

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

New Advances in Dependability of Networks and Systems

Proceedings of the Seventeenth
International Conference on
Dependability of Computer Systems
DepCoS-RELCOMEX, June 27 – July 1, 2022,
Wrocław, Poland

Contents

Robustness on Diverse Data Disturbance Levels of Tabu Search for a Single Machine Scheduling	1
Wojciech Bożejko, Paweł Rajba, and Mieczysław Wodecki	
Using Evolutionary Algorithm in On-line Deployment	11
Wiktor B. Daszczuk, Rafał Biedrzycki, and Piotr Wilkin	
Measures of Outlierness in High-Dimensional Data Under Correlation of Features – With Application for Open-Set Classification	22
Szymon Datko, Henryk Maciejewski, and Tomasz Walkowiak	
Performance of Modern Video Codecs in Real-Time Communication WebRTC Protocol	32
Aleksander Dawid and Paweł Buchwald	
Improved Software Reliability Through Failure Diagnosis Based on Clues from Test and Production Logs	42
Wojciech Dobrowolski, Maciej Nikodem, Marek Zawistowski, and Olgierd Unold	
Multiprocessor Tasks Scheduling. Fuzzy Logic Approach	50
Dariusz Dorota	
Anomaly Detection Techniques for Different DDoS Attack Types	63
Mateusz Gniewkowski, Henryk Maciejewski, and Tomasz Surmacz	
Nonparametric Tracking for Time-Varying Nonlinearities Using the Kernel Method	79
Purva Joshi and Grzegorz Mzyk	

Safety Assessment of the Two-Cascade Redundant Information and Control Systems Considering Faults of Versions and Supervision Means	88
Vyacheslav Kharchenko, Yuriy Ponochovnyi, Eugene Ruchkov, and Eugene Babeshko	
Network Anomaly Detection Based on Sparse Representation and Incoherent Dictionary Learning	99
Tomasz Kierul, Tomasz Andrysiak, and Michał Kierul	
UAV Fleet with Battery Recharging for NPP Monitoring: Queuing System and Routing Based Reliability Models	109
Ihor Kliushnikov, Vyacheslav Kharchenko, Herman Fesenko, Kostiantyn Leontiev, and Oleg Illiashenko	
Android Mobile Device as a 6DoF Motion Controller for Virtual Reality Applications	120
Maciej Kopczynski	
Performance Analysis and Comparison of Acceleration Methods in JavaScript Environments Based on Simplified Standard Hough Transform Algorithm	131
Damian Koper and Marek Woda	
Clustering Algorithms for Efficient Neighbourhood Identification in Session-Based Recommender Systems	143
Urszula Kuźelewska	
Reliability- and Availability-Aware Mapping of Service Function Chains in Softwarized 5G Networks	153
Jerzy Martyna	
Softcomputing Approach to Virus Diseases Classification Based on CXR Lung Imaging	163
Jacek Mazurkiewicz and Kamil Nawrot	
Single and Series of Multi-valued Decision Diagrams in Representation of Structure Function	176
Michał Mrena, Miroslav Kvassay, and Stanisław Czapp	
Neural Network Models for the Prediction of Time Series Representing Water Consumption: A Comparative Study	186
Krzysztof Pałczyński, Tomasz Andrysiak, Magda Czyżewska, Michał Kierul, and Tomasz Kierul	
Embedded Systems' Startup Code Optimization	197
Patrik Pankiewicz	
Labeling Quality Problem for Large-Scale Image Recognition	206
Agnieszka Pilch and Henryk Maciejewski	



Safety Assessment of the Two-Cascade Redundant Information and Control Systems Considering Faults of Versions and Supervision Means

Vyacheslav Kharchenko¹ , Yuriy Ponochovnyi² , Eugene Ruchkov³ ,
and Eugene Babeshko¹

