CYBER SECURITY FOR SMART SYSTEM IN INDUSTRY 4.0

Adelin-Marian Berindei
Valahia University from Targoviste
Email: adelin.berindei@gmail.com

Abstract - Industry 4.0 represents last generation in terms of production methods and implementation of new technologies in the manufacturing process. In the last decade it has known an immense development that managed to combine very effectively numerous technologies, low cost computing and ever-expanding networking, implemented in the very core of the factory. Because of its necessity of being integrated with other elements that come to complete the business enviroment such as connectivity between devices, analysis or human interaction, it must be taken into consideration all of the aspects that may interfere and alter the entire production process. When it comes to this, concerning that the entire industry is based on electronic or networking devices, they are used by people that need to be careful with the confidentiality of their accounts and passwords, the information circulating on the transmission medium may have a certain level of privacy, cyber security must be treated with greater importance. This paper introduces some elements that come in the composition of the Industy 4.0, benefits of it, and especially concepts of IoT security, security of the transport medium or cloud security and it describes in detail an infrasctructure model that those conceps can be applied on. It represents a portrayal of the central aspects and challenges that a still young industry has to take notice in order that it achieves its true potential.

Keywords: Cyber security, IIoT, Industry 4.0, Cyber-attacks, IoT security, Cloud.

1. Introduction

One event that has known a gradual and an outstanding growth due to countless elements comprising industrial systems that are interfaced with Internet communication technologies, to form smart factories and organizations of the future, is known as Industry 4.0. Industry 4.0 and related technologies, as those which are based on cloud design and Industrial Internet of Things manufacturing, are currently driven by a new disruptive innovation that engages to bring in countless new opportunities and rise the current market production value.

Numerous studies that have tried to quantify those opportunities are confident in talking about large numbers in terms of connected devices, global connections and of course, economic impact. It is estimated that by 2029 more than 15 billion IoT devices will be attached to the enterprise infrastructure, or in terms of mobility, are expected 27 million new IoT connections until 2026, registering an 120% growth compared to 2020.

In spite of all these overwhelming statistics, the existing Internet technologies are already affected by cyber security and personal data protection, issues that have to be taken into consideration when implementing new technologies, and Industry 4.0 has to face both traditional cybersecurity issues to which will be added its unique security and privacy challenges, which if not properly addressed, its true potential may never be achieved.

Year 2021 came with plenty of fresh domains in matter of technology, startig up with emergence of **free-to-use spectrum** 5G over CBRS (Citizens Breoadband Radio Service), in January 2020, the federal communications commission authorized the use of CBRS band of CBRS services, growth of the open source SDN platforms and development of edge cloud computing technology, which provide serious benefits for manufacturers and help achieving what is widely known as Industry 4.0 revolution and Industrial Internet of Things projects.

Industry 4.0 will encompass numerous technologies and associated paradigms. Some of these paradigms are the industrial Internet, Industrial IoT together with the new paradigms in the field of product development typical of the current century, among which can be listed: cloud-based design, cloud-based production or large-scale innovation.

2. Security Issues in Mechatronics Smart Systems

The perfect combination of low-cost computing and ever-expanding networking has allowed the IoT to evolve. Now, IoT encompasses all types of devices,

widely used, from home devices, watches to cars and trucks. Technically speaking, it is a collection of artifacts that combine electrical, mechanical, computing and communication systems that allow internet communication and data exchange. IoT is a key factor in the digital transformation in the enterprise with the potential to increase labor productivity, efficiency and profitability of the business, as well as the overall experience of employees. Nevertheless, growth of interconnected networks and devices automatically increases the number of entry points in these systems, which causes the systems to develop a wide range of vulnerabilities and allows intruders to take advantage of any weaknesses found in them.

