Criterion Of Cyber-Physical Systems Sustainability

Evgeny Pavlenko
Higher School of Cybersecurity and Information Security
Peter the Great St. Petersburg Polytechnic University
Saint-Petersburg, Russia
pavlenko@ibks.spbstu.ru

Dmitry Zegzhda
Higher School of Cybersecurity and Information Security Peter the Great St. Petersburg Polytechnic University
Saint-Petersburg, Russia
dmitry@ibks.spbstu.ru

Anna Shtyrkina
Higher School of Cybersecurity and Information Security
Peter the Great St. Petersburg Polytechnic University
Saint-Petersburg, Russia
anna_sh@ibks.spbstu.ru

***Abstract*—The article proposes a sustainability criterion for cyber-physical systems. The concept of information security for cyber-physical systems has been transformed due to the specifics of these systems. Cyber-physical systems combine information and physical processes, which requires the creation of new approaches to ensure their security. The sustainability property for such systems shows their ability to maintain correct functioning under cyber-attacks. The criterion proposed in the article uses the representation of the structure of the cyber-physical system in the form of a graph, where the processes performed by the system are reflected in the form of routes. In proposed approach sustainability criterion is the number of routes of a certain quality, which allow to perform the objective function. Such a representation of the system and the objective function provides convenient modeling of possible ways to rebuild routes. Attacking impacts and system restoration measures that prove the applicability of the criterion for assessing the sustainability of cyber-physical systems are considered.**

Keywords—sustainability; cyber sustainability; cyber resilience; cyber-physical system; information security; graph theory; cybersecurity; modeling.

I. Introduction

Cyber-physical systems (CPS) is a technological concept, which provides a close coordination between computing and physical resources. In general, CPS support the maintenance of real world processes using regular monitoring and a feedback loop [1-4]. As a result, physical processes influence on information processes and vice versa.

Vivid examples of CPS are industrial systems associated with critical areas of human activity [5, 6]. Unauthorized interference with such systems can lead to disastrous consequences; therefore, the question about CPS security is extremely important nowadays.

The close integration of physical and information processes leads to the fact that CPS security do not provide by classical concepts of confidentially, integrity and availability of information circulated in system [7]. The CPS protection from destructive impact is also important, since the physical processes implemented by system are irreversible. In this regard, the problem of maintaining the functional sustainability of CPS in the context of destructive interventions comes to the fore.

II. Related works

There are many approaches to maintain sustainability of CPS [8-19, 22]. One of promising approach uses a biology concept of homeostasis – mechanism that provide constancy of internal organism processes. This approach provides adaptation and self-regulation mechanisms of complex dynamic systems. Such features of the approach allow autonomous control and maintenance of the state of the system. Homeostatic approach for CPS was proposed in [11, 12] as an ability of self-adaptation. However, authors of these papers were focused on the operation correctness, but not on security aspects. Moreover, proposed model is not applicable because of high monitoring algorithm complexity in case of large dynamic systems. One more paper [13] focused from self-adaptive architectures to self-learning architectures to learn and improve QoS parameters over a time. However, such approach do not take into account structural parameters of CPS, but only time series and data stream.

Thus, due to dynamic behavior of CPS, homeostatic strategy can be separate on three stages: system monitoring, sustainability estimating and making decision to system recovery. To implement this strategy, a method is needed to evaluate the sustainability of the CPS at the current time, as well as to predict the maximum destructive load, which will lead to a complete loss of system functionality. Thus, second stage can be realized by different methods using mathematical statistics, game theory and so on. Paper [14] proposed novel algorithm for estimation of system state that resilient to different types of attacks. Proposed method uses principles of robust optimization and give a “frequentist” robust estimator. However, such method do not take into account structure of the CPS which can be represented as a network of devices. Paper [15] proposed game-theoretic concept to estimating system sustainability. This approach defined sustainability as power-form product of the survival probabilities of cyber and physical spaces, each with a corresponding correlation coefficient. Such method do not take into account a structure of the system and might not be as flexible as it needed for providing cybersecurity. Paper [16] proposes methodology to estimate environmental sustainability of CPS. This approach is scalable,

The study was carried out as part of the scholarship of the President of the Russian Federation to young scientists and graduate students SP-1689.2019.5.

economic perspective, however due to simplifications some failures can be missed. In addition, this method do not consider structural features of heterogeneous systems. In [17, 19] authors proposed to estimate CPS as rate of system recovery, however this method is posteriori, so this model allow only restoring system after destructive influences.

