Architecture of homeostatic security control for digital manufacture systems based on software-defined networks[a]

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

[1] Peter the Great St. Petersburg Polytechnic University, Institute of Applied Mathematics and Mechanics, 195251, 29, Politechnicheskaya st., Russian Federation

Abstract. The authors have offered the homeostatic control system architecture for digital manufacture security based on the software-defined network technology.We have highlighted the development features of digital manufacture systems and defined the technology advantages of software- defined networks, which allow these networks to be successfully applied with flexible and adaptive topology for a highly efficient new generation of cyber-physical systems. We have also described the main operating principles of software-defined networks in digital manufacture systems. A description of homeostatic security control technology, which includes a combination of engines to provide stability of the system's internal environment and structural and functional resistance to external disturbances, is provided. We have proposed and described in detail the homeostatic security control system architecture including three generalized components: monitoring unit, decision-making unit, protection and control unit.

1 Introduction

Active development of information technologies made it possible to develop a new type of industrial systems. Unlike industrial systems that are available now and include separate components interacting with each other through special interfaces, digital interfaces provide throughout integration and uniform data formats at all process stages. For this purpose, data from all the digital manufacture system components is collected in one center, where they are systemized and processed using up-to-date methods Data Mining and transmitted in the form that is convenient for decision making process with artificial intelligence method. This approach makes it possible to significantly enhance the performance of industrial systems, the decision- making speed with automatic systems exceeds that of automated ones. Digital manufacture systems are based on cyber-physical systems, which are multi-component, distributed systems operating independently from people and monitoring areas that are critical and important to population. These systems combine information modules physical process implementation modules [1].

[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

Digital manufacture systems are based on network interfacing technologies. Classic methods and network infrastructure and data stream control technologies, which are available in the computer networks now, cannot allow network interaction to develop in distributed digital manufacture systems. The development of such distributed systems has pushed for the need for flexible, reliable, scalable, well-controlled network backbones. A network interfacing system in large-scale digital manufacture systems cannot be set up by configuring each element separately and manually. A technology is needed to be developed that will allow controlling the network infrastructure as a single system. All the requirements for network interfacing systems are met by the software-defined network technology (SDN) in which the network infrastructure control level is separated from the data transmission level by automating the control functions and by transferring them into specialized software, which runs on a standalone computer [2].

In order to implement this idea open protocol OpenFlow is developed to control network equipment that is not designed for products of certain manufacturers of multi-protocol products. By using this protocol system administrators can set and monitor: who with whom, in what conditions, with what quality can interact within the network.

All the network equipment is combined under control of a SDN controller, which the network operating system is installed on: The network control system installed in OS provides the following functions:

- Network control access;
- Generation of data on status of network resources.
- Network infrastructure monitoring.

This technology makes it possible to implement strict data transmission rules within the network regardless of its topology as well as to provide intelligent response of the system to changes occurring within the network infrastructure.

Close integration of cyber-physical systems with manufacturing processes related to industrial manufacture and control of a great number of complex objects has brought up the requirement to change the existing security paradigm for digital manufacture. It is associated with the fact that direct transition of information security features such confidentiality, accessibility, integrity is impossible in digital manufacture because unlike information processes, physical processes are irreversible and it is impossible to implement the same monitoring and control level as for the information processes [3].

2 Software-defined network security control research

The topic of integrating the SDN technology with cyber-physical systems (in particular the Internet of Things systems) is widely covered in foreign publications. However, it should be noted that there are very few research papers dedicated to cyber-physical system security control based on SDN. The latest publications mainly focus on the integration process but not on the development of flexible and adaptive security control process by means of SDN engine.

In this paper [4] the authors offer a system architecture that is based on SDN controllers executing control over the infrastructure of various systems in the Internet of Things. We have also considered the issue of overriding a semantic break between the abstractions of high-level tasks and certain network devices and resources. A heuristic algorithm for planning streams for centralized coordination of resources, whose simulation has shown the best performance results in comparison with existing solutions. However, the offered infrastructure does not make the Internet of Things stable in relation to targeted destructive disturbances and requires more complex and reliable tools to be developed to ensure security.

