Information & Security

Published since 1998

V. Kharchenko, S. Dotsenko,
Y. Ponochovnyi & O. Illiashenko
vol. 47, no. 1 (2020): 77-90
https://doi.org/10.11610/isij.4705
ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Cybernetic Approach to Developing Resilient Systems: Concept, Models and Application

Vyacheslav Kharchenko [a], ***Sergiy Dotsenko*** [b], ***Yuriy Ponochovnyi*** [b,c] (✉), ***Oleg Illiashenko*** [a]

[a] *National Aerospace University "KhAI", Kharkiv, Ukraine, https://khai.edu*

[b] *Ukrainian State University of Railway Transport, Kharkiv, Ukraine http://kart.edu.ua/en*

[c] *Poltava State Agrarian Academy, Poltava, Ukraine, https://www.pdaa.edu.ua/en*

ABSTRACT:

The paper contains the results of the development and implementation of a cybernetic approach to the creation of resilient systems. The architecture of a resilient system contains redundant components compared to a traditional feedback control system. This is primarily due to the need to implement additional channels in the control system to respond to changes in requirements, environment, or unspecified faults and failures. The general structure of a resilient system is based on the principle of dividing control channels for functional and non-functional characteristics. This allows to react to changes in the information component of the environment during attacks on the system to ensure its cybersecurity. The case for a space resilient system with online verification is described. Three scenarios of the system behaviour to assure resilience are suggested and the first scenario is explored by the use of Markov model. That allows offering options for improving availability function and other indicators of resilient systems.

ARTICLE INFO:

RECEIVED: 02 JULY 2020
REVISED: 29 JULY 2020
ONLINE: 09 AUG 2020

KEYWORDS:

security, safety, resilience, resilience control system, online verification

✉ Corresponding Author: Tel.: +380509809957; E-mail: yuriy.ponch@gmail.com

Introduction

Motivation

Safety- and security-critical systems (such as aerospace on-board systems, railway control systems, instrumentation and control systems of NPPs and others) are operated under harsh physical and information environmental conditions. Requirements for functional and non-functional characteristics of these systems are tightened considering long time of functioning and possible their evolution, changing of environment characteristics, different cyber and physical threats and attacks. Hence, the systems should be self-adaptive and resilient during application.

There are number of proceedings and normative documents, which consider the content of the concepts of resilience and resilient systems, in particular, standards and reports of the NIST, [1-5] ASIS, [6] CNSS, [7] CSRC, [8] US Government [9] and so on. The definition of *resilience* is given in [3, 4], which emphasizes the ability to reduce the magnitude and / or duration of disruptive events to critical systems or infrastructure. The effectiveness of a resilient system depends upon its ability to anticipate, absorb, adapt to, and / or rapidly recover from a potentially disruptive event.

The standard [3] defines resilience as an ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning. Formal definition and models of resilient systems are described in [10].

In [11] examples of metrics application for an estimation of transport information systems resilience are considered.

Therefore, we can conclude that to ensure resilience it is necessary to develop a management system that will be able to quickly adapt and recover facing the changing operating conditions. This will allow predicting, eliminate or mitigate impacts, adapt and / or recover quickly from any known or unknown changes in the environment. To do this, it is necessary to analyze the main components of the "resilience" and "resilient systems" concepts, to justify the choice of quantitative indicators of resilience, as well as to propose a methodology for the resilience management system.

Taxonomy of Dependability and Resilience

To systematize the elements of the "resilience" concept the results described in [12] are used, which proposed a unified taxonomic scheme of dependability and resilience. Its elements are:

– threats F (faults, errors and failures, vulnerabilities and interferences),

– protection against threats mechanisms T (fault-tolerance and fault-safety),

– primary P_1 and secondary P_2 properties.

Physical faults or *malfunctions of hardware* (physical fault, f_p) lead to violations or errors of the computational process (error, e_p) which determine the

corresponding event for the system - *failure* or *denial* (failure, F_p) and the transition to inoperable (partially inoperable) state, that is, there is a pathological chain $f_p \rightarrow e_p \rightarrow F_p$.

