Wojciech Zamojski · Jacek Mazurkiewicz ·
Jarosław Sugier · Tomasz Walkowiak ·
Janusz Kacprzyk
Editors

Dependable Computer Systems and Networks

Proceedings of the Eighteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, July 3–7, 2023, Brunów, Poland

Springer

Contents

Line Segmentation of Handwritten Documents Using Direct Tensor Voting 1
Tomasz Babczyński and Roman Ptak

Practical Approach to Introducing Parallelism in Sequential Programs 13
Denny B. Czejdo, Wiktor B. Daszczuk, and Wojciech Grześkowiak

The Digital Twin to Train a Neural Network Detecting Headlamps Failure of Motor Vehicles 29
Aleksander Dawid, Paweł Buchwald, and Bartłomiej Pawlak

Dynamic Change of Tasks in Multiprocessor Scheduling 39
Dariusz Dorota

Regression Models Evaluation of Short-Term Traffic Flow Prediction 51
Paweł Dymora, Mirosław Mazurek, and Maksymilian Jucha

Performance Analysis of a Real-Time Data Warehouse System Implementation Based on Open-Source Technologies 63
Paweł Dymora, Gabriel Lichacz, and Mirosław Mazurek

Hammering Test on a Concrete Wall Using Neural Network 75
Atsushi Ito, Yuma Ito, Jingyuan Yang, Masafumi Koike, and Katsuhiko Hibino

Artificial Intelligence Methods in Email Marketing—A Survey 85
Anna Jach

Detection of Oversized Objects in a Video Stream Using an Image Classification with Deep Neural Networks 95
Przemysław Jamontt, Juliusz Sarna, Jakub Wnuk, Marek Bazan, Krzysztof Halawa, and Tomasz Janiczek

Reliability Model of Bioregenerative Reactor of Life Support System for Deep Space Habitation 105
Igor Kabashkin and Sergey Glukhikh

Safety Assessment of Maintained Control Systems with Cascade Two-Version 2oo3/1oo2 Structures Considering Version Faults 119
Vyacheslav Kharchenko, Yuriy Ponochovnyi, Ievgen Babeshko, Eugene Ruchkov, and Artem Panarin

CPU Signal Rank-Based Disaggregation in Cloud Computing Environments 131
Jakub Kosterna, Krzysztof Pałczyński, and Tomasz Andrysiak

New Approach to Constructive Induction—Towards Deep Discrete Learning 139
Cezary Maszczyk, Dawid Macha, and Marek Sikora

Softcomputing Approach to Music Generation 149
Jacek Mazurkiewicz

Identification of the Language Using Statistical and Neural Approaches 163
Szymon Nagel, Magdalena Nagel, Rozalia Solecka, Julian Szymański, David Gil, and Higinio Mora

Smart Data Logger with Continuous ECG Signal Monitoring 173
Jan Nikodem, Ryszard Klempous, Konrad Kluwak, Dariusz Jagielski, Dorota Zyśko, Bruno Hrymniak, Jerzy Rozenblit, Thomas A. Zelniker, and Andrzej Wytyczak-Partyka

Movement Tracking in Augmented and Mixed Realities Impacting the User Activity in Medicine and Healthcare 183
Jan Nikodem, Ryszard Klempous, Jakub Segen, Marek Kulbacki, and Artur Bąk

General Provisioning Strategy for Local Specialized Cloud Computing Environments 193
Piotr Orzechowski and Henryk Krawczyk

Tabular Structures Detection on Scanned VAT Invoices 207
Paweł Pawłowski, Marek Bazan, Maciej Pawełczyk, and Maciej E. Marchwiany

Automation of Deanonymization Queries for the Bitcoin Investigations 223
Przemysław Rodwald and Nicola Kołakowska

Structural Models for Fault Detection of Moore Finite State Machines 231
Valery Salauyou

Safety Assessment of Maintained Control Systems with Cascade Two-Version 2oo3/1oo2 Structures Considering Version Faults