In research [5] the authors offer architecture based on the software-defined network technologies taking into account the horizontal model of Internet of Things, whose aim is to

provide the total infrastructure for a wide range of application and to support functional compatibility at various levels. The system architecture includes four levels: device level collecting data, interaction level containing SDN-gates and routers, control level containing SDN-controllers and mechanisms for service billing and metering and application level. The proposed solution makes it possible to support new services quickly as well as to use devices and data jointly by several different applications. A significant disadvantage of this architecture is no security mechanisms to protect the central SDN-controller, provide stable operation of the overall system and security of separate connected resources and information.

In paper [6] the UbiFlow system is presented, which controls flows and coordinates resources in the Internet of Things employing the SDN technology. The key feature of this UbiFlow system is that it divides the entire network into small clusters, which are controlled by SDN controllers. Devices of the Internet of Things located inside a cluster can be connected to another access point to make different requests providing fault-free operation and scaling. However, the proposed system does not make it possible to forecast further behavior of the system and does not provide for compensation and control engines for functional stability of the entire system.

Publication [7] presents the architecture of protected Internet of things including transmitted data confidentiality, identification and authentication control, key control and protected routing blocks based on SDN. This architecture makes authentication of heterogeneous devices possible, at the same time the SDN controllers as a third, confidential party and control routing between the Internet of Things devices. However, this paper does not cover the issue of fall-over protection, stable operation of the system and its adaptation to external disturbances.

Publication [8] offers the security control architecture for the Internet of Things network based on SDN. The main focus area is to provide authentication of the Internet of Things devices using a SDN-controller. Thus, the controller itself acts as an interlink providing data source authenticity. In case of malfunction, the border controller will perform the security controller's functions, however these complex cyber physical systems such as the Internet of Things need intelligent stability engines to be implemented, which would not only allow optimizing the operating scenarios and timely response in case of malfunction of critical system components but also support the internal environment state in case of targeted sustained attacks by implementing additional compensating actions.

3 Operating principle of software-defined networks in digital manufacture systems

The main idea of this SDN technology is to create a single general-purpose control engine for stream table regardless of a network device manufacturer. The OpenFlow protocol is an open protocol, which successfully implements software control of network stream table regardless of a switch or router, where it is implemented. With this OpenFlow protocol help the network administrator can classify traffic depending on the operating environment of network equipment and monitor network streams, packet forwarding routes Data plane in the SDN network equipment is defined by the stream table and appropriate action associated with every rule given in this table [2].

The network equipment supporting the OpenFlow protocol-based operation includes three main components:

– Network stream table with action rules associated with every record;

– Control channel, which provides safe connection of network device and SDN controller to transmit control commands and network packets via the OpenFlow protocols;

– OpenFlow protocol support components, which implements standard controller and network device interfacing mechanisms.

Network switches supporting the OpenFlow protocol-based operation forward packets between ports depending on those set by the network stream and rules table controller; in this situation, it is possible to isolate network traffic streams according to different information. Each record in the network stream table associates with action that should be applied to packets belonging to this stream [9]. The main actions are as follows:

– Forwarding of packets of this stream, further to a set port or to several ports, in other words, traffic switching;

– Encapsulation and transmission of packets belonging to this stream to SDN controller via safe channel This rule always applies to the first packet from a new stream, in order to allow the controller to make a decision on adding a new network stream on the device.

– Discarding of all packets belonging to this stream. This rule can be utilized to provide security, deter "service denial" attacks or filter network traffic.

Each record within the stream table has the following structure:

– Rule for selecting packets belonging to this stream.

– Actions determining how this stream elements should be processed;

– Statistics, which monitors the quantity of this stream packet bytes as well the time that has passed since the last pocket from this stream popped up in order to delete inactive streams.

The SDN controller's main functions are to add and delete records from the network stream tables on the device. The controller dynamically analyzes the entire network status, which allows the system administrator to assess the network infrastructure state at the present moment. Thus, the software-defined network technology meets all the necessary requirements for efficient control of network resources and data streams within digital infrastructure system, which enables to:

– Separate the network equipment control plane and data transmission place, which is traditionally done by the switches. Features related to data plane are still implemented on the switch but the controller is now responsible for making decisions on high-level routing in SDN, as a rule, it is based on a standard server, which makes it possible to increase the network infrastructure traffic capability as well as enhance the digital manufacture system flexibility;

– Create a convenient and flexible control system for the entire network but not for standalone devices. It is possible to monitor the entire network on the SDN central controller, which greatly enhances control, security assurance and other tasks. Because the SDN technology allows the administrator to clearly see all the traffic streams, it will be easier for him to notice intrusions and identify other problems;

