The 11h IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2020
14-18 May, 2020, Ukraine, Kyiv

The availability model of two-zone physical security system considering degradation level from cyber attacks and software update

Vyacheslav Kharchenko[1,2], Yuriy Ponochovnyi[1,3], Al-Khafaji Ahmed Waleed[1], Oleg Ivanchenko[1,4],
Dmytro Uzun[1], Larysa Degtyareva[3]
[1] National Aerospace University, Kharkiv, Ukraine, V.Kharchenko@csn.khai.edu, eng_ahmed.waleed@yahoo.com,
d.uzun@csn.khai.edu
[2] Research and Production Company Radiy, Kirovograd, Ukraine
[3] Poltava State Agrarian Academy PSAA, Poltava, Ukraine, yuriy.ponch@gmail.com, ladegt12@gmail.com
[4] University of Customs and Finance, Dnipro, Ukraine, vmsu12@gmail.com

Abstract—**The article analyzes the process of functioning of physical security systems in the conditions of component failures, cyberattacks and software updates. A zonal model of physical security systems, which includes motion detection and access control subsystems, have been built. Updating the software functions of each zone, attacks on the physical component of the motion detection subsystem, and cyber attacks on the access control system have been investigated. To model software updates, a multi-fragment model, including 9 states of each fragment and program update states has been created. To study the behavior of the model while changing the input parameters, Matlab scripts have been developed. Simulation results allow to evaluate the availability function minimum value, availability function value in stationary mode, time interval for the transition of the availability function to the stationary mode.**

Keywords—Cyberphysical Security System; Markov and Multifragmental Model; Availability function; Degradation Levels; Software Update.

I. Introduction

Adequate modeling of physical security systems (PSS), considering multifunctionality and functioning in an aggressive environment, requires an appropriate representation of the zonal architecture of the system. Architectural construction is well displayed in Markov's models [1,2]. The mathematical apparatus of Markov's processes provides an assessment of the resulting availability indicator, which meets the requirements of standards and regulatory documents [3,4]. However, Markov's models are limited by assumptions on the simplest events [5, 6], and are also prone to the issue of increasing dimensionality, when dealing with a large number of external factors. The multi-fragment modeling apparatus [7] allows modeling systems with variable parameters, but does not solve the dimensional problem. In [7–9], Markov's and multi-fragment models of information-control systems as hardware-software complexes for a specific architecture have been investigated. However, the well-known works did not consider the influence of zonal architecture on the availability of the system from the point of both – reliability and security, when updating the software functions of the system.

This article discusses an approach for building multi-fragment models of the availability of physical security systems considering failures of their zones, functions, eliminating software defects and vulnerabilities while updating programs.

The rest of the article is organized as follows. The next section describes the construction of a multi-fragment model of availability: the assumptions are made, the states are defined, and a digraph is built. Section III presents the results of the research of the CPSS model with constant input parameters and with two of them changed at given intervals of values. We discuss related researches in Section IV and conclude our article in Section V.

II. Development and Research of the Availability Model of Physical Security Systems with Software Update

The availability model of a two-zone cyberphysical security system allows us to study the simultaneous effect of failures of the hardware component of zones and their functions, implemented through software. The article considers a two-zone PSS model (Fig.1), in which the first zone has an external perimeter and is susceptible to physical attacks, and the second zone implements access control functions via a remote connection (therefore, is susceptible to cyber attacks).

Modern systems can receive updates and patches of the software component as part of their development and modification cycles. After installing the update or patch, the program code and/or configuration files change, which directly affects the value of the input parameters of the failure flows and cyberattacks. In [7,9], such changes are modeled using the multi-fragment approach, which is the basis of the Multifragmental model of PSS.