III. Approach to CPS security

Homeostasis strategy was applied to security of CPS in [20]. The method of estimating CPS sustainability is determined by the way the system is presented and simulated. In case of CPS, one of the most common is a model based on graph theory. Graph theory allows us to consider not only the network of devices within an integrated CPS, but also the interaction of CPS components with each other. Since the processes in the CPS are carried out by exchanging data between devices, each process can be represented as a route on a graph. The presence of a large number of such routes, as well as their quality, determine the system's ability to function, thereby giving an assessment of its stability.

Paper [18] proposed graph model, according to which CPS is a graph $G=<V, E>$, where $V=\{v_1,v_2,\dots,v_n\}$ − is set of graph vertices representing the devices, and $E=\{e_1,e_2,\dots,e_n\}$ − set of edges representing connections between system components.

Each vertex is characterized by a tuple, which contains the characteristics, depending on its type. The important parameter of vertex is capacity of device $performance(v_i)$, where i is the node identifier. In addition to typical parameters, each vertex corresponds to a set of functions that it can perform $F(v_i)=(f_1,f_2,\dots,f_k)$. The set of functions that can be performed by components of the CPS is not homogeneous: it can include both trivial and more complex in terms of function implementation. Therefore, it is advisable to enter a measure for each of the functions that determines its complexity $f_i\rightarrow complexity(f_i)$. Knowing the node performance and the complexity of the functions it performs, you can find the execution time of the function f_j on the device v_i through the equation (1).

$$time(v_i, f_j)= complexity(f_j)/ performance(v_i) \qquad (1)$$

Each edge also has a parameter characterizing the data rate between vertices v_i and v_j: $time(v_i, v_j)$.

A process running in a CPS is characterized by a sequence of functions that are performed by the vertices of the graph $R_{process}=\{f_1,f_2,\dots,f_m\}$. It should be noted that complex functions can be decomposed as a sequence of simpler ones, which allows to effectively reconfigure the route in terms of destructive effects. This fact, as well as the fact that each function can correspond to several vertices of the graph with different performance, leads to the fact that each $process_i$ in the CPS corresponds to a set of working routes $path_j$ from $R_{process}$ differing in their characteristics.

As parameters of the routes, it is proposed to consider:

- route length.
- total route complexity.
- total route performance.
- time of route execution.
- energy characteristics of the vertex, determined by device type.

Thus, when calculating the characteristics of the route, all connections between the components of the system are taken into account, as well as the characteristics of the vertices that perform the functions included in the process. Intermediate nodes are not counted in the summation.

The presence of high-quality routes, for example, with a short execution time, determines the stability of the CPS in terms of destructive influences, since the reduction of such routes will lead to system downtime, which can lead to failures and of the target function - that is, to lose sustainability.

IV. Estimating of sustainability area

To estimate the CPS sustainability, the information system was modeled as a graph. The graph was constructed using Erdos-Renyi model [21] with the number of nodes equal to 30, and the probability, and the probability of edge appearance equal to 0.35. Each vertex of the graph was mapped:

- set functions that the vertex can perform and its complexity.
- performance of the device.
- time of function execution of the device.

Each edge is associated with a time rate between v_i and v_j time: $time(v_i, v_j)$.

While ensuring the CPS security, important parameters are times of attacks detection and CPS rebuilding to neutralize destructive impacts. Therefore, as the characteristics of the quality of the route were chosen the time of the route execution and its total performance.

As a part of study, a working route was defined, represented as a sequence of functions. To estimate CPS sustainability an algorithm was developed that performs a search for various routes on a graph, including a sequence of vertices that perform functions from the working route. The characteristics of the intermediate vertices were not taken into account. For each route found, time and performance were calculated. The bar plot for the values obtained are shown in Fig. 1.