Vyacheslav Kharchenko, Yuriy Ponochovnyi, Ievgen Babeshko, Eugene Ruchkov, and Artem Panarin

1 Introduction

At present a whole class of devices, hardware and software components important from the functional safety point of view involves the adoption of dedicated information and control systems. As a basis of such systems FPGAs and microprocessor platforms are utilized for critical domains [1]. An example is the RadICS modular platform [2] which is used to build fault-tolerant FPGA architectures meeting strict dependability, reliability and functional safety requirements nuclear international standards and normative documents [3, 4]. This necessitates the development of adequate and complete models for evaluating the parameters of reactor trip systems in nuclear field both at the design stage and during their operation.

Currently, various classes of such models are being developed and used: set-theoretic [5], Bayesian [6], FTA [7], Markov [8], semi-Markov [9], FMECA [10] and its modifications [11] and combinations [12]. The use of such models is advised by industry standards for electronic and programmable components and platforms from IEC 61508 series [13]. However, the scenarios of failures of hardware (HW) and software (SW) channels of redundant and diverse systems are constantly expanding, as new threats associated with malicious interference in the operation of these systems,

V. Kharchenko · I. Babeshko (✉)
National Aerospace University KhAI, Kharkiv, Ukraine
e-mail: e.babeshko@csn.khai.edu

V. Kharchenko
e-mail: v.kharchenko@csn.khai.edu

Y. Ponochovnyi
Poltava State Agrarian University, Poltava, Ukraine

E. Ruchkov · A. Panarin
Research and Production Company Radiy, Kropyvnytskyi, Ukraine
e-mail: rev@radiy.com

W. Zamojski et al. (eds.), *Dependable Computer Systems and Networks*, Lecture Notes in Networks and Systems 737, https://doi.org/10.1007/978-3-031-37720-4_11

the threat of hostilities, sabotage and cyberattacks appear [14]. In addition, when evaluating a traditional two-version system [5, 7], it is often assumed that the diagnostic and supervision means for both subsystems have perfect reliability.

The development of the Industry 4.0 concept and the application of Industrial IoT technologies lead to an increase in the requirements for the level of safety integrity SIL2-SIL3 [15]. All these factors determine the need to develop an adequate, complete model that will allow determining the resulting indicator with a high level of accuracy.

This work presents a macro model of operation for information and control system such as NPP RTS accommodating various failure types, in particular, faults of diagnostic and supervision means in both (main and diverse) subsystems. The paper continues investigating the microprocessor and FPGA based ICSs outlined in [16–18].

The object of the study is the process of ICS operation under conditions of failures caused not only by hardware and software version anomalies, faults of the diagnostic and supervision means and separated recovery of the ICS components.

The structure of the work is as follows: Sect. 2 provides reliability block diagram of RTS ICS, as well as discusses the main directions of expanding its state space. In Sect. 3, a macro model of the ICS operation and its separate part (sub-model) is built, which describes the manifestation of absolute faults of software versions. Analysis of modelling results has been the objective of Sect. 4. Finally, in Sect. 5 we summarize findings, provide guidance on usage of developed models and discuss the future work.

2 Block Diagram and Failure Model of Two-Version ICS

The ICS reliability block diagram presented in Fig. 1 is a modified 1oo2 redundant architecture, in which each channel has additional 2oo3 redundancy and built-in diagnostic and supervision means. Subsystems (main and diverse RTS subsystems) generate one-bit signals with priority for the shutdown signal. If the output channels retain identical states due to version errors (main and diverse software subsystems), their detection relies on built-in diagnostic means. Such redundant architecture contains a certain margin of reliability, which allows it to adequately withstand failures.

Using the RadICS platform provides a modular implementation of RTS [2]. This allows using the central diagnostic module (D) and means built into other modules to check the functionality of the signals from these modules. The output signal comparison module (module «≠») additionally increases reliability and safety, but at the same time it expands the space of diagnostic states, as well as general ICS state space.

Figure 2 illustrates directions of system state space.

