channels the dangerous failures appear but aren't found), S_7 (in one of channels the dangerous failure appears and is found, in two channels the dangerous failures appear, but aren't found), S_8 (in three channels the dangerous failures appear, but aren't found).

After detection of a dangerous failure reveal, the non-serviceable channel is disconnected and recovered with intensity μ_p, it is modeled by the appropriate transitions of $S_1 \rightarrow S_0$, $S_2 \rightarrow S_1$, $S_4 \rightarrow S_3$, $S_5 \rightarrow S_4$, $S_7 \rightarrow S_6$. The safety function PFD_{avg} is defined as:

$$PFD_{avg} = 1 - P_0(t) - P_1(t) - P_3(t). \qquad (1)$$

5.2 ICS RPS functional safety model with the single majority device without the “migration” of the failures, undetected by the diagnostic system (MSaf2)

The practice of use of the considered systems [4] shows that the hardware channel with the shown undetected dangerous failures continues to be used. In the course of its use the reveal of other defects which can be detected by the diagnostic system is probable. Respectively, the ICS, after the reveal of an undetected dangerous failure and the subsequent reveal of new failures (the found dangerous failure) can pass into the channel repair state.

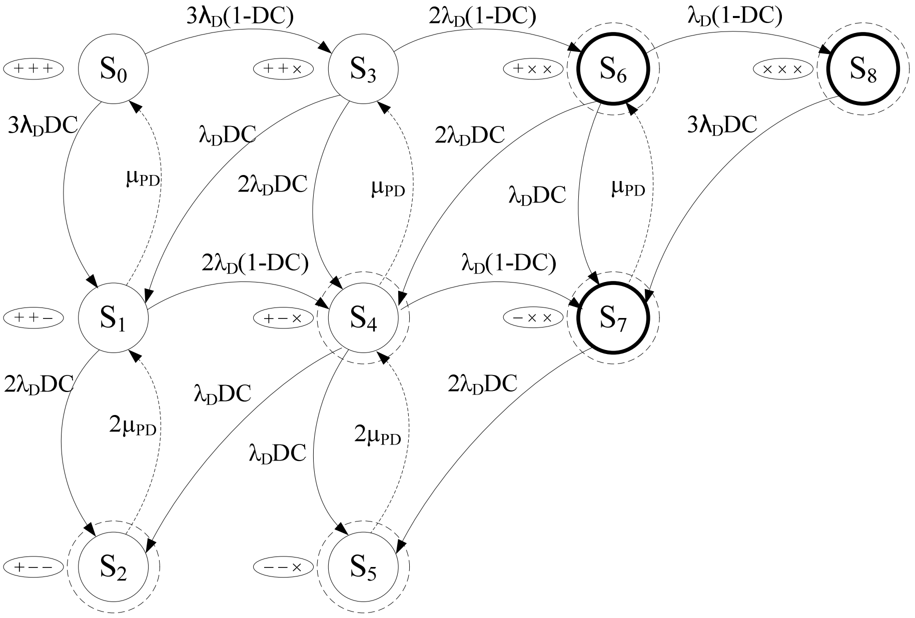


Fig. 4. The marked graph of the ICS RPS operation model without absorbing states (MSaf2)

At the same time, the complete diagnostics of the channel with elimination of all (found and undetected) defects is carried out during the recovery operations.

Also it effects on the duration of reveal duration, and respectively $\mu_{PD}=1/(MRT+T_D)<\mu_P$. Here MRT (Mean Time to Repair) is the average duration of repair of one ICS channel, T_D is an extra time of diagnosing of undetected failures. The marked graph of such model is provided on Fig.4.

The repeated reveal of the found dangerous failures on the graph is illustrated with transitions of $S_8 \rightarrow S_7$, $S_7 \rightarrow S_5$, $S_6 \rightarrow S_4$, $S_4 \rightarrow S_2$. Thus, a graph on Fig.4 doesn't contain the absorbing states.

The safety function PFD_{avg} is defined on (1), also, as well as in the MSaf1 model.

5.3 ICS RPS functional safety model with the majority device, initiating the enhanced diagnostic of the undetected failures (MSaf6)

The marked graph of such model is provided on Fig.5. The system is initially in operation (all three channels are in operation). In a case of the identified failures reveal the system alternatively passes into states of S_1 and S_2, with a possibility of resetting after repair.