Similar chains exist for *design faults* (design fault, f_d) and *interaction faults* (interaction fault, $f_a = \{f_{ap}, f_{ai}\}$ due to physical (f_{ap}) and *informational* (f_{ai}) *influences*, i.e.: $f_d \rightarrow e_d \rightarrow F_d$, $f_a \rightarrow e_a \rightarrow F_a$ ($f_{ap} \rightarrow e_{ap} \rightarrow F_{ap}$ and/or $f_{ai} \rightarrow e_{ai} \rightarrow F_{ai}$).

Based on these f-e-F chains, a special notation can be built to analyze events and model the behavior of a computer system. It is a modification of Occurrence Nets (Causal Nets or Occurrence Graphs) and was proposed for physical and design failures and is called Structured Occurrence Nets.[13] In addition to faults and the failures caused by them, there are other challenges associated with evolutionary factors:

– changes in system requirements (functional $\{r_{fq}\}$, q = 1..nf and/or functional requirements, in particular, the requirements for the dependability components $\{r_{cw}\}$, w = 1..nd), which must be implemented by the system;
– changes in environmental parameters $\{r_{ej}\}$, j = 1..ne, which must be considered.

The set R, which unites the sets $\{r_{fq}\}\{r_{cw}\}\{r_{ej}\}$, will be called evolutionary factors:

$$R = \{r_{fq}\} \cup \{r_{cw}\} \cup \{r_{ej}\}$$

Same to f-e-F-chains it is possible to construct an appropriate sequence for evolutionary factors or *evolutionary chains*. Due to the emergence of a new (change) requirement $r_h \in R$, the system undergoes an unspecified change of information according to the previous states (let it be called *an evolutionary error*, u) and the system will go into an unspecified state (this state can be considered as an *evolutionary failure*, D). Accordingly, having r-u-D-chains, which describe the behavior of the system in terms of evolution: rf → uf → Df, rc → uc → Dc, re → ue → De.

Thus, in the general case, three pairs of sets should be considered:

- fr = {f,r},
- eu = {e,u},
- FD = {F,D} and sequence fr → eu → FD.

In [12] it is proposed to call the mechanism of adaptation to such changes as *R-stability*, and the system in which it is implemented as *R-system*. Due to this mechanism, there is the primary property of evolution or *"evolvability"* and the system that has such a property, i.e. *"evolvable system"* or *"evolving system"*. Based on the accepted definitions of concepts related to resilience, it is possible to move to the formation of *the architecture of the functional model of the R-system*, taking into account the possibility of its evolution under the influence of environmental factors.

The question arises, to which class of control systems should R-systems be attributed? Preliminary analysis has shown that it is advisable to apply the theory of cybernetic systems, which takes into account various environmental factors and provides the possibility of its evolution.

Aim and Structure

The aim of the work is to develop a concept of R-system formation based on a cybernetic approach.

Structurally, the work consists of two sections: the first is devoted to substantiating the possibility of applying a cybernetic approach to the development and description of models of the R-system; the second is to present a practical case of the application of the cybernetic model for space control system with online verification. [14,15]

Cybernetic Approach to Developing a Resilience Control System

Cybernetic Approach to the R-system Models Development Rationale

The architecture of a cybersecurity management system, which should provide resilience, should have redundant components compared to a traditional feedback management system. This is primarily due to the need to implement additional channels in the control system to respond to changes in requirements, environment or unspecified faults and failures.

Taking into account the three change factors requires the implementation of additional design solutions in the architecture of the control system. In the simplest case, this can be done through three additional channels that work separately from each other. Fig.1 shows three circuits of system (Syst) resilience control, respectively, when changing system requirements ΔReq, changing environment parameters ΔEnv and changing system failures ΔFail by use of corresponding analysers.

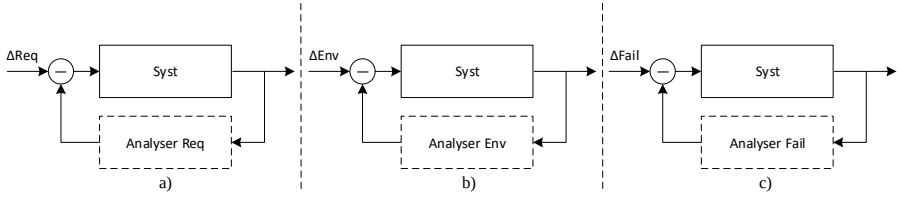

Figure 1: Circuit models of the resilience management system: when changing the requirements for the system (a), when changing the parameters of the environment (b), when changing the failures of the system (c).