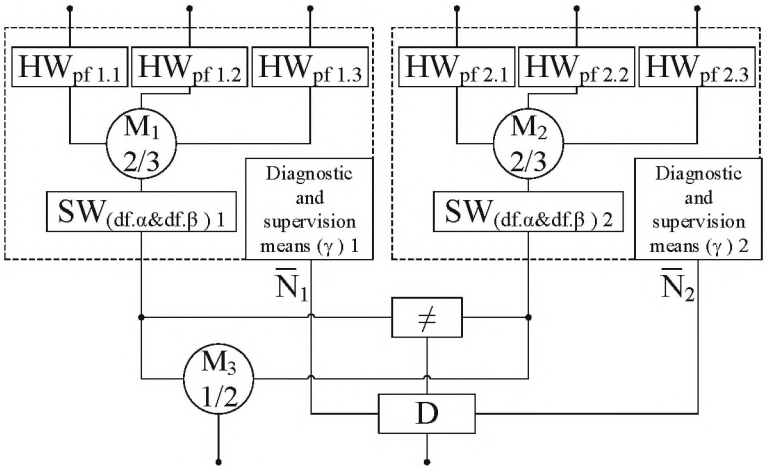

Fig. 1 ICS block diagram for modelling manifestation of physical faults (pf), design faults (df; absolute β and relative α) and faults of diagnostic and supervision means (γ)

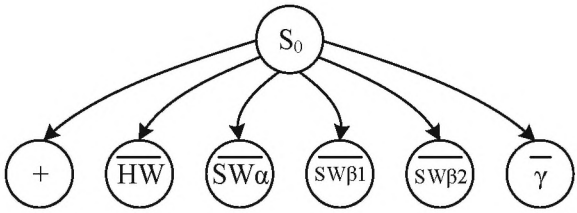

Fig. 2 Graph of RTS ICS states

The first transition illustrates operable space. The remaining 5 transitions describe the inoperable states caused by following failures: HW channels, SW versions (α—relative and β—absolute faults); γ for diagnostic and supervision means.

The generalized model of faults and failures was described in detail in the [16]. Recall that the related software design faults (α) are manifested separately in each version of the software, the model of their manifestation is described in the previous studies [16, 17] as well. Absolute faults appear simultaneously in both versions of software, the following details are introduced in the study: β1—absolute faults that cause different values of the output signal, β2—the most dangerous faults that cause the same values of the output signal and are not detected by the comparison system. The model of the manifestation of absolute faults will be investigated in this work.

3 Models of Two-Version ICS Availability Accommodating Failures of Supervision Means and Various Version Faults

3.1 Macro Model for Availability Assessment

As a basis of macro model a multi-fragmentation principle was used, which is described in [12]. This principle lies in usage of individual blocks (model fragments) where system operates in stationary flow of events context. Only in case of transitions between fragments failure rates could change according to given distribution laws.

The following are the main assumptions that were used to build the macro model of the RTS ICS operation:

- the flow of events, which causes the transition of the system from one operable state to another within one fragment, has the properties of stationarity, ordinariness and the absence of an aftereffect, the parameters of the model within one fragment are considered constant;
- when eliminating identified software faults, new faults are not introduced;
- after the elimination of the relative software fault, the software failure rate in model fragment is set as $\lambda_{\alpha\, i+1}$ and is defined as follows:

$$\lambda_{\alpha\, i+1} = \lambda_{\alpha\, i} - \Delta\lambda_{\alpha} \tag{1}$$

- after the elimination of the absolute software fault, the software failure rate in model fragment is set as $\lambda_{\beta\, i+1}$ and is defined as follows:

$$\lambda_{\beta\, i+1} = \lambda_{\beta\, i} - \Delta\lambda_{\beta} \tag{2}$$

The macro model is presented in Fig. 3 as a collection of fragments. When building the model, the design features of the ICS were taken into account, namely the use of the same hardware in both diverse channels (the hardware in each channel is characterized by the reliability parameters λp and μp).