978-1-7281-1733-1/19/$31.00 ©2020 IEEE

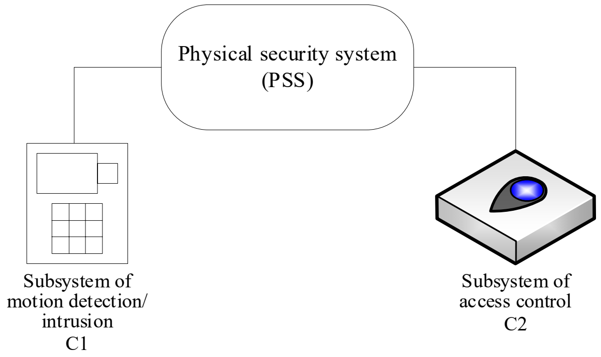

Physical security system (PSS)
Subsystem of motion detection/ intrusion
C1
Subsystem of access control
C2

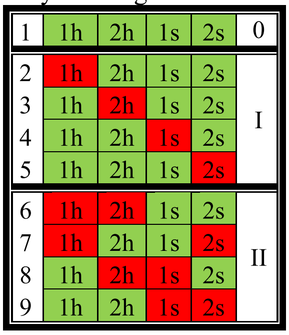
Figure 1. Two-zone architecture of physical security system includes motion detection and access control subsystems.

The assumptions of this Multifragmental model of PSS are expanded:

– the number 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;

– the elimination of software defects and vulnerabilities occurs during the upgrade process, new defects and vulnerabilities may not be found.

The state space of the Multifragmental model of PSS within one fragment has a dimension of 9 states (Fig. 2) and three levels of system degradation.



1	🟩 1h	🟩 2h	🟩 1s	🟩 2s	0
2	🟥 1h	🟩 2h	🟩 1s	🟩 2s	I
3	🟩 1h	🟥 2h	🟩 1s	🟩 2s	
4	🟩 1h	🟩 2h	🟥 1s	🟩 2s	
5	🟩 1h	🟩 2h	🟩 1s	🟥 2s	
6	🟥 1h	🟥 2h	🟩 1s	🟩 2s	II
7	🟥 1h	🟩 2h	🟩 1s	🟥 2s	
8	🟩 1h	🟥 2h	🟥 1s	🟩 2s	
9	🟩 1h	🟩 2h	🟥 1s	🟥 2s	

Figure 2. Combinations of zone failures that determine the states of the PSS model and degradation levels.

Figure 3 shows a marked graph of three fragments of the Multifragmental model of PSS. For compactness each fragment of the model was presented with a vertical arrangement of states.

While constructing the graph of the model (Fig. 3), the color marking of the states («Red», «Green», «White») was used to indicate that the states belong to different levels of degradation. Additionally, a «blue» marker was used to highlight SW update states (S10, S20), the system is inoperative in these states.

Availability functions for different levels of degradation are defined as:

$$A^{(0)}\left(t\right)=\sum_{i=1}^{Nf}P_{10i-9}\left(t\right);\;\; A^{(I)}\left(t\right)=\sum_{i=1}^{Nf}\sum_{j=1}^{5}P_{(10i-10)+j}\left(t\right) \quad (1$$

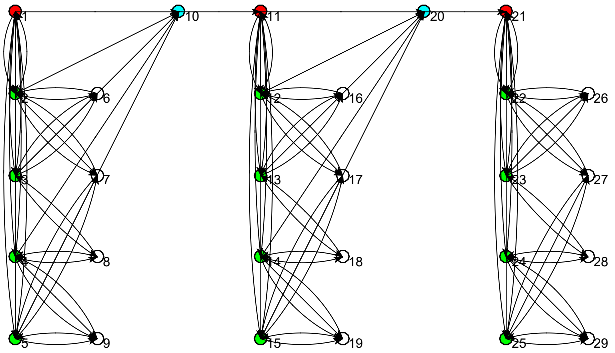


Figure 3. Marked graph of the three-fragment MPSS model.