Each of the defined circuits of the control system based on the control law by negative feedback provides stabilization of the information system parameters. With this approach, each of the channels operates independently. In real cybernetic systems, certain channels interact with each other. This should be reflected in the form of additional connections between the circuits, or it requires

the construction of an integrated system. An additional complicating factor is the requirements for the control system to implement support and functional and non-functional characteristics provision of the cybernetic system.

To form an integrated architecture of the system model, the methodology of a holistic approach to the formation of cybernetic (intelligent) systems was chosen according to [16]. This approach previses the selection of two parts of the cybernetic system, namely:

– first part – block "Functional characteristics", which displays the model (project) of the system;

– second part – block "Non-functional characteristics", which displays the real system and its parameters.

The purpose of control is to ensure compliance of the design parameters of the system with the real parameters under changed environmental conditions. To do this, the purpose, goal and functions of the system are adjusted.

The structure of the Resilience Control System

For the practical implementation of the approach to building a model of an integrated cybersecurity management system, an integrated cybersecurity control system of the information system is proposed (Fig. 2). In such a system, the cybersecurity property is regulated in the event of a change in the information component of the environment, for example, as a result of attacks on it.

In Fig.2. the structure of the resilience management system using the proposed cybernetic approach is given.

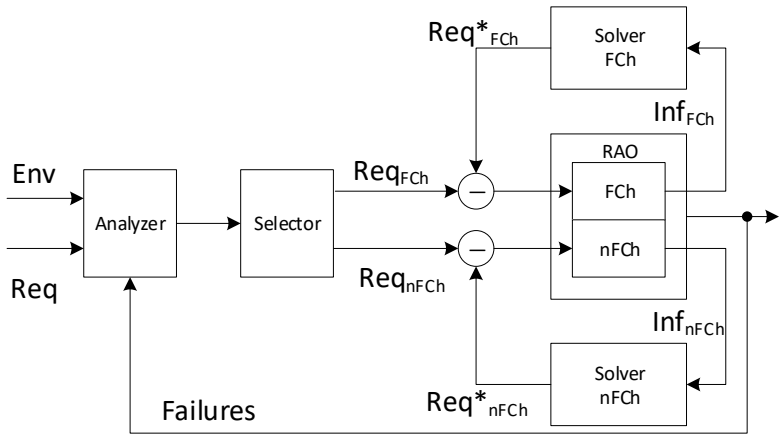

Figure 2: Integrated cybersecurity control system of the information system structure: FCh – Functional Characteristic, nFCh – non - Functional Characteristic, RAO – Resilience assurance object.

This system works as follows. When changing the parameters of the external environment (Env), and / or changing the system requirements (Req) and / or the occurrence of failures (Failures) in the block "Analyzer" the recognition and analysis of changes is held. After that, the corresponding control signals Req_{FCh} and Req_{nFCh} are generated in the "Selector" block, respectively, for functional and non-functional characteristics. These signals are transmitted through the adders to the subsystems FCh and nFCh Resilience assurance object. From the outputs of these subsystems, the parameters that characterize the state of resilience Inf_{FCh} and Inf_{nFCh}, come to the decisive devices "Solver". They generate signals based on the control law with negative feedback Req^*_{FCh} and Req^*_{nFCh}. Stabilizing signals are formed in the adders.

Therefore, the application of a cybernetic approach to modeling the R-system provides the ability to manage resilience in the face of changing requirements, environmental parameters and the accumulation of failures.

Application of the Cybernetic Approach for Resilience Assurance of Space System

Space Computer Control System with Online Verification

Space computer control system (SCCS) consists of on-board (BCS) and ground (GCS) subsystems. This allows, using a telecommunications channel to perform additional functions in automatic flight mode, in particular, online verification, because on Earth it is difficult and expensive (and sometimes impossible) to reproduce all the conditions of outer space, as well as the need to adjust (modify and reengineer) software during operation process. Currently, most composite manned space complexes have the possibility of hardware repair.

