Homeostatic approach to assessing digital manufacturing security[a]

Evgeny Pavlenko[1*] and *Dmitry* Zegzhda[1]

[1] Peter the Great Saint Petersburg Polytechnic University, Institute of Computer Science and Technology, 195251, Politechnicheskaya st., 29, Russian Federation

Abstract. This study suggests a new digital manufacturing security paradigm based on the bio-inspired homeostasis concept to provide structural and functional cyber resilience of digital manufacturing to external destructive actions. Digital manufacturing management state indices, in particular, cyber resilience indices, have been determined. Possible approaches to calculating indices of consistency of the information layer with the physical layer, self-adaptation capability, self-similarity of performance parameters and homeostatic capability have been formulated. The analysis of the suggested approach to ensuring cyber resilience of digital manufacturing has been carried out using the software-configurable network technology. The experimental results have demonstrated the effectiveness of the suggested approach. The developed homeostatic approach lays the groundwork for building a proactive security strategy due to development of predictive methods of processing the system status monitoring results.

1 Introduction

The analysis of modern science and technology development tendencies demonstrates that world industry is currently on the threshold of the forth technological revolution which means the adoption of completely automated digital manufacturing controlled by intelligent systems on a real-time basis, constantly interacting with the external environment, implying the prospect of uniting into a global industrial network of things and services.

Digitalization of life-building branches of activity has triggered appearance of a new type of entities and systems – cyber-physical entities and systems associated with manufacturing processes and having an informational control circuit constructed using sophisticated computer technologies.

Cyber-physical systems (CPS) are multi-component distributed systems which function independently of human being and monitor areas which are vital for the population. Such systems combine information modules with physical process implementation modules [1]. The CPS includes a set of interrelated physical components implementing a manufacturing process; information components controlling the process at different layers of automation;

[a] The work was funded by the Russian Federation Presidential grants for support of leading scientific schools (NSh-2992.2018.9), Contract No. 14.Y31.18.2992-NSh. January 17, 2018
[*] Corresponding author: pavlenko@ibks.spbstu.ru

and a communication environment providing information exchange within the system and with the external environment and transmitting control commands to actuating mechanisms.

Tight integration of the CPS with manufacturing processes associated with industrial manufacturing and management of a large number of complex objects capable of changing their behavior resulted in the necessity of modifying the existing security paradigm for digital manufacturing. This is due to the fact that direct transfer of information security concepts, such as confidentiality, availability and integrity, is impossible in digital manufacturing because in contrast to informational processes, physical processes are irreversible and cannot be monitored and control at the same layer as informational processes [2]. Therewith, the concept of availability as sustainability of manufacturing processes comes into the forefront.

With regard to a CPS for digital manufacturing, control over the system is the main target of an intruder rather than obtaining data on the operations being carried out. A digital manufacturing security paradigm should be based on new security principles which have to be invariant to attack mechanisms because the components of digital manufacturing are heterogeneous, digital manufacturing standardization is impossible in the foreseeable future and technologies are being actively developed and modified.

After being introduced into manufacturing, computer technologies have added one more requirement to digital manufacturing system security that is system control resilience to targeted external actions. Probability of such adverse actions is an inherent peculiarity of the modern architectural and algorithmic platform of computer systems which is proved by current practice. In general, adverse actions may occur on both the information layer and the physical layer. A system's ability to function within the pre-determined input and output characteristics despite of targeted external information actions is defined as cyber resilience [2].

2 Researches on CPS sustainability and reliability control

A large number of researches on sustainability and reliability control of digital manufacturing and CPS is known.

The publication [3] addresses the problem of assessing electric network intelligent system efficiency and reliability in case of cascade failure. To solve the problem, the authors calculate stability (sustainability) of the network at different load levels based on the estimated length of the transient state graph.

This approach is oriented on high-voltage networks; equipment reliability and uncertainty of external disturbances affecting system performance are not taken into account. The said approach cannot be applied to assessing resilience and stability of cyber-physical systems because a large number of uncertain external disturbances are characteristic of cyber-physical systems. Moreover, the structure of an electric network is static, and that cannot be applied to most cyber-physical systems a priori.

The research paper [4] is focused on maintaining stability of cyber-physical systems, in particular, maintaining stability of both the information component (computer network) and the physical component at the same time. The mathematical apparatus used in the research is represented by planning invariants and system physical state invariants which together allow maintaining system stability. The authors developed an adaptive algorithm to plan capacity migration between smart grid nodes.