III. Simulation and Comparative Analysis

A. The behavioral model without changing the input parameters

The Kolmogorov-Chapman differential equation system, built for the Multifragmental model of PSS fragment, is as follows:

$$\begin{cases}
dP_1\left(t\right)/dt=-\left(\left(a_{H1}+a_{H2}\right)\lambda_H+\alpha\gamma_H\right)P_1\left(t\right)- \\
\qquad -\left(\left(a_{S1}+a_{S2}\right)\lambda_{S(i)}+\beta\gamma_{S(i)}\right)P_1\left(t\right)+ \\
\qquad +b_{H1}\mu_H P_2\left(t\right)+b_{H2}\mu_H P_3\left(t\right)+ \\
\qquad +b_{S1}\mu_S P_4\left(t\right)+b_{S2}\mu_S P_5\left(t\right), \\
dP_2\left(t\right)/dt=-\left(a_{H2}\lambda_H+b_{H1}\mu_H\right)P_2\left(t\right)- \\
\qquad -\left(a_{S2}\lambda_{S(i)}+\beta\gamma_{S(i)}\right)P_2\left(t\right)+ \\
\qquad +\left(a_{H1}\lambda_H+\alpha\gamma_H\right)P_1\left(t\right)+b_{H2}\mu_H P_6\left(t\right)+ \\
\qquad +b_{S2}\mu_S P_7\left(t\right), \\
dP_3\left(t\right)/dt=-\left(a_{H1}\lambda_H+\alpha\gamma_H+b_{H2}\mu_H+a_{S1}\lambda_{S(i)}\right)P_3\left(t\right)+ \\
\qquad +a_{H2}\lambda_H P_1\left(t\right)+b_{H1}\mu_H P_6\left(t\right)+b_{S1}\mu_S P_8\left(t\right), \\
dP_4\left(t\right)/dt=-\left(a_{H2}\lambda_H+\beta\gamma_{S(i)}+b_{S1}\mu_S+a_{S2}\lambda_{S(i)}\right)P_3\left(t\right)+ \\
\qquad +a_{S1}\lambda_{S(i)}P_1\left(t\right)+b_{H2}\mu_H P_8\left(t\right)+b_{S2}\mu_S P_9\left(t\right), \\
dP_5\left(t\right)/dt=-\left(a_{H1}\lambda_H+\alpha\gamma_H\right)P_5\left(t\right)- \\
\qquad -\left(a_{S1}\lambda_{S(i)}+b_{S2}\mu_S\right)P_5\left(t\right)+ \\
\qquad +\left(a_{S2}\lambda_{S(i)}+\beta\gamma_{S(i)}\right)P_1\left(t\right)+b_{S1}\mu_S P_9\left(t\right)+ \\
\qquad +b_{S2}\mu_S P_7\left(t\right), \\
dP_6\left(t\right)/dt=-\left(\left(b_{H1}+b_{H2}\right)\mu_H\right)P_6\left(t\right)+ \\
\qquad +a_{H2}\lambda_H P_2\left(t\right)+\left(a_{H1}\lambda_H+\alpha\gamma_H\right)P_3\left(t\right),
\end{cases}$$

$$
\begin{cases}
dP_7(t)/dt = -\left(b_{H1}\mu_H + b_{S2}\mu_S\right)P_7(t) + \\
\qquad + \left(a_{S2}\lambda_{S(i)} + \beta\gamma_{S(i)}\right)P_2(t) + \\
\qquad + \left(a_{H1}\lambda_H + \alpha\gamma_H\right)P_5(t), \\
dP_8(t)/dt = -\left(b_{H2}\mu_H + b_{S1}\mu_S\right)P_8(t) + \\
\qquad + a_{S1}\lambda_{S(i)}P_3(t) + a_{H2}\lambda_H P_4(t), \\
dP_9(t)/dt = -\left(\left(b_{S1} + b_{S2}\right)\mu_S\right)P_9(t) + \\
\qquad + \left(a_{S2}\lambda_{S(i)} + \beta\gamma_{S(i)}\right)P_4(t) + \\
\qquad + a_{H1}\lambda_H P_5(t);
\end{cases}
$$

The system will be supplemented by normalizing the ratio:

$$
\sum_{i=1}^{10N_f-1} P_i(t) = 1; \; P_1(0) = 1;
$$

$$
\forall i \in [2\ldots(10N_f - 1)] \Rightarrow P_i(0) = 0.
$$

The values of hardware input parameters [1], summarized in Table 1, were used during the research.