¹ National Aerospace University KhAI, Kharkiv, Ukraine
{v.kharchenko, e.babeshko}@csn.khai.edu

² Poltava State Agrarian Academy, Poltava, Ukraine

³ Research and Production Company Radiy, Kropyvnytskyi, Ukraine
rev@radiy.com

Abstract. This paper studies functional safety and availability models of information and control system (ICS) with two-cascade 2oo3/1oo2 redundancy. First cascade has a two-version structure which is conventional for reactor trip systems. The structure being studied includes supervision means for each subsystem of the first redundancy cascade, as well as means for their outputs comparison. A peculiarity of developed models is that they consider failures of supervision means along with failures caused by different (single and multiple) faults of software and hardware versions of main and diverse subsystems. Markov models describe behavior of repairable system considering failures caused by physical faults of channels and version design fault supervision, detection and elimination means. During analysis of models the peculiarities of FPGA-based RadICS platform used for ICSs of nuclear power plants (NPPs) and other safety critical systems development were considered.

Keywords: Information and control system · Safety assessment · Availability function · Markov model · Two-cascade redundant structure

1 Introduction

Safety-related industrial information and control systems are being developed using CPU and FPGA-based platforms. Application of such system, in particular reactor trip systems (RTS), in nuclear power engineering is regulated by international standards and normative documents [1, 2]. IEC 61508-6 [3] provides a number of mathematical models and methods for safety assessment of NPP ICS based on electronic and programmable components and platforms [4]. The most safety critical systems have structure involving two (main and diverse) subsystems that implement three-channel 2oo3 voting. These subsystems are built using different software (SW) and hardware (HW) implementations, platform solutions and settings, and must conform to SIL3 safety integrity level

requirements [5]. Such ICSs designated as multi-version systems are covered in [6–10] where metric based techniques of diversity are suggested [6, 7], Bayesian [8] and Markov's [9, 10] models of NPP reactor trip system (RTS) are developed and studied.

Different scenario of ICS channels and subsystems failures, including failures caused by insider interventions and cyber attacks, necessitate particular emphasis placed on development process of adequate and complete safety and availability models. Despite extensive protective measures of NPP ICS, their isolation from environment and external information systems, cases of intervention into operation of such critical systems must not be ruled out [11]. Internet of Things technologies application in the industrial systems, advancement of Industry 4.0 concept [12, 13] are attended with rise of new threats and vulnerabilities that could be exploited for attacks [14, 15]. This fact motivates not only incorporation of through supervision and protection of systems, but their operation test as well.

In this work we present NPP ICS operation model with consideration for failures of supervision means in either (main and diverse) subsystem. These means are constituents of diagnostics module described in [16].

The object is the research of ICS operation during failure occurrence conditions, caused not only by software and hardware faults, but by supervision means failures as well. To accomplish this, extended failure model with consideration for their different combinations is being developed.

The rest of paper is organized as follows: Sect. 2 is dedicated to the description of enhanced system structure with embedded subsystems and channels supervision means, set of states with consideration for failure combinations; systems availability Markov models are proposed and studied in Sect. 3, as well as values of simulation input parameters are justified. 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 The Structure and Faults Model of the Two-Cascade Redundant ICS

2.1 The Two-Cascade Redundant Structure

The structure of two-version NPP ICS with embedded supervision means is shown in Fig. 1. This structure is modified in reference to one described in [17] through the use of cascade 2oo3 and 1oo2 redundancy. It allows eliminating hardware failures by majority voting at the first cascade, as well as tolerating version design faults (of main and diverse subsystems) by using 1oo2 version redundancy at the second cascade. The 1oo2 voting is made possible by the fact that subsystems generate single-bit signals with the priority for reactor trip signal. Utilization of supervision means admits detection of version faults in cases when the output channels retain identical states.

Such redundant architecture incorporates reasonable reliability margin allowing to withstand failures adequately. When assessing traditional two-version system [9, 10] it is often admitted that supervision means for both subsystems have the perfect reliability.

