INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2025, VOL. 71, NO. 3, PP. 1-7
Manuscript received February 15, 2025; revised July 2025. doi: 10.24425/ijet.2025.153618

Generalisation of availability models for resilient systems with online verification

Vyacheslav Kharchenko, Yuriy Ponochovnyi, Oleksandr Ivasiuk, Oleg Illiashenko, and Olena Ponochovna

***Abstract*—This paper analyses online verification methods for safety- and security-critical systems, including aerospace, nuclear instrumentation, and smart home systems. It emphasizes the need for resilience and adaptability in these systems to withstand various environmental conditions and potential threats. Several Markov models are developed to evaluate the dependability of control systems for small modular reactors. These models illustrate how online verification, by enabling early detection of failures, can enhance resilience and improve system performance. The findings suggest that optimising verification parameters is crucial for this enhancement, providing a foundation for future research in critical control systems.**

***Keywords*—instrumentation and control systems; online verification; Small Modular Reactors; dependability; resilience; Markov models**

I. Introduction

THE safety and security-critical systems, such as railway control systems, space and aerospace onboard systems, nuclear power plant Instrumentation and Control (I&C) systems (inc. I&C systems for Small Modular Reactors (SMRs)), Smart Home Systems operate under rigorous physical and informational demands [1]. These systems face stringent requirements for both functional and non-functional characteristics due to their long operational lifetimes, potential for evolution, changing environmental conditions, and exposure to various cyber and physical threats. As a result, they must be self-adaptive and resilient throughout their usage.

Aerospace and Space systems manage the control and monitoring of spacecraft or aircraft. Operating in extreme physical environments, they are designed for long-term reliability and must be resilient to factors such as high radiation, pressure variations, and mechanical stresses [2]. Instrumentation and control systems in nuclear power plants, including SMRs, are responsible for safely operating and monitoring nuclear processes. These systems must meet high safety standards to prevent catastrophic failures and ensure the long-term sustainability of energy production [3]. Smart homes rely on interconnected devices for automation, energy efficiency, and security. These systems must be resilient to cyber threats, operational disruptions, and physical damage, ensuring the home functions safely and efficiently, even when facing potential failures or attacks [4].

Numerous industry standards and normative documents, including those from NIST [5-7], ASIS [8], CNSS, CSRC, and ECSS, focus on resilience and resilient systems. As outlined in key sources [9], resilience refers to the ability to minimise the impact and duration of disruptive events on critical systems or infrastructure. A system's resilience depends on its ability to anticipate, absorb, adapt, and recover quickly from disruptive incidents.

For example, NIST [6] defines resilience as the capability to adapt and recover from known and unforeseen environmental changes through risk management, contingency planning, and continuity planning. Formal models and definitions of resilient systems are detailed in various sources, and specific metrics have been developed to assess the resilience of transport information systems.

The primary goal of verification of resilient systems is to confirm that the development results at a given stage meet the requirements formulated at the beginning or earlier. The verification process determines whether the software products, which are the result of specific actions, meet the requirements and conditions imposed on them by preceding actions [10]. Verification is conducted using various methods and tools to achieve maximum efficiency (in terms of undetected faults or confirming an acceptable risk of their presence per unit cost). Verification may include analysis, review, testing, and other methods described in international and national regulatory documents, which form the regulatory framework for various critical applications. It is analysed, in particular, in [11].

In most cases, verification is conducted before the system is operated. However, for certain I&Cs, such as spacecraft, replicating operational conditions during the design phase is impossible or too costly. Therefore, all requirements are confirmed after the spacecraft is launched into outer space. These procedures are referred to as online verification.

In conclusion, ensuring resilience requires a management framework capable of swift adaptation and recovery in changing conditions. This involves predicting, mitigating, and recovering from the impacts of environmental changes, whether known or unknown. To achieve these objectives, it is essential to analyse resilient system structures, generalise methods and scenarios of online verification of resilient systems, and develop availability models for various online verification scenarios.

Vyacheslav Kharchenko, Oleksandr Ivasiuk and Oleg Illiashenko are with the National Aerospace University "Kharkiv Aviation Institute" (e-mail: v.kharchenko@csn.khai.edu, o.ivasiuk@csn.khai.edu, o.illiashenko@khai.edu). Oleg Illiashenko is with the Institute of Informatics and Telematics of the National Research Council (IIT-CNR) (e-mail: oleg.illiashenko@iit.cnr.it).