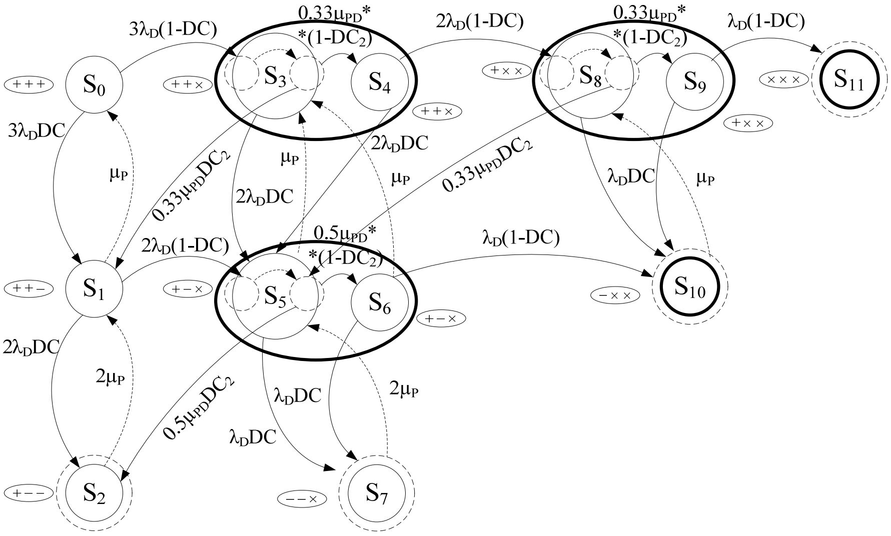


Fig. 5. The marked graph of the model of ICS RPS operation with the enhanced diagnostics on the majority device signal (MSaf6)

In the case of first undetected failure reveal the system passes into S_3 state. Further the majority device informs about the discrepancy of channels operation results, but it is unknown, in what channel is a failure, so the system channels are alternatively passing the enhanced diagnostics with a covering DC2. As a result, the undetected failure either reveals (transition to S_1 state) or does not reveal and the system passes into S_4 state. The duration of the enhanced diagnostics of one channel is equal T_{PD}, thus to check the three channels the transition with intensity $\mu_{PD} = 1/3T_{PD}$ is initiated.

As the initiation of the reinforced diagnostics happens practically right after detection of a discrepancy a majority organ, the state of S_3 is "assembly". It integrates the states of the hidden failure reveal and the beginning of carrying out the reinforced diagnostics. And unlike the previous models, the state of S_3 is non-serviceable (in it the reinforced diagnostics is carried out).

If it wasn't succeeded to find the hidden failure, the system passes into S_4 state (it is operable), from which two transitions are possible: reveal of one more hidden failure (transition to S_8 state), or reveal of the found failure – transition in state S_5.

The S_5 state is characterized by the fact that the system knows about the found failure of one of channels, but the majority organ informs about an undetected failure in one of two remained channels. The enhanced diagnostics of these channels, as a result of which the failure can be found (transition to S_2 state), is launched, or if it is undetected the transition to S_6 state is made.

Similarly the combination of states of S_8 and S_9 is explained.

As in the course of the reinforced diagnostics reveal as found, and undetected failures is possible, reveal of the found failures is modeled by transitions of $S_3 \rightarrow S_5$, $S_4 \rightarrow S_5$, $S_5 \rightarrow S_7$, $S_6 \rightarrow S_7$, $S_8 \rightarrow S_{10}$, $S_9 \rightarrow S_{10}$; reveal of undetected failures is modeled by transitions of $S_4 \rightarrow S_8$, $S_6 \rightarrow S_{10}$, $S_9 \rightarrow S_{11}$.

Thus, the states of S_{10} and S_{11} are most dangerous, as it is impossible to find failures in them neither with the system of diagnostics, nor in a majority organ. An additional periodic prevention of the hidden failures for their detection is necessary. The safety function PFD_{avg} is defined as:

$$PFD_{avg} = 1 - P_0(t) - P_1(t) - P_4(t). \qquad (2)$$

6 Discussion on definition of input parameters values

The values of input parameters were defined as a matter of experience practical operation of the considered class of systems, and also proceeding from the recommendations explained in [3].

As it is required to provide a measure value of the functional safety at the SIL3 level, that is $PFD_{avg} \in\ ]1e\text{-}4 \ldots 1e\text{-}3]$, it is necessary to conduct additional researches of models for the purpose of selection of values of input parameters. Values of input parameters concerning which researches are conducted are considered as basic and are shown in a Table 2.