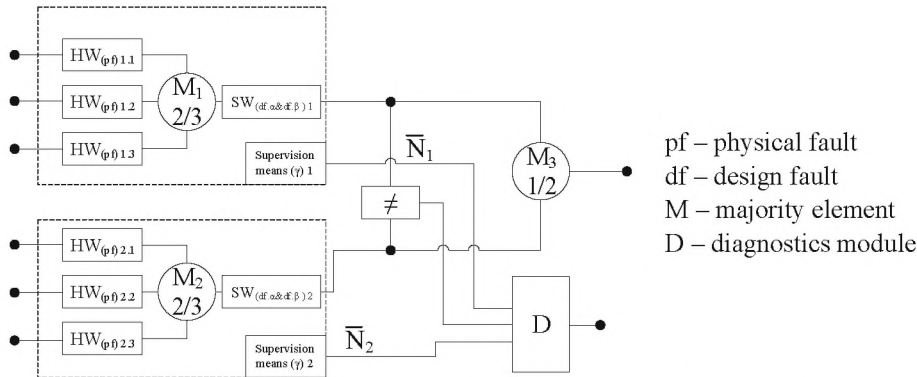


Fig. 1. RTS structure chart to consider physical faults (pf), design faults (df) and supervision system faults

Modular implementation of the system (for example, using RadICS platform [4, 5]) makes it possible to utilize individual modules of supervision system for either of diverse channels and supervise operability signals from these modules by means of diagnostics module D. Doing so along with an additional module of output signals comparison (module «≠») allows to extend space of diagnostic states. Application of additional signals requires extension of ICS state space.

2.2 The Faults Model

Figure 2 depicts space state that considers failures of software versions as well as supervision systems failures of first and second diverse channels. To reduce dimension, hardware failures state sets studied in [16] are not shown in Fig. 2.

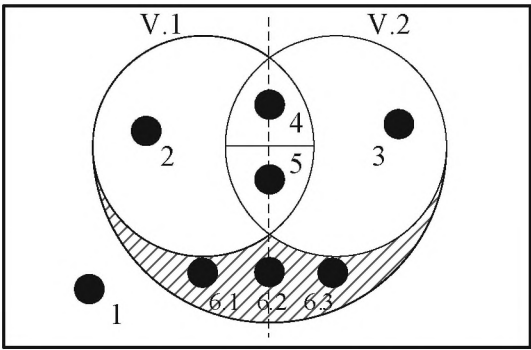


Fig. 2. Generation of RTS ICS failures intersection

Table 1 provides signals combinations that generate ICS failure space with consideration of software version failures and supervision system failures.

Table 1. Signal states at the diagnostics module input and ICS operability

Nº	State	Notation	Parameter	State of $\neq$ signal	State of N1 signal	State of N2 signal	General ICS operability	Number of operative versions
1	Operative state	S_0	–	0	0	0	1	2
2	Failure of main (first) version/system	S_1	$\alpha 1$	1	1	0	1	1
3	Failure of diverse (second) version/system	S_2	$\alpha 2$	1	0	1	1	1
4	Failure of both versions/systems with coincidence of output results	S_3	$\beta 1$	0	1	1	0	0
5	Failure of both versions/systems with different output results	S_4	$\beta 2$	1	1	1	0	0
6.1	Supervision means failure	S_K	γ	0/1	1	1	0	–
6.2	Supervision means failure	S_K	γ	0	1	0	0	–
6.3	Supervision means failure	S_K	γ	0	0	1	0	–

Two-version and two-cascade redundant structure with subsystems supervision is shown in Fig. 1. Supervision means from either subsystem generate operability signal. Generally they are designed in the similar way and have resembling hardware implementation, hence their reliability (γ parameter) could be treated as identical.