Yuriy Ponochovnyi and Olena Ponochovna is with the Poltava State Agrarian University (e-mail: yuriy.ponch@gmail.com, olena.ponochovna@pdau.edu.ua)

The remainder of the paper is organised as follows: Section 2 explores the methodology and generalisation of online verification methods for critical systems. Section 3 introduces structural models of I&C systems for small modular reactors with online verification. Section 4 presents and analyses the system availability of seven Markov models across different online verification scenarios, along with the rationale for the chosen simulation input parameters. Section 5 concludes with a summary of findings, recommendations for applying the developed models, and a discussion of potential future work.

II. Generalization of Online Verification Methods for Critical and Resilient Systems

The objectives and conditions for conducting online verification may include:

1. Performing system checks under conditions too complex or costly to replicate during production (e.g., space environments, nuclear reactions);

2. Testing non-critical functions where testing them during production is more expensive than during operation;

3. Continuously verifying the correct operation of a system during its functioning to detect hidden failures or malfunctions early and to assess whether the specified parameters in the technical requirements are being met.

During online verification, the following sources of input test values are identified and fed into the system under test:

– External sources, such as environmental or technological processes, where human influence on their formation is absent;

– Externally generated sources produced directly by the person conducting the test;

– Internal test signals, generated by the system under test itself.

Online verification can be classified by time interval as continuous and periodic.

The set, order, and values of input signals are categorised as follows:

– Constant, where they remain unchanged;

– Variable, where the sequence in which signals are fed or their values change over time.

Figure 1 presents a generalised model of the distinct states of multipurpose servicing: online verification (S3) and patching (S2), where patch installation occurs after detecting changes in environmental parameters.

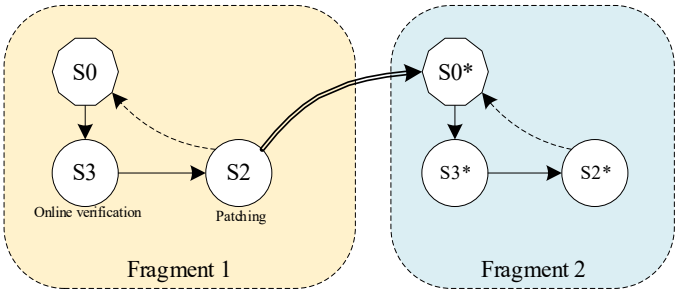


Fig. 1. Generalized model of states of online verification and patching of ICS in the form of a two-fragment graph of states and transitions.

Various scenarios can be used for online verification, as the conditions for conducting it may include the impossibility of pre-replicating real environment parameters (such as outer space in terrestrial conditions), the high cost of such simulation, tight project deadlines, or other constraints.

Three typical scenarios [12] have been proposed for a typical architecture of a control system model for dependability and resilience management.

Scenario 1: After the I&Cs has been put into operation, the system's non-critical functions are post-verified. Due to tight project deadlines, these functions were not verified before the system launch.

Scenario 2: Operational verification is carried out after faults detected during I&Cs operation are fixed.

Scenario 3: During operation, all functions that could not be tested during the design phase are verified. In this scenario, environmental parameters are refined, and based on the results, the identified faults are addressed.

In general, the dependability indicators of modern I&Cs operate with multiple hardware and software failures. The specifications for the causes of hardware and software failures depend on the specific domain of the I&Cs application, which will be discussed below. Models of system states and transitions (Markov [13], multifragment [14], and multiphase [15]) were built to evaluate the performance indicators, which are based on the representation in the form of a set of MS states and a set of ME state changes. Then:

$$MS = \{S_{UPi}, S_{Di}\} = \{S_{UPi\,HW}, S_{UPi\,SW}\} \cup \{S_{Di\,HW}, S_{Di\,SW}\}, \quad (1)$$

$$ME = \{E_{Fi}, E_{Ri}\} = \{E_{Fi\,HW}, E_{Fi\,SW}\} \cup \{E_{Ri\,HW}, E_{Ri\,SW}\}; \quad (2)$$

where $\{S_{UPi\,HW}, S_{UPi\,SW}\}$ is a subset of workable states of hardware and software, $\{S_{Di\,HW}, S_{Di\,SW}\}$ is a subset of inoperable states of hardware and software, $\{E_{Fi\,HW}, E_{Fi\,SW}\}$ is a subset of state changes caused by hardware and software failures, $\{E_{Ri\,HW}, E_{Ri\,SW}\}$ is a subset of state changes caused by hardware and software recovery.

