International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 9 ǁ September 2021 ǁ PP. 95-101

To provide security in IoT for industrial solutions

Anugnya Prabha Manjari
College of Engineering Bhubaneswar, Biju Pattnaik University of Technology, Odisha, India.

Abstract: *An Industrial Internet of Things (IIoT) system integrates and connects business processes, analytics, enterprise systems, and industrial control systems. An IIoT system enables significant gains in operations, cooperation, and decision-making among multiple increasingly autonomous control systems.These systems differ from traditional industrial control systems in that they are more diverse and have a larger scale due to their numerous linkages to other people and systems. They are distinct from traditional information technology (IT) systems in that they additionally make use of sensors and actuators in an industrial environment. These are typically systems that communicate with the external world, where uncontrolled modification could lead to hazardous circumstances. Safety, dependability, privacy, and resilience are more crucial due to this potential risk than they would be in many conventional IT setups. In addition to connection encryption, these IIoT systems may include data flows involving multiple intermediary entities, requiring more advanced security methods. IIoT systems are governed by regulations, have long lifespans, and incorporate legacy installations because of the possible threats to public health and safety. IIoT systems necessitate the merging of both cultures since the operational and information technology domains have distinct cultures. The security specifications for these systems are impacted by each of these differences. In order to guarantee the safety of the industrial sector, this paper outlines common vulnerabilities for Industrial IoT networks along with the policy to address these vulnerabilities.*

Keywords: *IIoT, M2M, IIOoT Risks, IIoT threats.*

I. INTRODUCTION:

According to recent projections, the Industrial Internet of Things is growing exponentially. Furthermore, by 2025, there will be over 75 billion linked devices worldwide, of which nearly a third will be used for industrial manufacturing applications. However, as this market's opportunities—especially in cloud-based, third-party service providers—keep growing, one problem becomes less of a growth obstacle and more of a warning sign that should not be disregarded. That warning sign is the constant need for security.

As the day goes on, there are new stories about data breaches at organizations that were believed to be safe from such incursions and in considerably larger databases than previously. The instances in which organizations have utilized or retained data in ways not originally intended by the individuals or enterprises who trusted them with the information are equally upsetting. Furthermore, the issue can worsen before becoming better as the proliferation of devices picks up speed.

Industrial control systems, enterprise systems, business processes, and analytics are all integrated and connected by an Industrial Internet of Things (IIoT) system. Significant improvements in decision-making, operations, and cooperation among numerous, increasingly autonomous control systems are made possible by an IIoT system.

These systems are different from conventional industrial control systems in that they have many connections to other individuals and systems, which increases their scale and diversity. They also use sensors and actuators in an industrial setting, which sets them apart from conventional information technology (IT) systems. Usually, they are systems that interact with the outside environment, where unchecked modification might create dangerous situations. Because of this possible risk, safety, dependability, privacy, and resilience are more important than they would be in many typical IT setups. These IIoT systems might also have data flows including a number of intermediary entities, necessitating more sophisticated security techniques than just connection encryption. IIoT systems have extended lifespans, involve legacy installations, and are subject to regulations due to the potential risks to public health and safety.

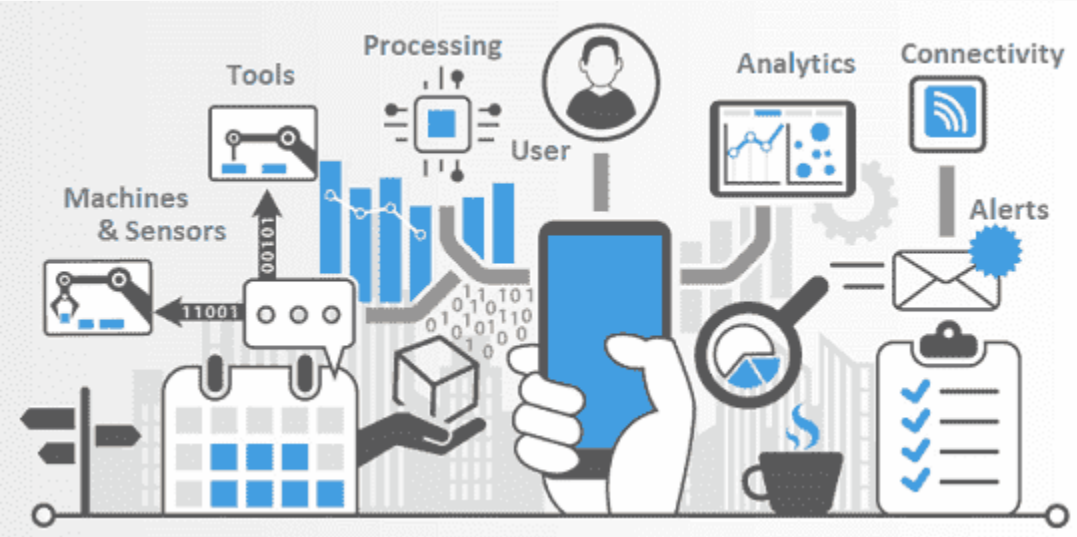
These systems differ from traditional industrial control systems by being connected extensively to other systems and people, increasing their diversity and scale. They also differ from traditional information technology (IT) systems in that they use sensors and actuators in an industrial environment. These are typically systems that interact with the physical world where uncontrolled change can lead to hazardous conditions. This potential risk increases the importance of safety, reliability, privacy and resiliency beyond the levels expected in many traditional IT environments. These IIoT systems might also have data flows including a number of intermediary entities, necessitating more sophisticated security techniques than just connection encryption. IIoT systems have extended lifespans, involve legacy installations, and are subject to regulations due to the potential risks to public health and safety. Because the cultures of the information technology and operational domains

