Information security of Smart Factories

R A Iureva, Y S Andreev, A M Iuvshin, A S Timko
ITMO University, 49 Kronverksky Av., St. Petersburg, Russia, 197101

E-mail: raddaiureva@corp.ifmo.ru

Abstract. In several years, technologies and systems based on the Internet of things (IoT) will be widely used in all smart factories. When processing a huge array of unstructured data, their filtration and adequate interpretation are a priority for enterprises. In this context, the correct representation of information in a user-friendly form acquires special importance, for which the market today presents advanced analytical platforms designed to collect, store and analyze data on technological processes and events in real time. The main idea of the paper is the statement of the information security problem in IoT and integrity of processed information.

1. Introduction
The industrial Internet of things (IoT) drastically changes the entire economic model of the "supplier-consumer" interaction. This allows one:
• to automate the process of monitoring and managing the life cycle of devices;
• to organize effective self-optimizing chains from a supplier to an end-user company;
• to go to the models of the "economy of sharing" and much more.

A smart factory is formed on the basis of high-tech equipment: 3D printers, CNC machines, robotic complexes, etc. The use of sensors, as well as automated process control systems and operational control systems for production processes at the shop level, provides the ability to perform fast and flexible "automated" readjustment of equipment. It is characterized by the use of digital modeling and design technologies for both the products themselves or production processes throughout the life cycle.

In the most advanced cases, Smart Factory based on IoT allows one not only to improve the quality of technical support of equipment using advanced telemetry tools, but also to provide a transition to a new business model of its operation.

The introduction of network interaction between machines, equipment, buildings and information systems, the ability to monitor and analyze the environment, the production process and its own state in real time, transferring management and decision-making to intelligent systems lead to a change in the "paradigm" of technological development, also called "The 4th industrial revolution".

And on the other hand, the problem of information security in the smart factory is sharply posed. Popular only ten years ago, Windows XP was critically vulnerable due to lack of updates and design weaknesses in terms of security. Similarly, ten years ago, smartphone manufacturers did not even think that their devices would be used by criminals to spread malicious software or illegal money making. After five years, the Smart Factories devices can realize the same fate, and the consequences
will be much more serious: imagine CNC machines infected with extortionists. This applies to many already installed devices that are designed for decades of operation.

Even if Smart Factories provide, unite and develop devices that can easily receive software updates, will this feature be used? Engineers do not want to install updates even on operating systems, although this is relatively simple, preferring to keep them open for cyber-attacks. If users are so careless about updates of their laptops and smartphones, is it worth waiting for them to upgrade each Smart Factory device?

2. Discussion

IoT allows us to implement complex end-to-end business processes in the virtual space arbitrarily that automatically perform optimization management (and engineering of various kinds of resources through the entire supply chain and creating value products - from the development of ideas and design to production, operation, and disposal). To implement such approach, it is required that all necessary data on the actual state of resources (raw materials and electricity, machinery and industrial equipment, vehicles, production, marketing, sales, etc.), both within one and at different enterprises, allows one to automate control systems of different levels (drives and sensors, control, production management, implementation).

Thus, one can say that IoT in Smart Factories is an organizational and technological transformation of production based on the principles of the "digital economy", allowing one to combine real production, transportation, human, engineering and other resources into virtually unlimitedly scalable program-driven virtual resource pools (shared economy) at the management level and provide the user not with the device, but with the results of its usage (device functions) through the implementation and production and business processes.

A distinction of the IoT system from traditional markets is the transformation of enterprises from isolated self-sufficient systems, within which all production and business processes which are necessary for the production of goods or services, are realized, into open systems of integrated highly automated processes. Such open systems are implemented according to the cloud services model in which the various market participants are united into a single platform for providing services to the end user, for the creation of which the main means of production are not the personnel but cloud services automatically manage pooled software-defined devices (Fig. 1).

![IoT Devices](image-url)
Information about the production process will come in large volumes, so the work of a smart factory depends on the quality of information exchange, its reliability. The virtual character of setting up production will open the possibility of producing products for an individual customer; therefore, infringements of information security can entail temporary and financial losses of the factory. In other words, for traditional enterprises and their systems (markets), the basic resource necessary for the direct management of all other types of resources is personnel, and as a result, the main type of information exchange in such systems is the exchange of voice and data information between people. And for IoT systems that do not use manual labor directly in the execution of production processes and whose control system automatically addresses directly to the necessary actuators and sensors, the basic resource is information. For example, sensors with RFID tags can be widely used in Smart Factories. With their help, one can monitor production processes, measure moisture, workplace conditions and nuclear waste. The technology offered by the University of Manchester experts can simplify the collection of information, has no wireless network limitations and is compatible with Wi-Fi and 5G networks.