TABLE I. THE VALUE OF THE HARDWARE PARAMETERS

Hardware input parameters	**Symbol / unit**	**Value**
Hardware failure rate caused by unintentional physical and design faults (pf and df)	λ_{HW} (1/hours)	$1\cdot10^{-3}$
Hardware recovery rate after failure, averaging is performed and recovery is considered for all reasons for failure (pf, df, hf, if)	μ_{HW} (1/hours)	1
Hardware failure rate due to intentional acts (if, vandalism)	γ_{HW} (1/hours)	$1\cdot10^{-3}$
Factor "aggression" intruders - vandals depends on external factors	α	10
Multiple coefficients hardware failure rates for different zones	ah1...ah2	1…2
Multiple coefficients hardware recovery rates for different zones	bh1...bh2	1…2

The values of the model input parameters related to the software functions are given in Table 2.

To build a matrix of the Kolmogorov-Chapman differential equations, matrixA function has been used [9]. To study the model, a script in the Matlab environment has been developed. Matlab ode15s solver has been used to solve the system of differential equations [10].

The simulation results are shown in Fig.4. The graphs of the Multifragmental model of PSS illustrate the typical nature of the change in the availability function for multi-fragment models [7,9]. In the initial period of operation, the availability of the system is reduced to a minimum, and then, as the elimination of SW faults and vulnerabilities, strive for a stationary value.

TABLE II. THE VALUE OF THE SOFTWARE PARAMETERS

Software input parameters	**Symbol / unit**	**Value**
Software failure rate due to design faults of an unintentional nature (df)	λ_{SW} (1/hours)	$5\cdot10^{-3}$
Software recovery rate. In the research, averaging is performed and recovery is considered for all causes of failures (df, hf, if). Recovery does not remove the cause of failure	μ_{SW} (1/hours)	2
Software failure rate due to intentional actions (if, viruses, cyberattacks)	γ_{HW} (1/hours)	$5\cdot10^{-3}$
Factor «aggression» intruders - cybercriminals depends on external factors	β	5
Multiple coefficients software failure rates for different zones	as1...as2	0.1…2
Multiple coefficients software recovery rates for different zones	bs1...bs2	0.3…5
The rate of the development and updating of software with the removal of the cause of failure	λupd (1/hours)	5e-3
The rate of the installation of software updates with removal the cause of failure	µupd (1/hours)	0,5
Change in the software failure rate due to the removal of design faults of an unintentional nature (df) after installing the software update	Δλsw (1/hours)	6e-5
Change in the software failure rate due to the removal of vulnerabilities after installing the software update	Δγsw (1/hours)	3e-4

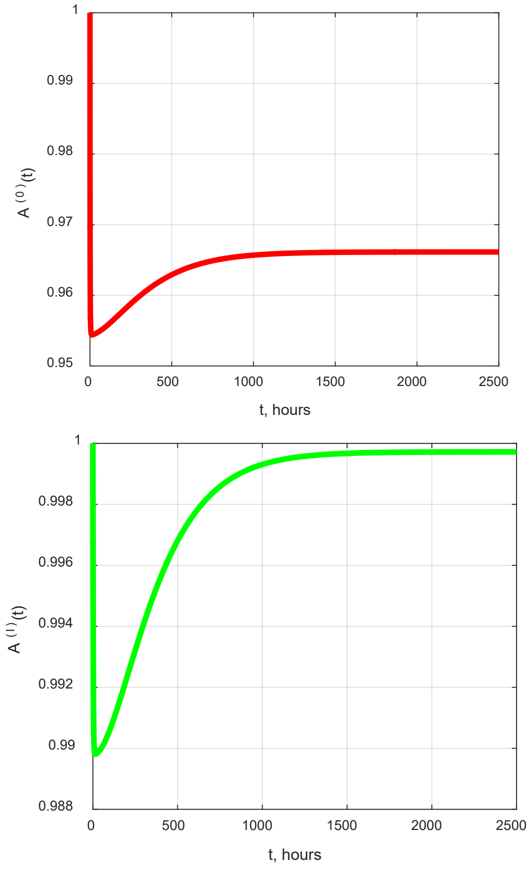


Figure 4. Results of availability simulations of two-zone CPSS for different levels of degradation