Macro graph shown in Fig. 3 includes:

- 24 basic fragments (total 24*11 = 264 states);
- 24 transitions that model manifestation and elimination of relative DD (24*10 = 240 states);
- 23 transitions that model manifestation and elimination of absolute DD (23*5 = 115 states);

i.e., in total, a complete directed graph should include 619 states.

The built macro model simulates the operation of the system with two relative design faults that appear separately in each software version (their manifestation is illustrated by the transitions of green color); and one design fault appearing in both versions of the software at the same time (illustrated by red transitions in Fig. 3).

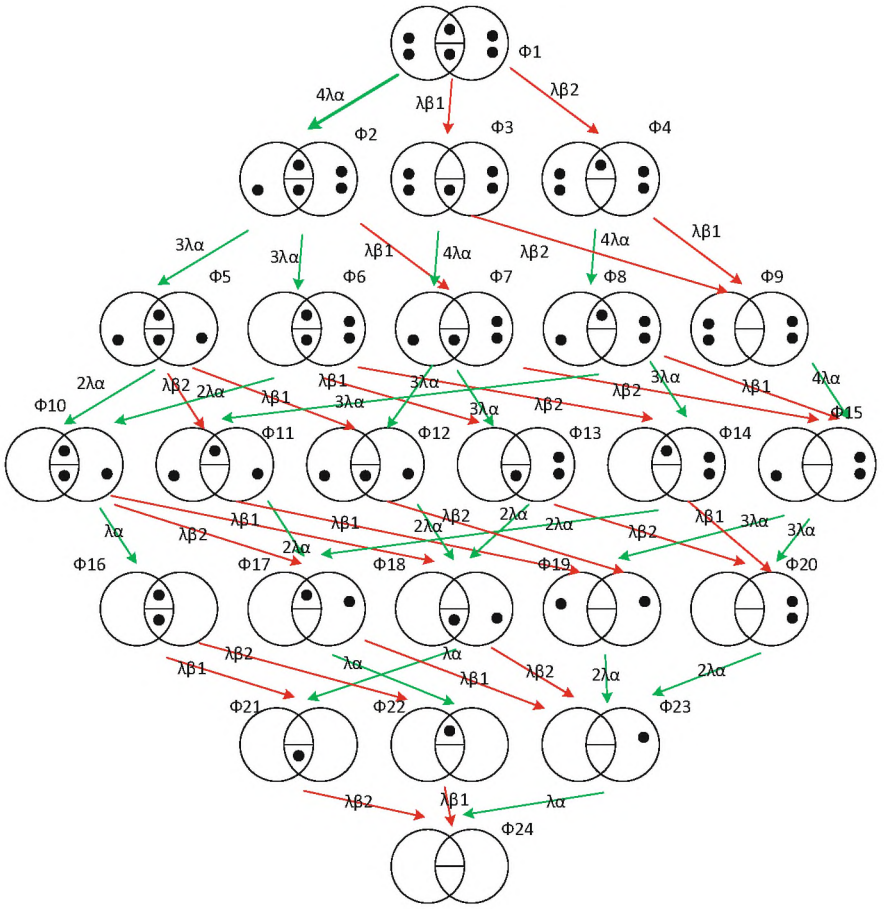

Fig. 3 Macro graph describing ICS operation with two version software configuration {nα1 = 2, nα2 = 2, nβ1 = 1, nβ2 = 1}

To build a complete directed graph of the model, automation tools of the Matlab environment and the grPlot library [19] were used.

We emphasize that working with models of this size is significantly complicated and requires consolidation of individual blocks and detailing of the system operation within individual fragments. A detailed description of software version relative faults manifestation processes of supervision means was carried out in [12]. Therefore, only the model of manifestation of absolute software versions is considered further.

3.2 *Multi-fragmental Markov Availability Model*

Manifestation of absolute software faults detected by diagnostics and supervision means leads the system to a safe failure state. After detecting such a fault, measures are taken to localize and eliminate it, which causes a change in the failure rate parameter $\lambda\beta$. In the model, such events are described using the mathematical apparatus of multi-fragment modeling [17, 19].