Table 2. ICS RPS functional safety models input parameters base values

#	Name	Base value	Variation range	Unit
1	$\lambda_D = 0.5*\lambda$	2.5e-5	[0.05 … 5]*1e-5	1/hour
2	$\lambda_{DD} = \lambda_D*DC$	2.25e-5		1/hour
3	$\lambda_{DU} = \lambda_D*(1-DC)$	2.5e-6		1/hour
4	$\mu_P = 1/MRT$	1/8		1/hour
5	$\mu_{PD} = 1/(MRT+T_D)$	1/(8+4)		1/hour
6	DC	0.9 (for MSaf1, MSaf2) 0.5 (for MSaf6)	[0.01…1]	
7	$\mu_{PD*} = 1/(MRT+T_D)$	1/(8+4)=1/12		1/hour
8	DC2=1–(1–DC)/10	0.95	[0.95…1]	

Also the Table 2 demonstrates the options of input parameters λ_{DU} and DC change, and also DC2 for the research of their influence on an function of the functional safety.

7 ICS RPS safety markov models research

To determine the resultant function PFD_{avg} for each graphs, given on Fig.3 – Fig.5, the differential equation system of Kolmogorov-Chapman was generated. Differential equation system solve was executed in the Matlab system by means of the ode15s method for time slot [0 … 500000] hours. The results of this modeling are given in Fig.6.

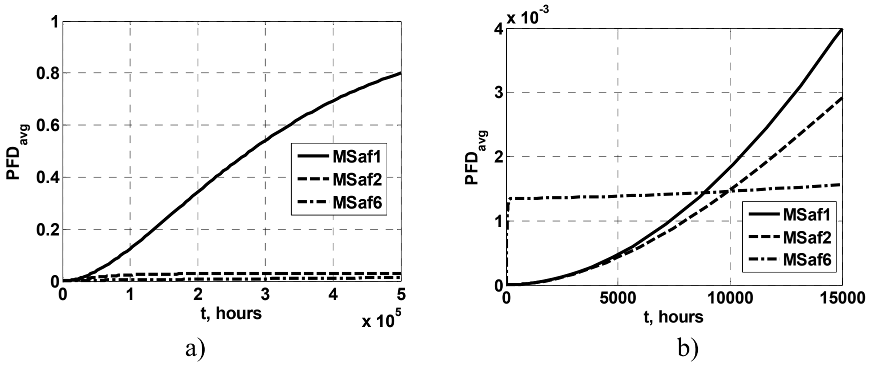


Fig. 6. The dependency of functions PFD_{avg} from the operation time on the interval [0…500000] hours (a) and [0…15000] hours (b)

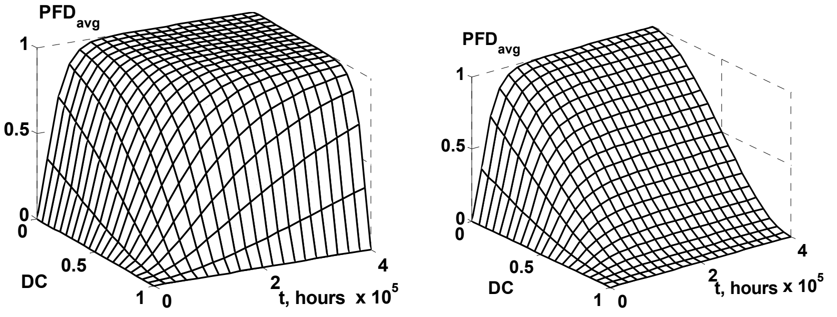
Fig.6 shows that the existence of the absorbing states in the MSaf1 model underlies the continuous growth of function PFD_{avg} to one. On the other hand, the MSaf2 model without the absorbing states illustrates the asymptotic convergence of the functional safety function to stationary of PFD_{avg} value = 0,028 through 16000 working hours. At the same time the SIL3 requirements are provided on time slot till 7200 operation hours (10 operation months) for the MSaf1 model; and on time slot till 8000 operation hours for the MSaf2 model.

At the basic parameter values from the Table 2, the SIL3 requirements in the MSaf6 model aren't satisfied. It is required to define the values of input parameters for this model, in case of which the PFD_{avg} <1e-3 condition will be satisfied.