For further analysis of the results, it is necessary to take into account the following groups of values of the resulting indicators for two levels of availability degradation:

a) for zero degradation level $A^{(0)}$

- availability function minimum value $A^{(0)}$min = 0.9544;

- availability function value in stationary mode $A^{(0)}$const = 0.9661;

- time interval for the transition of the availability function to the stationary mode $T^{(0)}$const = 3383,4 hours.

b) for the first degradation level $A^{(I)}$

- availability function minimum value $A^{(I)}$min = 0.9898;

- availability function value in stationary mode $A^{(I)}$const= 0.9997;

- time interval for the transition of the availability function to the stationary mode $T^{(I)}$const = 3328,3 hours.

B. Researching the model behavior while changing the input parameters

The availability function of the cyberphysical security system with PS updates has a long transition period (more than 3000 hours), therefore it is advisable to study the influence of input parameters on its behavior through the complete Kolmogorov-Chapman solution. To study the model, the following parameters have been selected [5] (Table 3).

TABLE III. VARIABLE VALUES INTERVALS OF MODEL INPUT PARAMETERS

#	Parameter name	Symbol	Interval	Unit
1.	The intensity of the development and updating of software with the removal of the cause of failure	Λupd	[5e-4…5e-2]	1/hour
2.	The intensity of installing software updates with the removal of the cause of failure	Mupd	[0,5..5]	1/hour

To study the influence of these parameters, special cyclic software constructs have been developed. The simulation results in the form of graphical dependencies are shown in Figs. 5-6.

Figure 5 in a three-dimensional format shows the behavior of the availability functions for various values of software updates intensity parameter. With an increase of the software updates intensity, the system moves to the last fragment in a shorter period of time. This leads to a nonlinear decrease in the minimum availability for zero and first levels of degradation ($A^{(0)}$ and $A^{(I)}$). An increase in the software updates intensity by 2 orders of magnitude does not affect the levels of stationary availability factors $A^{(0)}$ and $A^{(I)}$.

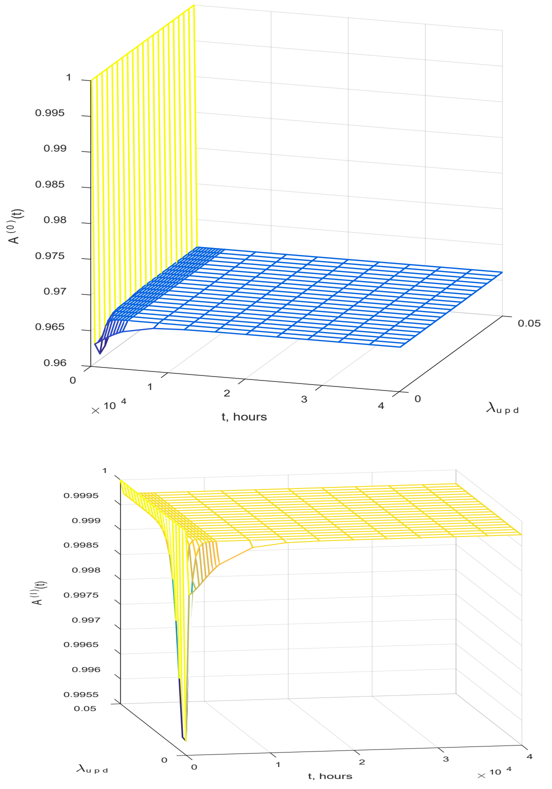


Figure 5. Graphs of changes in functions for different levels of degradation of the model for various values of the parameter λ_{UPD}