For non-regenerative systems (e.g., I&Cs of unmanned spacecraft), the dependability indicator is defined as:

$$R(t) = \sum P_i(t);\ i : S_i \in S_P;\ S_P \in M\{S_P, S_H\}; M\{E_{Ri}\} = \varnothing \quad (3)$$

For regenerative systems $M\{E_{Ri}\} \neq \varnothing$.

In the I&CS domains of spacecraft, hardware and software failures caused by physical and design faults were investigated. The availability function (for multifragment models [14]) and the averaged unavailability function for the multiphase model [15] were used as an indicator of guarantee capability:

$$A(t) = \sum P_i(t);\ i : S_i \in S_{UP};$$

$$S_{UP} \in M\{S_{UP\,HW}, S_{D\,HW\,pf}, S_{UP\,SW}, S_{D\,SW\,df}\} \quad (4)$$

$$U_{avg}(\tau) = \int_0^{\tau} U(t)\,dt = \int_0^{\tau} (1 - A(t))\,dt \quad (5)$$

$$ME = \{E_{Fi}, E_{Ri}, E_{Veri}, E_{Pathi}\} \quad (6)$$

where $\{S_{UP\,HW}, S_{D\,HW\,pf}\}$ is a subset of operational states of hardware and non-operable states of hardware caused by physical faults, $\{S_{UP\,SW}, S_{D\,SW\,df}\}$ is a subset of operational software states and non-operational software states caused by design faults, U_{avg} is the averaged unavailability function of

the ICS, $E_{Ver\ i}$ – set of state changes caused by operational verification procedures; $E_{Path\ i}$ is a set of state changes caused by software code patching procedures.

The availability function of the critical I&Cs with multi-purpose service has the following character of changes. In the first stage, the system availability decreases to a minimum; then, it asymptotically tends to a constant value. Thus, in the further analysis of the results, it is necessary to take into account three indicators:

– The minimum value of the availability function A_{Mmin};

– The value of the availability function in the stable mode A_{Mconst};

– The time interval for the transition of the availability function to the stable T_{Mconst} mode.

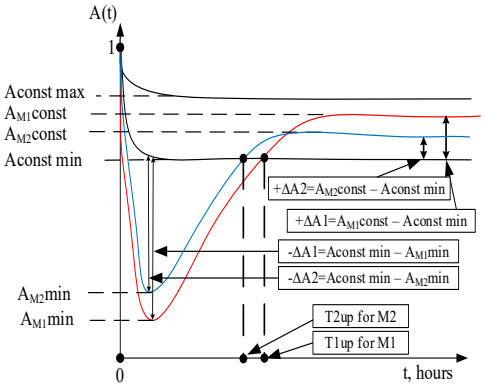


Fig. 2. Generalized Results of availability function simulation of critical I&CS.

In the case of using the proposed models for assessing resilience and comparing online verification strategies, additional resulting indicators were used (Fig. 2):

– decrease in the level of availability of a serviced system at the initial stage of operation relative to the availability factor of a system without online verification similar in terms of hardware and software configuration –ΔAi;

– the gain in availability of a system with online verification compared to a system without online verification similar in terms of hardware and software configuration +ΔAi;

– the Tiup time after which the serviced system has a gain in availability.

At least two additional models were built and tested to calculate the indicated additional resulting indicators for each group of models with online verification (Fig. 3).

The MDEP(1) model for determining the $A_{const\ max}$ indicator does not take into account non-warranty factors caused by failures due to software faults (Fd) or ageing (Fsa) and attacks on software vulnerabilities (Fa*). In this case, the availability function A(t) is not equal to unity due to hardware failures due to physical faults (Fp).

The MDEP(2) models for determining the $A_{const\ min}$ indicator and the T_{iup} time do not take into account countermeasures against the worst dependability factor (I&Cs without software recovery, I&Cs without vulnerability elimination, I&Cs without prevention of hidden failures), i.e. they do not model recovery measures and/or online verification. In this case, the availability function A(t) illustrates the worst-case scenario of using the I&Cs as intended. At the same time, as shown in Fig. 3, taking into account a larger number of types of failures in the model leads to a decrease in the level of availability of I&Cs.

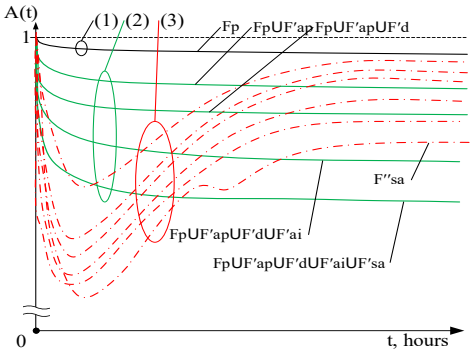


Fig. 3. Models with online verification and accompanying models for dependability and resilience assessment of ICS.