In this work we will not concern ourselves with situation related to operative state display error at the output of supervision means ($N1 = 0, N2 = 0$). When a failure occurs in either of supervision modules, system state should be changed to the safe failed state. Therefore, three states denoted as 6.1, 6.2 and 6.3 could be treated as one safe failed state so as to decrease the dimension.

3 Markov's Availability Model of Two-Cascade Redundant ICS Considering Faults of Supervision Means

3.1 The Model of Two-Cascade Redundant ICS Considering Faults of Supervision Means and Hardware Faults of Channels

Elements of base Markov model described as marked graphs are shown in Fig. 3. During model construction ICS design features were taken into consideration, namely, utilization of identical hardware in both diverse channels (hardware in every channel is characterized by reliability parameters λ_p and μ_p). In such a manner Markov model presented in Fig. 3a was obtained with operative states S1-S5 and safe failed state S6. The peculiarities of such models development are described in [16, 17]. To consider supervision systems failures this model has been modified (Fig. 3b).

The main point of modification shown in Fig. 3 lies in the fact that every operative state obtains corresponding inoperative state such that supervision system failure occurred with failure rate λ_γ (states S7...S11). After recovery of supervision means to the operative state with the rate μ_γ , system goes back to the corresponding operative state.

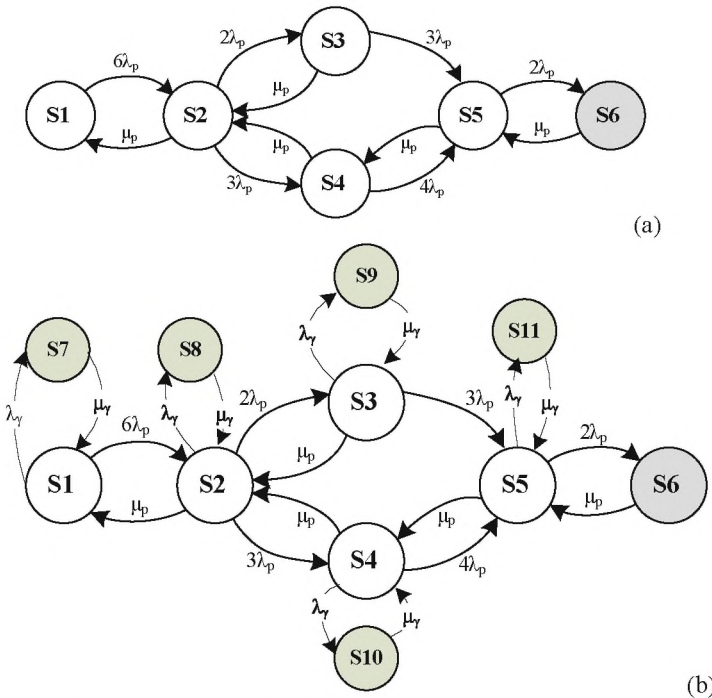


Fig. 3. Orgraph of RTS ICS base model fragment with consideration of design faults (a) and its modification for taking into account supervision means failures and recovery (b)

The availability function for orgraph presented in Fig. 3b is defined as (1):

$$A(t) = \sum_{i=1}^5 P_i(t). \quad (1)$$

Baseline conditions are the following: $t = 0$, $P_1(0) = 1$, $P_2(0) \dots P_{11}(0) = 0$.

3.2 The Model of Two-Cascade Redundant ICS Considering Hardware and Software Faults and Faults of Supervision Means

Occurrence of relative (individual) software faults causes hardware where such fault occurs be idled. After detection of such failure, isolating and elimination actions are being taken leading to the change of failure rate $\lambda\alpha$. In the model such events are described using multi-fragmentation modelling mathematical apparatus [9].

Considering ICS design features, the following assumption is being made: reliability parameters of both used software versions are equal ($\lambda\alpha_1 = \lambda\alpha_2 = \lambda\alpha$, $\mu\alpha_1 = \mu\alpha_2 = \mu\alpha$).