In the scheme below, it is displayed a functional system of Industry 4.0 and a brief analysis about security issues that might be encountered

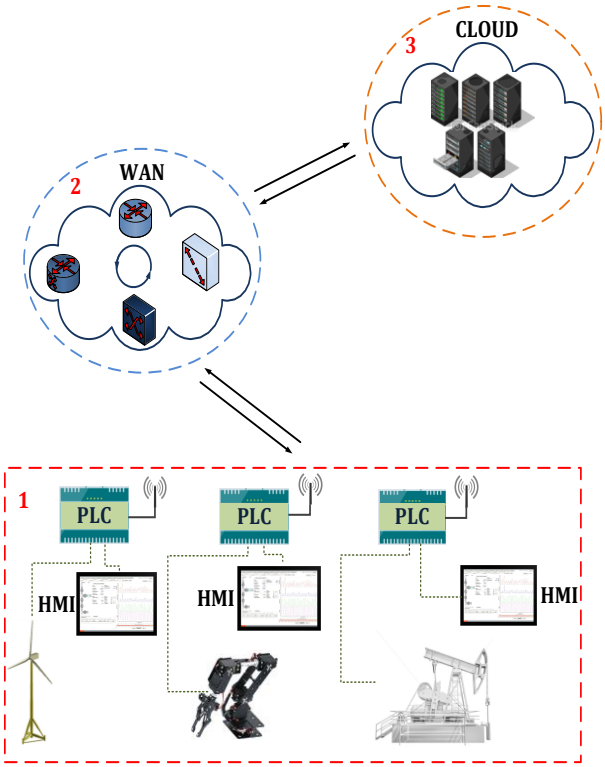

Figure 1: Functional system of Industry 4.0

Within the structural system of this industry, 3 different security levels can be distinguished:

1. **IoT security** – security of the electronic devices that are in contact with the external environment, systems that form operational technology, so called OT's

2. **Security of the transport medium** – represents protection of the network devices that includes network equipment, the fields that includes computer networks, which involves protocols, technologies, systems, tools and techniques to secure and stop malicious attacks.

3. **Cloud security** – the matter of security and confidentiality is amplified by sending out and storage data through many and different jurisdictions, with different levels of security. Despite advantages, interconnection of IoT impose a new challenge in terms of security that can overcome to the unmonitorized network end devices, to the enterprises. While IT departments are focused on taking protection measures on standard network devices, security preventions associated to IoT devices are less known, and those in question tend to be neglected. Reason for this seem to be twofolded.

Firstly, standard systems of cyber security seem to lack the ability of recognizing specific IoT network traffic, their unique risk structure and their exclusive behaviours.

Secondly, IoT devices are implemented by any business centre and are not recognized as proper IT integrated devices, causing their avoidance when managing and upgrading standard security devices. Certainly, this is generated by the first motive, not bringing up that most of IoT devices are based on a different specifc type of hardware, operating systems and antimalware software, and with an estimated life time much extended than cyber life.

IoT devices are labeled as targets by the hostile attackers due to the lack of care by the IT departments, in contrast to PC's, servers, laptops or phones. Without a proper traking and identification mechanism of IoT devices, these are demoted as unmanaged network end-devices and consequently are left exposed to vulnerabilities, password attacks or malware infiltration software's.

Traditionally, OT's cyber security was not absolutely demanded because their systems were not connected to the Internet. Very frequently, IT networks and OT's are kept apart one from another, which causes a double effort when it comes to security and avoiding transparence matters, because IT networks are unable to track the entire area of their manageable filed focusing only on their traditional, known network devices, and leaving almost half of the entire network ungarded. Moreover, this approach makes very difficult in identifying from where the attack might came from because these isolated teams are not aware of every device attached to their network.

Technology systems that are used in the operational environment, are in the most part, similar to the ones used in IT environment, but their employment have a different purpose. They are initialy designed as a way to interact with other machines, like ICS (Industrial Control Systems), and guarantee that their assest are operating correctly, in terms of availability or uptime requirements of their devices, rather than be used as an instrument for human interaction.