Given the design features of the ICS, the following assumption is made: the reliability parameters of different types of absolute software faults are not equal ($\lambda\beta 1 \neq \lambda\beta 2$, $\mu\beta 1 \neq \mu\beta 2$). Figure 4 shows transitions between two fragments that arose as a result of the manifestation and elimination of one absolute design fault, which is simultaneously manifested in both versions of the software.

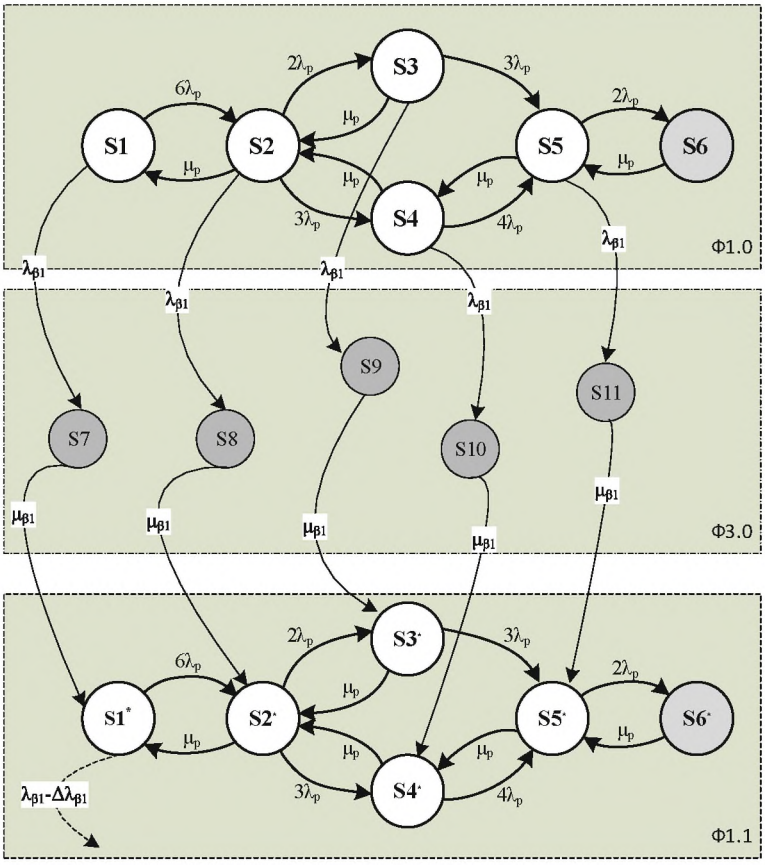

Fig. 4 Two-fragment directed graph that models manifestation of absolute design fault by transitions between fragments

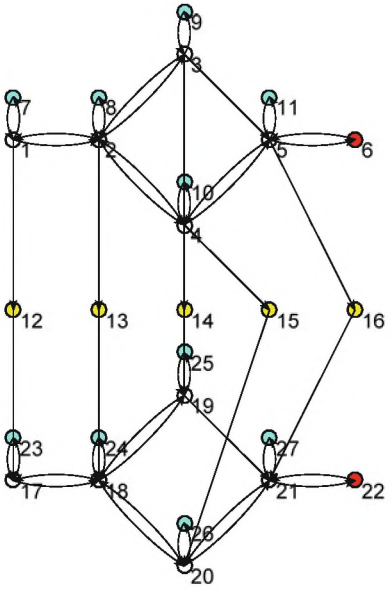

Fig. 5 Directed graph of model with fragments resulting from relative design fault in one of software versions

When constructing the directed graph in Fig. 5, the following color marking is used: white color is used to represent operational states, red color is used for safe failure states caused by hardware channel failures, blue color is used for safe failure states caused by control system failures. The yellow color is used to indicate safe failure states caused by the manifestation of absolute faults in the design of software versions.