3. Smart Factories Information Security

Figure 2 shows the dependence of the probability of achieving a goal by a system from the number of inoperative devices of IoT. These devices are so-called “malicious” devices which disturb information security of smart factory. As with the enlargement of malicious devices, the efficiency of the factory is reduced (fig.2).

The increase in IoT security risks, including the loss or inaccessibility of data, the spread of false data about the purpose of the system, and the use of distorted information, necessitates the evaluation of known and new algorithms from a security perspective. It should be noted that unified approaches to the provision of IB IOT, taking into account the specifics of this type of systems, have not been formed to the present day.

![Figure 2. Probability of achieving a goal by a system from the number of inoperative devices of IoT](image)

The main threats to information security of IoT include unauthorized passive interception of
messages during inter-agent communications, violation of the integrity of data transmitted over the network, unauthorized access to data, denial of service (DDoS attacks), interception of requests with subsequent modification and playback, receiving or sending data, etc. The decentralized nature of the construction, the absence of a single center, the heterogeneity of components, the potential for communication with any node make IoT maximally vulnerable to any of the listed threats. Besides, according to ISO 27001 and special features of Smart Factories and devices connected in IoT, it is important to mention such type of information security risk which sounds the following way “Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities” [10]. Threats to energy security in the case of IoT in a smart factory are short-term or long-term events, destabilizing the operation of the system, limiting or stopping power supply, which in turn can lead to negative outcomes. The system is in an energy-safe state if there is a safe sequence for performing all tasks in the system. A safe sequence of tasks is a sequence of rational execution of processes, in which each process takes only available resources. The final state of the power supply of the device is such that the device can recover its resources upon completion of the process. In addition, no device will remain without a task until it has a resource to run it. The need to take this aspect into account in the context of the information security of IoT is determined by the fact that an increase in energy consumption can lead to a significant reduction in the probability or impossibility of the main task of the system.

4. Results
In the world, there are various structures that develop the concept of IoT. However, if they act in isolation, this will slow IoT’s implementation. On the one hand devices in the smart factory will be able to conduct market research, pool statistics, to develop and to implement new solutions aimed at product improving. Besides, hacked devices in smart factory can be used as a path to an internal network of a company, and using all vulnerabilities of web cameras as a static picture in a robbery can be displayed. In this regard, it is necessary to develop common standards and requirements for research, technology, IoT’s safety, and operation. It is important to consider the compatibility of new technologies with existing IT systems. In the event of disagreement, all participants will incur material and time costs. In addition, international standardization will make it easier for IoT solutions to enter the global market. In modern high-tech production, the center of gravity shifts to the design stage, and it is done on the basis of mathematical modeling completely “in the shadow”, including a series of virtual tests. This allows one to eliminate possible errors and manage to make a product demanded by a market quickly and cheaply. And it is so-called “the window” to an opportunity to be faster and cheaper than competitors.

References
[1] Rubenstein M and Hoff N 2013 Kilobot: A Low Cost Scalable Robot System for Collective Behaviors Computer Science Group Harvard University 67 34-52
[2] Gjondrekaj E and Loreti 2012 Towards a Formal Verification Methodology for Collective Robotic Systems In Formal Methods and Software Engineering, Proceedings of the 14th International Conference on Formal Engineering Methods 7635 54-70
[3] Sarvapali D Ramchurn and Dong Huynh and Nicholas R Jennings 2004 Trust in multi-agent systems The Knowledge Engineering Review 19 1 1-25
[4] Reynolds C Flocks 1987 herds and schools: A distributed behavioral model Proc. of the 14th annual conference on computer graphics and interactive techniques 1 25–34
[5] Saif U and Greaves D J 2001 Communication primitives for ubiquitous systems or RPC considered harmful Distributed Computing Systems Workshop, 2001 International Conference on 1 240-245
[6] Massink M and Brambilla M 2012 Analysing Robot Swarm Decision-Making with Bio-PEPA In Swarm Intelligence, of Lecture Notes in Computer Science 7461 25-36
[7] Ruoklainen T and Kivtsonen 2005 Interoperability in Service-Based Communities Business
Process Management Workshops: BPM 2005 3812 317–328

[8] Yee WinShwe and Yung C Liang 2009 Smart Dust Sensor Network with Piezoelectric Energy Harvesting The 6th International Conference on Information Technology and Applications (ICITA 2009) 1 184-187

[9] ISO/IEC 27001:2005(E), Information technology — Security techniques — Information security management systems — Requirements

[10] Sushmitha S and Malathi K 2016 Home automation by means of Internet of Things Int. J. Pharm. Technol. 8 19874–19883

[11] Zhang K and Li H and Ma J and Liu X 2018 Efficient large-universe multi-authority ciphertext-policy attribute-based encryption with white-box traceability China Inf. Sci. 61 61-64

[12] Gonzalez N and Goya W 2017 Internet of Things: A Scientometric Review IEEE Computer Society: Washington, DC 61 1-32