Designing an Information Security System in Smart Factories of the Industry 4.0

D A Zakoldaev¹, A V Shukalov¹, I O Zharinov¹ and O O Zharinov²

¹Faculty of Information Security and Computer Technologies, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, 49, Kronverksky Av., Saint Petersburg, 197101, Russia
²Department of Problem-Oriented Computing Complexes, Saint Petersburg State University of Aerospace Instrumentation, 67, Bolshaya Morskaia str., Saint Petersburg, 190000, Russia

E-mail: mpbva@mail.ru

Abstract. The problem of designing an information security system in smart factories of Industry 4.0 is investigated. Information security system is a company infrastructure component to provide the company information security. In the example of typical smart factory structure cyber and physical components are defined which are mostly susceptible to the malicious software components implementations. Such components could be components with their own means of calculations and engaged in the production technological operations. Smart factory information security risks can be explained with program and technical means for the operator to control the cyber and physical configuration remotely and other components of the production infrastructure into a single digital space of the company. Measures are proposed to increase the information security level of the Industry 4.0 smart factory based on technical, organization and program solutions.

1. Introduction
The wide application of advanced informative technologies and digital cyber and physical systems in the Industry 4.0 [1, 2] companies provided a background for attackers specialized in unauthorized access to the production components and data rights obtaining [3]. Their special objects are separate cyber and physical systems (CPS), technological lines, production and finance data to characterize the company activity and some other components of the Industry 4.0 cyber and physical production, which are of interest for wicked competitors [4].

According to the tasks, the attackers could see their targets as follows [5, 6]:
- acquisition of technical and economic data on project and production company activity;
- intentional failure creation of some company production infrastructure components including the error of data access or integrity (technical documentation);
- temporal or constant unauthorized access to the company production components and other.

There are several ways for an attacker to hack the company infrastructure production components [7, 8]. In digitalizing project and production activity in most cases, the attackers implement a malicious software into company informative system. To prevent an attacker unauthorized access to the production infrastructure they must develop and implement into the company security system special...
organization, technical, program and other measures which together provides the company information security [9 ,10].

2. **Cyber and physical production as an unauthorized access subject**

Cyber and physical production information security is based on some scientific and practical tasks solution, which may include [11]:

- production division structure analysis and sorting out the components, which are potential targets for an attacker;
- detection of threats and risks, which are important for the company if the attacker unauthorized access to the production infrastructure components will be realized using one of the methods;
- development and research of the attacker model to understand its target, objectives, methods and means, which are helpful for an unauthorized access to the company production infrastructure granting;
- development, test and implementing to the company information security system the measures, methods and means reducing the probability that an attacker would be a threat to the production division.

Figure 1 there is a scheme of cyber and physical production division as an attacker unauthorized access subject. The main attention is paid to the objects detection, which are potentially vulnerable for an implementation of a malicious software.

![Diagram](image.png)

**Figure 1.** Cyber and physical production scheme as an unauthorized access subject (AWP – Automatic Work Place, IoT – Internet of Things).

The following groups of the company production infrastructure components could be susceptible to the unauthorized access threat [12]:

- cyber and physical production machines with their own calculation means are capable to register, store and execute the malicious software;
- server equipment with its own calculation resources is the company virtual environment based on which cloud services and applications are realized to provide CPS functionality;
- communication devices (phone, PC, tablet and other) grant to an operator the access to the production division components with its own operational system which is capable to execute potentially malicious software.

Cyber and physical production objects unification into a single technological line requires creating
the information security management system. The information security control is the procedure to provide automatic and continuous company production resources functionality, which may include:
- technical and program means of cyber and physical systems;
- technical and program means of the company virtual environment;
- production data base and cyber and physical production base of knowledge to provide information accompanying technological operations processes completion and other.

The information security management system of a company is placed in virtual environment of the company and functions based on production data transmitting communication environment [13].

3. Communication environment as a way of malicious software distribution

Cyber and physical components interaction is done with the production data information exchange in the company communication environment. Alongside with the good function of the company communication environment, there could be a potential information channel capable to distribute (to implement into the production components) malicious software of an attacker.

Cyber and physical production communication environment is formed by wired and wireless communication channels. The Ethernet wired link channel unites CPSs and company virtual environment servers. The IoT wireless channels and Bluetooth unite CPSs and grant them access to the cloud services and applications. CPS as an active smart factory production infrastructure Internet agent provides remote information data exchange with a computerized control system (For example, CPS messages about components and materials orders which are necessary to complete technological operations) which is a potential risk of malicious software distribution through the channels of information transmission within the entire company.

The attacker actions model who is interested to get right of an unauthorized access to the production components may include the following ways of malicious software distribution:
- connection to the external communication devices IoT channel, which contains the malicious software to place it in the production components;
- malicious software distribution to the production operator communication devices to implement the virus secretly into the production infrastructure;
- malicious software distribution to the company virtual environment server equipment through the channels of remote access through the Internet;
- malicious software distribution to the CPS controller with the Bluetooth channel in the remote control mode (servicing) of cyber and physical system with the following software distribution in the IoT net to all production components;
- connection to the Ethernet net to distribute in any available production component a malicious software;
- designer implementation to the program code of cloud services and applications a piece of malicious software which will be further distributed to the net of Ethernet and IoT to the cyber and physical system;
- CPS designer implementation to the integrated software a piece of malicious software code which permits an attacker to control remotely (say, to switch off) a CPS and other.