Such modifications can be considered as a reaction of the control unit of the cybernetic system to changes in R, and the set R can be interpreted as re - changes in the environment (sudden bursts of electromagnetic radiation, collisions with meteors, loss of landmarks, etc.) and changes due to faults rd - (manifestation of undetected design faults, hardware and parts of the code stored on the carrier damage, etc.). There is currently no confirmed information on the failure of composite space complexes due to interception of control channels in open sources, so the components of changes in F_{ai} and F_{ap} in this study are neglected, but they can be taken into account in the future.

The use of software with the ability to modify it allows more flexible distribution of verification steps. Thus, a number of non-critical software functions can be quickly verified after the launch of the spacecraft during its operation. After conducting online verification (OV) procedures, measures can be taken to eliminate the identified drawbacks and faults (corrective online verification, COV).[14,15] The ability to verify software and correct software code changes the structure of the SCCS hardware channel, as shown in Fig. 3.

Modern complexes provide the mandatory presence of a communication channel with GCS, in which the decision is made to correct the program code. From the terrestrial complex the initiating commands to start the verification

procedures come, which are performed by a special block of input data processing and decision-making (cancellation block).

Test sets for verification are stored in the block of online verification, in the same block preliminary processing of tests performance results in the main BCS information processing channel is carried out. If a failed section of the program code is detected, information about it is sent to the GCS, where a decision is made to eliminate the detected fault(s) and a section (module) of the replacement program code is formed, which is transmitted to the unit of corrective modules.

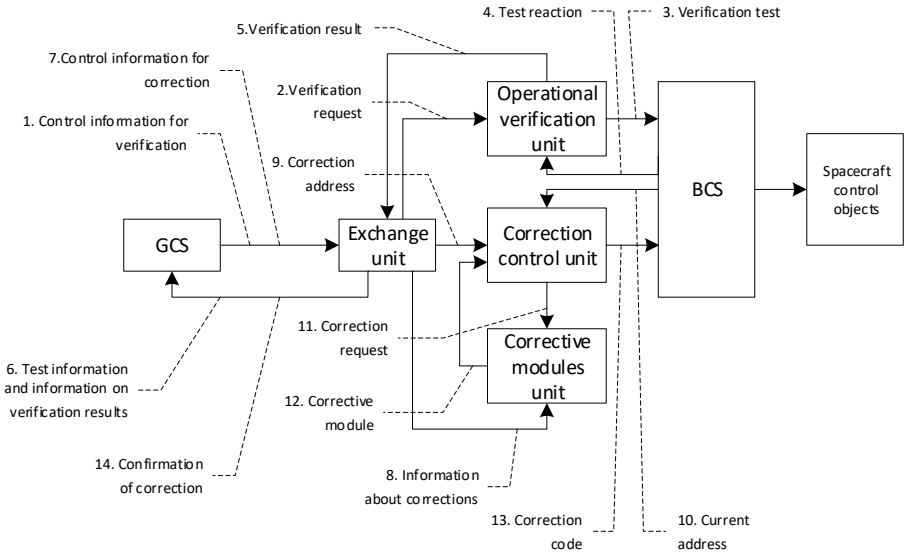

Figure 3: Dual-circuit cybernetic information and control system of the spacecraft with online verification and correction of software.

Next, in the correction control unit based on the information about the program code executable element current address the interception of control from the main information processing channel and the replacement of the failed section with the adjusted program code from the block of correction modules is held.

It should be noted that this construction of the cybernetic system involves its operation through direct connections between control channels ΔR, ΔE and ΔF. There is more detailed consideration. Changing the parameters of the environment (detected, in particular, during OV procedures) requires a response from the control unit (GCS), the reaction to ΔE is a change in the requirements for the spacecraft (change course, mode of operation of devices, folding batteries, switching to "sleep mode"). If such "reactions" are not provided for in the regular schedule, then GCS gives a command to correct the code responsible for

the operating modes of the spacecraft. This happens provided, if ΔE hasn't caused any new faults (ΔF). The purpose of such management measures is to preserve the working condition (rc→0).

