Enhancing the Challenges of Network Information Security using Industry 4.0 Paradigm

[1]Vinitha K, [2]Suruthi N
[1,2]II Year M.E Computer Science & Engineering
Parisutham Institute of Technology and Science, Thanjavur.

***Abstract*: Currently Information and Communication Technologies support most of the industrial manufacturing processes. The IT uprising has carried an important conversion in administrations with high impersonations which are comparable to the computerization and electricity brought in the first and second industrial revolution. This evolvement has promoted the emergence of cloud-based systems, the Internet of Things, Big Data, Industry 4.0, BYOD and CYOD trends. However new technicalresolutions always convey security impressions which most of time reveal unexpected risks. In fact with growingdependence on technology to gain inexpensivebenefitsafety issues have been one of the most critical and challenging requirements for conducting successful business. In this paper it is highlighted some reflections regarding the challenges of Industry 4.0 emphasizing the security issues, towards raising awareness for security good practices within Industry 4.0**

***Keyword: Industry 4.0; Cyber physical system ; Security Challenges; Security Incidents,cyber security*.**

I. INTRODUCTION

The first three industrial revolutions evolved through proper management of the mechanization, electricity and IT phenomenon. The moderndevelopment of the Internet of Things has hugely prejudiced the industrialbackground and thus encouraged the fourth industrial uprising Industry 4.0. The approaching businesses will certainly create Internet and include their equipment, warehousing systems and production facilities as internet-enabled cyber physical systems. In the industrialbackgroundthese cyber physical systems includeclevermachineries, apacking systems and production facilities capable of exchanging information, triggering actions and controlling each other independently. Commonly this conveys significant improvements to the industrial processes involved in industrial, trade, supply chain and life cycle management. In practice, products are uniquely identified, may be located at all times and it is possible to know their own history, current status and alternative routes for achieving their target state. It is deeply recognized and emphasized the huge potential of the Industry 4.0 among successful industrial companies, which will become true digital enterprises, with physical products at the core of its action, augmented by the digital interfaces and the development of innovative data-based services. For example, in Industry 4.0 dynamic business and engineering processes enable last minute changes to production and deliver the ability to respond with flexibility to the disruptions and failures on behalf of suppliers. End-to -end transparency is provided over the manufacturing process, facilitating optimized decision-making. Industry 4.0 paradigm will certainly also promote the development of new ways of creating value and innovative business models, in particular, it will provide startups and small businesses with opportunity to develop and provide downstream services [1]. It is undoubtedly that smart factories have already begin to appear, and introduce a completely new approach to production and supply chain management. But whenever there is a widespread change, new inherent challenges arise, particularly regarding information and communications security issues. The integration of new systems and their increased hypothetical potential third-party access mean that a whole new range of security issues arise in this context. Security is critical to the success of smart manufacturing systems. It is important to ensure the protection of the enterprise infrastructures as well as the data and information contained in their systems against misuse and unauthorized access.

In this paper, it is highlighted some reflections regarding the challenges of Industry 4.0 emphasizing the security issues, in order to raise awareness required in Industry 4.0. This paper is structured as follows: in section 2, it is introduced the current challenges of manufacturing industry processes, in the advent of Industry 4.0; in section 3, it is presented an overview of the security challenges organizations should be aware, including an overview of the major security threats; conclusions and further developments are presented in section 4.

II. CHALLENGES IN INDUSTRY 4.0

The term Industry 4.0 is recent and is related with the Information and Communication Technologies (ICT) evolvement, particularly the integration of information technology, into the production processes. Industry 4.0 refers to the fourth in a series of technological revolutions: the first Industrial Revolution brought through the invention of the steam engine and the increase use of water and steam power, resulting into the mechanization of the industry at the end of the 18th century; The second industry revolution labeled as the “Mass Production” was promoted by the introduction of electricity and the assembly line at the start of the 20th century; Finally, the third era of revolution came with the advent of computers and the beginning of automation, when robots and machines began to replace human workers on those assembly lines. This third revolution era was known as

"Information Age", evolving to "knowledge-based economy". The recognition of knowledge as "human capital" together with IT technology brought important impacts in economic growth, and consequently promotes the emergence of the fourth Industrial Revolution through the use of cyber technologies [2, 3]. The value proposition of the industry concept 4.0 is closely associated with the end-to-end digitization of all physical assets and with the integration into digital ecosystems of all value chain partners [4].