The MDEP(3) models of an online verification system demonstrate using different online verification strategies or one strategy with varying parameter values. For complex models that consider several factors of change (e.g., updating and ageing of software), the graph of the resulting availability function will have different minimum values at the initial stage of operation (Fig.3, curve F"sa).

III. MODELS OF I&C SYSTEM FOR SMALL MODULAR REACTORS WITH ONLINE VERIFICATION

Online verification of algorithm correctness enables early detection of potential failures. It allows for timely corrective actions without requiring the entire digital I&Cs to be placed in a safe state, which would otherwise trigger an automatic reactor shutdown. The system comprises four channels, as illustrated in Figure 4, where input signals are processed, necessary calculations are carried out, and when the calculated parameter exceeds the setpoint, a corresponding signal is generated and sent to the system level, where 2oo4 majority logic is applied.

Each of the four channels is based on a Programmable Logic Controller (PLC), which runs various algorithms for different reactor subsystems simultaneously. This digital I&Cs structure allows any channels to be placed into maintenance mode as needed, enabling the modification of algorithms or setpoint values within that channel.

The architecture of the I&Cs for small modular reactors consists of four hardware channels running two versions of the software (see Fig. 4). The model includes the following input parameters: a) hardware channel failure rate, λ_{HW} (failures per hour); b) system recovery rate after a hardware failure, μ_{HW} (recoveries per hour); c) software failure rate, λ_{SW} (failures per hour); d) system recovery rate after a software fault, μ_{SW} (recoveries per hour).

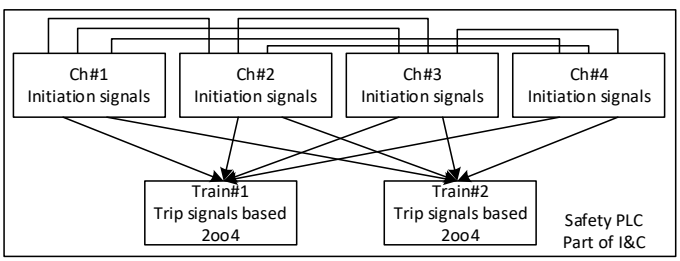


Fig. 4. Generalized functional-structural diagram of digital PLC.

This paper explores a scenario where a single channel, without and with online verification, is externally tested periodically with human intervention as the input source. In contrast, the system under test concurrently performs continuous internal self-diagnostics.

To denote the developed models, the unified record $M_{DEP}X$ is used, where M_{DEP} is a model of dependability (dependability explains the impact of failures and restorations of hardware and software, as well as verification operations); "X" is the serial number of the model. In the graphs, operational states are marked in green, inoperative states with OV are marked in yellow, and inoperative states caused by HW and SW failures are marked in white.

The $M_{DEP}1$ model (Fig.5) takes into account only hardware failures. The resulting graphs will show the limits of the availability function from above.

The $M_{DEP}2$ model (Fig.5) considers hardware and software failures without eliminating them. The resulting graphs show the "conditional" limit of the availability function from below.

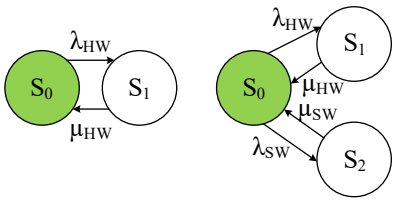


Fig. 5. Models without online verification $M_{DEP}1$ and $M_{DEP}2$.

The multifragment model $M_{DEP}3$ (Fig.6) simulates verification operations only under the condition that the system is operational and with "absolute" success – that is, during the verification, software faults are clearly identified and eliminated.

The operational process of the I&Cs proceeds as follows. Initially, the system performs all planned functions and remains in state S1. During operation, hardware faults may occur, causing a transition to state S2, after which the system is restored to state S1. Subsequently, a software fault may arise, moving the system into state S3. Once the software fault is addressed, the system is restored to state S1. After a specified time interval, defined by the parameter λ_{ver}, a verification of non-critical functions – those not completed on Earth due to project time constraints – takes place. This verification moves the system into an inoperable state, S4. Following corrective actions during online verification, the system advances to a new model fragment (state S5), characterized by a change in software failure rate.