The availability function for the directed graph in Fig. 5 is defined as (3):

$$A(t) = \sum_{i=1}^{5} P_i(t) + \sum_{i=17}^{21} P_i(t) \tag{3}$$

Basic conditions are the following: $t = 0$, $P_1(0) = 1$, $P_2(0) \ldots P_{27}(0) = 0$.

4 Modelling and Analysis of Results

The primary input parameters of the Markov models were determined based on the data of certification tests an operation experience for similar systems [12, 16, 18] for the previous samples of the versions of the RTS ICS. Their values are presented in Table 1.

To construct the matrix of Kolmogorov-Chapman differential equation system (DES) in Matlab, the matrixA function [15] was used. DES can be solved using analytical methods (substitution, Laplace transform, etc.). This approach can be

Table 1 Values of input parameters used for modelling

#	Symbol	Description	Value
1	λp	HW failure rate due to physical faults (PD)	1e−4 (1/h)
2	λα	SW failure rate due to relative design faults (DD)	5e−4 (1/h)
3	λγ	Failure rate of supervision means	1e−6 (1/h)
4	μp	HW recovery rate	1 (1/h)
5	μα	SW recovery rate	2 (1/h)
6	μγ	Supervision means recovery rate	0.25 (1/h)
7	Δλα	Change of SW failure rate after elimination of relative fault	1.25e−4 (1/h)
8	Nα	Expected number of relative design faults	4
9	λβ1	SW failure rate due to absolute design faults that cause different signals	1e−6 (1/h)
10	μβ1	SW recovery rate	0.0667 (1/h)
11	Nβ1	Expected number of absolute design faults of the first type	1
12	λβ2	SW failure rate due to absolute design faults that cause different signals	2e−6 (1/h)
13	μβ2	SW recovery rate	0.0714 (1/h)
14	Nβ2	Expected number of absolute design faults of the second type	1

applied to ICSs of small dimensions. In this work, a large-dimensional macro model (619 states) is considered, therefore, a universal approach to the numerical solution of the DES was chosen using the ode15s function [12, 20]. The simulation results are shown in Fig. 6.

To assess the impact of different types of (absolute and relative) design faults on the availability function, separate models were built for each of the indicated fault type. The input parameters of the simplified models are identical to the parameters of the macro model in Fig. 4. The results are presented as graphs of different colors in Fig. 7.

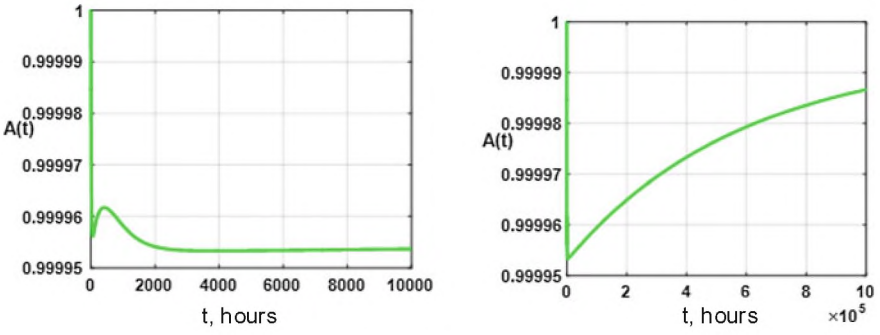

Fig. 6 ICS availability modelling results with the extension of time base to 10,000 h (**a**) and to 100,000 h (**b**)

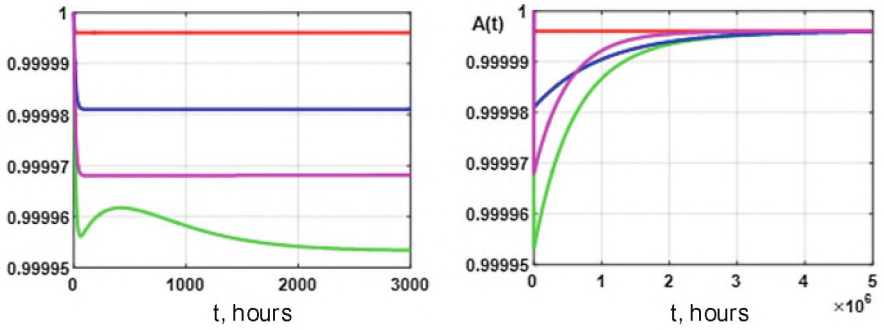

Fig. 7 ICS availability modelling results with the extension of time base to 3000 h (**a**) and to 500,000 h (**b**)

