THE CYBER SECURITY PARADIGM IN INDUSTRY 4.0

Adelin-Marian Berindei[1], Cristinel Ilie[12], Badea Florentina[3]
[1]UVT Doctoral School (Wallachian University of Târgoviște) Romania
[2]National Institute for Research and Development in Electrical Engineering ICPE-CA Bucharest, Romania
[3]National Institute of Research and Development in Mechatronics and Measurement Technique (INCDMTM)Bucharest, Romania
E-mails: adelin.berindei@gmail.com , cristinel.ilie@icpe-ca.ro , mihaiflori@yahoo.com

Abstract – This scientific paper emphasizes the paradigm of Industry 4.0 from the perspective of cybersecurity, in which if there are digitalized factories and a digital chain connected to them, there is also the need of an amplified security system, and the usual IT security procedures are not enough to protect the production lines. This article treats general concepts from IT security's perspective, as well as OT's security, and also about the joining of those two into a holistic approach combining people, processes and technology to properly defend against threats and build a security baseline. Digitization matter and analysis of industrial system evolution is taken into consideration in this paperwork, correlating them with cybersecurity. Ever evolving environment of technology influences the growth and diversity in the complexity of threats and security risks, such as cyber-attacks, and related works in the IT domain gives new security challenges.

Keywords: Cyber security, IIoT, Industry 4.0, IoT security, Operational Technology (OT), Information Technology (IT).

1. Introduction

The world finds itself in a transition period when considering technology involvement in the industrial processes, here comes the necessity of connecting machines to the internet, the existence of smart sensors network, growth of wireless communication, system development, as well as smart devices and robots, real time data collection and representation, with the goal of changing technologies from their grounds resulting a digital revolution – Industry 4.0.

However, for what we are concerned Industry 4.0 remains a continuous threat for the production lines, generating an unparalleled interconnectivity between production environments. By digitization of factories and supply chains, basic IT security solutions and approaches solve only half of the problem. Cybersecurity must become an integrated step in the digital transformation plan of a manufacturer, addressing both information and operational technologies that cover industrial control systems.

Operational technologies (OT) are also named automation and control systems like SCADA (Supervisory, Control and Data Acquisition System). These systems are utilised to monitor and control critical infrastructures, such as electrical energy, pipes, water distribution systems, sewers and production control systems.

This article is based on best practices regarding cybersecurity applied in Industry 4.0. In the past, Information Technology (IT) and Operational Technology (OT) were seen as two separate domains, meaning that OT wasn't given access to the internet, the only security measure taken into consideration being physical security. Evolution in the technology area made the desire of remote system control to arise and the two domains that were once separated, now started to intertwine. This convergence between them meant that the OT area had to be monitored and controlled from the internet/cloud, coming with all the security challenges that IT industry faces. OT data that now travels the internet include sensitive information such as pressure, temperature and proximity levels, control and sensor signals.

Now this data that once was traveling unaffected between the internal systems, needs to cross an unsecure medium and all the control mechanisms and data that OT covered became significantly vulnerable to cyber-attacks [3].

This paper is organized as follows. Section 2 presents main concepts about what OT industry represents and how its most vulnerable components can be protected once with internet exposure. Section 3 focuses on how IT and OT businesses intertwine from the cybersecurity perspective. Section 4 provides strong conclusions regarding how best practices can be used to protect OT specific assets against cyber-attacks.

2. Operational Demands in Relation with Cybersecurity in Industry 4.0

The cybersecurity in Industry 4.0 is a slightly different matter compared with the usual IT security way

of proceeding, meaning that the same rules that governed application security in IT industry, don't apply anymore. The idea that has to be understood by the OT industry is that information security doesn't represent another operational task [4] [5].

Firstly, a best practice for implementing security at its highest level, is for the manufacturers to classify and segregate assets from unauthorized users guided by the security standards for industrial environments protection, such as IEC 62443, ISO 27001 and 27002, NIST Special Publication IEC 800-82 and NIST Framework for Improving Critical Infrastructure Cybersecurity.

Secondly, it would be important for the assets that demand similar security measures to be organized in the same areas both at physical and logical level.