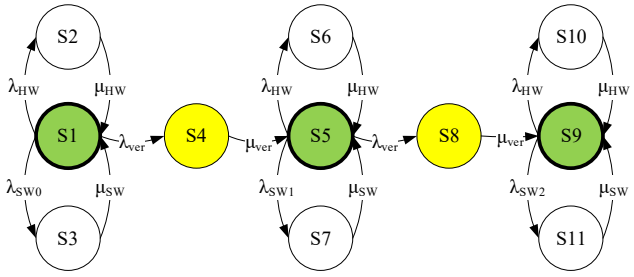


Fig. 6. Models with online verification $M_{DEP}3$.

The multifragment model $M_{DEP}4$ (Fig.7) simulates verification operations only after a software fault has appeared without "absolute" success – that is, during the verification process, there is a probability of not eliminating the detected software fault.

The operational process of the I&C system follows a similar sequence: Initially, the system performs all planned functions and remains in state S1. During operation, hardware faults occur, prompting a transition to state S2 and restoration to state S1. Later, a software fault emerges, moving the system into state S3.

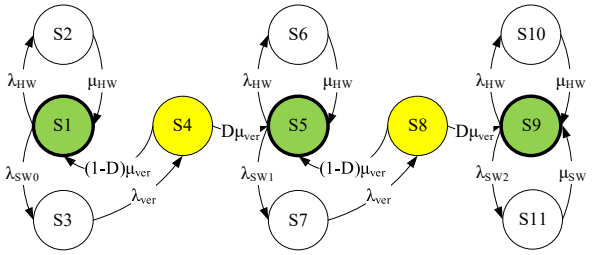


Fig. 7. Models with online verification $M_{DEP}4$.

Once this software fault is communicated to the ground control system, corrective measures are developed, and commands to modify the program code are issued. The parameter λ_{ver} defines the duration of these activities. If the fault is successfully resolved, the system transitions to a new model fragment (state S5); if not, the system returns to state S1. After addressing all potential unidentified faults, the system resumes normal operation, with only hardware failures being considered.

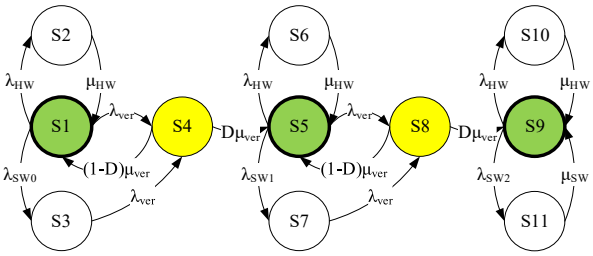


Fig. 8. Models with online verification $M_{DEP}5$.

The multifragment model $M_{DEP}5$ (Fig.8) simulates verification operations at any time, both from an operational state and after a software fault manifests without "absolute" success.

The operational process of the I&C system unfolds as follows: Initially, the system performs all planned functions and remains in state S1. During operation, hardware faults may occur, causing a transition to state S2, followed by restoration to state S1. A software fault may then arise, leading the system into state S3. In this scenario, the fault is due to incomplete information about external environmental parameters. As a result, the system stays in a state of software failure until the environmental data is clarified during corrective online verification procedures. Consequently, the system transitions to the corrective online verification state (S4) from either state S1 or S3 with intensity λ_{ver}. If the fault is successfully resolved, the system progresses to a new model fragment (state

S5); if not, the system reverts to state S1. Once all faults related to inaccurate environmental parameter assessments are addressed, the system continues operating in the event of hardware and software failures. Additionally, after software failures with known causes from the ground control system, the system recovers with intensity μ_{SW}.

The multifragment model $M_{DEP}6$ (Fig.9) simulates verification operations only after a software fault appears without "absolute" success and also models the system's return to an inoperable state if the software fault is not eliminated.

The multifragment model $M_{DEP}7$ (Fig.10) simulates verification operations at any time: both from an operational state and after the manifestation of a software fault, without "absolute" success. It also simulates the system's "return" to an inoperable state in the event that the software fault is not eliminated and additionally models the return of the system to an operational state after failed verification.

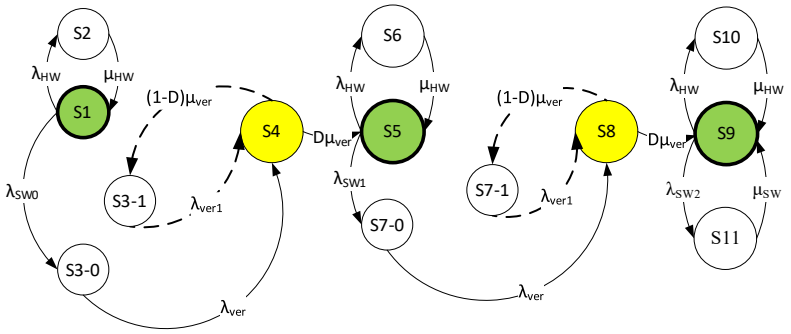


Fig. 9. Models with online verification $M_{DEP}6$.