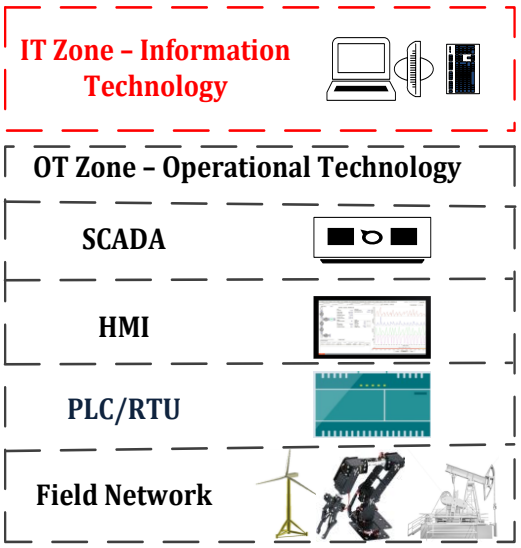

Figure 2: Convergence OT and IT zones in SCADA infrastructure

Cosidering this issue, cloud comes in response as an obvious solution in matters of integration, due to its capability to storage large quantities of information in scope of analysis. However, OT teams are not accoustumed with this aspect, not having an aquitance of control, autonomy or latency whatsoever. An alternate option that enterprises are heading towards would be edge computing, which seem to reassure both sides in question, allowing to the IT departement to have and complete image about the structure and can manage and monitor it from the core level, while it is still under the control of the OT teams.

IIoT can be imagined as the new generation of SCADA (Supervisory control and data acquisition) systems that provide the basic infrastructure mainly for the world's critical infrastructures, such as nuclear power plants, oil refineries, water treatment, manufacturing, energy and transportation. These systems have built their current infrastructure by integrating cloud technologies into their entire network topology. A SCADA system is a widely distributed computerized system that spans large geographical areas, collects and analyzes real-time data from field devices for the purpose of automating, monitoring and controlling physical processes. SCADA systems, in principle, monitor and control a network of PLCs (Programmable Logical Controllers) and RTUs (Remote Terminal Units), which use sensors to measure the performance of local operations and the spread of automation. A SCADA control center collects data from field devices and allows human surveillance and control of these devices from a central location.

The latest breakthrough in the development of SCADA systems comes in the form of IIoT which in turn is a significant part of Industry 4.0. It uses cloud computing and its commercial availability to improve productivity and reduce costs by adopting IoT technology.

When it comes to the security component of a system, which involves real-time data collection, a comprehensive analysis is needed, and it starts from understanding the concepts of protection of a network, management and physical systems. This problem becomes even more complex when it comes to migrating to the cloud.

Cyber attacks on SCADA systems can be categorized into: hardware attacks, software attacks and attacks on communication systems. The SCADA control center performs its processes based on information received from RTUs. Attacks that jeopardize the control process focus on changing control data or blocking data transfer. The main threats to SCADA systems are several forms of DoS (Denial of Service) attacks, such as DDoS or MITM (Man in the Middle).

3. Conclusions

An exhaustive analysis in matter of cyber security concerning a functional system of Industry 4.0 would mean dividing it into three large security categories (IoT Security, Security of Transport Medium and Cloud Security). Regarding this, security of IoT devices takes precedence.

Cyber attacks on SCADA systems can be divided in: hardware attacks, software attacks and attacks that are launched on communication systems. SCADA's control centre represents the core of the entire mechanism, where all the information gathered form RTU's is processed. Attacks that are launched over this comand and control process is centered to alter control data or block data transfer. Most common attacks of this type could be DoS (Denial of Service), DdoS or MitM (Man-in-the-Middle).

Systems that are based on cloud infrastructure, are also exposed to the same risks in matter of security, likewise all systems that are incorporated in cloud. Nevertheless, there are also many vulnerabilities that have to be taken into consideration when talking about SCADA systems integrated into public cloud. First of all, SCADA systems based on cloud tend to be very vulnerable to ordinary types of attacks, described above, by sharing the same network infrastructure with other unknown parties.

Secondly, there is the peril of network connections between SCADA systems and cloud, that tends to have and impact on the entire industrial control process. On the other hand, application protocols that SCADA systems are equipped with, like Modbis or DNP3, are completely insecure due to their inability of supporting authentication and encrypting algorithms.

Lastly, utilizing commercial solutions, which do not cover a large range of security issues, instead of propietary ones, will eventualy have an disastruous effect on the cyber security of the entire system.

There are many ways of stealing confidential information. One in particular is called passive traffic analysis, which consist in the injection of a corrupt code in operational applications to alter the control measures, steal end user virtual identity and gain acces to the information.