Last but not least, communication between areas has to be set under a certain level of control, using traffic filtering devices which manipulates the flow of the traffic between areas and in the same area. Still, first priority lies in prioritization, delimitation and understanding of operational demands of industrial technologies.

The image beneath this paragraph represents a prototype of a baseline architecture of a smart factory in the Industry 4.0, based on access levels, which includes the concept and the operational needs of implementing security in that specific factory. What I was trying to emphasize is that even if the merging between those important branches (IT and OT) poses a great amount of challenges to come across, this integration is possible and still be able to preserve the balance between the efficiency that must be kept for mechanical systems and the vulnerabilities of the computers, that once they are connected to the internet everything changes. As it can be seen, mechanical processes are standing at the end of the architecture and every piece of information that they transmit to the computers, and eventually to the end users is protected with the best measures that IT industry can provide, such as mounting firewall at the second level to protect and direct the valuable date, next the DMZ (a Demilitarized Zone Network) zone implemented to monitor which traffic has to cross the border to the internet or not, and finally at the forth level e-mail and web security applications that represent a last resort security measure to protect information.

Areas or zones can be classified in enterprise and control zones. In the enterprise zone, is where the split between internal intranet network and the internet that connects the manufacturers.

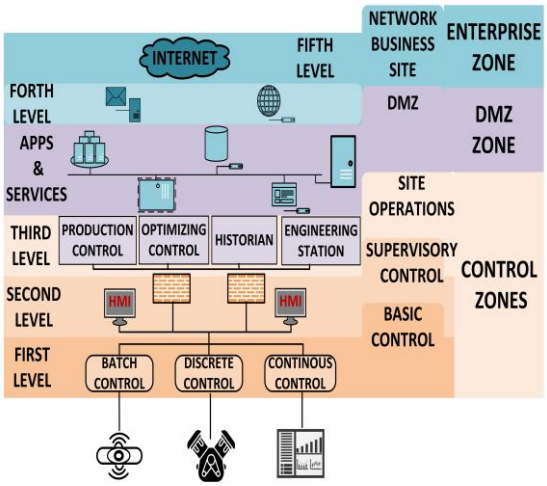

Figure 1: Functional system of Industry 4.0

Control zones are divided into operational control zones that store data history and also inhabit workstations, supervisory control zones that contain SCADA systems, HMI (Human Machine Interface) and DCS (Distributed Control System) through which terminal units are remotely managed, programmable logical controllers (PLCs) and smart devices and basic control zones that contain the control devices for valves, actuators, etc.

3. Cybersecurity Directions in Industry 4.0

Once that operational demands of smart industry are clearly defined a clear path regarding cybersecurity in Industry 4.0 can be instated. First of all, a separation between OT Security and IT Security has to be made, while safety is treated as number one priority: security procedures in the IT environment are different from the ones in the OT's, therefore the manner in which security measures and controls are implemented differ, as well as terminology does. Besides, security priorities in the IT industry related to confidentiality, integrity and availability are reversed in the OT industry. On the production line, the process itself must remain hidden from the outside world, but the factory safety is more important. If IT security were to be applied to OT environment, this would result into unwanted incidents and safety gaps. For example, a door that should be open, following IT confidentiality rules, from the OT perspective this would be opened for people's safety in case of an emergency.

Another reason for which the priorities are taken backwards is that confidentiality in OT could be completely covered by the IT. Only by understanding these principles and the differences between IT and OT security would be improved and optimized in both of those worlds.

In this image there is a representation of how principles and priorities are seen from both perspectives and there is illustrated a comparation between them:

