Industry 4.0 cyber threat recapitulation & Remedy: *An Initiative to Safeguard Manufacturing*

Dr. Subodh Kesharwani
Executive Editor

The rationale behind writing a note on behalf of an editor table on this particular theme ***“Industry 4.0”*** is well designed and premeditated for this particular issue (volume-1 number-5 October 2019)due to change in manufacturing philosophy and advent of smart factory in the year 2020.

The first two foremost articles nomenclature are Experimental Research Paper and talks about “Blockchain for Cybersecurity - Standards & Implications” and “Cyber risks in Industry 4.0 – Digital Supply Chain”. Next two articles taxonomy is Argument based and entitled*as “Forensic Crime Scene Officer”*and *“Cyber security Concerns for E-Services in the Digital Information Age”*.Next head in a line is a Scrutiny Tip whichrevolves around two articles

“Eight Steps to Protect against Rising Third Party Cyber Risks” and further in the last other three are columns written respective authors “Artificial Intelligence and Laws in India”, *“Challenges against Cybercrime”*&*“CyberSecurity Predictions 2020”*. We had also created some more innovative thoughts in this particular issue like a Power Point Snapshot which is a presentation entitled *“PPT Snapshot”* is placed after the end of articles for reader “Potential of Virtual Class Room Learn”. There are certain prefixes which would be common in all the heads

Observation & Excerpt of Industry 4.0

- Digital Transformation is accelerating across the value chain
- Major business drivers are costs reduction, Improvement in agility and speed to market.
- IoT, mobile and cloud solutions are crucial for the transformation
- IT/Legacy modernization is a key enabler

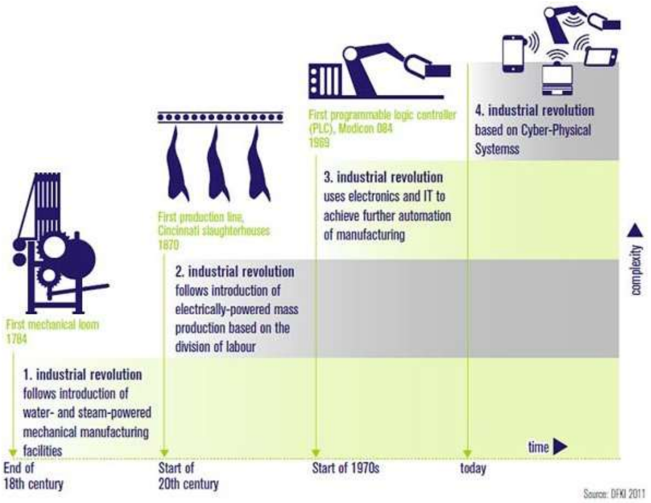
Business organizations are now a day coming across with the challenge of updating measures to ensure IT, OT, and IP against any weak link an adversary may take advantage of this thing. The physical and digital manufacturing components both are exposed with the unsupported operating systems, and exposed systems risk. Compromised systems can ruthlessly lead to the prompt data leakages, huge financial losses, and production downtime for the long run. This message from editor desk glances at the prospect threats and risks that can be posed to the manufacturing industry, highlights the challenges emerged due to the shift to industry 4.o and also state the best measure and practices for availing the economies of mass connected production. Securing the manufacturing industries against any kind of treat calls for continuous risk assessment and a vigilant cybersecurity framework that can detect, respond and protect against the variety of cyberattacks and cyberholes in a much sophisticated way.

In most of the countries, manufacturing industries are noteworthy economic drivers. It have been observed that in developing countries, these industries endeavoris to be a magnet for multinational companies by providing tax breaks, cheap labor,provisions for logistics and infrastructure which would be both in brick & mortar and click & mortar. The global extension of industry is on the threshold of paradigm shift as multifaceted and extremely competitive industry demands a change not because revision in decade but change in technological mindset. With the rapid advances in technology, new occurrences has come out in the current epoch, Industry 4.0 which is a 4thindustrial revolutions and are the most vital milestones which have changed the course of human history vis-à-vis industry expansion.

Industrial Revolution 4.0:

As per diverse researchers, in comparison to scientific revolution, industrial revolutions have been able to persuade people's lifestyle in a greater way. The fundamental values for the Information Revolution are globalization, thinning out thoughts, and restructuring societies and economies in totality and more important emphasize on sustainability. In wrapping up there are three basic revolutions they are Agricultural, Industrial, and Information Revolution.

- The first industrial revolution occurred from the period 1760 to 1840. This revolution was based on the facts that machines could substitute humans for betterment. This revolution offered many socio-economic reforms and many technical marvels. This revolution was known in the history as the era of mechanization. It was the period when different energy sources were identified. Invention of steam engines was done that helped in offering energy to advanced textiles inventions. All of this denotes the conversion from human power in homes to machine power in factories.