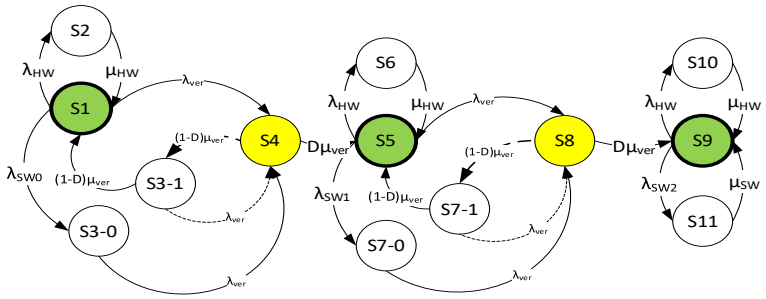


Fig. 10. Models with online verification $M_{DEP}7$

Thus, seven models have been developed that describe different system operation scenarios and account for various online verification scenarios. Given the number of models, it is advisable to outline/develop comparison options. Here, there are several research directions:

1. Comparing the models to identify exits/transitions/intersections/convergences of their readiness functions with the upper and lower bounds of models $M_{DEP}1$ and $M_{DEP}2$;
2. Comparing the models to observe and evaluate the consideration of one of three distinct effects:
   2.1. Transition to verification only from an operational state, from a failure state, or at any time;
   2.2. Consideration of "absolute" or non-absolute verification success;
   2.3. The system's return from post-verification to an operational, non-operational, or an additional non-operational state;
3. Investigating the models with different input parameters to determine under which conditions the readiness function will meet a specific requirement (for instance, achieving a readiness level of 0.99 after 500 hours of system operation with post-verification).

IV. Research of I&C System for Small Modular Reactors Models with Online Verification

To research the given models and compare the results values of the parameters were selected by use of the data provided in [16-18]. Since both models represent the same system, it is assumed at the initial stage of the study that they share the same input parameters, as shown in Table I. The online verification parameters are identical across all models during the initial research phase and are specified in positions 5-9.

TABLE I
NUMERICAL VALUES OF MODELS PARAMETERS

#	Parameter	Numerical Value	Unit
1	λ_{HW}	1,00E-05	1/hour
2	μ_{HW}	0,125	1/hour
3	$\lambda_{SW\,0}$	1,5E-03	1/hour
4	μ_{SW}	0,2	1/hour
5	$\Delta\lambda_{SW}$	5,00E-05	1/hour)
6	λ_{ver}	1,370E-03	1/hour
7	μ_{ver}	0,125	1/hour
8	D_{ver}	0,8	-
9	N_{ver} (Nfr)	30	-