Applying the approach requires complex mathematical models of a cyber-physical system to take into account, particularly, possible component dynamics and migration, that involves immense time expenditures and depends heavily on the type of a cyber-physical system and its operation conditions. The mathematical apparatus of invariants implies a long-term manual derivation of invariants and a vast object-oriented knowledge of the system. Moreover, invariants are obtained for particular expected physical relationships and they do

not include implicit internal relations between system components. Thus, the said approach is not effective enough for controlling sustainability of cyber-physical systems.

The publication [5] introduces the concept of stability for determining reliability of cyber-physical systems. This approach is oriented on providing reliability of cyber-physical system and aimed at ensuring control stability. However, it is focused on controlling the physical component of cyber-physical systems only and does not consider the possibility of system security violation by information actions. Thus, the said approach cannot be applied to resist security threats to cyber-physical systems.

It may be concluded that researches on providing cyber resilience of digital manufacturing are focused on ensuring proper CPS performance only, but the problem of information component security assurance and integration is not addressed.

3 Researches on developing approaches to digital manufacturing self-regulation and self-adaptation

The homeostatic approach to assuring CPS security consists in self-adaptation of the system when destructive actions occur.

The study [6] suggests an approach to adaptation of complex systems at the architectural level based on formal determination of limitations of the system architecture, architecture elements and supported adaptation operations.

Firstly, the said approach requires preliminary time-consuming work on preparing formal description of the system which is not always possible for large-scale cyber-physical systems. Secondly, it is aimed at determining such adaptation strategies which would transfer the system from an invalid state to a state meeting the architectural requirements.

Hence, the said approach cannot be applied to cyber-physical systems, because it considers structural and functional system properties, but does not take into account the system's target function which is a crucial factor for cyber-physical systems.

The research [7] is focused on performance check of self-adaptive systems and aimed at solving the problem of system efficiency and reliability assurance in case of self-adaptation. The said approach includes a model check of system behavior at the design stage, model-based testing at the design stage and post-adaptation diagnostics during operation.

However, it cannot solve the problem of self-adaptation assurance in cyber-physical systems. The said approach requires development of a formal model which is a time-consuming task in case of large-scale cyber-physical systems. In addition, a formal model may be used only to describe the target function of the system and limitations on operations implemented in the system.

Moreover, adaptation correctness diagnostics during operation of a cyber-physical system involves a considerable hazard if errors occur during adaptation. Incorrect functioning of cyber-physical systems may cause a significant financial loss and even harm to human health and environment.

Therefore, the said approach is not focused on security, but it is aimed at controlling the system performance and it does not solve the problem of self-adaptation of cyber-physical systems.

The research [8] suggests a model of an adaptive system as a multi-agent structure where the main role belongs to agents, i.e. autonomous entities located in the environment.

The said research is aimed at formulation of an approach to developing self-adaptive systems with well-defined and undefined requirements to self-adaptation.

The approach cannot be applied to cyber-physical systems because it does not consider that adaptation is necessary for not only the structure, but the content as well. Moreover, development of agents, effective sharing of tasks and functions between them and their integration into the system are very time-consuming and system-specific tasks.

However, self-adaptation must ensure correctness of both performance and the control data flow. The majority of researches associated with assurance of self-regulation and self-adaptation of digital manufacturing are aimed at maintaining system performance ability, and the information component is ignored.

4 Researches on homeostasis in digital manufacturing

The existing studies suggesting application of the concept of homeostasis to technical systems are connected to the theory of control of complex systems.

The research paper [9] considers homeostasis as an ability of cyber-physical systems to self-adapt, i.e. maintain their operational condition in case of any disruptions. The suggested approach is aimed at assuring CPS sustainability by modifying the system's architecture based on pre-defined self-adaptation strategies. The approach is initially oriented on assurance of correct system operation rather than assurance of cyber security. However, it may be partially applied to building a new cyber security paradigm.

The research [10] further develops the study [9] and suggests a formal model to ensure reliable operation of the system by simultaneous control of system requirements, possible system configurations and the state of the environment. The suggested model and a self-adaptation method to implement it allow for modifications in the system architecture during manufacturing processes.

It should be noted that all researches on CPS self-adaptation are oriented on maintaining correct CPS performance and ignore the information component that is why the homeostatic approach has never been applied to cyber security issues.