First mechanical loom
1784
1. industrial revolution
follows introduction of water- and steam-powered mechanical manufacturing facilities
First production line, Cincinnati slaughterhouses
1870
2. industrial revolution
follows introduction of electrically-powered mass production based on the division of labour
First programmable logic controller (PLC), Modicon 084
1969
3. industrial revolution
uses electronics and IT to achieve further automation of manufacturing
4. industrial revolution
based on Cyber-Physical Systemss
complexity
time
End of
18th century
Start of
20th century
Start of 1970s
today

Source: DFKI 2011

Figure 1: Phases of Industrial Revolution

- The second industrial revolution started from the beginning of 1870 and lasted until the period of 1914. The second industrial revolution was known as the age of science and mass making. This industrial revolution took a shift from conventional innovations and focused on utilizing the power of electricity, gas, steel, petroleum and oil etc. to allow faster expansion and transportation of material railroads were invented in this phase. This laid the footsteps for the third industrial revolution.

- Nearly in the second half the 20th century from the period of 1970's the third industrial started with immense potential to surpass its predecessors. This revolution was based on the nuclear energy and witnessed the emergence of various new technologies such as semiconductors, mainframe, and internet to give augment to the production of miniaturized material to support the extension of space and biotechnology industry.

- The fourth industrial revolution is the current and developing environment in which disruptive technologies and trends such as the Internet of Things (IoT), robotics, virtual reality (VR) and artificial intelligence (AI), Block Chain technology, Deep learning are changing the mode so tokeep going and strive There are definiterecompense of the industrial revolution which enables fabrication of goods on a scale and bring exceptional transformation in human history, that it straitlaced many people's standard of living, and finally expanded the economies of many nations.

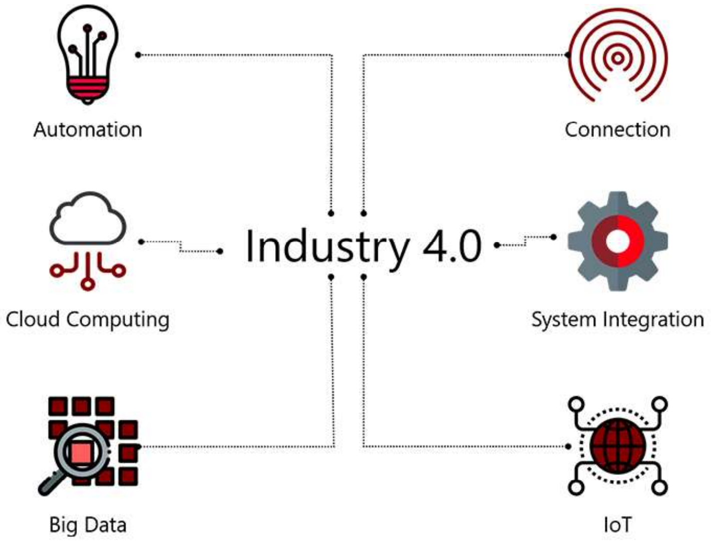
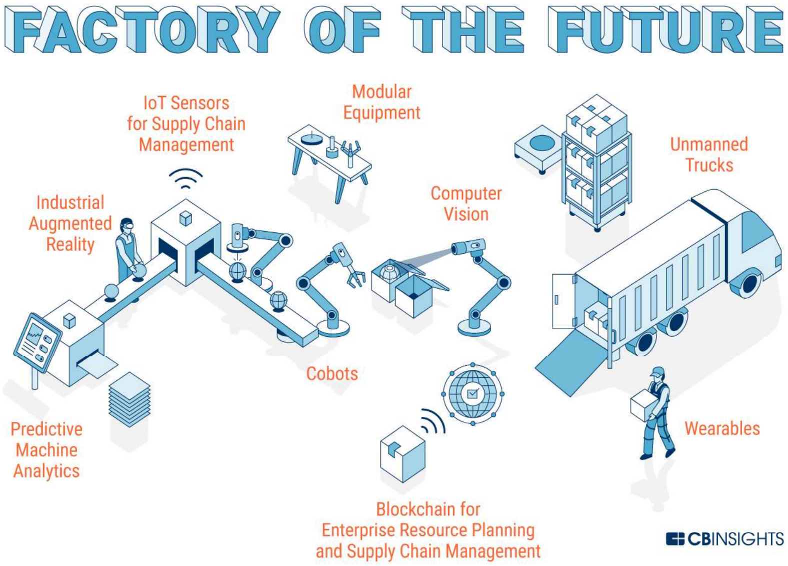


Figure 2: Industry 4.0 linkages with various contemporary thought

It is well versed that the industry of today and tomorrow intend to unite all production means rather integrate in order to facilitate the interaction in real time. ***"Factories 4.0"*** with the help of technology such as Big Data Analytics, Cloud and the Industrial Internet of Things (IIoT) enable communication between the diverse and connected objects and players of various fields. In some of the developed nations Industry 4.0 has by now been acknowledged as the part of their long-term strategies and imbibes in vision and mission of the future thought.