In the case when the change of environmental parameters caused the appearance of new faults ΔF and changes in dependability indicators rc, GCS decides either to correct or "parry" new faults, or even to disable faulty areas, i.e. partial degradation of spacecraft functions (chain re→rf) again to maintain a working condition (rc→0). However, in case of significant damage, the GCS may change the dependability requirements (ΔR) to save unloaded spacecraft units operation modes.

Scenarios of Online Verification for Resilience Control System

Different scenarios can be used for OV and COV, as the conditions for online verification conducting may be the impossibility of reproducing space parameters in terrestrial conditions, the high cost of such simulation, short design terms or other limitations.

As an example, three typical scenarios and their mapping for the proposed architecture of the resilience management system model are considered.

Scenario 1. In-flight verification of non-critical functions of the system is performed (Fig. 4). Verification of these functions in terrestrial conditions was not carried out due to short design terms. This scenario does not take into account non-critical non-functional requirements.

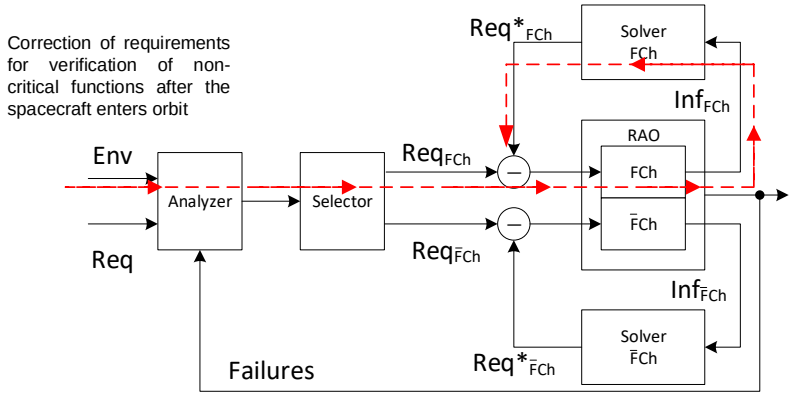

Figure 4: Scenario 1. Online re-verification of non-critical functions.

Scenario 2. Carrying out of online verification after elimination of the faults detected during flight.

Scenario 3. During the flight, verification of all functions that cannot be verified in terrestrial conditions is performed. In this scenario, the environment parameters are refined and the results are used to eliminate the detected faults.

Markov's Model of a Resilient System

Development of the BCS Model

Appropriate models need to be developed to assess resilience and other indicators depending on the OV and COV scenarios. The model of resilience BCS, taking into account the failures of hardware and software for the possibility of correction of software modules are considered. The change in failure rate λ_{SW} after COV procedures is taken into account using the apparatus of regular multi-fragment Markov models (RMFM).[15] To build the BCS resilience model, the following assumptions are made:

- resilience BCS at any time can be either operational or inoperable, and the flow of events that transfer the system from one functional state to another are the simplest (simultaneous failure of hardware and software channels is not simulated);
- in the resilience BCS process of online verification of program functions is performed, the state of verification is inoperable;
- no new faults are made during changes to the program code.

The marked Markov graph of the resilience BCS model (Model 1) for the first OV scenario is shown in Fig.5.

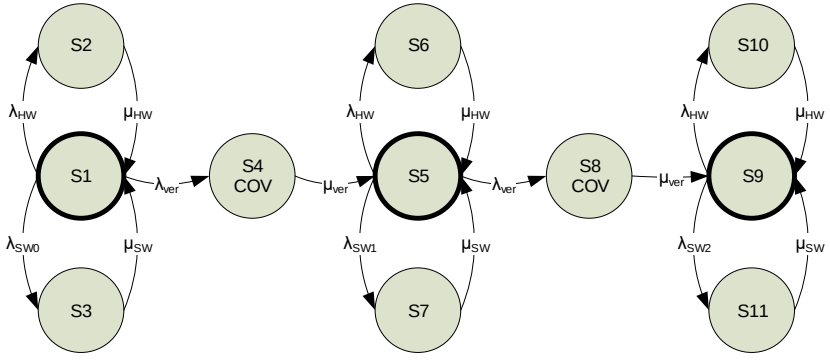

Figure 5: The marked graph of resilience BCS model functioning at carrying out online verification of noncritical functions.