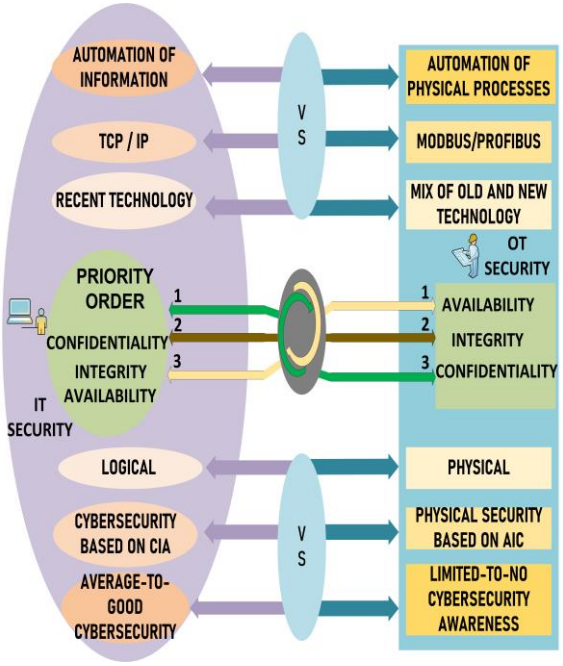

Figure 2: Base reference design and security policy

Creating a complete security frame inside Industry 4.0 brings a lot of challenges that are actually based on the convergence of the two security environments (OT, respectively IT), illustrated in the next Venn diagram below:

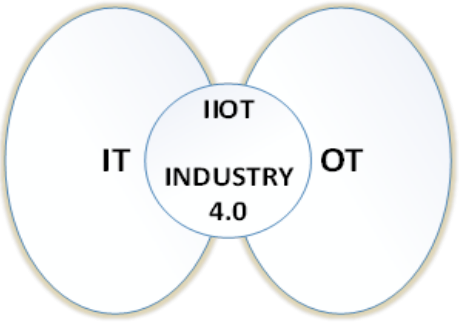

Figure 3: IIOT VENN diagram

IIOT security [1] [2] focuses on protecting IOT devices used in the smart factory and data that these devices collect and forward. IIOT devices are used for monitoring and controlling production processes and must be protected against cyber-attacks to avoid shutting down or malfunctioning of the production devices.

From the illustrations above there can be noticed that the final outcome is the same, but the priorities differ. OT needs availability and physical processes automation, comparing with IT that prioritizes confidentiality and information automation.

In the OT frame there are some security demands for the assets in the network and the workers that need to have applied personalized OT security policies, such as access management, physical and environmental security, hardening security, patching, backup, etc. For example, in most of the cases, patching procedures inside an OT medium are significantly different from the IT patching customs. Because availability in the OT medium represents a top priority, there are not much patches and restarts of the assets that can be done, and when is happening, this has to be for a predefined period of time.

Manufacturers that hold multiple locations are often facing challenges in implementing these policies to their multiple branches. Because of the diversification in the production environments, network infrastructure, suppliers and specific solutions that are done locally give the impression that although the factories belong to the same manufacturer to be in their very essence quite different. Developing a baseline design to describe the desired OT environment, including security solutions that the factories will inhabit, will eventually lead to an unparalleled industrial landscape.

4. Conclusions

In conclusion, cybersecurity represents a critical thing for the smart factory and for Industry 4.0. Protecting the networks, informatical systems, control devices and IoT devices is a crucial problem for the efficiency of a smart factory. Security teams that are responsible, have to strongly collaborate and implement the best practices and technologies available to protect smart factories from the ever-rowing threats in the cyber environment.

For example, the DMZ mentioned earlier, if it is implemented properly, it segregates efficiently the data flux used for the visualization and the Enterprise Resource Planning system. A well-documented network plan, in which a firewall installed before every point of exit of a critical information known as a Zoned Trusted Topology mitigates next to zero the chances of a cybersecurity attack to produce, from the outside at least.

IT and OT are two of the main systems nowadays that have the most influence on a company growth and productivity, and although they are seen as independent in the moment of speaking, for a manufacturer to continue to prosper has to follow a way to guide its company plan on the convergence of both IT and OT mediums to benefit from both operational efficiency and an up-to-date business.

A solution would be a unified platform to combine informational and operational data to increase the number of Key Performance Indicators (KPI) that the company is able to provide. For this to work, a series of mutual objectives have to be set to provide visibility on the whole company.

This transparency of operations results in business harmony on sites and departments, because of the threats that once infiltrated in the system do not trigger themselves immediately, but wait until an outside impulse activates them. Gap analysis can be performed to address this issue, by collecting data from each component of the factory to be further analysed, in order to compare the current state of things and what is needed to be done to reach the desired state.