are different, IIoT systems require the integration of these cultures. These variations all have an impact on the security requirements for these systems.

Within this article, we discuss common vulnerabilities for Industrial IoT networks as well as how you can address these vulnerabilities to ensure the safety of the network and business.

II. INDUSTRIAL IOT

Industrial IoT is an ecosystem of devices, sensors, applications, and associated networking equipment that work together to collect, monitor, and analyze data from industrial operations. It utilizes machine-to-machine connectivity and communication with a cloud-based platform to enable process improvement. It uses big data analytics, advanced machine learning algorithms, and other technology to deliver actionable insights to manufacturers.



a

IIoT represents the convergence of information technology (IT) and operational technology (OT), creating a fully integrated ecosphere where processes and industrial control systems are in a sophisticated network.
This network includes IIoT devices like sensors, controllers, industrial control systems, and other connected devices to measure production or assess machine health. Combined with edge computing and actionable insights generated from analytics, machines can receive instructions to perform autonomous or semi-autonomous tasks without the need for human intervention and at a speed more incredible than humans can achieve.

III. IIoT SECURITY

Industrial IoT (IIoT)/Industry 4.0 (I4.0) [1] is a concept of an innovative and intelligent fully connected factory implementing disruptive technologies (i.e., IoT, cloud computing, artificial intelligence, etc.) and innovative solutions (IIoT, automation, monitoring, etc.) collectively enhancing the production environment with lower costs, agility, efficiency, remote operations, etc. In such an autonomous environment, data and network security are key driving factors. With the growing implementations of IIoT applications and services, the spectrum of cybersecurity threats has changed with it and requires enhanced security measures and controls to be developed [2,3,4]. The threats and types of breaches possible on the internet during the pandemic must not be underestimated. Breaches happening in the industrial IoT domain would be critical due to specific exposures that are related to machine-to-machine (M2M) communication and environments [3]. M2M communication networks are an integral part of connected factories involving high dependency on next generation wireless communication systems (5G, time sensitive networking, etc.) [4,5] and involving self-automated, self-driven, and self-learning network characteristics. The future M2M devices are anticipated to work independently and make decisions based on artificial intelligence and machine learning algorithms. These types of devices where human intervention will be minimal require high levels of operational security because they may cause disruptive hazards [3].

The main source of threats for M2M communications comes from unanticipated breaches arising from the internet, software which are mostly identified post implementation, limited capabilities due to low-energy, cost, remote locations, bandwidth, legacy systems, etc. There is a substantial gap between the existing information technology and operational technology (IT/OT) domains which makes the IIoT environment more vulnerable to existing security issues [5,6,7,8,9,10]. With billions of IoT/M2M devices connected in the

industrial environment, it may potentially create multiple weak-entry points and lead to compromised assets/information/privacy issues. Without appropriate standards and security controls in place, it will be hard to classify the cyber threat impact and the information altered/manipulated. Identifying the breach before damage has incurred is critical to the whole environment [5].

Industrial IoT security is critical. One primary consideration is the danger of business data loss. With more connections today than ever before, losing access to internal systems could seriously damage a company's ability to do business or even survive.

The same is true for medical, aerospace, and defense industries, where patents, trade secrets, and regulated confidentiality require heightened accountability. The loss of ownership and use of these valuable intellectual assets could impact a company financially or put them in jeopardy of serious liability claims due to a breach of confidentiality.