– Afford an opportunity to implement a customized model for network traffic classification. The SDN technology makes it possible to assign priorities to different traffic types. For example, the controller can order the switches to implement rules for certain network traffic streams. In particular, these rules can ensure that data are forwarded via the fastest routes or via the routes with minimum quantity of transit points, in other words, enhance the data transmission system performance as well as make it possible to control data streams [10];

– Enhance network performance and provide quick recovery after errors. With switches no longer responsible for processing traffic associated with control plane, the SDN allows these devices to allocate all their resources to speed up traffic as well as develop network action plans to be followed during clogging or equipment problems [11];

– Provide efficient data transmission with due consideration of infrastructure and network purpose. The SDN technology makes it possible to create virtual network topologies, build up, when necessary, virtual or global networks without physical changing the main network. For this purpose, it is possible to develop centralized virtual control plane, providing network administration functions.

With the SDN technology applied the controller directly sets rules and settings for processing network traffic streams on equipment. Using a special language defines what action needs to be taken on an incoming packet: send a packet further, discard a packet or change some field in the header. Selecting any action depends on many parameters, such as: Presence of some specific bits in a network packet; priority to process network packets of this configuration; status of network equipment processing this packet. Thus, the SDN technology makes it possible to break down the entire network infrastructure into logical parts, in other words, it is possible to define potential routes for some network stream.

4 Homeostatic security control

The task of implementing digital manufacture in all the branches of activity is slowed down at the moment in connection with the fact that it is necessary to develop a strategy that will provide security and stable running of digital manufacture in conditions of targeted destructive disturbances. The relation of digital manufacture systems with critical branches of activities makes them an attractive target for intruders' attacks.

The specific features of digital manufacture systems shaping the developed protection strategy requirements are laid down in source [12]. These features presume that the digital manufacture security methodology should be based on the methods that support and ensure that the manufacturing process continues in preset dynamics in conditions of destructive disturbances, safeguard correct addressing of control commands and allow parameters and structure to adapt in order to counteract external and internal destructive disturbances and keep the manufacturing process stable. In this case, what significantly complicates this task is the fact that these digital manufacture systems are dynamic.

The authors of this article earlier offered a homeostatic control idea, which imply a combination of mechanisms providing stability of the system's internal environment and system's structural and functional resistance to external destructive disturbances. This control technology is implemented on the basis of homeostat – a self-organizing specialized subsystem aimed at supporting the system's key parameter values within a great variety of allowable values [13, 14].

In this situation, this subsystem shall always come up with a resolution to controversy of two control loops, one of which characterizes intruder's destructive actions during attacks on the system and the second one tries to make changes to the system in such a manner so that to eliminate destructive influence and maintain the system's target functions. On one side this contradiction provokes a threat of stability loss and on the other side self-regulation, which involves a mechanism for developing behavior strategies for system's self-improvement by changing its block diagram. The specific features of homeostatic security paradigm consist in resolving the Pareto-optimization task, in other words, finding the area of unimprovable solutions [15] ensuring that security and functionality are maintained within preset limits. This is connected with the fact that an intruder can control the cyber physical system components exploiting errors and weaknesses in the security subsystem and homeostat cannot control this intruder.

The range of allowable structural changes that allows the system to counteract external disturbances is a domain of permissible strategic managerial solutions in order to support the entire system's dynamic stability. The system that allows homeostatic control to occur should have a capability for structural changes; consequently it should have some "reserve" of key units that can be activated when the system gets closer to unstable state. In this cases, it is also required that the system would have a well-developed structure defining the limits, which allow the system's structure to vary without permissible loss of functional features.

5 Architecture of homeostatic security control system for SDN-based digital manufacture

With approaches and evaluations proposed [12] the authors offer a general architecture of security control unit for cyber-physical systems and digital manufacture as a whole, which is shown in Fig. 1. This security control unit includes three generalized components. Monitoring unit, decision-making unit and protection and control unit.

