ROLE OF CYBER SECURITY IN INDUSTRY 4.0

[1]Hari Prasada Rao J
[1]Associate Professor
[1]Department of Computer Science
[1]Aurora's Degree & PG College, Hyderabad, India.

Abstract:Nation Crime Record Bureau (NCRB) report indicates that speedy increase in Cyber- attacks in India by 50% from 2018 to 2020. In future the cyber-attacks will continue to become more innovative and sophisticated. There have been several incidences of cyber- attacks on business and individual level of digital transactions in the past few years. Putting the data of billions of people on the cloud could be risky and could threaten the security. Hence the Digital India project demands very strong network security at all levels of operation. Industry 4.0 (I.4.0) can be the substance of changes in different fields like governance , management and administration of smart cities and other applications which are driving the vision of Digital India. Theme of the paper presentation is to make awareness on the cyberattacks and levels of security measures in the field of Digital transactions, footprints of data and E-commerce websites. The essential steps that to be implemented in the process of Industry 4.0.

Keywords: Industry 4.0, Cyber –Attacks, E-commerce, Security,Digital India.

Introduction:

Industry 4.0 (the 'fourth industrial revolution') refers to the current trend of improved automation, machine-to-machine and human-to-machine communication, artificial intelligence,continued technological improvements and digital is ation in manufacturing[18].

Industry 4.0 has been driven by 4 disruptors;[11]

- A rise in datavolumes.
- Computational power andconnectivity.
- Emergence of analytics and businessintelligence.
- Improvements in transferring digital instructions to the physical world such as advanced robotics and 3Dprinting.

The fourth industrial revolution brings with it a new operational risk for connected, smart manufacturers and digital supply networks. The interconnected nature of Industry 4.0 driven operations and the pace of digital transformation mean that cyber attacks can have far more extensive effects than ever before, and manufacturers and their supply networks may notbe preparedfortherisks.[21]

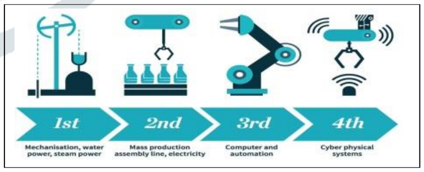
1st
Mechanisation, water power, steam power
2nd
Mass production assembly line, electricity
3rd
Computer and automation
4th
Cyber physical systems

Figure- 1: industry 4.0revolution

For cyber risk to be adequately addressed in the age of Industry 4.0, cyber security strategies should be secure, vigilant, and resilient, as well as fully integrated in organizational and information technology strategy from the start. [27]

In fact, it's estimated that 85% of companies will have implemented Industry 4.0 solutions in all important business divisions in five years time. By 2020 that will represent
€140 billion spent annually in Europe1. In manufacturing, these cyber-physical systems cover smart machines, storage systems and production facilities – not just in one factory but across many.[24]

Smart factories take a completely new approach to production – products can be identified, located and moved by alternative routes as needed. Manufacturing systems are connected with business processes as well as external networks, across the value chain, and managed in real-time. [28]

What is Industry 4.0?

Today the computers and automation, however, the focus has shifted to technologies like Internet of Things (IoT),Artificial Intelligence (AI), blockchain, robotics, etc. which are defining the new work culture across almost all industries. Industry 4.0 primarily merges automationwithadvancedmanufacturingtoreducedirecthumaneffortandresources. Effectively, these technologies make the manufacturing system a “smart networked factory”, where all activities are digitally controlled and are thus, immutable.[27/28]

The Origins of Industry 4.0:

The Industry 4.0 concept comes from Germany is not surprising, since Germany has one of the most competitive manufacturing industries in the world and is even a global leader in the sector of manufacturing equipment. Industry 4.0 is a strategic initiative of the German government that traditionally heavily supports development of the industrial sector. In this sense, Industry 4.0 can be seen also as an action towards sustaining Germany’s position as one of the most influential countries in machinery and automotive manufacturing. The basic concept was first presented at the Hannover fair in the year 2011. Since its introduction, Industry 4.0 is in Germany a common discussion topic in research, academic and industry communities at many different occasions.[15]

The main idea is to exploit the potentials of new technologies and concepts such as:[22]

- availability and use of the internet andIoT
- integration of technical processes and business processes in thecompanies
- digital mapping and virtualization of the realworld
- ‘Smart’factoryincluding‘smart’meansofindustrialproductionand‘smart’products.

