Mathematical Methods and Models in the Security of the Digital Manufacturing using a Homeostatic Control

Maria A. Poltavtseva[1], Maxim O. Kalinin[2],
Dmitry P. Zegzhda[3], Evgeny Yu. Pavlenko[4]
Chair of Information Security of Computer Systems
Peter the Great St.Petersburg Polytechnic University
St. Petersburg, Russia
[1]poltavtseva@ibks.spbstu.ru, [2]max@ibks.spbstu.ru, [3]dmitry.zegzhda@ibks.spbstu.ru, [4]pavlenko@ibks.spbstu.ru

***Abstract*— Changes in the control of manufacturing systems, the change in the character and type of attacks, led to the emergence of new requirements to ensure information security in the manufacturing. Since it is not possible to describe the full range of attacks on digital manufacturing systems, the paper suggests a new approach to modeling and assessing the security of such systems, which is invariant to any type of attack. Authors consider an approach to analyzing state of modern manufacturing systems and external influences on the basis of self-similarity, and also mathematical estimates of their security. Sustainability and homeostatic control of digital manufacturing systems are proposed in the work as the main approaches to ensuring information security.**

Keywords*— *digital manufacturing; mathematical methods in information security; mathematical models in information security; homeostatic control; security of digital manufacturing

I. FEATURES OF ENSURING SECURITY OF DIGITAL MANUFACTURING

Digitalization of technology industries, caused by the development of the Internet of things, sensor and cloud technologies, has led to great changes of the entire technological infrastructure. A lot of production and business processes are now implemented by intelligent systems, which are not information, they are cyber-physical systems (CPS), implementing physical processes through the implementation of information processes [1]. Participants of information processes in CPS are "smart" devices that are able to communicate with each other and with the environment, as well as to change their state in accordance with the environmental parameters [2].

Ample opportunities for automation of technological processes have become a trigger for the development of digital manufacturing, while opening up opportunities for cyber attacks. Statistics shows that in 2017, the majority of cyberattacks on CPS were directed at critical infrastructure sectors, such as energy, water supply systems, transport facilities. At the same time, the source [3] shows increasing number of security incidents in the second half of 2017 compared to the first half of the year.

The range of attacks on CPS is extremely large and it is not possible to describe all of them, due to the extremely large number of possible entry points for attacker and to zero-day vulnerabilities. That complicates the challenge of ensuring security of digital production systems. In addition, it should be noted that the use of traditional for information systems and client-server networks security methods will not be effective for CPS, as was shown earlier by the authors in [4].

This research work expands the scientific reserve of the authors, which is dedicated to the development of a new approach for securing CPS. CPS security assesment is based on the self-similarity assessment and control, since CPS processes of digital manufacturing are periodic and they are practically unaffected by human influence, so the violation of self-similarity of their functioning will indicate the impact on their functioning. Authors propose to call the preservation of self-similarity of the processes implemented by CPS as the sustainability of CPS control under targeted impacts. The property of the system to maintain its operation in a given range of input and output characteristics under targeted external information impact is called cyber-sustainability [5].

In [6], authors proposed a homeostatic technology for CPS security control, it allows to implement multi-level control of digital production by combining distributed and centralized hierarchical management, expanding the number of control circuits and the range of control factors. To assess the state of CPS security, this approach involves the use of fractal indicators that take into account both information and functional components, this approach is aimed at control of self-similarity of the system. The self-similarity of system allows to maintain a balance in the compensation of external factors, which is the essence of homeostatic control. At the same time, the proposed self-similarity estimates take into account both long-term data dependences, manifested in periodicity at large intervals, and short-term dependences observed at a smaller scale.

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.

978-1-5386-5824-6/18/$31.00 ©2018 IEEE

II. FRACTAL METHODS FOR SECURITY ASSESSMENT OF DIGITAL MANUFACTURING

Technological processes of CPS in digital manufacturing can be considered as stationary, that is, as processes, statistical properties of which do not change over time [7]. Invariance of the characteristics suggests that the process under study has the property of fractality or self-similarity.

Importance of evaluating the self-similarity of digital production is that any violation of the correctness of at least one process will be reflected in data flows, since the functioning of digital production is controlled by the exchange of information between its components. Therefore, it is proposed to detect cyber threats by analyzing the self-similarity of time series formedgenerated by parameters of CPS components.