Figure 4 presents inter-fragmental transitions resulted from occurrence and elimination of one relative design fault of the first software version. For the case of fault occurrence in the second version of software, inter-fragmental states would be identical. Considering that during occurrence of one relative design fault of hardware channels with another software version remain operative, in the inter-fragmental space hardware physical faults continue to occur. This fact justifies transitions between states S7–S8; S8–S9; S10–S11; S11–S12. Moreover, for all operative states it is necessary to further model occurrence of supervision system faults (not shown in Fig. 4). Such model is shown in Fig. 5, where the following marking is applied: white color is used to present operative states, red color is used for safe failed states caused by software design faults, and blue color is used for safe failed states caused by supervision system faults.

The availability function for orgraph in Fig. 5 is defined as (2):

$$A(t) = \sum_{i=1}^5 P_i(t) + \sum_{i=12}^{13} P_i(t) + \sum_{i=15}^{16} P_i(t) + \sum_{i=22}^{26} P_i(t) \quad (2)$$

Baseline conditions are the following: $t = 0$, $P_1(0) = 1$, $P_2(0) \dots P_{32}(0) = 0$.

3.3 Models Assumptions and Input Parameters

The main assumptions of this Markov models are:

- the flow of events that transfers the system from one functional state to another one within the same fragment has the properties of stationarity, ordinariness and the absence of aftereffect, the model parameters within one fragment are assumed to be constant;
- during the elimination of software faults, new faults are not introduced;

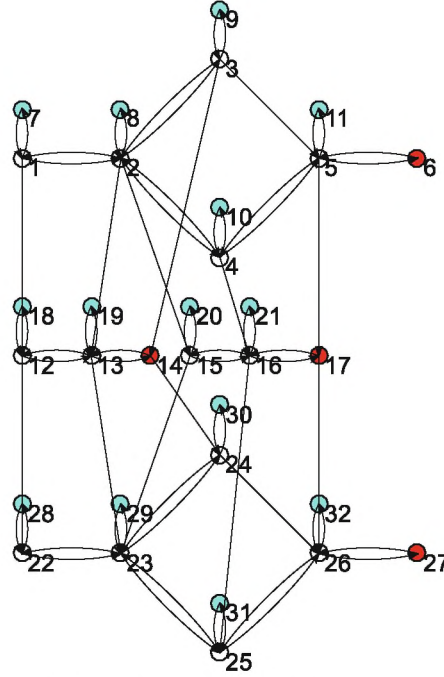


Fig. 5. Orgraph of model with fragments, resulted from occurrence of the relative design fault in the one of software versions

Table 2. Values of simulation processing input parameters

#	Sym	Parameter	Value
1	λp	HW failure rate due to physical faults (pf)	$1e-4$ (1/hour)
2	$\lambda \alpha$	SW failure rate due to design faults (df)	$5e-4$ (1/hour)
3	$\lambda \gamma$	Supervision means failure rate	$1e-6$ (1/hour)
4	μp	HW recovery rate after failure	1 (1/hour)
5	$\mu \alpha$	SW recovery rate after failure	2 (1/hour)
6	$\mu \gamma$	Supervision means recovery rate after failure	0.25 (1/hour)
7	$\Delta \lambda \alpha$	SW failure rate change after fault elimination	$1.25e-4$ (1/hour)
8	$N \alpha$	Assumed number of design faults	4

4 Simulation and Analysis

To build the matrix of Kolmogorov-Chapman system of differential equations (SDE) in Matlab, matrix A function was used [18]. The SDE can be solved using analytical methods (substitutions, Laplace transforms, etc.). But this approach is applicable for systems of small dimension. In this paper, we consider a single-fragmentation model

of medium dimension (11 states in Fig. 3b) and a multi-fragmentation model of large dimension (95 states for $N\alpha = 4$, Fig. 4, Fig. 5), therefore, an approach that is universal for both models to the numerical solution of SDEs was chosen. The SDE solution is obtained using the ode15s function [19]. The simulation results are shown in Fig. 6.