These cyber-technologies are leading to the creation of a "smart" and highly versatile cyber-physical production environment. It involves various smart sensors, connected self-configuring robots, cloud computing, 3D printing, device to device (D2D) communications, big data analytics and communication channels sending and receiving massive amounts of data. The integration of cyber-technologies turns products and services as internet-enabled, which facilitates the integration of processes and systems across sectors and technologies and thus contributes to a bettercommunication and cooperation with each other in a new intelligent way, revolutionizing production, services provision, logistics and resource planning in a more effective way and cost efficient manner [5][6][7]. Additionally, it creates innovative services such as Internet-based diagnosis, maintenance, operations, mobility et cetera, which enhances the development of new business models, operating concepts and smart controls, mainly focusing on the user needs. The "Internet of Things" (IoT) has also affected the industrial sector and brought new benefits for customers, as it is evidenced by shortened production cycles, incorporation of customer needs in real time, maintenance is largely carried out automatically, orders are automatically filled in the right order, shipped and dispatched.

In practice, the goal of the Industry 4.0 is the emergence of digital manufacturing or also named as "smart" factory, which means smart networking, mobility, flexibility of industrial operations and their interoperability, integration of customers and innovative business models [2].

2.1. Smart networking

Internal logistics systems and operating supplies as well as automated systems and equipment are usually operated through the help of cyber technologies, such as wireless communication services, smart sensors and 5G telecommunication technologies [8]. These facilitate the accessibility to the resources used and a smart control, adding value to the business performance. Smart networking in smart factories requires "Plug&Work" synchronized networking, distributed processing capabilities, heterogeneous sensor interfaces and layered cyber-security. Software Defined Networks (SDN) is an essential element for the implementation of smart networking [9]. Furthermore, a cloud-assisted Industrial Wireless Network (IWN) can be suitable for supporting the adoption of the smart factory concept, as well as to support the implementation of the IoT paradigm and desirable services [10, 11].

2.2. Mobility

Smartphones and tablets have already made changes in industrial automation. In fact, they provide a temporally and spatially independent access to processes and services of the automated systems, introducing efficient mechanisms in the diagnostics, maintenance and operation of these systems. Mobility allows, using cloud-based platforms, to use system-based applications, real-time end-to-end planning and horizontal collaboration. With these systems, companies can become more efficiently integrated with horizontal value chain partners, including suppliers and key customers, and also significantly improve efficiencies and reduce inventories. In addition, the use of Device-to-Device (D2D) communications, can be used to track-and-trace devices on products allowing a better inventory performance and reduced logistics cost. Normally, each company develops a cloud-based system for connecting machines and devices from a variety of companies, facilitating transactions, operations and logistics, and collecting and analyzing data [4, 12].

2.3. Flexibility and interoperability

In the development of automated systems, it is possible to select the best offer from a large number of suppliers' components, modules and services. For example, the operations diagnosis can be carried out partly by the user, through access to the information retrieved on-demand, intelligently used and linked. The Big Data certainly provide important inputs, not only in the automation operation, but as well in the maintenance, diagnosis and development. Additionally, the integration of diverse organizational systems promotes their interoperability, which means that machine, devices, sensors and people are connected and can communicate with each other.

Over time, the IoT dissemination will force companies to move away from proprietary to open standards-based industrial solutions that will facilitate the connectivity and interoperability between devices. The industrial devices are commonly based in proprietary designs that not use standard communication protocols. Therefore, these industrial settings tend to be extremely inflexible and consequently it will limit the full potential of IoT implementation [13].

2.4. Integration of customers

Organizations are developing incommensurable efforts to facilitate the customization of their products according to specific individual needs of customers. Customers will be at the center of the changes to value chains, in the conception and definition of products and services. By integrating new methods of data collection and analysis, companies will be able to generate data on its product use and subsequently redefine products to meet the increasing needs of the end-customers [13].

The Industry 4.0 paradigm is about attaining a perfect alignment between companies and costumers through e-commerce, digital marketing and social media, as well as through monitoring closely the costumers' experience. Companies that properly address efforts on these purposes will gain outstanding advantages in customer service,

flexibility, efficiency and cost reduction. This business goal cannot be fully achieved without the integration of the supply chain, namely by connecting suppliers, manufacturing, logistics, warehousing, and costumers, conveniently driven through a cloud-based command center which continuously accesses the performance and the feedback of each supply chain member and of its stakeholders. The main goal of the digital supply chain is to deliver the right product into the customer's predefined spot as quickly as possible. Additionally following a responsively and reliably way, will certainly increase performance and efficiency, and increasingly reduce costs through automation [14].