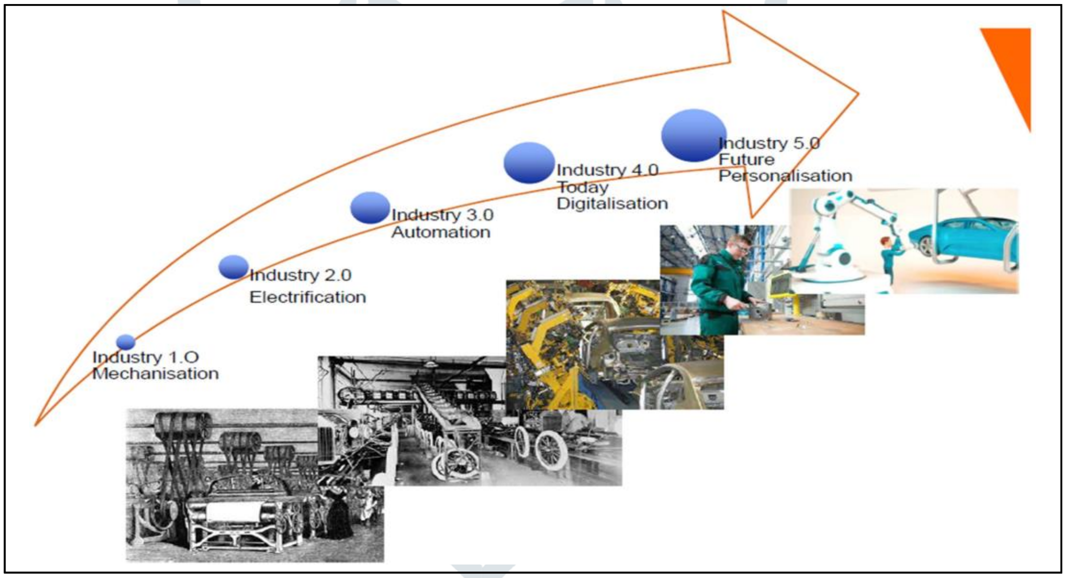

Figure-2. The Era of Industry 4.0: Internet of Things and Smart Manufacturing

There are also a number of other advantages and reasons for the adoption of this concept including: (1) a shorter time-to-market for the new products, (2) an improved customer responsiveness, (3) enabling a custom mass production without significantly. The useofITtocomputerizemanufacturingisviewedasthefourthindustrialrevolution.[13]

Industry 1.0: water and steam power used to mechanize production

Industry 2.0: electric power driving mass production

Industry 3.0: IT power to automate production

Industry 4.0: The term Industry 4.0 (Industry 4.0)is more commonly known in some countries as the Industrial Internet.

Industry 5.0: The Industry 5.0 is focused on interaction between humans and machines. In fact, the shift from Industry 4.0 to 5.0 means more emphasis on human manufacturers. In terms of thesocial environment, Industry 5.0 will return focus to the human aspect of manufacturing whereas Industry 4.0 focused solely on the technology. It depends on how willing you are to embrace Industry 5.0 as well as how quickly you choose to adopt and implement the technologies necessaryto bring the next Industrial Revolution to your plant floor. [2]