However, there are studies which include attempts to formulate key features of CPS control systems to response to attacks. In the research paper [11], redundancy is identified as a CPS characteristic to response to denial-of-service attacks. The above mentioned approach may be used for the purpose of implementation of the homeostatic approach to assure CPS security.

The prospects of applying the homeostatic approach suggested herein are substantiated by the fact that it will simultaneously assure both information security and functional/process security consisting in maintaining correct CPS performance in case of destructive actions.

5 Self-similarity as a criterion of digital manufacturing sustainability

Sustainability of a cyber-physical system may be identified by assessing the capability of the system to stay in a stable state [2], and such assessment must be carried out for the entire system, not just for its separate elements. In this case, cyber-physical system sustainability indices are applied as set forth in [12]. Self-similarity of a system is determined using the fractal method based on the Hurst coefficient (1) and the Fano factor (2).

$$H = 1 - \frac{\beta}{2} \tag{1}$$

$$\Phi(n) = \frac{\delta^2(n)}{m(n)} \tag{2}$$

Self-similarity is applicable to assessing sustainability of cyber-physical systems which enable functioning of digital manufacturing due to the fact that the key feature of such cyber-physical systems is periodicity of manufacturing processes to be carried out. Periodicity is

explained by a target function of each cyber-physical manufacturing system which is implemented when digital manufacturing components implement a finite set of functions transferring the digital manufacturing into different states, the aggregate of which is finite and, possibly, countable.

Periodicity of manufacturing processes implemented by transferring the control flow of commands and messages between digital manufacturing components suggests stationarity of manufacturing processes. According to [13], this means that statistical properties of a process do not change in time, so its characteristics are invariant with respect to time shifts. Invariance of characteristics allows suggesting that the manufacturing process under study have a property of fractality or self-similarity.

Assessment of self-similarity of digital manufacturing is so important because it is self-similarity which is able to comprehensively characterize manufacturing performance both on the layer of information flows and at the physical layer where its components function. Any cyber security violation aimed at illegitimate modification of control data flow, disruption of communication channels between digital manufacturing components, or its particular components will be reflected in the data flow because digital manufacturing is managed by the information component. Therefore, cyber threats may be effectively monitored due to assessment of self-similarity of time series characterizing the control data flow during the manufacturing process.

6 Concept of homeostatic control and self-similarity assessment of digital manufacturing

Due to the need to simultaneously assure both information and process security, a common mechanism has to be developed to control and maintain cyber resilience of the entire digital manufacturing; such cyber resilience meaning resilience to circulating information and its functioning. Hence, it is necessary to consider the capability of digital manufacturing to self-adaptation.

The ability of a system to self-adaptation is defined by cross-correlational relationships within the system which are defined as (3),

$$r(t,\tau) = E[c_n^T(t+\tau)X(t)] \tag{3}$$

the system's controllability (4),

$$CT_p(t) = \begin{cases} \dfrac{\sum_{i=1}^{N} path\_num\_t_i}{\sum_{i=1}^{N} path\_num_i}, если \sum_{i=1}^{N} path\_num_i > 0 \\ 0, если \sum_{i=1}^{N} path\_num_i = 0 \end{cases} \tag{4}$$

constancy of performance (5)

$$Op = \frac{\partial \operatorname{Re} s_{sp}}{\partial t} \tag{5}$$

and the degree of scalability of the system (6).

$$S_c[k,n] = (\Delta CT(t), \Delta R_{\max}, \Delta O_p, \Delta T) \quad (6)$$

The use of sustainability and self-adaptation assessment in the context of CPS specifics results in a modification of the concept of digital manufacturing system security management. In view of the above mentioned features, we believe that arrangements for digital manufacturing security should be classified as dynamic systems, the security policy must provide for:

– maintenance of the manufacturing process according to the pre-defined dynamics in case of destructive actions;

– maintenance of correct addressing of the control data flow;

– ability to adapt digital manufacturing parameters and structure to response external and internal destructive actions and maintain sustainability of the manufacturing process;

– in prospect, in view of intellectualization of certain digital manufacturing components, maintenance of the ability to analyze the state of the environment and the digital manufacturing in order to decide on proactive adaptation of the digital manufacturing to external attacks by way of anticipation and reasoning ability when choosing an adaptation strategy.