2.5. Innovative business models

The increase development and use of the word-wide-web have promoted the expansion of on- line transactions enabling a flexible distribution of organizational products and services. In fact, organizations are also conducting their businesses on-line through the use of e-commerce platforms, in order to offer their customer innovative services and also to reach other markets. The trend is to offer modular and configurable products, in order to adapt the product to the specific requirements.

The main goal of all these technological challenges is to computerize as much as possible the manufacturing industry without the need for human involvement. The financial investments in technology are carried out to achieve a higher level of automation, in order to supply chains and production lines become more sophisticated, which means machines using self-optimization, self-configuration and even artificial intelligence to complete complex tasks allowing to deliver vastly superior cost efficiencies and better quality goods and services. The IoT and cyber-physical systems such as, for example, the increase volume of sensors promotes the collection of data, which can be used by manufacturers and producers to act upon quickly. In practice, the supply chains and production lines could be more readily controlled when there is data at every level of the manufacturing and delivery process; Computer control could produce much more reliable and consistent productivity and output, and the results could be increased revenues, market share and profits [15].

However, the beginning of this innovative era brings new and critical risks, especially in the security domain. In fact, whenever there is a widespread change, new inherent challenges arise, particularly regarding information security issues. The integration of new systems and their increased access may greatly raise new data security breaches. In practice, organizations should be able to identify their critical assets, and by critical it is meant, the organizational resources needed to operate normally, and after that identify the adequate secure mechanisms to be implemented, in order to ensure the reliability and stability for successful communications, as well as ensuring the confidentiality, integrity and availability of their automated systems.

III. THE SECURITY CHALLENGES IN MANUFACTURING INDUSTRY

The technological evolution has conducted to significant changes to the way organizations daily operate creating unprecedented pressure towards efficiency and performance. Actually, organizations heavily relay on the performance of their information systems to develop their business activities, resulted from their conveniences together with the emergence of new technologies. The clouding-based systems, Internet of Things (IoT), Industry 4.0 and the so-called Bring Your Own device (BYOD), or as IT professionals also call it “bring your own demon”, and Choose Your Own Device (CYOD) trend, has brought new enterprise technological changes but with increased security risks. The trend of everything around us becoming smart is not going to stop and engineers who design new innovative systems shouldhave in mind their security implications. In fact, “Smart” is not just about creating more opportunities and building faster and more valuable communications, it is also about making responsible infrastructure for those gains, and building robustness into the framework. The interconnected organizational systems significantly increase the exposure to many security risks, with critical and financial impacts. Malicious hackers exploit software vulnerabilities in the system components to disrupt the whole production chain, potentially for long periods of time if attacks are physically destructive.

Furthermore, subtle flaws can be introduced in the manufactured product which might compromise the image of the company or even attack the users of the manufactured or processed product. For example, a Trojan horse in a dashboard of every manufactured car can steal the personal information of their drivers. A more visible security incident detected was Stuxnet virus [16], which exploited vulnerabilities in the Supervisor Control and Data Acquisition (SCADA) systems [17]. Physical attacks and cyberattacks have evolved and are getting more sophisticated, in order to compromise critical assets, and cause a serious and global impacts. In this context, it is encourage fostering appropriate knowledge of security and awareness for security good practices, in order to build secure systems from the beginning rather than discover that what it was built was a pool of security flaws.

It is noticed, that government’s bodies’ worldwide have been advocating to cybersecurity issues and have developed significant efforts and resources to strengthening a cyberdefense posture. The strategy is to increase collaboration between governments, private sector and academia.

In this context, and in order to reinforce these actions, the European Parliament has recently (April of 2016) published and approved Directive 2016/679, requiring all European organizations to prove their capability to protect their organizational processing activities and the free flow of personal data between Member States [19]. This will force organizations to implement an information security plan, to enable them to recover from a security incident. However most of the organizations are facing serious difficulties. First, most of the organizations have a

completely lack of knowledge of this EU Directive. Second, they do not know how to translate organizational procedures into security policies and, much less, how to implement and manage a set of mechanisms to enforce those policies. Third, and with special concerning, small and medium enterprises cannot afford to invest the required budget in their IT infrastructure protection and workforce and thus to be in compliance with this Directive.

This EU Directive in conjunction with the new security challenges, which daily emerge, demand highly skilled workforce capable of responding to a dynamic and rapidly evolving threat scenario. In this context, academia and organizations should join efforts to offer information security, cybersecurity education, training and certification, with well-defined skilled objectives and competences aligned with organizational and social current security needs, at all necessary levels to make it effective to every segment of the population - which is far from being a simple task.