A. Self-similarity assessment based on the calculation of the Hurst exponent

Hurst exponent H determines the degree of self-similarity of the process. The closer this parameter is to one, the more clearly the fractal properties are manifested [8], while the equality H=0.5 indicates the absence of self-similarity. According to the source [9], statistics of the normalized range or R/S statistics can be used to calculate the value of the Hurst exponent. To do this, we need to calculate the range R of the series, which is the difference between the maximum and minimum values of the series, and the standard deviation of the series S:

$$R = \max_{1 \le u \le N} \left(\sum_{i=1}^{u} (x_i - \bar{X}) - \min_{1 \le u \le N} \left(\sum_{i=1}^{u} (x_i - \bar{X}) \right), \right.$$

$$S = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (x_i - \bar{X})^2},$$

where $\bar{X} = \frac{1}{N-1} \sum_{i=1}^{N} x_i$ is the arithmetic mean of a series of observations for N periods. Then the Hurst exponent H is calculated as follows: $H = log \frac{R/S}{log(\alpha N)}$, where α – is the specified constant, α > 0.

B. Assessment of self-similarity on the basis of multifractal indicators calculation

In paper [10] the use of fractal methods for security assessment and control of stability of CPS functioning is offered as technological processes proceeding in CPS possesses property of self-similarity which violation can testify to deviations and anomalies in system.

The following characteristics of the multifractal spectrum depicted in Fig. 1 were chosen as the characteristics used to detect anomalies in the CPS functioning [11]:

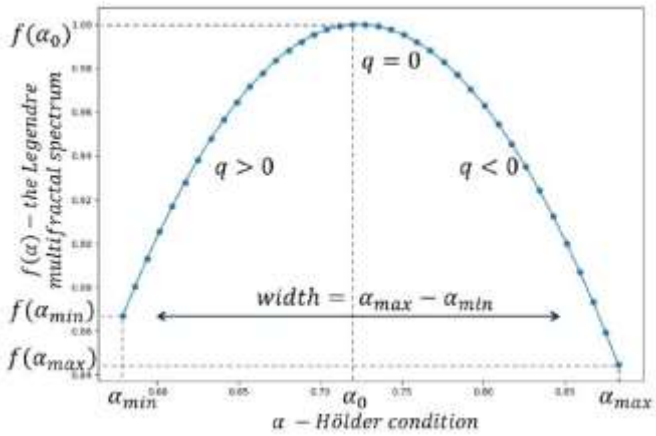

Fig. 1. Multifractal spectrum

- width of spectrum (*width*), calculated as $width = \alpha_{max} - \alpha_{min}$;
- value of the Hölder exponent at the maximum of multifractal spectrum α_0;
- value of the width of right "branch", calculated as $width_{right} = \alpha_{max} - \alpha_0$;
- value of the width of left "branch", calculated as $width_{left} = \alpha_0 - \alpha_{min}$;
- value of the height of left "branch", calculated as $high_{left} = f(\alpha_0) - f(\alpha_{min})$;
- value of the height of right "branch", calculated as $high_{right} = f(\alpha_{max}) - f(\alpha_0)$.

III. EXPERIMENTS

A. Experimental cyber-physical system

As part of study of the effectiveness of security and sustainability indicators appliance to assess the CPS state under targeted external destructive impact, a pilot plant was used, organized at the center for cyber security studies of the Singapore university of technology and design [12]. The test bench implements process of wastewater treatment, which can be divided into six different stages: collection and preparation for manufacturing of incoming wastewater, pre-treatment of wastewater, during which water quality is assessed, ultrafiltration and backwash, dechlorination, reverse osmosis, collection of treated water, backwash and treatment (Fig. 2).

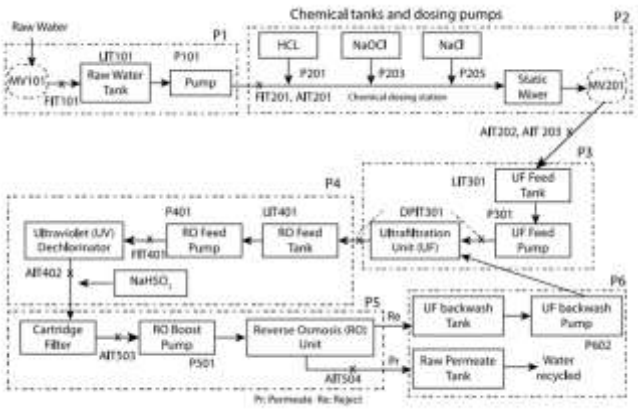

Fig. 2. The architecture of CPS

Each subprocess is associated with a given set of devices. The architecture of the cyber-physical system includes:

- sensors (flow meters, pressure meters, level transmitters, analyzers of water chemical properties, etc.);
- actuators and other devices (motorized valves, pumps, dechlorinators, etc.);
- programmable logic controller, which are responsible for controlling actuators;
- network devices;
- PC and workstations intended for processing and storing data, monitoring and visualizing the system state.