The process of functioning of resilience BCS is held as follows. At the initial moment, the system implements all the planned functions and is in state S1. In the operation process, hardware faults appear, as a result of which the system goes into state S2 with rate λ_{HW} and is restored (the system returns to state S1 with rate μ_{HW}). After a certain time interval, the system fails due to a software fault, and it goes into state S3 with rate $\lambda_{SW\,0}$. After the manifestation of the software fault, the system is restored and returns to state S1 with rate μ_{SW}. After a certain period of time determined by the parameter λ_{ver}, a verification of noncritical functions, which did not have time to verify on Earth due to time constraints of the project is held. The system enters state S4 (inoperable). After the

COV procedures, the system moves to a new fragment of the model (state S5 with rate μ_{ver}), which is characterized by a change in the intensity $\lambda_{SW\,i} = \lambda_{SW\,0} - i*\Delta\lambda_{SW}$.

Using the same approach Markov graphs for second and third scenarios are developed and researched as well (Models 2 and 3, in this article is not considered).

Research of the BCS model

The input parameters values of the BCS model shown in Table 1. Consideration of the methods for calculating input parameters is given in [14,15] and is beyond the scope of current study.

Table 1. Resilience indicator assessment model parameter values.

#	Parameter	Value for Model 1
1	λ_{HW} (1/hours)	**3,00E-05**
2	μ_{HW} (1/hours)	**0,00297619**
3	$\lambda_{SW\,0}$ (1/hours)	**4,00E-04**
4	μ_{SW} (1/hours)	**0,2**
5	$\Delta\lambda_{SW}$ (1/hours)	2,00E-06
6	λ_{ver} (1/hours)	0,010416667
7	μ_{ver} (1/hours)	0,25
8	N_{ver}	20…100

The deviation of the availability function from the stationary value was chosen as the resilience metric. The essence of measuring the indicator is illustrated in Fig.6. As a model of the system without COV, a single-fragment hardware/software model (SFM) with the values of the input parameters is selected, which are bold in Table 1.

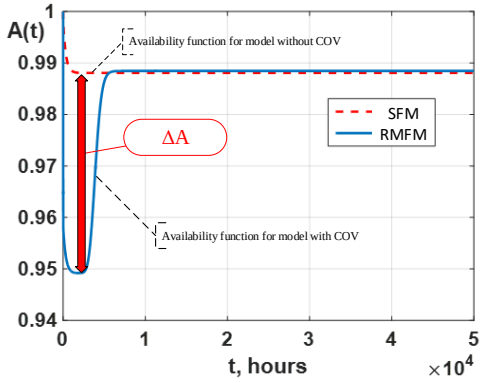

Figure 6: Explanation of the resilience metrics ΔA choice.

Figure 7 shows the of COV model in scenario 1 study results. When transferring the verification procedures to the post-launch period of the spacecraft operation, there is a decrease in the availability of the system at the initial stage of operation. With the increase in the volume of verification (N_{ver}), there is a nonlinear growth of the indicator ΔA.