The graphs in Fig. 7 marked as the follows:

- for the model that accommodates the manifestation of HW physical faults, the failure of supervision means and the manifestation of relative SW design faults (red),
- for the model that accommodates the manifestation of SW design faults according to the beta1 parameter (blue),
- for the model that accommodates the manifestation of SW design faults according to the beta2 parameter (purple) and the general macro model (green).

The graphs of the ICS model (Figs. 6 and 7) illustrate the typical nature of the change in the availability function when it is reduced to the stationary coefficient $A = 0.9999955$ during the first 30 h of operation. During the next 2000 h, an improvement in system availability is observed due to the elimination of relative (α) software faults. Further, the availability of the system continues to increase, this is due to the elimination of absolute (β) software faults.

5 Conclusion

The paper provides results of development and research of two-version safety system models with cascade 2oo3-1oo2 redundancy, which take into account the reliability of the operation of supervision means. The structure of the system with self-diagnosis functions is presented, which consists of a subsystem of supervision means, means of cross-channel comparison and analysis. Such a structure makes it possible not only to detect failure states of individual channels, but also to ensure verification of supervision means and reduce the risk of dangerous and undetected failures.

The construction of Markov models describing the manifestation of physical and design faults and failures of diagnostic and supervision means was carried out in stages. To model behavior of the system considering the failures of individual versions

and the elimination of design faults, a multi-fragment macro model was proposed and discussed. Its main feature is a detailed analysis of the combination of faults described by the inter-fragmental part of the model.

Accommodating the failures of supervision means, the manifestation of three types of faults, it is possible to increase the accuracy of the assessment of the availability factor at the initial stage of system operation by $\Delta A = 4e{-}6$. This is important considering the high requirements for the RTS ICS functional safety (more than 0.99999). At the same time, the influence of relative software faults on the overall availability of the entire system remains within $\Delta A = 2e{-}8$ in the interval [0…2000] h due to the two-version structure. However, the overlap of absolute version faults and diagnostic failures is more critical and is eliminated only after 30 000 h of operation time.

Further research should be devoted to the development of analytical models of availability and functional safety designed to assess the impact of possible attacks on the system [14, 21]. In case of cyberattacks or any intrusions, the results of the vulnerability analysis should be taken into account in such a way to parameterize and replan the Markov model or to implement a combined assessment methodology [12].

References

1. Yastrebenetsky, M., Kharchenko, V. (eds.): Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control, p. 501. IGI-Global, PA, USA (2020). https://doi.org/10.4018/978-1-7998-3277-5
2. FPGA-Based Safety Controller (FSC) RadICS. Results of the IEC 61508 Functional Safety Assessment. V4R3, p. 26 (2020). https://www.exida.com/SAEL-Safety/rpc-radiy-fpga-based-safety-controller-fsc-radics
3. Guidance on using IEC 61508 SIL certification to support the acceptance of commercial grade digital equipment for nuclear safety related applications. Revision 1 (2011). https://www.nrc.gov/docs/ML2133/ML21337A380.pdf
4. IEC 61511-1:2016. Functional safety—safety instrumented systems for the process industry sector—part 1: framework, definitions, system, hardware and application programming requirements (2016). https://webstore.iec.ch/publication/24241
5. IAEA Safety Standards Series No. SSG-2 (Rev. 1). Deterministic safety analysis for NPPs (2019). https://www-pub.iaea.org/MTCD/publications/PDF/PUB1851_web.pdf
6. Zhao, X., Wang, X., Golay, M.W.: Bayesian network–based fault diagnostic system for nuclear power plant assets. Nucl. Technol. **209**(3), 401–418 (2023). https://doi.org/10.1080/00295450.2022.2142445
7. Kim, J.S., Han, S.H., Kim, M.C.: Direct fault-tree modeling of human failure event dependency in probabilistic safety assessment. Nucl. Eng. Technol. **55**(1), 119–130 (2023). https://doi.org/10.1016/j.net.2022.08.029
8. Liang, Q., Yang, Y., Zhang, H., Peng, C., Lu, J.: Analysis of simplification in Markov state-based models for reliability assessment of complex safety systems. Reliab. Eng. Syst. Saf. **221**, 108373 (2022). https://doi.org/10.1016/j.ress.2022.108373
9. Liang, Q., Peng, C., Li, X.: A multi-state semi-Markov model for nuclear power plants piping systems subject to fatigue damage and random shocks under dynamic environments. Int. J. Fatigue **168**, 107448 (2023). https://doi.org/10.1016/j.ijfatigue.2022.107448