Affect the normal function of the routing protocol using interference to disturb the communication

Take advantage of the software vulnerabilities, in order to deplete resources and take control of the devices or infect them with malware

Take control of routing information and affect network traffic, as in a Sybil attack. By doing this, paves the way to other types of attacks such as DoS or black hole.

Scan and detect vulnerable devices in the network infrastructure by using side-channel attacks, which helps the hacker to have access to the device condition such as battery or memory, the way they are interconnected or routing information.

Falsify network nodes which gives the attacker the ability to insert corrupt traffic and gain access to a wide range of network devices and execute eavesdropping attacks.

Lacking responsibility in terms of access control that leads to unwanted guests to access the resources.

Another way that can put a organisation at risk is to take advantage of the cloud computing concept. Many enterprises use to store their data by making use of cloud infrastructure, but sharing a common infrastructure with plenty of different costumers can pose a series of serious troubles such as:

- Perform DDoS attacks in which the perpetrator makes use of the inside vulnerabilities in the scheduler component of some hypervisors and cause an unavailability of service;
- Insert malicious software into the cloud in order to imitate a virtual machine, and gain access to the information that otherwise would be transferred through the original one;
- Execute side-channel attacks that helps the attacker to survey electromagnetic field near the devices and access resources;
- Scan and study different clients with access to different applications, which can allow the hacker to get information about account names, passwords and inject malicious services in the cloud.

It has to be taken into consideration that majority of these attacks can be performed only by experienced attackers who have a lot of resources at their disposal.

References

[1] A review of industry 4.0 manufacturing process security risks, Appl. Sci., vol. 9, 2019 - J. Prinsloo, S. Sinha and B. von Solms

[2] A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories", IEEE Access, vol. 7, 2019 - T. M. Fernández-Caramés and P. Fraga-Lamas

[3] Addressing industry 4.0 cybersecurity challenges. 2019 - G. Culot, F. Fattori, M. Podrecca and M. Sartor

[4] Agile service engineering in the industrial Internet of Things. 2018 - Usländer, T.; Batz, T.

[5] Current cyber-defense trends in industrial control systems. 2019 - J. E. Rubio, C. Alcaraz, R. Roman and J. Lopez

[6] Cybersecurity Considerations for Digital Twin Implementations. 2019 - Hearn, M.; Rix, S,

[7] Cybersecurity data science: an overview from machine learning perspective. 2020 - Sarker IH, Kayes ASM, Badsha S, Alqahtani H, Watters P

[8] Cybersecurity for industrial control systems: A survey. 2020 - D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan and N. Meskin

[9] Cybersecurity for Industry 4.0. 2017 - Lane Thames, Dirk Schaefer

[10] Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. 2020 - A. Corallo, M. Lazoi and M. Lezzi

[11] Cybersecurity in industrial control systems: Issues technologies and challenges. 2019 - M. R. Asghar, Q. Hu and S. Zeadally

[12] Developing a Digital Twin and Digital Thread Framework for an 'Industry 4.0'. 2021 - Toh Yen Pang, Juan D. Pelaez Restrepo , Chi-Tsun Cheng, Alim Yasin, Hailem, Miro Miletic

[13] Network and information security challenges within industry 4.0 paradigm. 2017 - T. Pereira, L. Barreto and A. Amaral

[14] Protection of Intellectual Property of the Plant Continuity through IT/OT Cyber Security Measures and Governance into Industrial Automation & Control Systems. 2018 - Mason, A

[15] Protecting Information with Cybersecurity. 2019 - Borky, J.M.; Bradley, T.H

[16] Safety and security in cyber-physical systems and Internet-of-Things systems. 2018 - M. Wolf and D. Serpanos

[17] Secure cloud computing model for communication network management. 2019 - J Intell Fuzzy Syst

[18] Security Model of Internet of Things Based on Binary Wavelet and Sparse Neural Network. 2019 - Wang Z, Yang J, Guo B, Zhang X

[19] Warranty and maintenance analysis of sensor embedded products using internet of things in industry 4.0. 2019 - Alqahtani AY, Gupta SM, Nakashima K.