

*J.R. Maletic, M.Sc.,  
highschool professor*

*GSP College,  
Belgrade, Serbia*

*Z.P. Cekerevac, Dr., Dr. h. c.,  
full professor,*

*Faculty of Business and Law, University "Union - Nikola Tesla",  
Belgrade, Serbia*

## **IIoT SECURITY IN SUPPLY CHAIN**

### ***Annotation***

*As the use of IIoT is expanding, there appears an increasing concern about how to protect the huge amount of data that needs to be transferred and stored. This is particularly true for supply chains (SC) and their implementation. Reliability problems of data transfer and protection of the entire SC require protection of codes, detection of unauthorized access, protection against keys and security information stealing, protection against Trojan horses, malware, viruses, worms, logic bombs, and other malicious software that sabotage system operation. Industrial Internet of Things needs protection of physical devices that are far from immediate control, data, networks, and MultiPoint Control Units that support standard encryption, decryption and authentication verification. Some safeguards that are important in the design of SC digitalization are given in this paper.*

***Keywords:*** *IIoT, security, safety, reliability, sensors, networks*

Due to the rise in computer crime and other risks, organizations have developed numerous safety and security techniques to protect their systems and data in physical and virtual environments. Basically, one can talk about privacy, security, and safety of people, companies, and environments. Safety and security are inseparable. Workplace safety is a complex issue of vital importance for the protection of workers, avoidance of production and distribution interruptions, and achievement of operational excellence. IIoT allows connecting participants to the SC, which enables better visibility of the security system, identification of security risks, reduction of the risk impact, better assessment of the use or abuse of the security system and improved compliance of the measures with the system [1]. Some measures are designed to limit the physical access to computers and devices, some are related to backups, some use standard privacy and individual rights protection systems, aiming to reduce threats to people and organizations, software and hardware malfunctions. Lately, to increase security, the emphasis has been put on using Blockchain and Cloud. Term *IIoT Security* implies the protection of industrial and other organizations from cyber threats in their LANs. Integrated network-controlled

devices and sensors (NoT-Network of Things) on the Internet face and are vulnerable to "hacking", especially on malicious IP or URL addresses, and malware. The IP address only determines the location while the URL specifies the location, protocol, and a specific resource. The basic elements of IIoT, and therefore NoT [2], are sensors, aggregators, communication channels, e-utilities, and decision triggers. Each element with its properties and role, integrates into a unique information system, in a way that affects the reliability of NoTs.

**Sensors and their clusters.** The sensor detects, measures or points to a specific physical dimension, converting signals from one energy domain into an electrical impulse and is part of a more complex system that provides access to the main control system or device (processor or microcontroller). The sensors have built-in IP support or can be easily adapted for IPs, using TCP/IP as a common networking platform, which can be considered suitable for the Internet. Today, more and more are talking about wireless SMART sensors that make up an integral part of the IIoT. Smart sensing capabilities are significantly increased, enabling processing and analysis of data at a source or near source (Edge computing). The information moves between devices and platforms within two-way communication using built-in microchips to perform predefined functions after receiving certain data, and then process these data before transmitting them. [3]. The sensors have IP65 and higher-level protection, transmission distance 300 to 700 m (in free space), supporting protocols compatible with TCP/IP networks, RS 232, etc. Although they lose sensitivity and/or calibration, their life expectancy is over one million operations. Reliability of the work and condition of the sensor depend on the exposure to heat, water, dust and other negative effects, that resulting in problems in data reading and malfunction, which reduce the life of the sensors together with increasing the risks in transmission and the accuracy of the data. Sensors do not have the ability to defend themselves and must rely on special security protections, such as firewalls and/or intrusion detection/prevention systems. The firewall is most often placed between a LAN and a public network (the Internet), and its purpose is to protect the network data from unauthorized users (blocking access according to security rules that have been previously adopted). This protection has evolved from Access Control Lists (ACL) of routers, through Proxy firewall, Stateful inspection as the third generation of firewalls, to the Next Generation Firewall (NGFW) and Palo Alto Networks (PAN), which can "see" and control most well- and lesser-known applications whose traffic goes through the network, regardless of which port and protocol they use or if they use some hiding tactic. The lack of security tools on the sensors and devices itself greatly complicates the safety of IIoT because they are usually set up in an open space or in remote locations where they are easily accessible. That increases security problems significantly. Security and safety should be embedded in the design of the IIoT system, with strict controls of reliability, authenticity, encryption data verification procedures, and interoperability standards. Sensors can communicate directly one to another and, also, in some situations, become aggregators.

**Aggregators.** In IIoT, millions of sensors will transmit data across the gateways that efficiently compress gigabytes of raw data. Aggregators help manage Big Data,

whether virtual or physical. From the aspect of implementation, they require strong computers, good connections and a quality network that will not cause data and information loss. Security is a general problem for aggregators due to the sensitivity of their aggregated data, especially when receiving inadequate data, when they are under attacks, or when they are faced to other unforeseen conditions (introducing fake sensors, power failure ...). Such events may cause application crashes and system security breaches.

**Communication channels.** When transmitting data, channels have virtual (protocols and applications) and/or physical (wires, sensors, aggregators) dimension, which in relation to flows (one-way and two-way), complexity of interconnection and communication between entities using different protocols, and their burden, create conditions for reducing reliability and security on the network, through various disruptions, sensor failure, eavesdropping, delays, and disruptions in data distribution. Wireless channels over IEEE 802.11 have greater reliability, although redundancy can also improve the reliability of the communication channel.