Another critical consideration for Industrial IoT security is safety. There is an internal and external concern for IIoT for public and corporate safety. A security breach that allows outside access to devices could lead to injury or loss of life. And a violation that will enable the change of a formula in pharmaceuticals or a part performance characteristic in aerospace could extend the safety risk for many people outside the company.

a. Localizing the security concerns

As hackers become more sophisticated in the use of the same data tools and AI technology as those building out IoT systems, the risk of a data breach grows. Within a factory and its connected systems, there are a number of locations where a illegal access like a breach can occur:

- Insecure Web Interfaces**:** The location where users interface with IoT devices suffers from issues such as inadequate default passwords, lockout and session management issues and credential exposure within the network.
- Insecure Network Services**:** This is where hackers may be able to gain access to the network itself as through open ports, buffer overflows and Denial-of Service attacks.
- Weak Encryption**:** Weak encryption, or in some cases no encryption, can allow intruders the ability to gather data during the exchange between devices.
- Insecure Mobile Interfaces**:** As many companies offer field service as an extension of their manufacturing operation for repair and maintenance, mobile interfaces suffer from the same issue of encryption and authentication.

b. The Challenges of IIoT Security

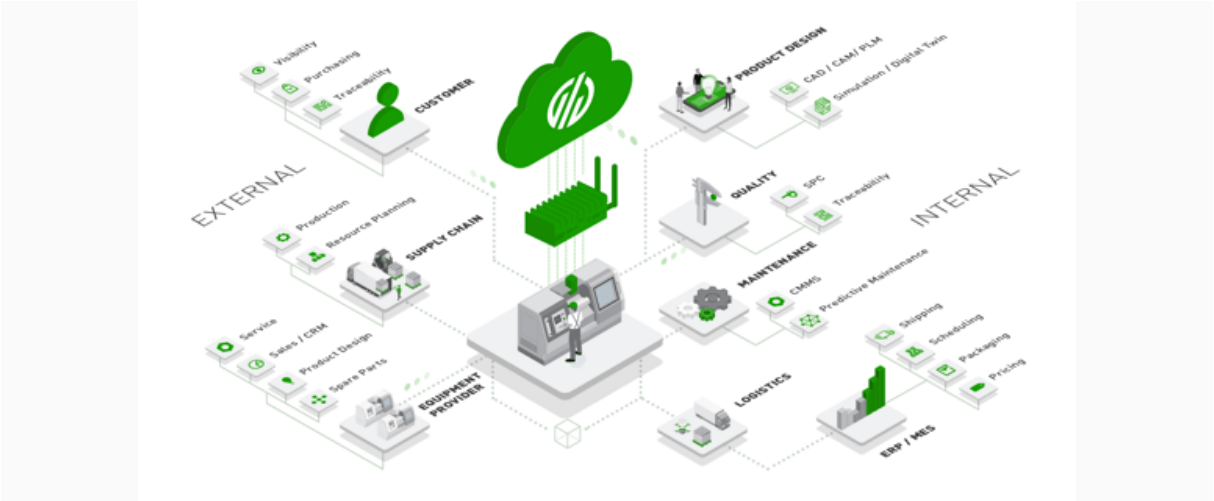
Many businesses already have weak or improper security in place to begin with, which places a strain on IoT providers supplying both services and devices. More than 50% of all critical infrastructure operations utilize outdated Microsoft software and a full 40% of all industrial sites are using the public internet.

This puts machine infiltration as a key risk as IIoT devices proliferate, meaning that sophisticated hackers could conceivably secure remote access to an entire factory and either severely disrupt or damage the production capabilities for a lengthy period. Security vulnerabilities could also pose physically dangerous conditions as a direct or indirect result of an intrusion.

The security of legacy systems is also a concern. One of the key value propositions for Industrial IoT deployment is that legacy equipment and legacy devices can be retrofitted with IoT devices. This allows longer equipment lifecycles and full integration for building out a smart factory without triggering expensive capital equipment purchases. But the choice must be made alongside a careful consideration of which devices can be properly secured for use within the system, a skillset that a company may not have and one it may not realize it needs.

Lack of standards and protocols in an industry still in its infancy, but growing astronomically, are also hampering coherent IIoT security progress. The feeling is that IoT service providers as a business community and industrial organizations will come together and self-regulate to develop standards and protocols for all development and to mitigate any security risk.