Fig.7 demonstrates in three-dimensional representation the dependence of the functional safety $PFD_{avg}(t)$ on values of input parameter $DC \in [0 \ldots 1]$ for the MSaf1 and MSaf2 models.

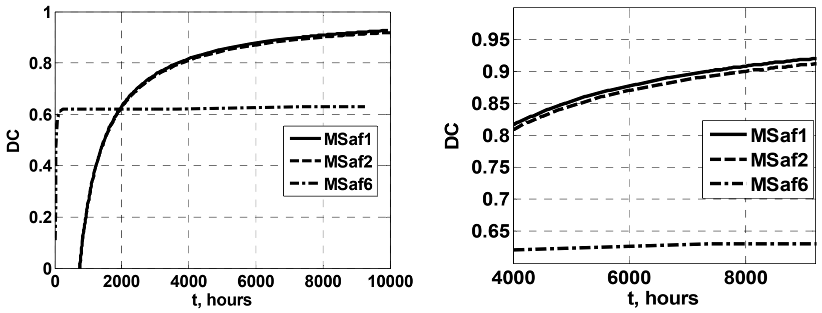
Analyzing the diagrams, it is possible to mark that in the absence of dangerous failures diagnostics (DC = 0), the both models show the identical behavior of the $PFD_{avg}(t)$ function (diagrams match). In the case of detection of all dangerous failures (DC=1) both models show the identical behavior of the $PFD_{avg}(t)$ function, such as the asymptotic convergence to the settled value.

The dynamics of $PFD_{avg}(t)$ functional safety function change shows that value of input parameter of spanning by diagnostics of DC influences duration of the temporal period of execution by system of requirements of SIL3. The diagram of the three-dimensional figure projection to the plane [t, DC] on the level PFD_{avg}=1e-3 (Fig.8) demonstrates such influence [t,DC] in more details. For the best visualization of a graphics are shown in different scales concerning an axis DC. For the MSaf6 model in case of DC=0.64 value execution of requirements of SIL3 on all temporal interval of research is provided.



a) b)

Fig. 7. Function PFD$_{avg}$(t) behavior dependence on the input parameter DC (diagnostic coverage) for MSaf1 (a) and MSaf2 (b)



a) b)

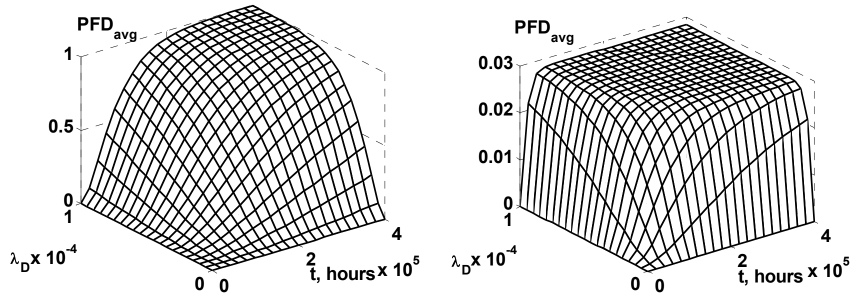
Fig. 8. Projections of function PFD$_{avg}$ on the plane [t,DC] on level PFD$_{avg}$=1e-3 on a scale t∈[0…10000] hours (a) and t∈[4000…10000] hours (b)

Fig.9 represents in three-dimensional representation the functional safety PFD$_{avg}$(t) dependence on the dangerous failures rate value λ_D for the MSaf1 and MSaf2 models.

At first sight, the MSaf2 model (without the absorbing states) illustrates the best result as an function PFD$_{avg}$(t) in it aims to the settled PFD$_{avg}$ value = 0,028 (value is caused by a stable combination of parameters DC = 0.9 and μ_{PD} = 0.0833).