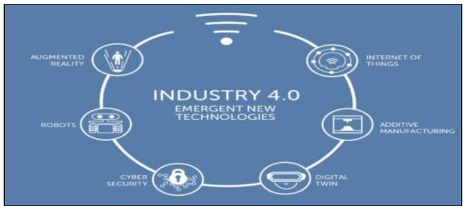

Figure-3 The Component of Industry 4.0

The Basic Components of the Concept Industry 4.0:

1. Internet of Think : It is a system of inter connected computing devices, mechanical and digital machines, objects or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. Devices and sensors are used to collect datafrom everywhere – home, cars, office, manufacturing plant, hospital, etc. Indeed, both the terms ‘Internet of Things’ (IoT) and ‘Internet of Services’ are considered elements of Industry 4.0.[16]
2. Additive Manufacturing(AM): Additive (Manufacturing) technology offers the ability to produce personalized products with lower development costs, shorter lead times, less energy consumed during manufacturing and less material waste. It can be used to manufacture complex parts, and enables manufacturers to reduce inventory, make products on-demand, create smaller localized manufacturing environments, and even reduce supply chains. Two industries will deliver the most disruptive application of AM: healthcare and space.[3]
3. Digital Twin: A digital twin is the concept of maintaining a dynamic digital equivalent of physical assets, processes, and systems, utilizing data from various sources like sensors. The stream of data that connects the digital twin and its physical counterpart is called the digital thread[4]

   As per Dr. Grieves, digital twins can be classified into the following forms:[5]

   1. Digital Twin Prototype(DTP)
   2. Digital Twin Instance(DTI)
   3. Digital Twin Aggregate(DTA)
4. Cyber Security: The interconnected nature of industry 4.0–driven operations and the pace of digital transformation mean that cyber attacks can have far more extensive effects than ever before, and manufacturers and their supply networks may not be prepared for the risks. The cyber risk to be adequately addressed in the age of industry 4.0, cyber security strategies should be secure, vigilant, and resilient, as well as fully integrated into organizational and IT strategy from the start.[6]
5. Robots: In the race to build the digital factory, manufacturers will find robots the perfect physical and cognitive partner. These machines make themselves indispensable with the ability to perform tasks, collect and analyze data on productivity, quality, and reliability and cost for themselves and other equipment in the process and make the insights available for interpretation and action. Where do you see the greatest potential for robots to contribute to the brave new world of digital manufacturing?[7]
6. Augmented Reality: Augmented reality is one of the cutting edge technologies involved in the industry 4.0 trend when talking about smart manufacturing; AR improves reliability and safety of robotic systems showing to workers the intentions of robots, it reduces costs and improves performances of maintenance systems or it shows precisely any discrepancies of products superimposing models on the real object.[9]
7. Cloud Computing: Processing of information retrieved byIIoT (Industry IoT) devices, cloud-based manufacturing. The most common attack goes against its availability, by means of a Denial of service (DoS) attacks against the infrastructure. Confidentiality problems arise when putting trust in the service provider, who has total access to the stored data. [8/12]
8. Big Data: Under Industry 4.0, big data analytics is useful in predictive manufacturing and is a major theme for industrial technology development. To assist manufacturers in maintaining a competitive edge in operational management control andin improving their production efficiency and yield rates, ITRI has developed a big data analytics solution with integrated ensemble learning capability. An advanced machine learning algorithm analyzes process data collected for productionsystems to provide early warning for anomalies and system failures and to predict product quality.[10]

Cybersecurity risks in industry 4.0: The technological developments which are at the base of Industry 4.0 do raise at the same time a vast number of associated of security concerns. Industry 4.0 means Opportunitie and challenges6. As the malware exploits unknown security holes, firewalls and network monitoring software are unable to detect it.[1]

Thus cyber risks in an industrial setting, although still associated with the classic computer and network security perspective, develop a numberof