Any of those attacker options to implement a malicious software to the production components leads to the quick distribution of the virus and causes the breakdown of the company control computerized system. Nowadays to detect those software components or attempts to implement them, the company should create machine and program means of protection, which are meant to be stationary installed in the production components but also they could be mobile which are used in the smart factory control technological processes.

The cyber and physical production communication environment organization scheme based on heterogeneous nets apart from threats of information security in the same net is susceptible to the threats arisen from distributed character of production resources and data. Local nets of Ethernet and Bluetooth of cyber and physical production are of attacker’s interest to receive the rights of unauthorized access to the production data and to violate the production data integrity.

In the industrial Internet of Things, there is also the threat for company information security net such
as blocking the message transmission between CPSs and cloud services and applications, as well as possible failure of CPS servicing (CPS data accessibility). The global IoT net threats are normally remote.

A cyber and physical production must have preventive measures against the following:

- an unauthorized connection to the company net;
- an unauthorized corrections of the cloud services and applications;
- an unauthorized protocol changes of production data transmission;
- an unauthorized changes of identification order and authentication participants of production process and other.

The company information security task is further complicated by the fact that all types of technological equipment have software components including CPS operational system from different manufacturers. Wide range of CPSs, mobile means of communication and integrated systems program applications practically exclude the creation of compact security system to provide high-level protection of the company resources.

In addition, equipment from different manufacturers normally functions properly with additional software components to automatize the production activity. When a heterogeneous cyber and physical production is projected, it necessary to choose inter-operable components to minimize the company necessity of additional software application.

4. Conclusion

The Industry 4.0 production company information security is a multi-factor task with deep automatizing of technological processes and application of cyber and physical systems to implement digital ways of automatic control. By implementing digital technologies in production, the task of company information security increases.

The most effective protection against the company information security threats are machine and program ways of the company information protection.

The machine ways of the company information protection are based on the attacker counter-measures technologies, which block potential channels of the information flow away (production data) and channels to implement malicious software into production infrastructure. The machine ways of information protection help to identify potentially susceptible objects of the company infrastructure, investigate methods efficiency and means of protection and also to detect attempts of attackers.

The program ways of the company information protection are based on the technologies of the functionality control and the operator restricted access rights with CPS to the production data and production components. The access rights restriction for the production company personnel is performed using an anti-virus software, decryption and cryptography software, virtual nets and inter-net screens software and other.

Unlike the machine information protection means dedicated to protection of the production infrastructure in general, the program means of protection can be locally placed as a part of the production objects with their own calculation means. Protection means localizing can increase the company security level with the ability to detect an attempt of unauthorized information access before the malicious software distribution in all production components.

An important aspect of the cyber and physical production information security increase is an operator and CPS actions protocols, which will be analyzed later by the artificial intelligence system placed in the company cloud environment. The analysis of production process participants’ behavior scenarios may detect in time an attempt of the attacker’s unauthorized access to the production information and operator and CPS actions correctness in production.

The practical realization of information security of a digital company having cloud services and applications distributed in a territory including a trans-country space is based on some regulations and standards, which exist in some countries only and in international affairs. In this regard, to provide the Industry 4.0 digital factory, smart factory and virtual factory information security it is necessary to develop the standards of new generation compliant with the condition of digital economy in the
international level.

References
[1] Elvik R and Goel R 2019 Accident analysis and prevention 129 136-147
[2] Lai X, Balakrishnan A, Lange T, Jenihhin M, Ghasempouri T, Raik J and Alexandrescu D 2019 Microprocessors and Microsystems 71 102867
[3] Bogatyrev V A, Parshutina S A, Poptcova N A and Bogatyrev A V 2016 Communications in computer and information science 678 337-348
[4] Rauch E, Linder C and Dallasega P 2019 Computers and industrial engineering 2019 127 105644
[5] Singh P and Singh L K 2019 Nuclear engineering and technology 51 1289-96
[6] Ribeiro da Silva E H, Shinohara A C, Pinheiro de Lima E, Angelis J and Machado C G 2019 Procedia CIRP 81 240-245
[7] Gurjanov A V, Zakoldaev D A, Shukalov A V and Zharinov I O 2018 IOP Conference Series: Materials Science and Engineering 327 022110
[8] Zakoldaev D A, Shukalov A V, Zharinov I O and Zharinov O O 2018 Journal of Physics: Conference Series 1015 052033
[9] Mogos M F, Eleftheriadis R J and Myklebust O 2019 Procedia CIRP 81 624-629
[10] Li D, Landstrom A, Fast-Berglund A and Almstrom P 2019 Procedia CIRP 84 380-386
[11] Alcacer V and Cruz-Machado V 2019 Engineering science and technology, an international journal 22(3) 899-919
[12] Barreto L, Amaral A and Pereira T 2017 Procedia manufacturing 13 1245-52
[13] Kravchenko P and Oleshchenko E 2017 Transportation research procedia 20 367-372