This would eliminate the chance of competing or overlapping "local" protocols and would be most cost-effective for the client. Until then, the lack of standard makes ad hoc security a norm and stresses the capabilities of the client's existing security system, which may already have its own weaknesses.



Cybersecurity Challenges in IIoT

This section focuses on different security issues (i.e., denial of service, data theft, manipulation, eavesdropping, etc.) [**8**,**9**,**10**,**11**]. The authors relate these concerns to the IIoT/I4.0 domain and highlight how these unresolved issues [**12**,**13**] leave the industrial environment susceptible to security breaches.

IT/OT (Data Security Issues)

Cyberattacks at the operational technology (OT) level have grown considerably recently, as it involves integrating new interfaces (i.e., IT systems, cloud, etc.) [**14**,**15**] providing flexibility and remote access to both new/old OT (i.e., SCADA, PLCs, etc.) systems. One of the reasons for the increased awareness in this domain is a significant increase in ICS cyberattacks (i.e., the USA's largest fuel-pipeline ransomware attack) [**16**]. Additionally, proprietary production knowledge becomes an IT security problem [**3**] with IIoT exposed to various types of cyber threats due to its dependency on new communication models and devices. The OT domain's major focus depends on availability and integrity of ICS whereas the IT sector focuses on confidentiality and integrity of applications, services, and supporting technologies. Lack of convergence between IT and OT systems develops knowledge gaps [**17**] allowing sophisticated and targeted cyberattacks to take place.

IIoT Communication and Security Risks

IIoT and machine-to-machine (M2M) communications characteristics depend primarily on high throughput and low latency, and utilize new communication technologies such as 5G, Wi-Fi 6, and Time Sensitive Networking (TSN) [**4**]. These new communication models and devices expose the IIoT environment to a wide range of cyber threats. With the increased usage of IoT-based devices, assessing, monitoring, and securing the endpoints of these devices is subject to various security-based challenges (e.g., lack of standard regulations for all IoT devices from different vendors [**9**,**10**], trusting third-party cloud vendors). Besides this, there are a number of other risks associated with securing the M2M communication environment such as [**10**,**18**,**19**,**20**] poorly configured devices, malicious IoT node injection, and standardization of M2M communications (IoT, cloud, edge, etc.). The sensitivity of compromised M2M devices may be assessed on the basis of the impact type, i.e., materialization of a threat leads to compromised confidentiality, and/or availability, and/or integrity of the network, and the impact factor/scale, in terms of users, downtime duration, number of cells affected, sensitivity of the information altered/accessed, etc.

Security Controls and Standardization

Security standards and security controls enable the industrial environment to implement the best security practices available and make it easier to identify a breach when it takes place as the risk factors associated [**2**] are known and thereby can reduce the incident response and recovery times. Other benefits of applied standards are discussed below.

Visibility, insights, and control are critical for the fully automated vertical model which relies on ultra-reliable low latency communications (URLLC), massive machine type communications (mMTC), and enhanced mobile broadband (eMBB) [**2**]. With such M2M service requirements, standards and security controls can grant transparency in assessing the potential security risks at the production levels.

The majority of industries put commercial standards (security controls, IT/OT standards, communication standards, etc.) [**21**] into practice without understanding and evaluating their production environment. This can develop disparities and leave the IT/OT domains vulnerable to cyber threats and data

security vulnerabilities. With escalating cyberattacks (i.e., malware, phishing, etc.) on the ICS environment, it is necessary to lay down a defensive approach for identifying the threat actors. Threat intelligence frameworks provide visibility and classify threats based on predefined metrics [**22**,**23**]. They play an integral role in securing I4.0, however, complete reliance on a certain framework or model is not always advisable to provide a comprehensive security strategy. Outdated and legacy systems deployed in the production environment reduce the efficiency and impact of security controls. Legacy systems with custom configurations, root of trust, identity protocols, etc. add complexity to setting up new security controls to old interfaces and securely extracting data.

A fully connected factory involves different applications, services, communication models, and cloud structures. Service level agreements [**1**] are of high importance for assessing, aligning, and controlling the security, privacy, and quality of service (QoS) metrics associated with the I4.0 environment. Situations where SLAs are not assessed and monitored properly may lead to unexpected service disruption, downtime, and third-party subcontracting vendor issues [**4**].

Around 48% of manufacturing industries have suffered a cyberattack, and as per InfoSys [**24**] 89% of manufacturing sectors understand the importance of data standards but only 11% of them invest in implementing relevant security controls and standards. Failure to meet the desired security levels and standards makes it hard to classify the threat impact and potential breaches.