The concept of homeostatic control better corresponds to the above listed requirements to ensure cyber resilience. Homeostatic control is a bio-inspired concept of managing intelligent technical systems and consists of provision of a relational balance of the system maintained by self-regulation mechanisms. Homeostasis implies a combination of mechanisms which ensure constancy of the system's internal environment and its structural and functional resilience to external destructive actions [12].

By analogy with biological systems, three homeostasis layers are defined in digital manufacturing:

1. Homeostasis at the layer of parametric control of manufacturing processes.
2. Homeostasis at the layer of control of the relationships between digital manufacturing components.
3. Architectural homeostasis to completely readjust digital manufacturing: control parameters and relationships between components.

A distinctive feature of the homeostatic approach to security management is that digital manufacturing is controlled by two independent systems having opposite purposes, thus, a homeostat is a mechanism of contradiction management. As any conflict, such contradiction is twofold: on the one hand, it is a threat of loss of stability, on the other hand, in case of self-regulation; it is a tool to develop behavior strategies for self-improvement of the system by modifying its structure. The range of permissible structural variations within which the system remains tolerant to external actions includes space for permissible strategies of managerial decisions to maintain dynamic sustainability of the entire system. To implement homeostatic control, a system must be redundant to some extent and have a well-developed structure defining the limits within which structural variations in the system are permissible without the permissible loss of functionality. The specific feature of the homeostatic approach is impossibility to control the external circuit (an intruder) while the intruder may control digital manufacturing due to errors in the digital manufacturing security subsystem. Thus, the homeostatic paradigm in assuring security differs from the adaptive strategy by the ability to solve the problems of Pareto optimization i.e. find areas of best possible solutions to maintain the criteria of security and functionality within pre-defined limits.

7 Approaches to assessing digital manufacturing sustainability

When developing approaches to assessing self-similarity and sustainability, the type of digital manufacturing must be take into consideration since types of digital manufacturing vary much and, consequently, have key differences with regard to functioning organization.

The source [12] includes the CPS systematization which allows distinguishing five main types of digital manufacturing:

1. The Internet of Things is a network of physical entities united by embedded technologies to communicate, response and interact within themselves and with the external environment, independently of humans
2. Multi-agent systems (MAS) are systems built by several interacting intelligent agents and the industrial Internet of Things
3. Computer-aided manufacturing (CAM)
4. Moving object systems (VANET – Vehicular Ad Hoc Networks, FANET – Flying Ad Hoc Networks)
5. Robot intelligent systems.

For the above listed types of digital manufacturing, the source [14] also suggests cyber resilience assessment indices which characterize consistency of the information layer with the physical one, self-adaptation capability, self-similarity of performance parameters, and homeostatic capability.

The information-and-physical-layer consistency index is suitable for all types of digital manufacturing and can be calculated using the coefficient of concordance in dynamics (7).

$$k_S = \frac{\sum_i \bar{\Delta}^i y \bar{\Delta}^i x}{\sqrt{\sum_i (\bar{\Delta}^i y)^2 \sum_i (\bar{\Delta}^i x)^2}} \tag{7}$$

The self-similarity index of digital manufacturing CPS functional parameters may also be applied to all types of digital manufacturing. It is calculated based on the Hurst coefficient (1) and the Fano factor (2).

The homeostatic capability index of the system for the simplest digital manufacturing types based on the Internet of Things concept can be calculated using the method of principal components and estimation of eigen values, the matrix of functional indices of the system (8).

$$a_k = \arg\min_{\|a_k\|=1} \left(\sum_{i=1}^{m} \left\| x_i - a_k (a_k, x_i) \right\|^2 \right) \tag{8}$$

For more complex digital manufacturing systems, such as MAC and SCADA, the homeostatic capability index may be calculated using the assessment of adjacency matrix and reachability matrix of a graph representation of the given digital manufacturing system (9).

$$E^* = E \vee E^2 \vee \ldots \vee E^n = (e_{ij}^*)_{n \times n} = (e_{ij} \vee e_{ij}^2 \vee \ldots \vee e_{ij}^n) \tag{9}$$

For the most complex digital manufacturing systems, such as systems of unmanned vehicles and intelligent robots, the homeostatic capability index may be calculated using the method of calculation of an autocorrelation function (10).

$$K(\tau) = \mathrm{E}\{X(t) X^*(t-\tau)\} \tag{9}$$

8 Experimental studies

A series of experiments consisting of emulation of a destructive action have been carried out for the purpose of analyzing applicability of the suggested homeostatic approach to assuring cyber resilience by controlling a digital manufacturing systems based on the software-configurable network technology.