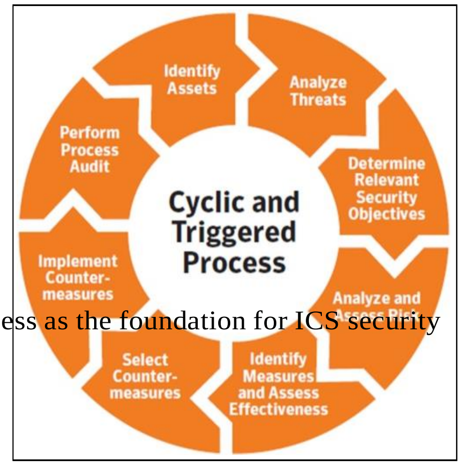
Identify Assets
Analyze Threats
Determine Relevant Security Objectives
Analyze and Assess Risk
Identify Measures and Assess Effectiveness
Select Counter-measures
Implement Counter-measures
Perform Process Audit
Cyclic and Triggered Process

Figure 4: A cyclic GRC process as the foundation for ICS security

specific features7. They might affect sharing data across the Digital Supply Networks (DSN) which does imply increased access to data for more stakeholders and vendor acceptance and payment in a broader market. New cyber challenges are created also by connected production. Misused or manipulated requests for ad-hoc production lines can result in financial loss, low product quality, and even safety concerns forworkers[14].

Managing Cyber Risk: This involves:

1. Prioritizing risks, defining policies and automating assessment processes (IT Governance, Risk and Compliance (IT GRC) – that span all of your IT and OT/ICS environments.[26]
2. Enforcing IT policies and automate compliance (ISO 27005) – with built-in automation and workflow to not only identify threats, but also remediate incidents as they occur or anticipate them before theyhappen.[23]
3. Communicating IT and OT risk in business-related terms – using the IT GRC framework, which involves various steps from identifying critical assets through to continuous audit processes [25](see figure4).

The cyber risks of sharing data across the DSN: [17/18] As the DSN evolves; one expected outcome is the creation of a network that allows real-time, dynamic pricing of materials or goods based upon the demand of purchasers relative to the supply available. But a responsive, agile network of this nature is made possible only by open data sharing from all participants in the supply network, which creates a significant hurdle; itwill likely be difficult to strike a balance between allowing transparency for some data and maintaining security for other information. Organizations may thus want to consider ways to secure that information to prevent unauthorized users from accessing it across the network. They would also likely need to remain disciplined about maintaining those safeguardsacross all supporting processes, such as vendor acceptance, information sharing, and system access. Not only may these processes be proprietary in their own right, they may also potentially serve as access points to other internalinformation.

Key Principles of cybersecurity: The deployment and management of cybersecurity shouldbeorganisedinsuchawayastosafeguardsystemsfromtheconsequencesofsecurity incidents.Activities may be organized according to the phases set out above . It is an on-going process that requires continuousefforts.[19/20]

1. Awareness-raising amongpersonnel
2. Assets management and riskanalysis
3. Prevention: the concept ofDefence-In-Depth
4. Monitoring and detection ofincidents
5. Incident handling, alertchain
6. Monitoring of threats andvulnerabilities
7. Disaster Recovery Plan and Business Continuity Plans(DRP/BCP)

Conclusion:

In Germany, the subject is driven above all by the Government and various associations. The German Federal Government actively supports Industries 4.0 by means of, for example, projects for autonomics, production technologies, smart data/smart services and IT security. In these subjects, decisive for digitalization, there is still a great need for research. The efforts being made to strengthen research and innovation must therefore not be allowed to abate, to ensure that Germany, and indeed Europe, do not fall behind with respect to otherregions.

In the USA, the subject is addressed by company consortia, for example IIC or the Smart Manufacturing Leadership Coalition. In the US Government is supporting manufacturing innovation through the National Network for Manufacturing Innovation (NNMI), an initiative by President Obama to bring together industry, academia, and government partners to leverage existing resources, collaborate, and co-invest to advance manufacturing innovation and accelerate commercialization. In India, the “Make in India” program aims at encouraging innovations, simplifying investment, strengthening the manufacturing infrastructure and extending qualifications with the goal of increasing the growth of the Indian manufacturing industry to over ten percent perannum.