3.1. The major security threats facing Industry 4.0

Industry 4.0 and the technology involved have security vulnerabilities as other organizational systems. They have to manage the same external and insider threats as all businesses of all sizes have to handle in the current sophisticated cyber security sphere. The smart factory by its nature, is interconnected to many other systems, consequently any extended system is complex and with complexity comes significant increases of unexpected security vulnerabilities. Next, are presented some security threats that Industry 4.0 players need to focus on, and try to mitigate its impact [20] [21].

3.1.1 Enterprise Cyber-Espionage, Confidential Information and Intellectual Property

Industry 4.0 is more vulnerable to cyber-espionage because of the smart and connected business processes. Currently it has been seen the development of well organized groups of cyber-criminal with excellent skills used to targeting specific industries, towards hacking sensitive information and intellectual property. One example of such a group is the Black Vine group [22], which focuses on industries such as aerospace, energy and healthcare. Examples of actions performed by these types of groups are for instance the recent allegations of the US steel industry, which has accused the Chinese government of stealing intellectual property through a sustained hacking attack. The problem associated to this phenomenon is not confined to its impact on sales but also include damage to organizational image, loss of know-how and reduced level of competitiveness by the affected organizations. The targeted theft of corporate and product know-how starts to becoming increasingly common, especially in the form of software and functionalities that currently continue to be very easy to copy. In the scope of Industry 4.0 these threats assume even greater importance resulted from the cooperation between different partners in the network. Therefore, it is important to find solutions that guarantee trust and transparency within the platform, as well as the protection of the critical know-how business [1]. A security approach to be considered includes data loss prevention solutions in conjunction with encryption algorithms to protect high value data assets.

3.1.2 Denial-of-Service

Denial-of-Service (DoS), also known as a Distributed Denial of Service (DDoS), is the process of making a system or application unavailable. For example, a DoS attack might be accomplished by bombarding a server with huge number of requests to consume all available system resources, by passing the server malformed input data that can crash a process, by infiltrating a virus, or by destroying or disabling a sensor in a system, not allowing it to operate normally [23]. Industry 4.0 relies on a great number of interconnected systems and processes, the DoS attacks are a very important threat in such environments. Additionally as cloud computing gains popularity, and it is has been widely used in the smart factory concept, it is likely that more criminals find new ways to exploit system vulnerabilities like applying Denial-of-Service. The damage caused by a Denial-of -Service cyberattack can wind up being very costly for a company. Such an attack causes material damage (servers and sensors need to be replaced or put back to normally work; network needs to be reprogramed; systems need to be redesigned) but also operational and financial to cause damage (service interruption, complex protocols for resuming operations, new training for machine operators). In this context, for the industrial sector, DoS attacks are often unforeseeable and very difficult to control.

3.1.3 Supply Chain and the Extended Systems

One of the Industry 4.0 features is the ability to connect across organizational environments, which has the potential to make the supply chain more efficient. However, the supply chain systems have inherent security vulnerabilities, which are exploited by attackers. One of the security vulnerabilities starts with the supplier, which is vulnerable to phishing attacks and the stolen of privileged credentials, resulting in mass data exposure. The major vulnerability is in the top of the supply chain, reaching the rest of the organizational processes through its dependent actors [21]. Security awareness, control access through authentication mechanisms, cryptographic processes, and behavioral analysis are the security mechanisms that can help to prevent a supply chain hacking.

3.1.4 Smart Security and the Smart Factory

The same way the industrial revolution of the 18th and 19th centuries evidenced massive industrial and societal changes, Industry 4.0 will also bring diverse changes in the way industries work and the way they collaborate and innovate. Highly connected industries can offer improvements across all of manufacturing industries, utilities and even healthcare manufacturers [20]. Big data generated through the IoT can give useful information regarding how things work and what can be improved. However new “things” usually bring unexpected security vulnerabilities and threats to exploit and the attackers are actively working to ensure they get their share of Industry 4.0. Using smart security which means by implementing

preventive security policies, instead of responsive procedures, will be able to mitigate the impact of smart security' vulnerabilities exploitation. Additionally, it is also crucial to raise awareness among all the people involved in production, from skilled machine operators to secure software developers and planning engineers working in the field of plant engineering. When security solutions are implemented within an organization, it is not enough to simply install technical products. Employees need to be conveniently trained with regard to the security requirements and standards. The implementation of awareness-raising campaigns requiring the involvement of all manufacturing environment could help to overcome the current shortcomings in this area [21]. Additionally, the introduction of compulsory classes and research groups on this topic at higher education institutions would help to prepare the workforce for the future.