The SCN technology was chosen as a technology for organizing network interactions because it allows structural reconfiguration of a network in accordance with homeostasis mechanisms. The SCN technology provides for [15]:

1) separation of the network infrastructure control layer from the data communication layer using a dedicated software which provides communication between a network device and a control system (PCS controller) operating on a dedicated computer;

2) transition from controlling separate units of network equipment to configuring the entire network as a whole, which enables to distribute the load in the network and ensure network traffic with required parameters.

A SCN uses a common, unified, supplier-independent interface between the control layer and the data communication layer; logically centralized network control by a controller with an installed network operating system and network applications and by virtualization of physical resources of the network. The architecture [15] includes an infrastructure layer (in fact, a set of network devices), a control layer (system software) and a network application layers which actually control network operation.

The following control parameters are used:

- network capacity
- the number of network ports
- packet capacity
- the number of lost packets
- round-trip delay
- device recovery time after restart

For the purpose of security management, a mechanism of homeostasis was initiated (availability of more than one SCN controllers in the system meant that the distributed system is capable of homeostasis).

Three different attacks on the software-configurable network have been emulated during the experimental study of the possibility to use the suggested homeostatic control technology:

- a DoS attack aimed at disabling one of the network nodes;
- a substitution attack aimed at substitution of operating parameters of one of the network infrastructure components;
- an attack aimed at disruption of the communication channel between the server and the OpenFlow switch.

The mathematical apparatus of the method of principal components was used to assess cyber resilience, since, due to a strong correlation relationship of parameters; the state of a CPS may be described by one variable, i.e. the first principal component in the following form (10),

$$PC_1(X) = \alpha_i X \tag{10}$$

where α_i are weighing coefficients which are components of the respective eigen vector of the covariance matrix of the CPS control parameters. In addition, the following condition must be met (11),

$$\lambda_1 \geq 0{,}9 \sum_{i=2}^{n} \lambda_i \tag{11}$$

which represents the condition of considering the first principal component of 90% parameter spread of the entire system. Thus, cyber resilience is assessed by meeting the following condition (12).

$$PC_1(X) \in W \,\&\, \lambda_1 \geq 0{,}9 \sum_{i=2}^{P} \lambda_i \tag{12}$$

The results of the experiments shown in Fig. 1 demonstrate that the condition of sustainability is not met during attacks on digital manufacturing systems aimed at substitution of control parameters. The area of sustainability during attacks on the digital manufacturing systems is shown by a dashed line.

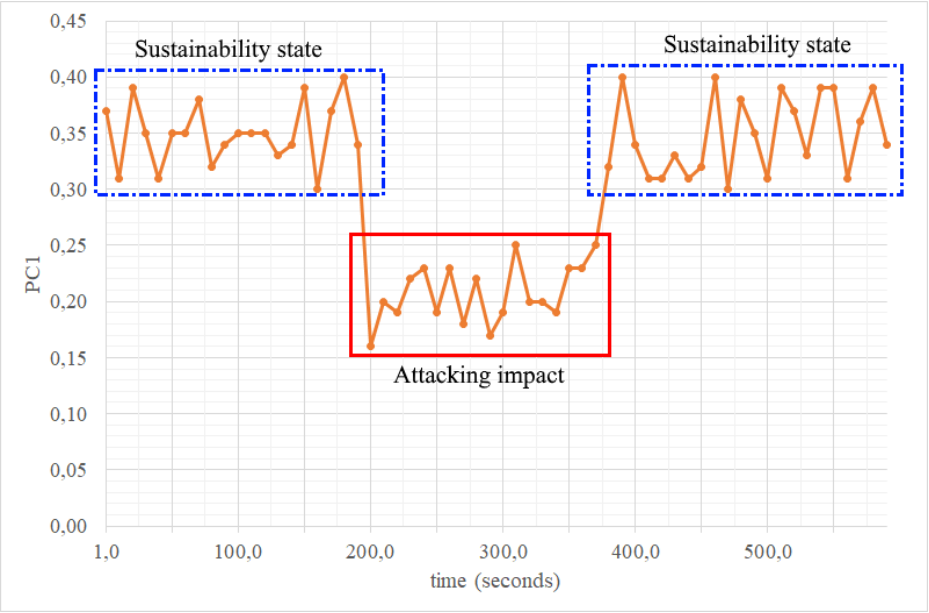

Fig. 1. Principal component value.