10. Lo, H.-W., Liou, J.J., Yang, J.-J., Huang, C.-N., Lu, Y.-H.: An extended FMEA model for exploring the potential failure modes: a case study of a steam turbine for a nuclear power plant. Complexity **2021**, 1–13 (2021). https://doi.org/10.1155/2021/5766855
11. Babeshko, I., Illiashenko, O., Kharchenko, V., Leontiev, K.: Towards trustworthy safety assessment by providing expert and tool-based XMECA techniques. Mathematics **10**, 2297 (2022). https://doi.org/10.3390/math10132297
12. Kharchenko, V., Ponochovnyi, Y., Ivanchenko, O., Fesenko, H., Illiashenko, O.: Combining Markov and semi-Markov modelling for assessing availability and cybersecurity of cloud and IoT. Cryptography **6** (2022). https://doi.org/10.3390/cryptography6030044
13. IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems (2010). https://www.iec.ch/functional-safety
14. Pickering, S.Y., Davies, P.B.: Cyber security of nuclear power plants: US and global perspectives (2021). https://gjia.georgetown.edu/2021/01/22/cyber-security-of-nuclear-power-plants-us-and-global-perspectives
15. Gomes, F.C., de Andrade, A.A., Gasi, F.: Instrumentation and control systems applied to high-risk operating technologies: paving the way to the industry 4.0 at nuclear power plants. In: 2021 14th IEEE International Conference on Industry Applications (INDUSCON) (2021). https://doi.org/10.1109/induscon51756.2021.9529836
16. Kharchenko, V., Ponochovnyi, Y., Ruchkov, E., Babeshko, E.: Safety assessment of the two-cascade redundant information and control systems considering faults of versions and supervision means. In: New Advances in Dependability of Networks and Systems, pp. 88–98 (2022). https://doi.org/10.1007/978-3-031-06746-4_9
17. Kharchenko, V., Butenko, V., Odarushchenko, O., Sklyar, V.: Multifragmentation Markov modeling of a reactor trip system. J. Nucl. Eng. Radiat. Sci. **1**, (2015). https://doi.org/10.1115/1.4029342
18. Babeshko, E., Kharchenko, V., Leoniev, K., Ruchkov, E.: Practical aspects of operating and analytical reliability assessment of FPGA-based I&C systems. Radioelectron. Comput. Syst. **3**(95), (2020). https://doi.org/10.32620/reks.2020.3.08
19. Iglin, S.: grTheory—graph theory toolbox (2023). https://www.mathworks.com/matlabcentral/fileexchange/4266-grtheory-graph-theory-toolbox
20. Solve stiff differential equations and DAEs—variable order method—MATLAB ode15s (2023). https://www.mathworks.com/help/matlab/ref/ode15s.html
21. Lysenko, S., Kharchenko, V., Bobrovnikova, K., Shchuka, R.: Computer systems resilience in the presence of cyber threats: taxonomy and ontology. Radioelectron. Comput. Syst. **1**, 17–28 (2020). https://doi.org/10.32620/reks.2020.1.02