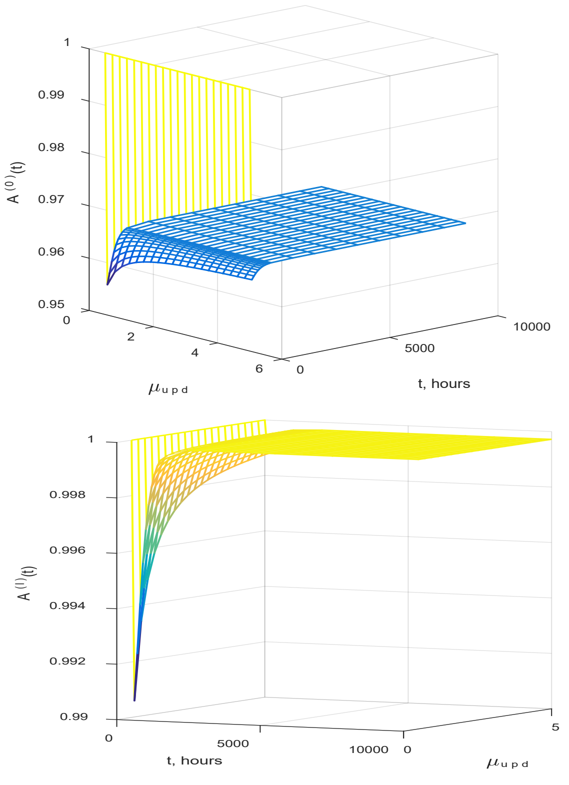


Figure 6. Graphs of changes in functions for different levels of degradation of the model for various values of the parameter μ_{UPD}

Figure 6 in a three-dimensional format shows the behavior of the availability functions for various values of the parameter μ_{UPD}. As the intensity of recovery after updates increases, the probability of the system being at inoperative states S10 and S20 is reduced. This leads to a nonlinear decrease in the minimum availability for zero and first levels of degradation ($A^{(0)}$ and $A^{(1)}$). An increase in the intensity of recovery does not affect the levels of stationary availability factors $A^{(0)}$ and $A^{(1)}$, and the interval of their transition to a stationary state.

IV. Related Works

The works of K. Trivedi et al. [5] analyze Web Servers considering the dependability and cybersecurity factors. Despite their focus on Markov's models, K. Trivedi prefers to use the apparatus of Petri nets. Also, these articles do not take into account the software update processes (alternatively, the software aging processes are considered).

The works of B. Volochiy, et al. [11] analyze Critical NPP I&C Systems taking into account the factors of change in the parameters of event flows. Changing in parameters is modeled through the approximation of the nonexponential distribution law. The formal method is used for the main representation of the model, the graph image is used auxiliary.

In the works of O. Odarushchenko, et al. [7], the Reactor Trip System considering the availability and functional safety factors is analyzed. To study the functioning of systems in conditions of changing failure flow parameters, the multifragmental modeling apparatus was used.

They are summarized in Table IV.

TABLE IV. Related Works Studying the reliability and security of information systems

Paper	Type of system	Evaluation technique	Accounting degradation levels
K. Trivedi, et al. [5]	Web Servers	Analytical, Markov chain Perti Net modelling	partially
B. Volochiy, et al. [11]	Critical NPP I&C Systems	Analytical, Formal metod, Markov chain modelling	no
O. Odaru-shchenko, et al. [7]	Reactor Trip System	Markov chain, multifragmental modelling	no