We can conclude that digital manufacturing security may be expressed in terms of cyber resilience. Cyber resilience of digital manufacturing should be understood as a capability to maintain self-similarity of the system in case of external actions. The simplest method to develop a control, that is selecting one of the pre-defined homeostatic scenarios, has been implemented as a part of the experiments:

– for the DOS attack, the volume of traffic to the network node under attack was limited by reconfiguration of the OpenFlow switch;

– for the substitution of operating parameters of one of the network infrastructure components, the OpenFlow switch which made the substitution was disconnected and the data communication routes in the network were changed;

– for disruption of the communication channel between the server and the OpenFlow switch, the data communication routes were also changed and a new route was implemented for the given server.

9 Conclusion

The study suggests a new digital manufacturing security paradigm based on the bio-inspired homeostasis concept to provide structural and functional cyber resilience of digital

manufacturing to external destructive actions.

The possibility to apply the concept of homeostasis to digital manufacturing systems has been demonstrated; digital manufacturing control state indices, in particular cyber resilience indices, have been identified. Possible approaches to calculating indices of consistency of the information layer with the physical layer, self-adaptation capability, self-similarity of performance parameters and homeostatic capability have been formulated.

The suggested approach is invariant to attacks on digital manufacturing and suitable for different digital manufacturing systems; moreover, the suggested approach solves all security issues for the new-type systems: attack detection, control, interaction optimization, incident management etc. The developed approach combines information security and physical sustainability and gives an opportunity to automate the synthesis of homeostatically stable structures for digital manufacturing systems of any complexity.

The analysis of homeostatic approach applicability to assurance cyber resilience of digital manufacturing have been carried out using the software-configurable network technology which allows to effectively simulate the digital manufacturing control process due to flexible modifications to its structure.

Thus, the suggested homeostatic security control technology enables the implementation of multi-layer control of digital manufacturing by combining distributed and centralized hierarchical control which increases the number of control loops and expands the range of control factors (parameters and structural characteristics).

To assess the system security state, the approach suggests using universal indices which consider both information and functional components aimed at system self-similarity which is represented by the hierarchical set of criteria. System self-similarity allows maintaining the balance of external factor compensation which is the essence of homeostatic control.

The homeostatic approach lays the groundwork for building a predictive and proactive security strategy due to development of predictive methods of processing of the system status monitoring results.

References

1. R. Seiger, S. Huber, P. Heisig, U. Assmann, LNBIP, **248** (2016)
2. D. P.Zegzhda, Aut. Cont. and Comp. Scien., **50** (2016)
3. C. Liang, Z. Wu., Int. J. Electr. Pow. Ener. Syst., **33** (2011)
4. A. Choudhari, H. Ramaprasad, T. Paul, J. W. Kimball, M. Zawodniok, B. McMillin, S. Chellappan, COMPSAC (2013)
5. M. Rungger, P. Tabuada, IEEE Trans. on Aut. Con., **59** (2014)
6. K. M. Hansen, M. Ingstrup, SAC (2010)
7. D. Weyns, WODA, **24-29** (2012)
8. X. Mao, M. Dong, L. Liu, H. Wang, J. of Inform. Scien. and Eng., **30** (2014)
9. I. Gerostathopoulos, D. Skoda, F.Plasil, T.Bures, A.Knauss, ECSA (2016)
10. I. Gerostathopoulos, T. Bures, P. Hnetynka, J. Keznikl, M. Kit, F. Plasil and N. Plouzeau, The J. of Syst. and Soft., **122** (2016)
11. A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, Work. on fut. direct. in CPS sec. (2009)
12. D. P. Zegzhda, M. A. Poltavtseva, D. S. Lavrova, Aut. Cont. and Comp. Scien., **51** (2017)
13. D. S. Lavrova, Aut. Cont. and Comp. Scien., **50** (2016)

14. D. P. Zegzhda, E. Yu. Pavlenko, Aut. Cont. and Comp. Scien., **51** (2017)
15. M. O. Kalinin, E. Yu. Pavlenko, Aut. Cont. and Comp. Scien., **49** (2015)