Attacking impacts can be directed both on separate components of one subprocess, and on components of several subprocesses. The intensity of external influences is determined by the number and arrangement of elements, the compromise which leads to the successful implementation of the attack, and can be ranked as follows [12]:

- Impact on a single component in a single processing stage (Single Stage Single Point, SSSP).
- Impact on multiple components in a single processing stage (Single Stage Multi Point, SSMP).
- The attack is aimed at several stages, each of which involves the compromise of one component (Multi Stage Single Point, MSSP).
- The attack is aimed at several stages, each of which involves the compromise of several components (Multi Stage Multi Point, MSMP).

The analyzed data for each system process is a multivariate time series formed by the indicators of the sensors involved in the current process. For the detection of cyberthreats, it is possible to use the Hurst exponent, the dynamics of which change allows us to monitor the violation of the process self-similarity (Fig. 3).

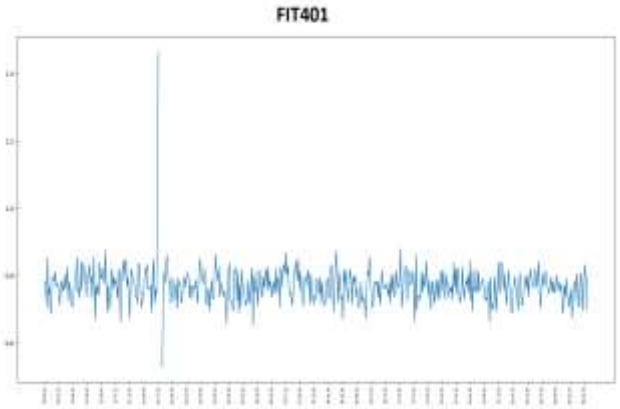

Fig. 3. Attack detection on the FIT-401 by analyzing the dynamics of Hurst exponent

Analysis of multifractal spectrum allows detecting changes in sensor indicators. Fig. 4 shows changes of the Legendre multifractal spectrum width, height and width of the spectrum left "brunch" for flow transmitter FIT-401, located in the dechlorination block Fig. 5 shows changes of another multifractal spectrum characteristics (Holder exponent in the spectrum maximum, height and width of the spectrum right "brunch") for level transmitter LIT-301. Occurring outliers from median values allows indicating attacks on a certain component of the cyberphysical system. In particular, changes of FIT-401 values led to the pump shutdown, that directs dechlorinated water to the reverse osmosis; falsification of LIT-301 values led to the water tank emptying and to tank damaging during the first attack. Also it leds to water tank overflow during the second attack.

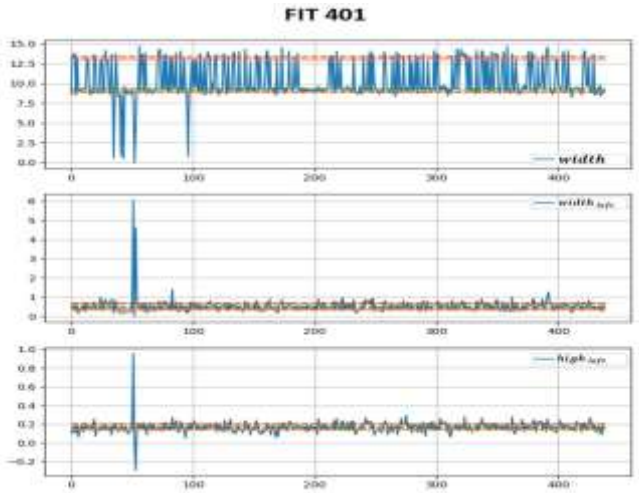

Fig. 4. Attack detection on the FIT-401 using multifractal spectrum characteristics