Components of Industry 4.0:

Industry 4.0 is a complex and abstract term consisting of various components of our society's current and digital trends.To promote from the advantages that Industry 4.0 can fetch, it's significant to comprehend its terminology. The next stage in the evolution of industry, like the previous three, the fourth revolution is a response to the rise of new technologies.


FACTORY OF THE FUTURE
IoT Sensors for Supply Chain Management
Modular Equipment
Unmanned Trucks
Industrial Augmented Reality
Computer Vision
Cobots
Predictive Machine Analytics
Wearables
Blockchain for Enterprise Resource Planning and Supply Chain Management
CBINSIGHTS

Source: https://www.cbinsights.com/research/future-factory-manufacturing-tech-trends

Figure 3: Factory of Future

There are certain terms and technologies which are stated below:

- **Advanced manufacturing technologies:** Including robotics and 3D printing
- **Automation**: It describes the use of digital systems to control equipment and machinery within a factory.
- **Big data:** It enables organizations to have information about every part of their business and use it to predict and plan future production and supply possibilities.
- **Blockchain:** The block chain is a digital distributed ledger technology which stores all the data exchange by time-stamping it. Because of this tracking of data becomes very easy with Blockchain technology. A block chain is a continuously growing list of decentralized, digitized public records, called blocks, of all crypto currency transactions, which are linked and secured using cryptography.
- **Build to Order (BTO): It is production process where the products are not built until the order to do the same is received and confirmed. It followed to avoid any inventory and resources wastages.**
- **Cloud robotics**: Communication between the physical and digital worlds that is controlled in the cloud and extended to robots used in mobile applications.
- **Connected Factory:** This term is commonly used as synonym to "smart factory". It refers to an industrial environment where Industry 4.0 technologies such as cloud computing and networked activity are used.
- **ERP software:** refers to business-management software, usually comprising a suite of integrated applications, that an organization uses to collect, store, manage and interpret data from its many business activities
- **Fog computing:** Extending cloud computing to the edge of an enterprise's network, reducing the amount of data transferred to the cloud for processing and analysis, improving security. This creates efficiencies and has opportunities for companies concerned with compliance issues.
- **Human-Machine-Interface (HMI):** HMI is the space where interactions between humans and machines take place. Applications within Industry 4.0 centre on machine control achieving new levels of safety and efficiency.
- **Internet of Things (IoT):** A network of physical devices, vehicles, home appliances and products embedded with electronics, software, sensors, actuators and connectivity enabling connection via wireless technology.
- **Mobile Robot: They are most commonly used in various researches and exploration. They are the automated machines typically vehicles which are capable of functioning in a particular set of environments through proper set of instructions.**
- **Mobile solutions:** Including smart phones, tablets, wearable sensors and smart glasses
- **Open data:** Data that is available for public use without restraint for all.
- **Overall Equipment Effectiveness (OEE):** The evaluation of how effectively equipment is working in a manufacturing environment.
- **Platform:** A system comprising a hardware device together with an operating system that an application, program or process can run upon.

- **Virtual Reality (VR):** A computer-generated simulation of a three-dimensional image that can be interacted with in a seemingly real or physical way by a person using special electronic equipment. In the manufacturing environment it can allow for rapid visualization, prototyping and simulation.
- **Wearable Technology:** Devices that are integrated into the objects that are worn on the body such as clothing and accessories and execute tasks similarly to computers and mobile phones. Because of their sensory and scanning features, they are more sophisticated as compared to hand-held technology.

With the help of cyber-physical systems that monitor physical processes, a virtual copy of the physical world can be premeditated. Thus, these systems have the capacity of making decentralized decisions on their own and accomplish a high degree of sovereignty. As a result, Industry 4.0 networks a wide variety of new technologies to generate value.

Industry 4.0 Cyber threat

The increased connectivity of machinery undoubtedly raises the stakes. Industry 4.0 with the usages of smart and autonomous technologies attempts to change the world through its acts to drive smart factories and advanced manufacturing. But these revolutionary changes also possess new threats for which industry is not ready. Development of a fully integrated strategic approach to cyber risk is primary to manufacturing value chains which emphasize on addressing new risks and concerns. Cybersecurity should be integrated part of systems, strategies, designs and operations from the beginning itself. Industry 4.0 has led to the introduction of open and general purpose systems as it requires high level of connectivity. In present days, industrial control systems that permanently connect via TCP/IP and Ethernet are a common sight, as is the use of standardized wireless systems. All these protocols have been developed and analyzed comprehensively, and they proffer the maturity and reliability that the new Industry 4.0 demands.Cyber incidents are not limited to cyber attacks. A cyber attack on a manufacturing capability would be detrimental, but it's not the most well-knownpain in the neck to a network's operational stability. In fact, miniature to foremost network or process disruptions due to misconfigurations, erroneous commands, software errors or device failures, can occur almost on a daily basisprovidentially.In the table below the modern connected digital supply networks, smart factories, and connected device are examined respectively focusing on the unique cyber risks faced by each.Moving through the production life cyclefrom the digital supply network, to the smart factory, and finally to the connected object—we explore the actions operations and information security executives can take to anticipate and effectively address cyber risks as well as proactively integrate cybersecurity into their strategy in the age of Industry 4.0.