**E-utilities.** As a software or hardware products or services, they should provide new supporting services and products that will be embedded in new future applications, especially in the cloud applications, databases, mobile devices, identity verification, and so on. Maintaining the cloud server system is done during system operation, and can lead to delays in verification, which is a system failure that makes the resource unavailable, and therefore the services are unreliable.

**Decision trigger.** A decision trigger is a condition that activates the action if the permissible threshold of a certain measured value, that is obtained from the sensors, actuators or some transactions from a specific IIoT, is exceeded. These are coded "rules" that inform the user as the decision-maker that certain operations should be executed or denied. The decision trigger can be followed by automatically invoking the next operation or referred to a further procedure, or adapted to changing environmental conditions, which indicates that they can have a virtual implementation at a specific time or be continuous. In addition to malware, problems can appear because of delays in data collection, sensor interference, eUtilities, communication channels, and low-performance aggregators, and other causes of the system crash. Reliability is essential, pointing to the need for continuous control of unauthorized access, loss of data integrity, not accepting malicious inputs, etc.

According to [4], in 2018, a total of 65 cyber-attacks were reported directly affecting SC operations, of which only in November 2018 it was achieved the largest number of attacks, more than 20. Of reported attacks during the year 2018, in 10 cases manufacturers were attacked, six times airports and airline companies, five times courier and postal services. Five attacks were reported in ports or shipping companies, and two on the rail. Increasing the number of attacks in cybersecurity that affect the SC organization and infrastructure are complex. Threat actors increasingly see SC and traffic infrastructure as a good target, regardless of whether their goal is to find out business secrets, blackmail or cause economic damage. Moreover, the increase in digital integration, combined with the development of IIoT

technology (where some elements are poorly secured), provides new opportunities for offenders to enter and disrupt the processes of the SC.

In order to increase reliability, security, and safety, it is increasingly being insisted on the use of Blockchain and Cloud. According to [5], blockchain allows easy tracking of all network transactions in blocks because they are timed, they provide valid information and high confidentiality of members of the network by cryptography of keys and user codes, and inaccessibility to blocks. In the case of DDoS attack, the system can function continuously and normally thanks to multiple copies of the ledger, complete data integrity, accurate and constant quality of encrypted data, reduced risks of cyber-attacks and errors, and so on. There is a risk that encrypted data cannot be recovered if the user loses the private key needed for decryption. The problem can also appear due to the processing speed of a large amount of data, so cloud computing has become necessary. It needs to be managed through planning and policy, which will significantly impact on raising the level of security and security of clouds and data in it. Different cloud models have different risks and control modes. The development of this technology will enable better customer demand analysis, more sophisticated architectural planning, more flexible risk acceptance processes, and so on.

### ***Conclusions***

Nowadays, in addition to industrial control systems, there are authentic platforms for protection against various external and internal attacks on the IIoT, such as Critical System Protection (Symantec), DigiCert security (Digicert), BrightCloud (Webroot). Most of these platforms are based on "cloud", they do not affect the performance of the devices and thus the network flow. They can protect the system in real time at very low risk. Using Edge technology can increase the security of the IIoT devices by minimizing the exposure of the network and reducing the space and intensity of the attack. There is a lack of standards for auto-identification and approval of the IIoT edge device. Alarm sensors and digital controls (IP, CCTV, HDCVI, HDTVI ...) use IIoT most commonly for detecting theft and protecting property. As complete protection is difficult to achieve, it is necessary to determine safety priorities. One huge area for logistical organizations is the safety of workers, by monitoring the condition of equipment, handling procedures, predicting failures, reducing the risk of injuries at work and all overall occupational safety.

New security technologies are needed, that will support sophisticated security approaches to protect IIoT devices and platforms from attacks and malware, including DDoS. A typical example of the urgent need for new security technologies is the recent attack on many well-known servers from millions of IP addresses. The attack was carried out using infection with Mirai malware.

Which security and safety measures will be used depends on achieving the appropriate degree of reliability, on the environment, introduction costs, geographical location, connected devices, the openness of the system, pre-known type patterns of future demand, and other characteristics of the system.

## REFERENCES

[1] Maletić, J. & Radičević, V. (2018). Some aspects of automatization of the supply chain. *FBIM Transactions*, 15 Apr, 6(1), pp. 46-58. [http://fbim.meste.org/FBIM\\_1\\_2018/11\\_05.pdf](http://fbim.meste.org/FBIM_1_2018/11_05.pdf)

[2] Voas, J. "Networks of Things". (2016). NIST Special publication 800-183. Computer security. US Department of Commerce. Information Technology Laboratory. Gaithersburg, MD, USA.

[3] Cekerevac Z.P, Prigoda L.V, Maletic E.R. (2018). *Supply chains - visualization and IIOT*. IV Mezhdunarodnaya nauchno-prakticheskaya konferentsiya Nauchno-tehnicheskiye aspekty innovatsionnogo razvitiya transportnogo kompleksa. Doneck.

[4] Hartmann S. (2019). *Resilience360 Annual Risk Report 2018*. Troisdorf/Spich. Germany.

[5] Banafa A. (2016). *A Secure Model of IoT with Blockchain*. Technology-Digital World.