V. Conclusion and Future Work

The article investigates the multi-fragment model of dual-zone CPSS availability to cyberattacks and software updates. Analysis of the CPSS availability simulation results for different degradation levels showed that:

a) when increasing the intensity of updates by 2 orders, the system goes to the last fragment 6 times faster; this leads to a nonlinear decrease in the minimum availability for zero and first levels of degradation ($A^{(0)}$ and $A^{(1)}$) by 3% and 6% corespondingly; and does not affect the levels of stationary availability coefficients $A^{(0)}$ and $A^{(1)}$;

b) with an increase in the intensity of recovery after updates by an order of magnitude, the probability of the system being in inoperative states S10 and S20 decreases. This leads to a nonlinear decrease in the minimum availability for zero and first levels of degradation ($A^{(0)}$ and $A^{(1)}$) by 2% and 5%. An increase in the intensity of recovery by an order does not affect the levels of stationary availability coefficients $A^{(0)}$ and $A^{(1)}$, and the interval of their transition to a stationary state.

Further research should be directed to the development and research of both Markov's and multi-fragment availability models of multi-zone CPSS, that remove the assumption of high reliability of the cloud service.

References

[1] A. Waleed, V. Kharchenko, D. Uzun and O. Solovyov, "IoT-based physical security systems: Structures and PSMECA analysis", *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2017. Available: 10.1109/idaacs.2017.8095211.

[2] C. Boano, K. Römer, R. Bloem, K. Witrisal, M. Baunach and M. Horn, "Dependability for the Internet of Things—from dependable networking in harsh environments to a holistic view on dependability", *e & i Elektrotechnik und Informationstechnik*, vol. 133, no. 7, pp. 304-309, 2016. Available: 10.1007/s00502-016-0436-4.

[3] "IEC 60050-192:2015 | International Electrotechnical Vocabulary (IEV) - Part 192: Dependability", *Webstore.iec.ch*, 2015. [Online]. Available: https://webstore.iec.ch/publication/21886. [Accessed: 21- Jan- 2020].

[4] "IEC 61703:2016 | Mathematical expressions for reliability, availability, maintainability and maintenance support terms", *Webstore.iec.ch*, 2016. [Online]. Available: https://webstore.iec.ch/publication/25646. [Accessed: 21- Jan-2020].

[5] Z. Zheng, K. Trivedi, N. Wang and K. Qiu, "Markov Regenerative Models of WebServers for Their User-Perceived Availability and Bottlenecks", *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 1, pp. 92-105, 2020. Available: 10.1109/tdsc.2017.2753803.

[6] "IEC 61165:2006 | Application of Markov techniques", *Webstore.iec.ch*, 2006. [Online]. Available: https://webstore.iec.ch/publication/4721. [Accessed: 21- Jan-2020].

[7] V. Kharchenko, V. Butenko, O. Odarushchenko and V. Sklyar, "Multifragmentation Markov Modeling of a Reactor Trip System", *Journal of Nuclear Engineering and Radiation Science*, vol. 1, no. 3, 2015. Available: 10.1115/1.4029342.

[8] E. Asl, M. Sabahi, M. Abapour, A. Khosroshahi and H. Khoun-Jahan, "Markov Chain Modeling for Reliability Analysis of Multi-Phase Buck Converters", *Journal of Circuits, Systems and Computers*, p. 2050139, 2019. Available: 10.1142/s021812662050139x [Accessed 8 March 2020].

[9] V. Kharchenko, Y. Ponochovnyi and A. Boyarchuk, "Availability Assessment of Information and Control Systems with Online Software Update and Verification", *Information and Communication Technologies in Education, Research, and Industrial Applications*, pp. 300-324, 2014. Available: 10.1007/978-3-319-13206-8_15.

[10] "Solve stiff differential equations and DAEs — variableorder

method - MATLAB ode15s", *Mathworks.com*. [Online]. Available: https://www.mathworks.com/help/matlab/ref/ode15s.html. [Accessed: 21- Jan- 2020].

[11] B. Volochiy, L. Ozirkovskyy, O. Mulyak and S. Volochiy, "Safety Estimation of Critical NPP I&C Systems via State Space Method," *2016 Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management (SMRLO)*, Beer-Sheva, 2016, pp. 347-356.