Production Life Cycle Stage	Cyber Imperatives And Risks	Objective
Digital Supply Network 	Data sharing	Ensure integrity of systems so private proprietary data cannot be shared
	Vendor processing	Maintain trust when processes cannot be validated
Smart Factory 	Health and safety	Ensure safety for both employees and environment
	Production and process resilience/ efficiency	Ensure continuous production and recovery of critical systems
	Instrumentation and proactive problem resolution	Protect the brand and reputation of the organization
	System operability, reliability and integrity	Support the use of multiple vendors and software versions
	Efficiency and cost avoidance	Reduce operating costs and increase flexibility with remote site diagnostics and engineering
	Regularity and due diligence	Ensure process reliability
Connected Devices 	Product design	Employ secure software development life cycle to produce a functional and secure device
	Data protection	Maintain the safety of sensitive data throughout the data life cycle
	Remediation of attack effects	Minimize the effects of an incident while quickly restoring operations and security

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

Table 1: Cyber risk associated with various production life cycle stages

IoT (Internet of Things) in industry or IIOT (Industrial Internet of things)

Industrial transformation leaders are embracing a myriad of digital technologies including IIoT platforms to drive unprecedented operational efficiencies. Do you want to know how they are planning for success?

Source: https://www.se.com

Figure 4: Industry IoT

As the industries are taking steps towards the automation, it has been observed that manufacturing is becoming more and moredigitized. The IIOT has successfully brought technologies such as AI, Robotics, and cloud computing to the physical factories. The cyber physical system of today inclusive of both operational and information systems are taking over the outdated machineries. Factories implementing all the technologies are known as smart factories, and this is what experts and industrialists call as fourth industrial revolution industry 4.o. Digitization of factories contribute significantly in superior effectiveness in production and quality of product and for more plasticity for working progress. Manufacturers must be proactive by upgrading infrastructural devices such as firewalls, switches, anti-virus, cloud managed solutions, providing continuous training to their employees etc.

Role of Big data and analytics:

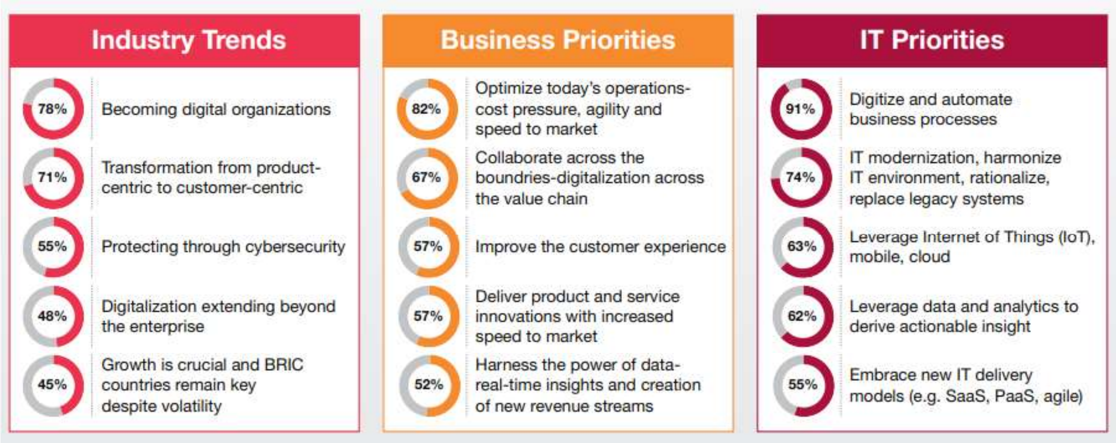
The modern and communication information technologies that are currently budding like cyber-physical stems, big data analytics, cloud computing immensely helps in timely detection of any production failure and defect that leads to the prevention and higher productivity, agility and quality benefits that can result in a significant component advantages to the host company over others. In current cyber physical systems environment and integrated industry 4.0 era the big data analytics consists of 6C's given below:

- Connection (sensor and networks)
- Cloud (computing and data on demand)
- Cyber (model & memory)
- Content/context (meaning and correlation)
- Community (sharing & collaboration)
- Customization (personalization and value)

By looking at the visible and invisible concerns in industrial factories, the information generation algorithm must be competent for detection of invisible concerns like component wear, machine degradation and others. In this kind of circumstance, data needs to be processed using advanced tools for generation of significant information.