Moving towards Industry 4.0 is a huge task and has impacts in many areas in today's manufacturing industry, particularly in security. Most of manufacturing companies are not fully aware of the security risks that came with the adoption of Industry 4.0 paradigm. Normally, they only handle security issues, when a serious incident occurs. So, it is essential, and urgent, that organizations embrace the development of a strategy to deploy and run security compliance processes that Industry 4.0 requires, especially towards reducing the organizational level of exposition as well as to proper manage the mitigation procedure of its impacts.

IV. CONCLUSIONS AND FURTHER DEVELOPMENTS

In the organizational context, security usually means financial investments with no return of investment (ROI), which explains the fact that security incidents are usually handled once the development process is over and when a critical security incident occurs, with serious and dramatic impacts to the organization. However, this procedure is costly and also often fails to deliver a permanent solution to the relevant problem. Moreover, it might condition the source of differentiation among competitors and ruin the competitive advantages and the organizational confidence in their business activities.

Moving towards Industry 4.0 brings diverse technological challenges, with high impacts in many areas in today's manufacturing industry especially in the security domain. To meet the technological challenges raised by the Industry 4.0, it is essential to develop a strategy to all the actors involved in the entire value chain, to reach a consensus on security issues and the relevant architecture before implementation begins. Security issues are now starting to be discussed. The EU directive 2016/679 comes to reinforce the concern regarding security and the implementation of adequate organizational secure actions to ensure the protection of the processing activities. The discussion around the importance of protecting IT of the various types of industrial equipment, it will certainly move Industry 4.0 forward and thus turn this new stage of industrial development eventually safer and securer for everyone.

The specialists working groups indications will be critical towards enlighten the different possibilities that organizations will be able to implement or adopt into the near future. Notwithstanding, it will be extremely important to compile and to benchmark the solutions with better results attained and that might benefit the level of security of all stakeholders within the different business sectors.

Therefore, it is intended to develop some case-studies about security policies and strategies developed in the organizations within the Industry 4.0 paradigm. The development of these case studies will be important to determine the level of existent awareness within organizations, as well as to explain the difficulties and pointing out the overall benefits of its implementation.

REFERENCES:

[1] H. Kagermann, W. Wahlster, J. Helbig, Securing the future of German manufacturing industry. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industry 4.0 Working Group. National Academy of Science and Engineering, Germany, April 2013
[2] J. Nasser, Cyber physical systems in the context of Industry 4.0. Automation, Quality and Testing, Robotics, 2014 IEEE International Conference on. IEEE, 2014.
[3] M. Boban, Econ. Soc. Dev. (2016) 191-201.
[4] R. Geissbauer, J. Vedso, S. Schrauf, 2016. Industry 4.0: Building the digital enterprise. Available at: https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf (2017, March 10).
[5] A. Gilchrist, Industry 4.0 - The Industrial Internet of Things, Springer, New York, 2016.
[6] C. Baur, D. Wee, 2015. Manufacturing's next act. Available at: http://www.mckinsey.com/business-functions/operations/our-insights/manufacturings-next-act (2017, March 10).
[7] V. Koch, S. Kuge, R. Geissbauer, S. Schrauf, 2014. Industry 4.0: Opportunities and challenges of the industrial internet. Available at: http://www.strategyand.pwc.com/reports/industry-4-0 (2017, March 10).
[8] A. Varghese, D. Tandur, 2014 International Conference on Contemporary Computing and Informatics (IC3I), 634.
[9] T. Lins, M.J. Silva, R.A.R. Oliveira, Proceedings of the 20th Advanced International Conference on Telecommunications. Valencia, Spain, pp. 34–39, 2016.
[10] R. Drath, A. Horch, IEEE Ind. Electron. Mag. 8 (2) (2014) 56–58.
[11] S. Wang, J. Wan, D. Li, C. Zhang, Int. J. Distrib. Sens. Networks. 12 (1) (2016) 10.
[12] A. Gilchrist, Industry 4.0 - The Industrial Internet of Things, Springer, New York, 2016.
[13] R. Geissbauer, J. Vedso, S. Schrauf, 2016. Industry 4.0: Building the Digital Enterprise. Available at: https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf (2017, March 10).
[14] S. Schrauf, P. Berttram, 2016. Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused. Available at: http://www.strategyand.pwc.com/media/file/Industry4.0.pdf (2017, March 10).
[15] B. Marr, 2016. What Everyone Must Know About Industry 4.0. Forbes 20. Available at: https://www.forbes.com/sites/bernardmarr/2016/06/20/what-everyone-must-know-about-industry-4-0/#2df5b7c8795f (2016, February).
[16] N. Falliere, L. O. Murchu, E. Chien, W32.StuxenetDossier. Symantec, February 2011.