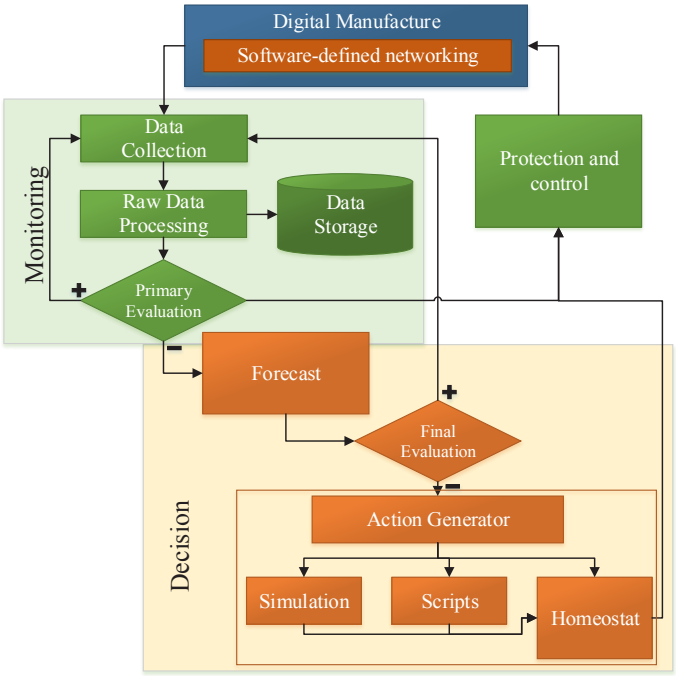

Fig. 1. General architecture of digital manufacture system control unit.

Monitoring of the digital manufacture system status and diagnostics of malfunctions and possible security problems are an integral part of general control process. The purpose of monitoring is to determine primary evaluation of the system's status to make a decision on required interference. This unit implements the following functions:

- Data collection from digital manufacture system components;
- Data processing to bring them to the same format and reduce their size;
- Data storage management;
- Data analysis to obtain primary evaluation.

In conditions of digital manufacture for the purpose of data collection it is necessary to implement MDC-systems (MachineDataCollection) making it possible to control operation of all the digital infrastructure objects: equipment, workstations, services etc.

To process digital manufacture system data it is expedient to use such BigData methods as aggregation, normalization and filtration. Aggregation in accordance with time parameter makes it possible to combine a great number of messages from one device into a single message, thus to reduce data size. The data aggregation diagram of digital manufacture systems in accordance with a time parameter is shown in Fig. 2.

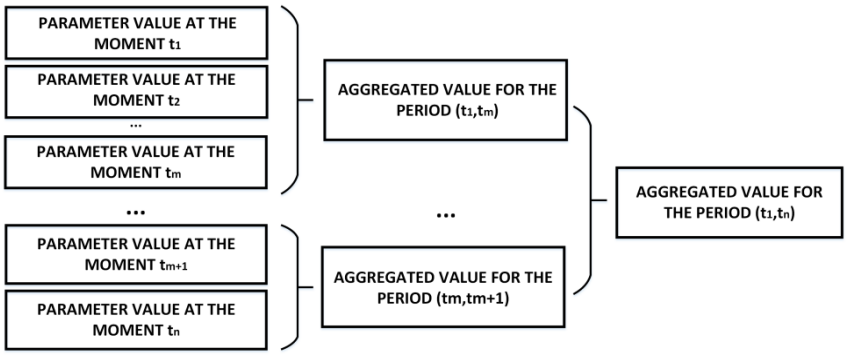

Fig. 2. Data aggregation diagram of digital manufacture system in accordance with time parameter.

In addition, it is possible to aggregate data coming from similar type devices implemented within the same digital manufacture subsystem. Data normalization will bring data to the same format, which may be relevant in conditions of no interaction standards for digital manufacture systems as well as in conditions of a great number of vendors supplying industrial automation devices (transmitters, actuators and controllers). Data filtration will make it possible to discard information, which is not needed by the analysis module for primary evaluation.

Data storage management is closely interrelated with the type of digital manufacture systems and prevailing data type circulating in them. In this case, it is necessary to determine what time periods should cover stored data in order to arrange the data storage and update process in an efficient manner.

The primary system status evaluation consists in calculating metrics and indicators characterizing the range that covers the monitored system parameter values. In accordance with obtained values the system makes a conclusion whether it is necessary to interfere in the system's operations in order to correct it.