Securing Industry 4.0 by taking a help of a cyber: Some facts and figure

Industry 4.0 combines appropriate physical and digital technologies, including analytics, additive manufacturing, robotics, high-performance computing, natural language processing, artificial intelligence and cognitive technologies, advanced materials, and augmented authenticity.



Industry Trends		Business Priorities		IT Priorities	
78%	Becoming digital organizations	82%	Optimize today's operations-cost pressure, agility and speed to market	91%	Digitize and automate business processes
71%	Transformation from product-centric to customer-centric	67%	Collaborate across the boundries-digitalization across the value chain	74%	IT modernization, harmonize IT environment, rationalize, replace legacy systems
55%	Protecting through cybersecurity	57%	Improve the customer experience	63%	Leverage Internet of Things (IoT), mobile, cloud
48%	Digitalization extending beyond the enterprise	57%	Deliver product and service innovations with increased speed to market	62%	Leverage data and analytics to derive actionable insight
45%	Growth is crucial and BRIC countries remain key despite volatility	52%	Harness the power of data-real-time insights and creation of new revenue streams	55%	Embrace new IT delivery models (e.g. SaaS, PaaS, agile)

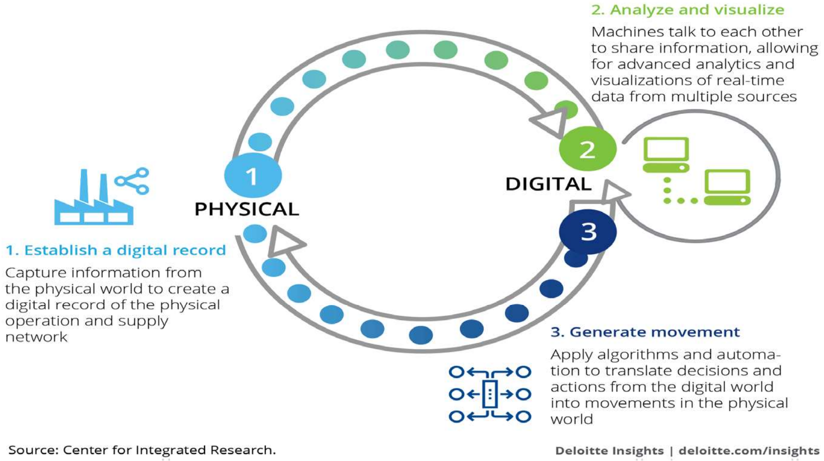
Source: Figure: CGI Global 1000 (2016) manufacturing industry insights

Figure-5: Manufacturing Insight with respect to Industry trends/ Business Priorities/IT Priorities

In 2016, CGI consultants interviewed more than 1,000 executives in 10 industries and 20 countries. In the year 2016, more than 1000 business and technology executives were interviewed through face to-face conversations in 10 industries and 20 countries, this fetches together the results, insights and viewpoints on strategic topics.

Loop and related technology

- **Physical to digital**: Capture information from the physical world and create a digital record from physical data
- **Digital to digital**: Share information and uncover meaningful insights using advanced analytics, scenario analysis, and artificial intelligence
- **Digital to physical**: Apply algorithms to translate digital-world decisions to effective data, to spur action and change in the physical world


2. Analyze and visualize
Machines talk to each other to share information, allowing for advanced analytics and visualizations of real-time data from multiple sources
2
DIGITAL
1
PHYSICAL
3
1. Establish a digital record
Capture information from the physical world to create a digital record of the physical operation and supply network
3. Generate movement
Apply algorithms and automation to translate decisions and actions from the digital world into movements in the physical world

Source: Center for Integrated Research. Deloitte Insights | deloitte.com/insights

Source: https://www2.deloitte.com/us/en/insights/focus/industry-4-0/overview.html

Figure-6: Physical-to-digital-to-physical loop related technologies

It is very clear from the above figure that it moves in three layer manner. The above three points is in real sense leads to reconciliation and secured.

Security has become the buzzword of the century due to the rise of ransomwares and other emerging crippling cyber-attacks due to data breaches and several other reasons.According to the Cisco's annual report on cybersecurity, ransomware is growing immensely at an annual rate of 350% and the FBI estimates the annual global market to be around one billion dollars. Therefore, to realize their potentials to the fullest, organizations must incorporate a valid holistic cyber-savvy thinking to all aspects of the industrial processes to be digitally changed. The Industry 4.0 concept is called as the comprehensive transformation of the whole sphere of industrial productionbut its ideals have become a flagship in todays' time.To bring Industry 4.0 into realization, it requires adoption from the infrastructure up, integrating Internet of Things (IoT), cyber physical systems, networking systems, wireless technologies, cloud computing and enhanced security directly into your manufacturing process, regardless the business size.