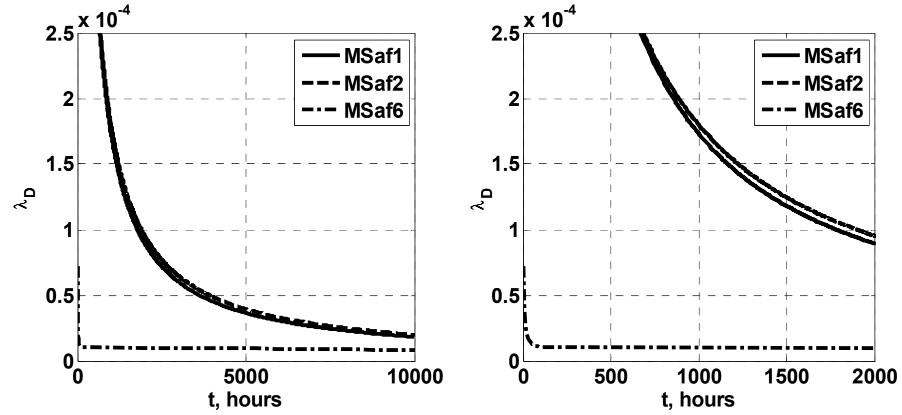
Model MSaf1 illustrates the convergence of function PFD$_{avg}$(t) to 1. And than more the dangerous failures rate is, the approximation of PFD$_{avg}$(t) function to the steady-state mean is faster.

However, if we look at the projection of three-dimensional figures on Fig.9 to the plane [t,λ_D] on the upper cutoff of requirements of SIL-3, then the difference between results of simulation of MSaf1 and MSaf2 doesn't exceed Δt=100 hours in case of λ_D=1e-4 1/hour (Fig.10).



a) b)

Fig. 9. Dependence of PFD$_{avg}$(t) function behavior from the input parameter λ_D for MSaf1 (a) and MSaf2 (b)



a) b)

Fig. 10. Projections of function PFD$_{avg}$ to the plane [t,λ_D] on the PFD$_{avg}$=1e-3 level on the scale of t∈[0…10000] (a) and t∈[0…2000] (b)

For the MSaf6 model for basic values of input parameters (in particular DC=0.5) the requirements of SIL3 are fulfilled in case of λ_D< 1e-5 1/hr.

8 Conclusions

The analysis of ICS functional safety simulation received results showed that:

a) in case of the accounting of secondary manifestation of dangerous failures and detections their diagnostic system (model MSaf2) for base-line values of input parameters reaches the settled PFD$_{avg}$ value = 0.028 that it isn't enough for safety arrangements of the SIL3 level;

b) in case of value of dangerous failures rate λ_D = 2.5e-5 (1/hour) the considered system meets requirements of SIL3 during the first 8000 operation hours; for extension of this period till 10000 hours it is necessary to increase spanning by diagnostics to the DC=0.92 level (models MSaf1 and MSaf2);

c) if it is impossible to increase the spanning by diagnostics, then it is necessary to reduce failure density of each channel to $\lambda = 2^*\lambda_D = 4e\text{-}5$ 1/hour for the extension of the temporal period of SIL3 requirements support till 10000 hours (models MSaf1 and MSaf2);

d) for the system with majority device which initiates additional diagnostics of the hardware channels (model MSaf6) a sufficient condition of support of requirements of SIL3 is the spanning by diagnostics DC>0.65.

The developed Matlab-programs which can be used in engineering practice are a subject of practical interest.

The essential lack of the developed models is the absence of taking note of software failures in ICS channels. The accounting of manifestation of software defects and their elimination during rescue and recovery operations as it is described in [8], is the direction of further researches and improvement of the developed models. Also, further researches and improvement of the developed models is to analyze software features and interactions with hardware failures in instrumentation and control system channels.

References

1. IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements (2010)
2. Sklyar, V.V. Elements of the information and control systems functional safety analysis methodology. Radioelectronic and computer systems 6(40), 75--79 (2009)
3. IEC 61508-6:2010. Functional safety of electrical/electronic/programmable electronic safetyrelated systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (2010)
4. Bahmach, E.S. Siora, A.A. Sklyar, V.V. Tokarev, V.I. Kharchenko, V.S. FPGA-based NPP information and control systems safety accession and provision Radioelectronic and computer systems 7, 75--82 (2007)
5. 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)
6. Al-Kuwaiti, M., Kyriakopoulos, N., Hussein, S.: A comparative analysis of network dependability, fault-tolerance, reliability, safety, and survivability. IEEE Communications Surveys & Tutorials 11(2), 106--124 (2009)
7. Trivedi, K.S., Dong Seong Kim, Roy, A., Medhi, D.: Dependability and safety models. In: Proceedings 7th International Workshop on the Design of Reliable Communication Networks (DRCN 2009), pp. 11-20, IEEE Press, Washington, DC (2009)
8. Ponochovny, Y.L., Siora, A.A., Kharchenko. V.S. Models of dual-channel information management system readiness considering the software updating. Radioelectronic and computer systems 6(70), 135--139 (2014)