The graphs of the NPP ICS model (Fig. 6a) illustrate the typical nature of the change in the availability function with a decrease to a stationary coefficient $A = 0.999996$ during the first 30 h of operation. Consideration of supervision means failures allows improving availability function assessment by $\Delta A = 4e-6$ (shown as difference between red and blue levels at the chart). As this takes place, impact of failures resulted from relative software version faults is not traced in the chart.

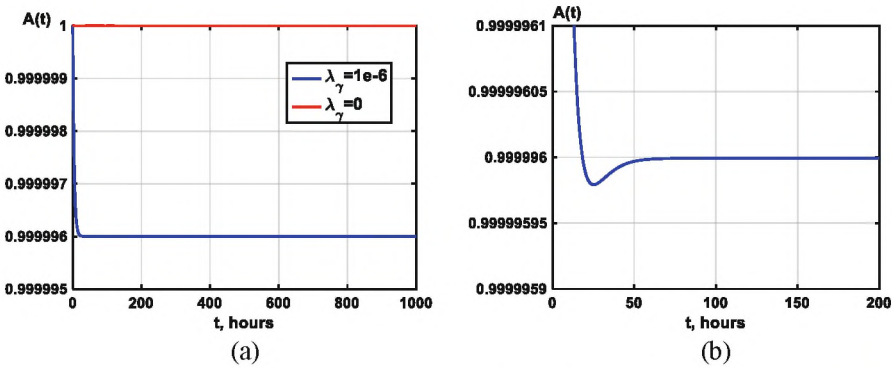


Fig. 6. Results of availability simulations of NPP ICS: a) from parameters value in Table 1, b) from $\lambda\alpha = 5e1$ (1/hour)

To assess the impact of relative software failures on availability, their occurrence rate was increased by three degrees. Chart shown in Fig. 6b depicts decay of availability curve on the interval 20..70 h by $\Delta A = 2e-8$ when $\lambda\alpha = 5e-1$ (1/hour).

5 Conclusion

Paper provides development and research of models two-version safety system with two-cascade redundancy, making it possible to consider supervision means failures. System structure with self-supervision is presented, comprising of subsystem supervision means, inter-channel comparison and analysis means. Such structure makes it possible not only identify subsystem failures states, but also provide a check of supervision means and decrease risk of unsafe and undetected states.

Construction of Markov models that describe occurrence of physical faults in the hardware channels and supervision means failures is discussed by stages. To simulate system behavior considering version (subsystems) design faults occurrence and elimination the multi-fragmentation Markov model has been suggested and researched. Main its particularity is detail analysis of fault combination described by inter-fragmental part of the model.

Considering supervision means failures allows improving accuracy of stationary availability factor by $\Delta A = 4e-6$ (from $A = 0.99999999673858$ to $A = 0.999995999689761$). It is important taking into account high requirements to availability of RTS (more than 0.99999). Therewith impact of relative software failures with rate $\lambda\alpha = 5e-1$ to the general availability of the whole system is within $\Delta A = 2e-8$ due to two-version structure. However, the overlap of version and control failures can be more critical.

Further research should be devoted to the development of analytical models intended for assessment of impact of the whole set of design faults (including 4 and 5, Fig. 2) to the availability and safety, as well as to possible attacks to the system [14, 20]. In case of attacks or any intrusions results of the vulnerability analysis should be taken into account so as to parametrize and redevelop Markov model or develop combined technique of assessment.