Potential threats with a case analysis:

Along with its huge advancement, advantages and popularity potential threats of industry 4.o cannot be ignored. The associated risks of industry 4.0 threats range from physical security compromise and fraud to mass production downtimes, product spoilage, and plant tackle break. By looking at the pace of digital transformation and with the interconnected nature of industry 4.0 driven operations any kind of cyber threats can have more extensive and severe effects than ever. Digital supply network possess more operational risk for smart manufacturers and their digital supply networks. The CEO of IBM Mr. Harriet Green has even envisaged scenarios where IoT devices are able to communicate with the blockchain to update or validate smart contract that can be more than threatful to any organization if used maliciously.

A step forwards: Ease of Doing

Industry 4.0 was designed to revolutionize the manufacturing industry with smart factories. This means that factories' physical processes are monitored by cyber-physical systems that afterward make entrust decisions based on the information they congregate. There are certain steps which played a pivotal role in ease of doing initiative either by government of a particular country or incorporation of Industry 4.0.

- The German government has resolute a road map, jointly with its architecture, in a report illuminating its strategic plan for 2020.
- EICOSE (European Institute for Complex Safety Critical Systems Engineering) is a group, which is formed by different European institutions. This aims at researches security for critical systems and primarily on developing methods, processes and systems which assurances security in critical entrenched environments.
- Connected Industry 4.0. Is a project that has been launched by the Spanish Government that operates publicly and privately both, intends to persuade a digital transformation in the Spanish industry.

- Being a global concept, Industry 4.0 can take various forms and names throughout the world. In the United States, the focus inclines on a more holistic digital evolution and a lot of use the term digital supply network.

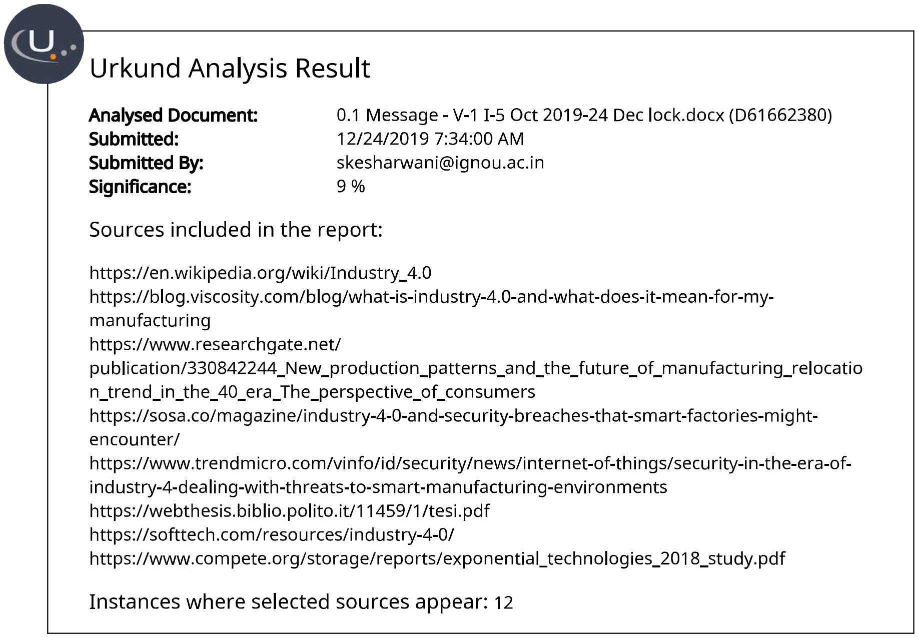
Finally it is well versed that Industry 4.0 symbolizes the industrial future. As much as most investors and owners may be unenthusiastic to squeeze the smart system, it reduces labor expenses to enhance the return on investment ratio. So, to take full advantage of profits, industries will have no alternative but to cuddle the use of industry 4.0 technology.

Digital transformation in manufacturing is driven by the interconnected nature of Industry 4.0, since information technology (IT), operational technology (OT), and intellectual property (IP) all unite for supporting the recognition of "smart factories."Industry 4.0 is a emergent concept, then also it has started having an impact across Europe, and it will be relentless as suggested by the varying evidences. Cyber security is fundamental for the working of Industry 4.0 both in the terms of technology and processes in the value chain: the risks and responsibilities need to be defined for each of the agents. Cybersecurity must therefore be thought of as a protective mechanism and crucial requirement in order for business to continue. In extremely aggressive market of these days must effectively incorporate proper cybersecurity framework by implementing the industry 4.0, big data and IoT solutions to stand out in their industries. The need for improving the cyber security of Industry 4.0 is even further essential, since the probable impact of relevant threats ranges from compromising physical security to production downtimes, spoilage of products to damaging equipment as well as ensuing financial and reputational losses.Industrial organizations should consider IIoT and advanced analytics plus a wide range of other digital technologies. Additionally, a key indicator of digital readiness is the aptitude and willingness to shadow multiple technologies at the same time.