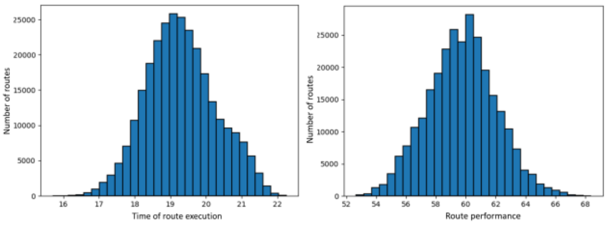

Fig. 1. Bar plot for time and performance of working routes.

To estimate the number of routes depending on the time of their execution, a cumulative function was built (Figure 2). The argument of this function is an ordered set of time values, and the function values are the number of routes that have a time execution less than the value of the argument. Thus, judging from Fig. 2, the number of routes that have an execution time less than 19 is approximately 100,000.

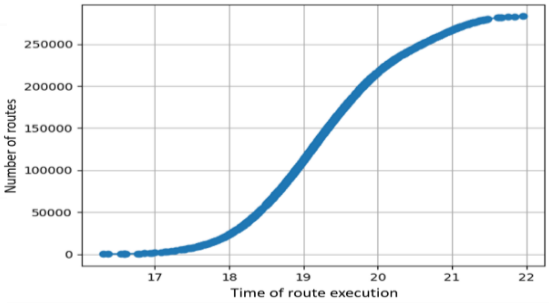

Fig. 2. Cumulative function for route time execution.

In a case of performance estimation, the best quality route will have a large total performance value. Therefore, the cumulative function for the performance of routes is constructed as follows: the number of routes whose performance is greater than the value of the performance taken as the value of function (Fig. 3).

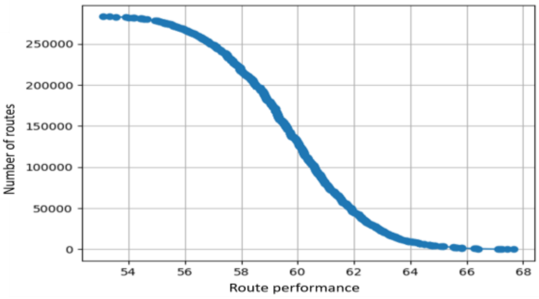

Fig. 3. Cumulative function for route performance.

For further analysis, the normalization of the values of performance and execution time of the route was carried out. The graphs for both characteristics were combined, and then the intersection point was found (Fig.4).

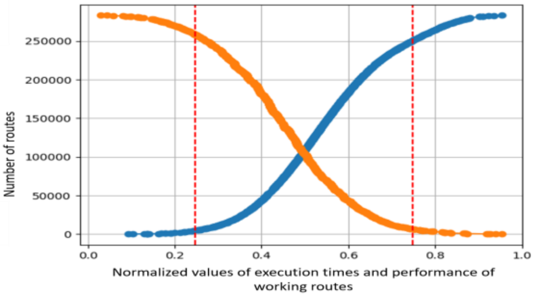

Fig. 4. Intersection of execution and performance curves for working routes.

The left area of the graph corresponds to routes with lowest performance; the right area corresponds to routes with longest execution time. Thus, routes in the middle part of plot on Fig. 4 can be interpreted as area of system sustainability. It is proposed to limit the sustainability area by symmetric intervals of length 0.25 from the intersection point. The right boundary refers to the execution time of the routes — that is, routes from the sustainability area should not run for longer than a certain time. The left border, respectively, refers to route performance.

For fix values of execution time and performance of working route on x axis the number of routes suites to such characteristics was calculated. The largest value observed at the intersection point of two curves (Fig. 5). Since the number of routes is also a quality criterion, to limit the area of sustainability, it is proposed to cut off a part with characteristics for which the number of routes is less than 20,000.

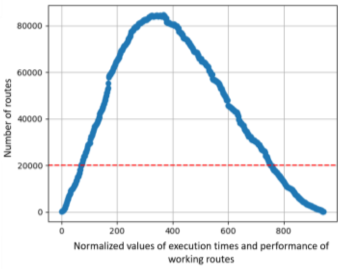

Fig. 5. Number of routes for the fixed values of execution time and performance of working route.

Thus, the paper proposed the criterion for CPS sustainability, which is number of working routes in system with optimal values of execution time and performance. In order to check the applicability of the criterion, it is necessary to simulate destructive influences and to check reaction of criterion to changes in system structure.