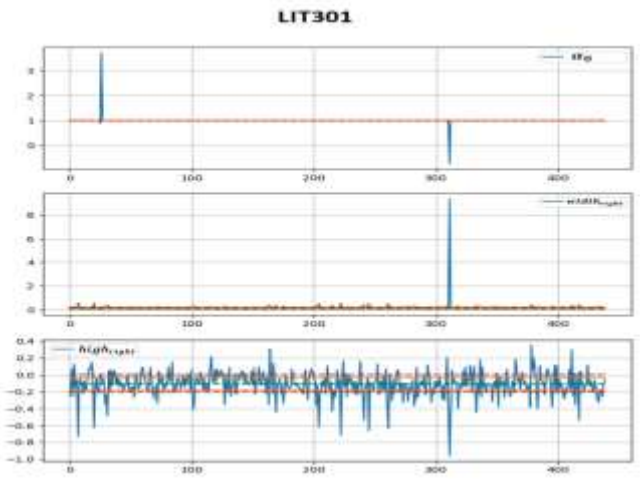

Fig. 5. Attacks detection on the LIT-301 using multifractal spectrum characteristics

IV. Conclusion

In this paper authors propose mathematical tool, used to estimate the security digital production systems. Analysis of features and exploring invariance of technological processes that occur in digital production systems allows using fractal methods for detecting cyberthreats and destabilization of cyber-physical system.

As indicators for estimating cyber-physical system stability Hurst exponent and the Legendre multifractal spectrum characteristics were chosen. Experimental results represent the effectiveness of proposed methods. Using self-similarity property of technological processes for detecting attacks is a new approach that allows detecting cybertheats in complex digital production systems.

References

[1] Zegzhda P.D., Poltavtseva M.A., Lavrova D.S. Cyber-physic system systematization and security evaluation. Problems of information security. Computer systems (Problemy informatsionnoy bezopasnosti. Kompyuternye systemy). 2017. Vol. 2. Pp. 127-138. (In Russian).

[2] Lavrova D.S. An approach to developing the SIEM system for the Internet of Things. Problems of information security. Computer systems (Problemy informatsionnoy bezopasnosti. Kompyuternye systemy). 2016. Vol. 2. Pp. 50-60. (In Russian).

[3] Kaspersky Lab ICS CERT. Threat landscape for industrial automation systems in h2 2017. URL: https://ics-cert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017. (In Russian).

[4] Zegzhda D.P., Pavlenko E.Y. Cyber-physical system homeostatic security management. Automatic Control and Computer Sciences. 2017. Vol. 51(8). Pp. 805-816.

[5] Zegzhda D.P. Sustainability as a criterion for information security in cyber-physical systems. Automatic Control and Computer Sciences. 2016. Vol. 50(8). Pp. 813-819.

[6] Zegzhda D.P., Pavlenko E.Y. Homeostatic strategy of security of cyberphysical systems. Problems of information security. Computer systems (Problemy informatsionnoy bezopasnosti. Kompyuternye systemy). 2017. Vol. 3. Pp. 9-22. (In Russian).

[7] Lavrova D.S. An approach to developing the SIEM system for the Internet of Things. Automatic Control and Computer Sciences. 2016. Vol. 8. Pp. 673-681.

[8] Trenogin N.G., Sokolov D.E. Fractal properties of network traffic in the client-server information system. Bulletin of the Research Institute of the Siberian State University of Telecommunications and Informatics (Vestnik NII Sibirskogo gosudarstvennogo universiteta telekommunikatsiy i informatiki). 2003. Vol. 1. Pp. 163-172. (In Russian).

[9] Petrov V.V., Platov V.V. The study of the self-similar structure of the wireless network. Radio engineering notebooks (Radiotekhnicheskiye tetradi). 2004. Vol. 30. Pp. 58-62. (In Russian).

[10] Zegzhda D.P., Pavlenko E.Y. Security indicators for digital manufacturing. Problems of information security. Computer systems (Problemy informatsionnoy bezopasnosti. Kompyuternye systemy). 2018. Vol. 2. (In Russian).

[11] Zegzhda P.D., Lavrova D.S., Shtyrkina A.A. Multifractal analysis of backbone network traffic for denial-of-service attacks detection. Problems of information security. Computer systems (Problemy informatsionnoy bezopasnosti. Kompyuternye systemy). 2018. Vol.2. (In Russian).

[12] J. Goh et al. A dataset to support research in the design of secure water treatment systems. International Conference on Critical Information Infrastructures Security. Springer. Cham.2016. Pp. 88-99.