References:

1 https://www.infosecurityeurope.com/novadocuments/304922?v=636135137079870000

2 https://blog.gesrepair.com/industry-5-0-will-affect-manufacturers/

3 https://atos.net/en/blog/industry-4-0-future-additive-manufacturing

4 https://dzone.com/articles/redefining-businesses-through-digital-twin-technol

5 https://www.wipro.com/en-IN/digital/whitepaper-the-digital-twin-realizing-business-value-from-physical-digital-convergence/

6 https://www2.deloitte.com/insights/us/en/focus/industry-4-0/cybersecurity-managing-risk- in-age-of-connected-production.html

7 https://www.forbes.com/sites/jimlawton/2018/03/20/the-role-of-robots-in-industry-4-0/#20801642706b

8 https://www.inglobetechnologies.com/smart-manufacturing-ar-industry-4-0/

9 http://www.imedpub.com/articles/augmented-reality-in-industry-40.php?aid=2216810

https://www.itri.org.tw/eng/content/msgpic01/contents.aspx?&SiteID=1&MmmID=620651706136357202&CatID=620653256103620163&MSID=711022154112316330

11 https://www.headland.com.au/industry-4-0-cheat-sheet-industry4-0-cloud-computing-smart-factory-internet-of-things/

12 https://www.reply.com/en/content/cyber-security-and-cloud-computing-in-the-industry-4-0-era

13 Analysis of cyber security threats in Industry 4.0: the case of intrusion detection- Rodrigo Roman, JavierLopez.

14 https://dupress.deloitte.com/dup-us-en/focus/industry-4-0/cybersecurity-managing-risk-in- age-of-connected-production.html

15 “Industrie4.0”“SmartFactories”“CyberSecurity”,siemensbyRajivSivaRaman.

16 Atamli, A. W. & Martin, A. (2014, September). Threat-based security analysis for the internet of things. In 2014 International Workshop on Secure Internet of Things (SIoT), (pp. 35–43).IEEE.

17 http://eurlex.europa.eu/legalontent/EN/TXT/PDF/?uri=CELEX:52016DC0180&from=EN

18 https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/manufacturing/ch-en- manufacturing-industry-4-0-24102014.pdf

19 http://www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux/

20 http://www.ssi.gouv.fr/ebios/

21 FR website:http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html

22 Lee, J.; Kao, H.-A.; Yang, S. Service innovation smart analytics for industry 4.0 and big data environment. Procedia CIRP 2014, 16,3–8.

23 Industry 5.0: Combining strengths of humans and robots for better and healthier manufacturing Prof drir BramVanderborghtB. Sniderman, K. Marchese and T. Ott, “Industry 4.0 and manufacturing ecosystems,”11 2016. [Online]. Available:https://dupress.deloitte.com/dup-usen/multimedia/podcasts/manufacturing-ecosystems-exploring-world- connectedenterprises.html.[11] W.MacDougall,

24 EnterpriseForward(22ndFebruary2016),‘ThePathtoSelf-disruption:NineStepsofaDigital Transformation Journey’. Available at https://hpeenterpriseforward. com/eiu-pace-of-disruption/(accessed15thMay,2017).

25 https://www.symantec.com/connect/blogs/iot-security-risks

26 Presentation at the French Embassy in the Germany, “Industry of the future“, 2015. Availableat.http://www.ambafrance-de.org/Vorstellung-des-neuen-franzosischen- Plans-Industrie-du-Futur-in-der-Botschaft. Last accessed:24.11.2016.

27 W. MacDougall, “Industrie 4.0: Smart Manufacturing for the Future,” 2014. [Online].Available:https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Brochures/Industries/industrie4.0-smart-manufacturing-for-the-future- en.pdf.