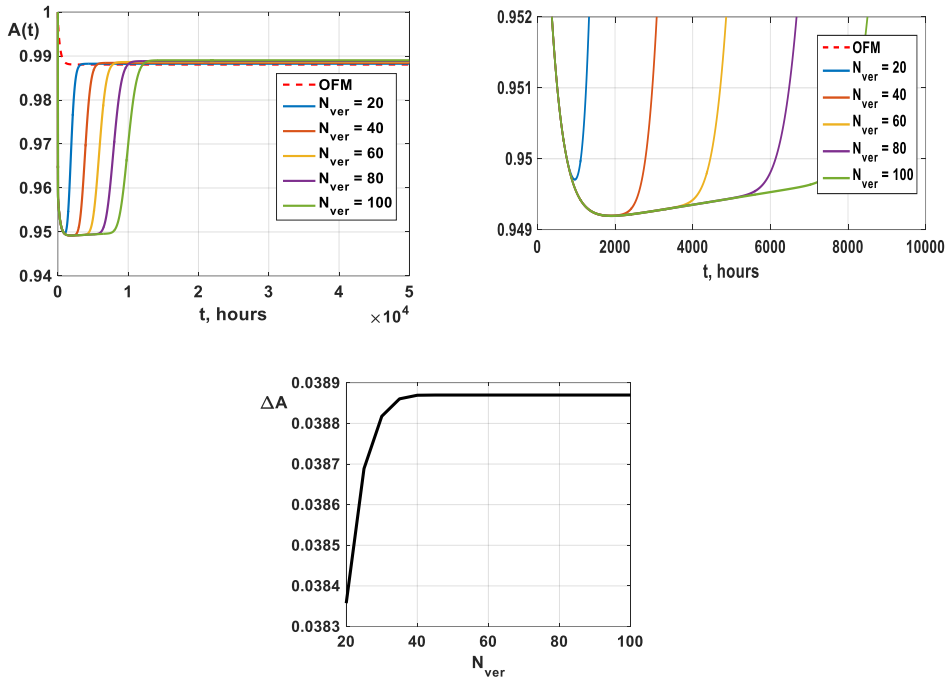

Figure 7: The results of modelling the COV according to the scenario 1 (verification of non-critical functions after start of the spacecraft).

Some results of research of the developed models are the following:

- with an increase in the number of functions that need to be verification in 5 times, the resilience index ΔA increases by 1.3 %;
- with an increase in the intensity of COV procedures to refine the parameters of the environment in 3 times, the resilience index ΔA increases by 85.7 % (this is an additional study, it is not illustrated in Fig. 7).

To improve resilience through COV procedures, it is necessary to reduce the duration of their implementation, or to implement them without complete loss of operability of the main functions of the system.

Conclusions

The suggested cybernetic approach to building of resilience control system is based on considering changing requirements, environment parameters and failures specification. It allows developing of resilient systems as a cybernetic system. This approach has been implemented for a few industrial systems. More detailed case for space control systems has been analysed.

The future steps can be connected with application of cybernetic approach and models for:

- industrial resilience assurance considering integrated cybersecurity and safety management systems for enterprises in frameworks of Industry 4.0 based on combining IT, OT and ET levels of information security, functional and ecological safety;[17]
- improving of smart building automation systems (BAS) resilience taking into account strategies of combine and separate maintenance considering a set of politics of BAS reliability and cybersecurity assurance during operation.

Acknowledgments

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

The authors very appreciated to scientific society of consortium and in particular the staff of Department of Computer Systems, Networks and Cybersecurity of National aerospace university "Kharkiv Aviation Institute" for invaluable inspiration, hardworking and creative analysis during the preparation of this paper.

References

1 National Institute of Standards and Technology, "Managing Information Security Risk: Organization, Mission, and Information System View," Special Publication 800-39, 2011, https://doi.org/10.6028/nist.sp.800-39.

2 National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," Special Publication 800-53, 2013, https://doi.org/10.6028/nist.sp.800-53r4.

3 National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," Special Publication 800-53, 2013, https://doi.org/10.6028/nist.sp.800-53r4.

4 National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," Special Publication 800-30, 2012, https://doi.org/10.6028/nist.sp.800-30r1.

5 National Institute of Standards and Technology, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," Special Publication 800-37, 2018, https://doi.org/10.6028/nist.sp.800-37r2.

[6] "ASIS SPC.1-2009 - Organizational Resilience: Security, Preparedness, And Continuity Management Systems - Requirements with Guidance for Use," *Webstore.ANSI.Org*, 2009, https://webstore.ansi.org/standards/asis/asisspc2009.

[7] Committee on National Security Systems, "Committee on National Security Systems (CNSS) Glossary," CNSSI, no. 4009, April 6, 2015, https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf.

[8] "Resilience," Glossary, CSRC, *Csrc.Nist.Gov,* Accessed 22 June 2020, https://csrc.nist.gov/glossary/term/resilience/.