Dr Subodh Kesharwani

References

- Marr, Bernard. "Why Everyone Must Get Ready for The 4th Industrial Revolution". Forbes. Retrieved 14 February 2018
- Bonner, Mike. "What is Industry 4.0 and What Does it Mean for My Manufacturing?". Retrieved 24 September 2018.
- Hermann, Pentek, Otto, 2016: Design Principles for Industries 4.0 Scenarios, accessed on 4 May 2016
- https://blog.global.fujitsu.com/fgb/2018-12-17/the-cybersecurity-challenge-of-industry-4-0/
- https://www.essentracomponents.com/en-gb/news/infographics/industry-4
- https://en.wikipedia.org/wiki/Industry_4.0
- https://blog.viscosity.com/blog/what-is-industry-4.0-and-what-does-it-mean-for-mymanufacturing
- https://www.researchgate.net/publication/330842244_New_production_patterns_and_the_future_of_manufacturing_relocation_trend_in_the_40_era_The_perspective_of_consumers
- https://sosa.co/magazine/industry-4-0-and-security-breaches-that-smart-factories-mightencounter/
- https://www.trendmicro.com/vinfo/id/security/news/internet-of-things/security-in-the-era-ofindustry-4-dealing-with-threats-to-smart-manufacturing-environments
- https://webthesis.biblio.polito.it/11459/1/tesi.pdf
- https://softtech.com/resources/industry-4-0/ https://www.compete.org/storage/reports/exponential_technologies_2018_study.pdf



Urkund Analysis Result

Analysed Document: 0.1 Message - V-1 I-5 Oct 2019-24 Dec lock.docx (D61662380)
Submitted: 12/24/2019 7:34:00 AM
Submitted By: skesharwani@ignou.ac.in
Significance: 9 %

Sources included in the report:

https://en.wikipedia.org/wiki/Industry_4.0
https://blog.viscosity.com/blog/what-is-industry-4.0-and-what-does-it-mean-for-my-manufacturing
https://www.researchgate.net/publication/330842244_New_production_patterns_and_the_future_of_manufacturing_relocation_trend_in_the_40_era_The_perspective_of_consumers
https://sosa.co/magazine/industry-4-0-and-security-breaches-that-smart-factories-might-encounter/
https://www.trendmicro.com/vinfo/id/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments
https://webthesis.biblio.polito.it/11459/1/tesi.pdf
https://softtech.com/resources/industry-4-0/
https://www.compete.org/storage/reports/exponential_technologies_2018_study.pdf

Instances where selected sources appear: 12

Communication from Executive Editor's Writing Table

Digital systems have changed, and will carry on transform our world. They have the prospective to distribute noteworthy benefits to society and are innermost to our safety measures, comfort and economic enlargement. To realize these benefits, we will need robust cyber security. The purpose behind launching Cyber security is that only. When research is done in the field of Cyber vis-à-vis its economics, it has a overflowing crash and implication not only for the corporate world but also for academia. Fostering Cyber research and providing a podium to make public good quality research papers based on empirical or scholarly research work has been a never-ending venture of a magazine. We are truly honored to have been selected as the Executive Editors of the new monthly periodical Cybernomics. Being an executive editor I am highly indebted to scholastic seed Inc for providing me an opportunity. We are also very proud to be working in tandem with an outstanding team of managing editor/Associate Editors and members of the Editorial Board. The latter have been selected as a balanced universal illustration of the guidance in our territory. This is an editorial team that is fully betrothed and devoted to the success of these outstanding periodicals. In this new epoch of Cyber there are a number of changes that we would like to draw attention to the periodical's readers, as we are self- assured such changes will entreat to a widespread range of academic and information technology interests. Cybernomics is a collectively designed by our leadership team that aims to represent the global network of our community from cyber society. We recognize the importance of ensuring that our initiatives in an academic format would represents the work and research being conducted in all regions of the world, and at the same time also highlights key issues critical to technocrats not only in developed countries but also in low-resource countries. Second, the periodical will feature original articles that showcase important issues related to cyber and burgeoning terms which revolves around it. The response to our appeal to authors for contribution has been devastating. In spite of our superlative hard work, due to an assessment of editorial board and the referee review board, some of the articles/papers could not be incorporated in the present issue of Oct 2019, but this shall not put a ceiling on any of the authors to send their original articles, case studies, research reviews or empirical contributions for publication in our magazine. As an executive editor, and on behalf of our editorial team we be acquainted with the value authors place on high-quality and unbiased peer review conducted in an suitable mode. In totaling, we value the significance of rapid publication, and so to that end we have structured our editorial team to encompass Associate Editors, a Social Media Editor, and a Video Editor so we are capable to expedite the processing of submitted manuscripts. We have instructed all those involved with the periodical in an attempt to endow with the highest standard of manuscript review, editing, and publishing. We have implemented rigorous peer review criteria, and this will be reflected in the quality of published articles. We also want to persuade all those who are interested in being part of this energetic and enthusiastic team to contact us, as we will welcome your contribution. We invite colleagues working in related disciplines of cyber and Information technology as an appropriate medium for the publication of your own high-quality research. Manuscript submissions are being accepted for Volume-1, Issue-6, 2019 which will be in the regular format. Original articles can be submitted to the Executive Editor (Word document, by email only, at scholastic.seed@gmail.com or at editorial.scholastic.seed@gmail.com . Articles for columns should be arranged with the respective column editor. Cybernomics is a right platform for academicians, industry executives, researchers and students for sharing the views and the news of the management in terms of research papers, articles and case analysis, reviews etc. the more detail of the nomenclature is mentioned in a booklet and available online at www.cybernomics.in . We are hard about the ensuing issues of the periodical with regard to quality and coverage. We hope that within short time this periodical will make the academicians, industry executives, researchers and students to travel from the point of recognizing something to concede the whole thing. We wish the periodicals for its endeavor and permanence of its rhythm in the same direction in the days to come. Our sincere thanks to all the contributors for their support and attention. We yet again apply for all academician and researchers to propel their unpublished articles/papers for publication in our periodical to comprehend the economics of Cyber.