V. Simulating if destructive influences

As part of the study, an attack was modeled, consisting in sequential removal of half of the vertices. For the resulting graph, number of routes was calculated, characteristics of time and performance that was in area of the system sustainability (Fig. 6).

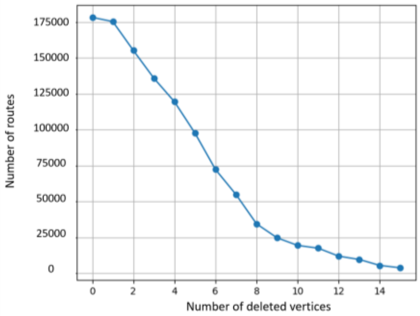

Fig. 6. Number of routes in sustainability area depending on the number of deleted vertices.

The second model of the attack influence is to delete the vertex, which has a certain degree of criticality. As an indicator of the vertex criticality, is it proposes to use the ratio of working routes number passing through the vertex to the total number of working routes. Number of routes depending on criticality of deleted vertex was evaluated for fixed values of execution time and performance of routes (Fig. 7).

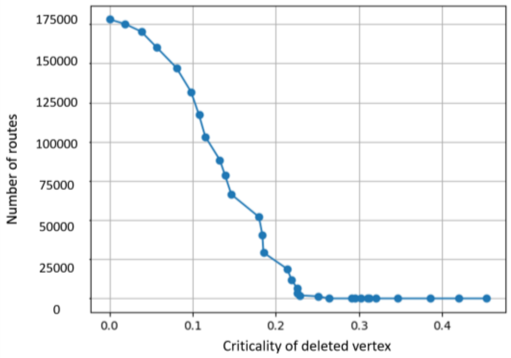

Fig. 7. Number of routes in sustainability area depending on criticality of deleted vertex.

As experiments show, at a certain criticality of vertex, number of routes in the sustainability area reaches zero, which indicates the complete inability of system to function along a given sequence of functions.

During the simulation of attacking influences, proposed criterion of sustainability showed high sensitivity to structural changes in CPS.

VI. Approach to System Recovery

Taking into account the proposed criterion, recovery of system functionality is reduced to problem of changing the graph in such a way that number of routes satisfying the given characteristics increases. An increase in the number of routes is possible through implementation of various scenarios:

- Rebuilding and reconfiguration of CPs to improve the graph connectivity, which will lead to emergence of new routes or change their length.
- Definition of new sequence of performing target function due to possibility of representing the functions as a decomposition of other functions.
- Improving device characteristics, in particular, increasing the performance of certain type devices.

The tasks of reconfiguring the network structure and setting new routes can be associated with high computational costs for implementing mathematical algorithms, as well as time costs for rebuilding the system, which can lead to system downtime and, consequently, affect the speed of the target function. Therefore, these methods are recommended in most serious cases. The approach of changing the characteristics of devices implies the allocation of additional resources to increase devices performance.

Obviously, due to varying complexity of functions performed by devices, an increase in performance of different types of vertices affect the number of suitable routes in different ways. As part of the work, an experiment consists in increasing performance of certain type vertex twice, was conducted. Results are presented in Figure 8.

Abscissa axis indicates type of functions that can be performed by system components, arranged in order of increasing complexity. The first point on the plot corresponds to the initial value of number of routes in graph without changing the performance of devices of a particular type.

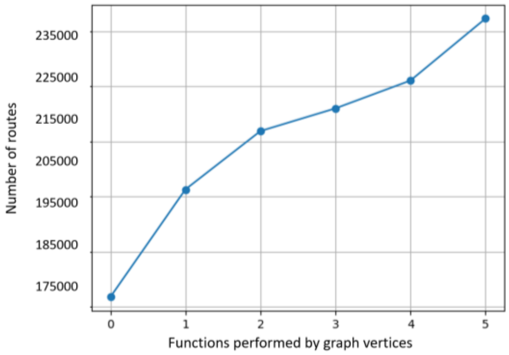

Fig. 8. Sustainability criterion depended on changing performance of certain type vertices.

It should be noted that in Figure 8, the observed linear relationship is determined by the fact that the sequence of functions includes all the functions performed by system. If, however, we increase length of working route and duplicate occurrence of f_3 function, then a small jump will be observed precisely with an increase in performance of devices implementing this function, as shown in Fig. 9.