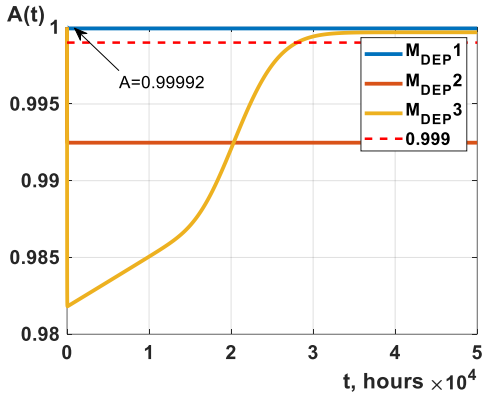


Fig. 11. Comparison of the results of models $M_{DEP}1$, $M_{DEP}2$, $M_{DEP}3$

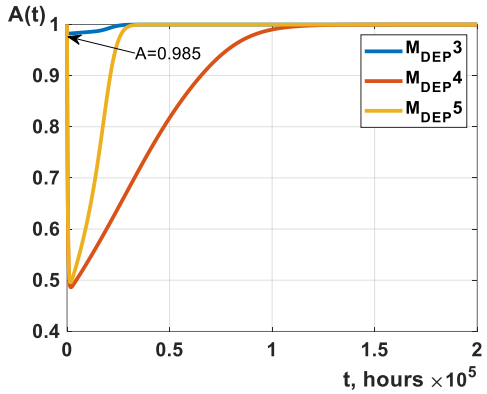
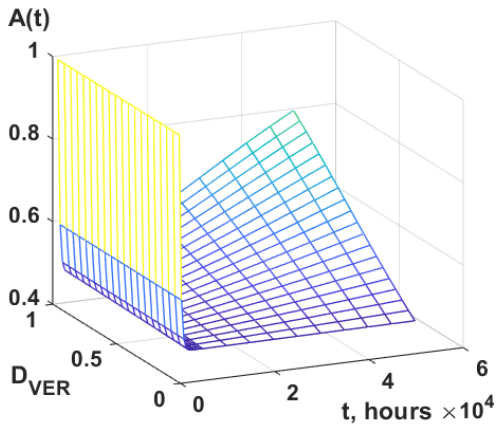


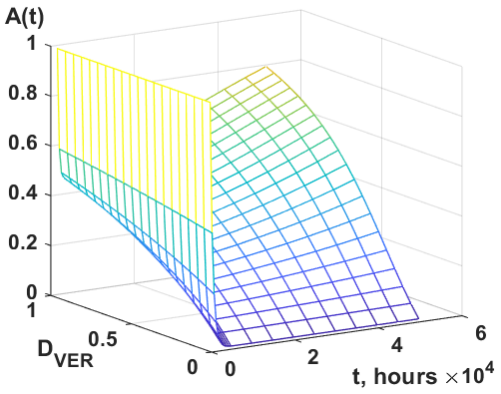
Fig. 12. Comparison of models $M_{DEP}3$, $M_{DEP}4$, $M_{DEP}5$ under the condition $D_{VER}=1$

Fig. 11 illustrates a classic situation where a model $M_{DEP}3$ with online verification at the initial stage has lower availability than model MDEP2 with unremoved software faults. However, with time after the faults are removed, system availability increases.

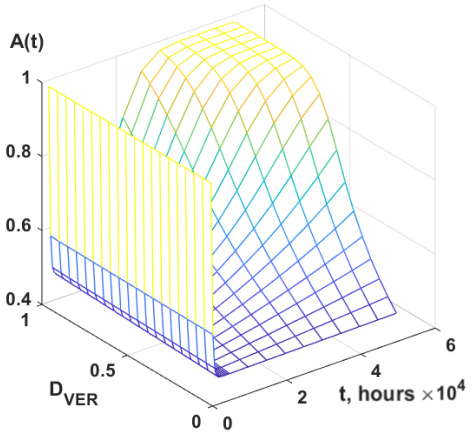
With $\mu_{SW} = 0.2$, Model $M_{DEP}3$ proves to be more advantageous in terms of system readiness compared to entering the inoperable verification state in Models $M_{DEP}4$ and $M_{DEP}5$, as shown in the graphs in Fig. 12. Additionally, we observe an advantage of Model $M_{DEP}5$ over Model $M_{DEP}4$, since in $M_{DEP}5$, verification can be initiated from two previous states. In contrast, in $M_{DEP}4$, it is possible from only one.



$M_{DEP}4$



$M_{DEP}6$



$M_{DEP}7$

Fig. 13. Comparison of models under the different values D_{ver}

The graphs in Fig. 13 provide a detailed illustration of how the D_{ver} parameter influences the behaviour of the availability functions of the models $M_{DEP}4$, $M_{DEP}6$, and $M_{DEP}7$ in a three-dimensional projection. Analysis of the graphs indicates that for the $M_{DEP}4$ model, the D_{VER} parameter does not impact the minimum value of the availability function. In contrast, such an effect is observed in the $M_{DEP}6$ model. For all models, increasing the D_{VER} parameter to a value of 1 accelerates the transition of the availability function to its steady state.

CONCLUSION

This work modelled various online verification scenarios for critical control systems, such as the I&Cs for small modular reactors. Seven Markov models were developed to evaluate the dependability and resilience of such systems. The research findings demonstrated the following:

– Online verification can significantly improve the dependability and resilience of critical control systems. Regular system function checks enable the detection and rectification of potential issues at early stages, preventing severe failures;

– The optimal online verification scenario selection depends on specific system operating conditions. Certain scenarios, such as frequent fault detection or critical functions, may be more effective under particular circumstances;

– Online verification parameters, including verification frequency and fault detection efficiency, substantially impact system dependability and resilience. The appropriate selection

of these parameters can significantly enhance the effectiveness of online verification.

The developed models can be applied to assess the dependability and resilience of critical control systems, such as the I&C system for small modular reactors. They can aid in determining optimal online verification parameters and developing strategies to improve availability.