Scholastic Seed Inc.
www.scholasticseed.in

Citation

Subodh Kesharwani
"Industry 4.0 cyber threat recapitulation & Remedy:
An Initiative to Safeguard Manufacturing"
Volume-1, Issue-5, Oct 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had
no conflict neither financially nor academically.

Subodh Kesharwani is an academician with a bronze medal in his Post graduate and Doctorate in ERP System in 2002 from Allahabad Central University. He is one of the researchers who had concentrated his research on Total Cost of Ownership [TCO] & critically evaluate ERP vendors including SAP. Dr. Kesharwani is presently an Associate Professor, School of Management Studies with a total 20 years of hardcore teaching and research in Information System and its linkages with various domains of management at Indira Gandhi National Open University, New Delhi. He is presently an expert in various burgeoning areas and had delivered a talk as a trainer on MOOCs, Team Building, E-commerce, Technology Enabled Learning, E-resource, Technology Uses in research, Block chain, Internet of Thing, Enterprise Information System, Free & Open Source Software, etc. Dr. Subodh had developed and coordinated a program in Entrepreneurship & Business Skills in collaboration with Rajiv Gandhi Foundation (RGF), India and Commonwealth of Learning, Vancouver, Canada which provides training to the trainers at IGNOU. He is presently a program coordinator of IGNOU-ICWAI alliance. He is also a founder Editor-in-chief of a peer reviewed refereed journal entitled "Global Journal of Enterprise Information System [GJEIS] from 2009 onwards, which has completed its 10 years term and published 40 issues till date both in printable and virtual format. The Journal GJEIS is equipped with DOI from Crossref USA and listed in almost 50 directories in the world with an impact factor of 2.68 of 2017-18. Dr. Kesharwani had participated as a debater in diverse TV show and participates in Interactive Radio Counseling including Gyanvani and Gyandasrshan. He had written a Book entitled "ENTERPRISE INFORMATION SYSTEMS-Contemporary Trends and Issues" in a co-authorship with Professor David L Olson (University of Nebraska, USA. which was published by WORLD SCIENTIFIC, USA. http://www.worldscibooks.com/business/7287.html

He had another text book on ERP system which caters a B.Tech VI Semester CS and IT Students. He had developed educational contents for various academic Institutions such as ICAI, IGNOU and contributed articles for various journals/ Magazines, etc. He had chaired a good number of technical sessions at various conferences & seminars nationally and globally. He is presently running a "Blockchain Federation for Indian Researcher" which he thinks can bring paradigm shift holistically. Dr. Kesharwani had been awarded "IT Innovation & Excellence Award 2012" in the field of ERP solutions, by KRDWG's Selection Committee at IIT Delhi. He is in the panel of the Steering Committee of the International Journal of Computing and e-Systems, TIGERA-USA. He was in the key panel of round-table workshop conducted by Ministry of Corporate Affairs in Association with Indian Institute of Corporate Affairs to streamline "Corporate Data Management and Governance". He was one of the resource person who shared the experience with the 12 different ITEC countries participants who had attended International MDP.