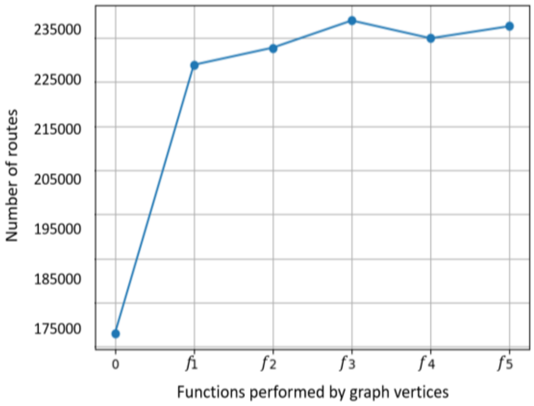

Fig. 9. Sustainability criterion depended on changing performance of certain type vertices.

Thus, for effective CPS recovery and increasing number of suitable routes that satisfy the specified characteristics, it is necessary to give preference to types of devices that perform more complex functions if the ratio of functions of different types in a given sequence is approximately the same.

VII. Conclusion

CPS security reduces to maintaining system sustainability. For solving this problem criterion on sustainability is needed. This criterion should take into account not only information and physical parameters of system devices, but also structural characteristics of CPS network.

Using graph representation of CPS, the processes in the system can be represented as a set of routes that include a given sequence of vertices, each of which performs set of specific functions. Mapping set of qualitative characteristics to vertices and connections, leads to simple evaluating the optimality of the route as total value of vertices and links characteristics containing in the route.

Thus, number of routes with optimal value of quality characteristics determines sustainability of CPS. Applicability of this criterion was verified by modeling destructive effects, as a result of which proposed sustainability assessment demonstrated high sensitivity to changes in the graph describing CPS.

References

[1] D. Lavrova, M. Poltavtseva, A. Shtyrkina, “Security analysis of cyber-physical systems network infrastructure,” IEEE Industrial Cyber-Physical Systems (ICPS), pp. 818-823, May 2018. DOI: 10.1109/ICPHYS.2018.8390812.

[2] Zegzhda D., Vasilev U., Poltavtseva M., Kefele I., Borovkov A. Advanced Production Technologies Security in the Era of Digital Transformation. Voprosy kiberbezopasnosti [Cybersecurity issues], 2018, No 2 (26), pp. 2-15. DOI: 10.21681/2311-3456-2018-2-2-15.

[3] Kotenko I., Levshun D., Chechulin A., Ushakov I., Krasov A. Integrated Approach to Provide Security of Cyber-Physical Systems Based on Microcontrollers. Voprosy kiberbezopasnosti [Cybersecurity issues], 2018, No 3 (27), pp. 29-38. DOI: 10.21681/2311-3456-2018-3-29-38.

[4] N. Sadiku, Y. Wang, S. Cui, M. Musa, “Cyber-physical systems: a literature review,” European Scientific Journal, vol. 13, num. 36, pp. 52-58, 2017. DOI: 10.1142/S2424862217500129.

[5] D. P. F. Möller and H. Vakilzadian, “Cyber-physical systems in smart transportation,” 2016 IEEE International Conference on Electro Information Technology (EIT), Grand Forks, ND, pp. 0776-0781. 2016. DOI: 10.1109/EIT.2016.7535338.

[6] O. Givehchi, K. Landsdorf, P. Simoens and A. W. Colombo, “Interoperability for Industrial Cyber-Physical Systems: An Approach for Legacy Systems,” IEEE Transactions on Industrial Informatics, vol. 13, num. 6, pp. 3370-3378, Dec. 2017. DOI: 10.1109/TII.2017.2740434.

[7] Y.Ashibani and Q. H. Mahmoud, “Cyber physical systems security: Analysis, challenges and solutions,” Computers & Security, vol. 68, pp. 81-97, 2017. DOI: 10.1016/j.cose.2017.04.005.

[8] V. Marquis, R. Ho, W. Rainey, M. Kimpel, J. Ghiorzi, W. Cricchi, N. Bezzo, “Toward attack-resilient state estimation and control of autonomous cyber-physical systems,” 2018 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, pp. 70-75. 2018. DOI: 10.1109/SIEDS.2018.8374762.