Future research can focus on expanding the functionality of the developed models, considering additional factors such as the influence of external threats and changes in operating conditions. Additionally, the possibility of applying these models to other critical control systems can be explored.

REFERENCES

[1] R. K. Kaur, L. K. Singh, and B. Pandey, "Security analysis of safety-critical and control systems: A case study of a nuclear power plant system," Nuclear Technology, vol. 197, no. 3, pp. 296–307, Feb. 2017. https://doi.org/10.1080/00295450.2016.1273702

[2] R. Peldszus, "Resilience of Space Systems: Principles and practice," Handbook of Space Security, pp. 127–143, 2020. https://doi.org/10.1007/978-3-030-23210-8_87

[3] J. Hartmann, J. Hyvärinen, and V. Rintala, "The operator and the seven small modular reactors — an estimate of the number of reactors that a single reactor operator can safely operate," Nuclear Engineering and Design, vol. 418, p. 112929, Mar. 2024. https://doi.org/10.1016/j.nucengdes.2024.112929

[4] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, "Review of smart-home security using the internet of things," Electronics, vol. 13, no. 16, p. 3343, Aug. 2024. https://doi.org/10.3390/electronics13163343

[5] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, NIST Special Report 800-160, Vol. 2. Developing cyber-resilient systems, Dec. 2021. https://doi.org/10.6028/nist.sp.800-160v2r1

[6] NIST Interagency Report 8074 Volume 2. Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity. (2015). https://doi.org/10.6028/nist.sp.800-30r1

[7] M. Hogan and E. Newton, Supplemental information for the interagency report on strategic U.S. government engagement in International Standardization to achieve U.S. objectives for cybersecurity, Dec. 2015. https://doi.org/10.6028/nist.ir.8074v2

[8] American National Standards Institute (ANSI) DS 3001:2009. Organizational Resilience: Security, Preparedness, And Continuity Management Systems - Requirements With Guidance For Use. 2009. https://webstore.ansi.org/standards/ds/ds30012009

[9] Computer Security Resource Center. Glossary. Resilience. https://csrc.nist.gov/glossary/term/resilience/

[10] J. C. Santos, S. Suloglu, N. Cataño, and M. Mirakhorli, "A methodological approach to verify architecture resiliency," Lecture Notes in Computer Science, pp. 321–336, 2023. https://doi.org/10.1007/978-3-031-36889-9_22

[11] J. Zhang, G. Li, and X. Liu, "Compare of formal analysis and testing for verification of safety-critical systems: A case study," Proceedings of the 2nd International Conference On Systems Engineering and Modeling, 2013. https://doi.org/10.2991/icsem.2013.179

[12] V. Kharchenko, Y. Ponochovnyi, S. Dotsenko, O. Illiashenko, and O. Ivasiuk, "Models of Resilient Systems with online verification considering changing requirements and latent failures," Lecture Notes in Networks and Systems, pp. 90–99, 2024. https://doi.org/10.1007/978-3-031-61857-4_9

[13] L. Wang, "A Markov model-based fusion algorithm for Distorted Electronic Technology Archives," Computational Intelligence and Neuroscience, vol. 2022, pp. 1–11, Apr. 2022. https://doi.org/10.1155/2022/4202181

[14] V. Kharchenko, Y. Ponochovnyi, A. Boyarchuk, and E. Brezhnev, "Resilience assurance for software-based space systems with online patching: Two cases," Advances in Intelligent Systems and Computing, pp. 267–278, 2016. https://doi.org/10.1007/978-3-319-39639-2_23

[15] L. Ozirkovskyy, B. Volochiy, O. Shkiliuk, M. Zmysnyi, and P. Kazan, "Functional Safety Analysis of safety-critical system using state transition diagram," Radioelectronic and Computer Systems, no. 2, pp. 145–158, May 2022. https://doi.org/10.32620/reks.2022.2.12

[16] Instrumentation and Control Systems. Chapter 7. Hermes Non-Power Reactor Preliminary Safety Analysis Report, revision 0, September 2021, Kairos Power LLC

[17] Safety evaluation. Docket 50-7513. Related to the Kairos Power LLC Construction Permit Application for the Hermes Test Reactor. 2023. https://www.nrc.gov/docs/ML2310/ML23108A119.pdf

[18] Y. Ponochovnyi, V. Kharchenko, "Dependability assurance methodology of information and control systems using multipurpose service strategies," Radioelectronic and Computer Systems, no. 3, pp. 43-58, September 2020. https://doi.org/10.32620/reks.2020.3.05