References

1. IEC 61513:2011. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems (2011). <https://webstore.iec.ch/publication/5532>
2. IEC 60880:2006. Nuclear power plants. Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category A functions (2006). <https://webstore.iec.ch/publication/3795>
3. IEC 61508-6:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (2010). <https://webstore.iec.ch/publication/5520>
4. Sklyar, V.: Safety-critical certification of FPGA-based platform against requirements of US nuclear regulatory commission (NRC): industrial case study. In: Proceedings of the 12th International Conference on on ICT in Education, Research and Industrial Applications (2016)
5. D7.24-FSC(P3)-FMEDA-V6R0. Exida FMEDA Report of Project: Radiy FPGA-based Safety Controller (FSC). 69 p. (2018)
6. NUREG/CR-7007. Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems (2010). <https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr7007/index.html>
7. Kharchenko, V., Siora, A., Sklyar, V., Volkoviy, A., Bezsalii, V.: Multi-diversity versus common cause failures: FPGA-based multi-version NPP I&C systems. In: Proceedings of the 7th Conference NPIC&HMIT (2010)
8. Littlewood, B., Popov, P., Strigini, L. DISPO project: a summary of CSR work on modelling of diversity. Centre for Software Reliability. City University, London, UK (2006)
9. Kharchenko, V., Butenko, V., Odarushchenko, O., Sklyar, V.: Multifragmentation Markov Modeling of a Reactor Trip System. J. Nuclear Eng. Radiat. Sci. 1 (2015). <https://doi.org/10.1115/1.4029342>
10. Kharchenko, V., Ponochovnyi, Y., Boyarchuk, A., Andrashov, A., Rudenko, I.: Multifragmental Markov's models for safety assessment of NPP I&C system considering migration of hidden failures. In: Ermolayev, V., Mallet, F., Yakovyna, V., Mayr, H.C., Spivakovsky, A. (eds.) ICTERI 2019. CCIS, vol. 1175, pp. 302–326. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-39459-2_14
11. Johnson, G.: Cyber Robust Systems: The Vulnerability of the Current Approach to Cyber Security (2020). <https://www.igi-global.com/chapter/cyber-robust-systems/258678>

12. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., Meskin, N.: Cybersecurity for industrial control systems: a survey. *Comput. Secur.* **89**(101677) (2020). <https://doi.org/10.1016/j.cose.2019.101677>
13. Thames, L., Schaefer, D. (eds.): *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing*. Springer, Cham (2017)
14. Kolisnyk, M.: Vulnerability analysis and method of selection of communication protocols for information transfer in internet of things systems. *Radioelectron. Comput. Syst.* **1**(97), 133–149 (2021). <https://doi.org/10.32620/reks.2021.1.12>
15. Morozova, O., Nicheporuk, A., Tetskyi, A., Tkachov, V.: Methods and technologies for ensuring cybersecurity of industrial and web-oriented systems and networks. *Radioelectron. Comput. Syst.* **4**, 145–156 (2021). <https://doi.org/10.32620/reks.2021.4.12>
16. Ponochovnyi, Y., Bulba, E., Yanko, A., Hozbenko, E.: Influence of diagnostics errors on safety: indicators and requirements. In: IX International Conference on Dependable Systems, Services and Technologies, pp. 53–57 (2018). <https://doi.org/10.1109/DESSERT.2018.8409098>
17. 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
18. Solve stiff differential equations and DAEs – variable order method – MATLAB ode15s. <https://www.mathworks.com/help/matlab/ref/ode15s.html>. Accessed 1 Jan 2022
19. Kharchenko, V., Ponochovnyi, Y., Boyarchuk, A.: Availability assessment of information and control systems with online software update and verification. In: *Information and Communication Technologies in Education, Research, and Industrial Applications*, pp. 300–324 (2014). https://doi.org/10.1007/978-3-319-13206-8_15
20. Shelekhov, I., Barchenko, N., Kalchenko, V., Obodyak, V.: A hierarchical fuzzy quality assessment of complex security information systems. *Radioelectron. Comput. Syst.* **4**(96), 106–115 (2020). <https://doi.org/10.32620/reks.2020.4.10>