[9] I. Kolosok and E. Korkina, “Cyber resilience of SCADA at the level of energy facilities,” V-th International workshop " Critical infrastructures: Contingency management, Intelligent, Agent-based, Cloud computing and Cyber security" (IWCI 2018), vol. 158, pp. 100-105. 2018. DOI: 10.2991/iwci-18.2018.18.

[10] N. Voropai, I. Kolosok and E. Korkina, “Resilience Assessment of the State Estimation Software under Cyber Attacks,” E3S Web of Conferences, vol. 58, pp. 1-6. 2018 DOI: 10.1051/e3sconf/20185802013.

[11] I. Gerostathopoulos, D. Skoda, F.Plasil, T. Bures and A. Knauss, “Architectural Homeostasis in Self-Adaptive Software-Intensive Cyber-Physical Systems,” Tekinerdogan B., Zdun U., Babar A. (eds) Software Architecture. ECSA 2016. Lecture Notes in Computer Science, vol 9839, pp. 113-128, 2016. DOI: 10.1007/978-3-319-48992-6_8.

[12] I. Gerostathopoulos, T. Bures, P. Hnetynka, J. Keznikl, M. Kit, F. Plasil and N.Plouzeau, “Self-adaptation in software-intensive cyber–physical systems: From system goals to architecture configurations,” Journal of Systems and Software,vol. 122, pp. 378-397, 2016. DOI: 10.1016/j.jss.2016.02.028.

[13] H. Muccini and K. Vaidhyanathan, “A Machine Learning-Driven Approach for Proactive Decision Making in Adaptive Architectures,” 2019 IEEE International Conference on Software Architecture Companion (ICSA-C), Hamburg, Germany, 2019, pp. 242-245, 2019. DOI: 10.1109/ICSA-C.2019.00050.

[14] S. Z. Yong, M. Q. Foo and E. Frazzoli, “Robust and resilient estimation for Cyber-Physical Systems under adversarial attacks,” 2016 American Control Conference (ACC), Boston, MA, 2016, pp. 308-315, 2016. DOI: 10.1109/ACC.2016.7524933.

[15] F. He, J. Zhuang, N. S. V. Rao, C. Y. T. Ma and D. K. Y. Yau, “Game-theoretic resilience analysis of Cyber-Physical Systems,” 2013 IEEE 1st International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), Taipei, 2013, pp. 90-95, 2013. DOI: 10.1109/CPSNA.2013.6614252.

[16] S. Thiede, “Environmental Sustainability of Cyber Physical Production Systems,” Procedia CIRP, vol. 69, pp. 644-649, 2018. DOI: 10.1016/j.procir.2017.11.124.

[17] D. Wei, J. Kun, “Method for quantitative resilience estimation of industrial control systems,” U.S. Patent Application No. 13/703,158, 2010.

[18] Barabanov A., Markov A., Tsirlov V. Procedure for Substantiated Development of Measures to Design Secure Software for Automated Process Control Systems. In Proceedings of the 12th International Siberian Conference on Control and Communications (Moscow, Russia, May 12-14, 2016). SIBCON 2016. IEEE, 7491660, 1-4. DOI: 10.1109/SIBCON.2016.7491660.

[19] Markov A., Barabanov A., Tsirlov V. Periodic Monitoring and Recovery of Resources in Information Systems. In Book: Probabilistic Modeling in System Engineering, by ed. A.Kostogryzov. IntechOpen, 2018, Chapter 10, pp. 213-231. DOI: 10.5772/intechopen.75232.

[20] D.P Zegzhda and E. Y. Pavlenko, “Cyber-physical system homeostatic security management,” Automatic Control and Computer Sciences, vol. 51, num. 8, pp. 805-816, 2017. DOI: 10.3103/S0146411617080260.

[21] P. Erdos and A.Rényi, “On the evolution of random graphs,” Publication Of The Mathematical Institute Of The Hungarian Academy Of Sciences, vol. 5, pp. 17-61. 1960.

[22] Petrenko A.S., Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V. The IIoT/IoT device control model based on narrow-band IoT (NB-IoT). In Proceedings of the the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (29 Jan.-1 Feb. 2018, Moscow and St. Petersburg, Russia) EIConRus, IEEE, 2018, pp. 950-953. DOI: 10.1109/EIConRus.2018.8317246.