On the border of the monitoring and decision-making unit there is a forecast component determining the system's behavior trends. A forecast model should also be selected taking into account the digital manufacture system features. For complex systems it is expedient to apply simulation modeling methods during forecasting and use the formal apparatus of mathematic logic, the theory of probabilities and statistic method, the image discrimination theory, the fuzzy-set theory, artificial neural and immune networks, research and information model methods. Following the forecast results the decision-making unit makes the final conclusion whether it is necessary to interfere in the production complex operation.

In case of unsatisfactory forecast the compensation action generation unit activates, which enables an action generator and action development components based on simulation and known response scenario database and homeostatis unit, which implements an integrated approach to control interference synthesis based on the abovementioned principles.

A certain number of response scenarios allowing the system to self-adapt in order to bring the system back to stable state and maintain its correct operation should be introduced in accordance with key features of each digital manufacture system.

Response scenarios can be divided into 3 groups:

– Scenariosresponsible for creation of new system objects or activation of already existing one, in this situation in order to implement this strategy it is expedient to provide for some redundancy within the system, this will enhance its stability;

– Scenarios being responsible for interaction of system object and their joint operation;

– Scenarios defining the entire system's behavior and setting connection between the digital manufacture system object and control action stream circulating between them.

In this case for some digital manufacture systems it is expedient to provide possible setting to return to previous stable state.

Introducing changes to the system's operating process should not be rapid, for this purpose the compensation action generation unit is provided with a simulation function that prepares a plan of operation changes on the already operating system.

5 Conclusion

In this article the authors have offered the general architecture of security control unit for cyber-physical systems and digital manufacture systems. This unit is a key module within digital manufacture systems, it is the unit that detects security problems (monitoring), predicts further system's behavior trends and makes a decision on whether it is necessary to introduce changes to current operation of the system, exercises compensating effects on the system using built-in response scenarios.

In order to implement control functions in accordance with the proposed architecture we have applied a technology of software-defined networks being a single general-purpose control engine for stream table regardless of a network device manufacturer. The SDN technology makes it possible to divide the network equipment control plane and data transmission plane, which significantly enhances the SDN-based digital manufacture system security level. Applying the SDN technology in complex, large-scale systems makes it possible to efficiently control all the network nodes and monitor traffic streams, which is achieved by transferring the main network control logic onto the SDN controllers. In this case, an important feature of the SDN technology is possible implementation of your own network traffic control model, therefore, for each digital manufacture system, it is possible to arrange network interaction in accordance with system's specific features.

Digital manufacture systems are mainly large-scale systems, therefore, an importation task in their operation is to provide high performance in conditions of intensive network interaction. Applying the SDN technology will make it possible to enhance the network communications performance; because the switch load will be reduced and consequently these network switches will be able to allocate all the resources to speed up the data exchange process.

References

1. R. Seiger, S. Huber, P. Heisig, U. Assmann, LNBIP, **248**, (2016)
2. M. O. Kalinin, E. Y. Pavlenko, Aut. Cont. and Comp. Scien., **49** (2015)
3. D. P. Zegzhda, Aut. Cont. and Comp.Scien., **50** (2016).
4. Z. Qin, G. Denker, C. Gianelli, P. Bellavista, N. Venkatasubramanian. NOMS (2014)
5. Y. Li, X. Su, J. Riekki, T. Kanter, R. Rahmani. IEEE Int. conf. on ICC (2016)
6. D. Wu, D. Arkhipov, E. Asmare, Z. Qin, J. McCann. INFOCOM (2015)
7. S. Chakrabarty, D. Engels. CCNC (2016)
8. K. Sahoo, B. Sahoo, A. Panda. MAMI (2015)
9. I. Z. Bholebawa, R. K. Jha, U. D. Dalal, Wir. Pers. Comm., **86** (2016)
10. B. Ng, M. Hayes, W. K. Seah, IFIP Net. Conf., IFIP, 1-9 (2015)
11. S. Kaur,J. Singh, AISC, **434** (2016)
12. D. P. Zegzhda, E. Yu. Pavlenko, Aut. Cont. and Comp. Scien., **51** (2017)
13. I. Gerostathopoulos, D. Skoda, F. Plasil, T. Bures, A. Knauss, ECSA (2016)
14. I. Gerostathopoulos, T. Bures, P. Hnetynka, J. Keznikl, M. Kit, F. Plasil and N. Plouzeau, The J. of Syst. and Soft., **122** (2016)
15. I. Kuwajima,Y. Nojima,H. Ishibuchi, Artif. LifeandRobot., **1**(2008)