[9] Michael Hogan and Elaine Newton, "Supplemental Information for the 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.ir.8074v2.

[10] Nicolas Guelfi, "A Formal Framework for Dependability and Resilience from A Software Engineering Perspective," *Open Computer Science*, no. 3 (2011): 294-328, https://doi.org/10.2478/s13537-011-0025-x.

[11] Deborah Bodeau, Richard Graubart, Rosalie McQuaid, and John Woodill Jr., "Cyber Resiliency Metrics and Scoring in Practice--Use Case Methodology and Examples," The MITRE Corporation, 2018, https://www.mitre.org/publications/technical-papers/cyber-resiliency-metrics-and-scoring-in-practice-use-case-methodology.

[12] Vyacheslav Kharchenko, "Dependable systems and multi-version computing: aspects of evolution," *Radioelectronic and computer systems*, no. 7 (2009): 46-59 (in Ukrainian), http://nbuv.gov.ua/UJRN/recs_2009_7_9.

[13] Maciej Koutny and Brian Randell, "Structured Occurrence Nets: A Formalism for Aiding System Failure Prevention and Analysis Techniques," *Fundamenta Informaticae* 97, no. 1-2 (2009): 41-91, https://doi.org/10.3233/fi-2009-192.

[14] Vyacheslav Kharchenko, Yuriy Ponochovnyi, Artem Boyarchuk, and Eugene Brezhnev, "Resilience Assurance for Software-Based Space Systems with Online Patching: Two Cases," *Dependability Engineering and Complex Systems* 470 (2016): 267-278, https://doi.org/10.1007/978-3-319-39639-2_23.

[15] Vyacheslav Kharchenko, Yuriy Ponochovnyi, and Artem Boyarchuk, "Availability Assessment of Information and Control Systems with Online Software Update and Verification," *Information and Communication Technologies in Education, Research, and Industrial Applications* 469 (2014): 300-324, https://doi.org/10.1007/978-3-319-13206-8_15.

[16] Sergiy Dotsenko, "Principle of the total organization of intellectual systems," *Radioelectronic and computer systems* no. 1 (2019): 4-16. (In Ukrainian). https://doi.org/10.32620/reks.2019.1.01.

[17] Sergiy Dotsenko, Oleg Illiashenko, Sergii Kamenskyi, and Vyacheslav Kharchenko, "Integrated Security Management System for Enterprises in Industry 4.0," *Information & Security: An International Journal* 43, no. 3 (2019): 294-304, https://doi.org/10.11610/isij.4322.

About the Authors

Prof. Vyacheslav **Kharchenko**, Doctor of technical science, is head of the department of computer systems, networks and cybersecurity, National aerospace university "Kharkiv Aviation Institute," Kharkiv, Ukraine, and Head of the Centre for safety infrastructure research and analysis, RPC Radiy. His research interests are in fundamentals and methods of critical computing, safety and security IT-engineering, technologies of regulation, development, assessment of dependable software and systems.

Sergiy **Dotsenko**, Doctor of technical sciences, is associate professor in the department of specialized computer systems at Ukrainian State University of Railway Transport, Kharkiv, Ukraine. His research interests are in models, methods and instrumentation tools for cybersecurity assessment, safety and cybersecurity co-engineering, dependability and resilience of embedded, web, cloud and IoT systems.

Yuriy **Ponochovnyi**, PhD, is associate professor in the department of information systems and technologies, Poltava State Agrarian Academy, Poltava, Ukraine. His research interests are related to models, methods and tools for assessing and ensuring the dependability of information & control systems, its hardware and software in the context of reliability, safety and cybersecurity; development of separate and mixed maintenance strategies of these systems.

Oleg **Illiashenko**, PhD, is associate professor in the department of computer systems, networks and cybersecurity, National aerospace university "Kharkov Aviation Institute," Kharkov, Ukraine. His research interests are in models, methods and instrumentation tools for cybersecurity assessment, evaluation and assurance of cybersecurity of software and hardware, safety and cybersecurity co-engineering, dependability and resilience of embedded, web, cloud and IoT systems.