Another thing that must be taken into consideration is the resilience of such a hybrid system (IT and OT). Because of all these important processes that take place in a given smart factory, testing if all the security measures have been implemented, such as following NIST or ISO standards, is a must. Pen-testing is paradoxically, one of the best ways to measure the defense, although it represents a way of attack. However, this controlled form of attack has to be performed with very much amounts of care, and after it has been proved that its necessity is needed. It can represent a high vulnerability that in the moments of pen-testing the system, a threat to be infiltrated without noticing.

This paradigm of cybersecurity in the industrial environment given by the unification of the two technologies, forces security solutions from a smart factory to integrate and work along to assure an increased protection against cyber threats. To do this, a strong cooperation between the teams in charge of securing IT and OT network has to exist. These teams have a mutual objective of evaluating the risks in the cyber world to enforce proper security solutions.

Moreover, a template of security procedures well defined, such as providing training and adequate instructions is necessary for the company workers, is a necessity in helping them to understand security risks and to take the best decisions to manage or to avoid them.

Nowadays for a factory it is important to have in use the ultimate technology in place, like artificial intelligence solutions and automated learning, that can and help to detect and prevent cyber threats. These technologies can be put to monitor systems or production networks, to identify suspicious behaviour and prevent cyber-attacks.

References

[1] Hazra, A.; Adhikari, M.; Amgoth, T.; Srirama (2021) A Comprehensive Survey on Interoperability for IIoT: Taxonomy, Standards, and Future Directions

[2] Lelli, F. (2019) Interoperability of the Time of Industry 4.0 and the Internet of Things. Future Internet

[3] Apostolos M., Christina S., Agellos K., (2019) ENISA - Industry 4.0 Cybersecurity: challenges & recommendations

[4] Kamel O. S., Hegazi N. , (2018) A Proposed Model of IoT Security Management System Based on A study of Internet of Things (IoT) Security

[5] Bhamare D., Zolanvari, M., Erbad, A., Jain R., Khaled K., Meskin N., (2020) Cybersecurity for industrial control systems: A survey, http://doi.org/10.48550/arXiv.2002.04124

[6] Lane T., Dirk S. (2017) Cybersecurity for Industry 4.0.: Analysis for Design and Manufacturing, Springer, ISBN-10 : 3319844563

[7] Angelo C., Mariangela L., Marianna L, (2020) Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts

[8] Hu Q., Asghar, M. R., Zeadally S. (2019) Cybersecurity in industrial control systems: Issues technologies and challenges, https://doi.org/10.1016/j.comnet.2019.106946

[9] Angelo C., Mariangela L., Marianna L, (2019) Cybersecurity for Industry 4.0 in the current literature: A reference framework, vol. 103, pp. 97-110, 2019

[10] Pereira T., Barreto L., Amaral A., (2017) Network and information security challenges within industry 4.0 paradigm, https://doi.org/10.1016/j.promfg.2017.09.047

[11] Aske H.K., Jens M.P., Mikki A., Mousing S., Theis D. V. (2017) Security in the Industrial Internet of Things, eBook ISBN: 9781003337812

[12] Good practices for security of Internet of things in the context of smart manufacturing, (2018) – ENISA, ISBN: 978-92-9204-261-5 DOI: 10.2824/851384

[13] Alqahtani A.Y., Gupta S.M., Nakashima K., (2019) Warranty and maintenance analysis of sensor embedded products using internet of things in industry 4.0., International Journal of Production Economics, Elsevier, vol. 208(C), pp. 483-499, DOI: 10.1016/j.ijpe.2018.12.022

[14] K Mcy - McKinsey Glob, (2019) Perspectives on transforming cybersecurity

[15] Janusz H., Ryszard J., Szymon O. (2021) Security Challenges in Industry 4.0 PLC Systems, *Appl. Sci.* 2021, *11*(21),9785, https://doi.org/10.3390/app11219785

[16] Malik, V., Singh, S. (2019) Security risk management in IoT environment, https://doi.org/10.1080/09720529.2019.1642628

[17] Cyber Security for Consumer Internet of Things. 2019, ETSI – available online https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (accesed on 14 January 2023)

[18] State of OT/ICS Cybersecurity Survey, SANS 2019 - available online https://www.forescout.com/resources/2019-sans-state-of-ot-ics-cybersecurity-survey (accesed on 20 February 2023)