The IIoT will streamline manufacturing sectors where the focus will shift to integration, digitization, and management of all physical resources through a uniform and flexible approach, making the cybersecurity landscape even more challenging, since the potential damages incurred on the production environment due to a breach could be serious.

c. IIoT Security Threats

IoT Botnets

Botnet owners find IoT devices to be an attractive target. Many devices have weak security configurations, which make them easy to enlist into botnets.[15]

Attackers can infect IoT devices with malware via unprotected ports, phishing scams, or other techniques and incorporate them into IoT botnets used to launch massive cyberattacks. These botnets are often used in distributed denial of service (DDoS) attacks that overwhelm the target network with excessive traffic.

IoT Ransomware

IoT-related ransomware attacks are on the rise as corporate networks are increasingly connected to unsecured Internet of Things devices. Hackers can infect devices with malware that turns them into malicious bots, probes entry points to the network, and retrieve valid credentials from the device's firmware that can be used to infiltrate the network.[15]

With access to the network via an IoT device, an attacker can exfiltrate proprietary data to the cloud and extort the organization unless a ransom is paid. In some cases, even if organizations pay, ransomware deletes their files anyway. Ransomware affects organizations of all sizes, from small businesses to critical organizations such as government services and food suppliers.

Shadow IoT

IT administrators do not always have control over devices connected to the network. This creates a security threat known as Shadow IoT. Devices with IP addresses, such as digital assistants, fitness trackers, and wireless printers, can increase personal convenience and help employees get their work done, but they don't always meet an organization's security standards.[24]

Without adequate visibility into the shadow IoT landscape, IT administrators cannot verify that devices and software have built-in security features or monitor these IoT endpoints for malicious traffic. Once hackers gain access to shadow IoT devices, they can escalate access privileges to reach sensitive information on the compromised corporate network or use the devices for botnets and DDoS attacks.[20]

IV. IIoT Security Solutions

According to security experts, over 40% of all breaches consist of either malware or brute force attacks. But there are numerous other forms of intrusion as well. Because of the number of ways a company's devices and systems could be accessed, security is viewed as consisting of four tiers; device, communication, cloud, and lifecycle management. Because of the speed at which the industry has grown, this complicates security solutions as there is no end-to-end, out-of-the-box security solution.

But there are steps that can be taken by providers and companies in the interim as end-to-end solutions are developed.

One such step would be to segment the IT network so that anything that controls equipment is maintained in a separate network from the rest of a company's IT infrastructure. These distributed control

systems would route network traffic over multiple channels and achieve security by decentralizing the network to protect industrial settings.

A second step that service providers can take is to ensure the "basics" like secure network communications. Basic structures such as credential lockout after a small number of tries and default credentials that must be changed upon activation will help secure access at the web interface[18]. Likewise, mandating strong password rules and two factor authentication can limit unauthorized access.

At the IT level, making sure that services aren't vulnerable to buffer overflow and ports are closed when not used will shut off avenues of intrusion as well. The same precautions can be built into mobile device interfaces for password, lockout and default password rules. And of course, better discipline in producing and deploying firmware upgrades will help reduce system degradation.

Perhaps the biggest step that could be undertaken to get ahead of security risks would be for the industry to collaborate toward self-regulation in the development of industry standards and protocols[22]. By defining a base architecture for many of the issues above and standardizing and mandating their inclusion, service providers and their programming teams would be freed from the smaller security concerns and left to concentrate on larger and more intensive security issues as they evolve.

The setting of basic standards would put a minimum security "floor" under all systems to protect both the companies that purchase the services as well as the providers when deploying systems in companies with inadequate or weak security systems.

V. CONCLUSION:

The security challenges facing Industrial IoT service providers and their client companies are growing. Industries should emphasize the security side of the equation strongly. It is preferable to have IoT devices and services if security solutions were part of the package. But as the industry continues to grow, new services including security as part of the platform, or strong partnerships with third-party security providers, will gain a stronger footing in the market.

References

[1]. Dhirani, L.; Newe, T. Hybrid Cloud SLAs for Industry 4.0: Bridging the gap. Ann. Emerg. Technol. Comput. **2020**, 4, 41–60. [**Google Scholar**] [**CrossRef**]

[2]. European Union Agency for Cybersecurity. ENISA Threat Landscape for 5G Networks. Available online: **https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks** (accessed on 22 December 2020).

[3]. Bartoli, A.; Dohler, M.; Kountouris, A.; Barthel, D. Advanced security taxonomy for machine-to-machine (M2M) communications in 5G capillary networks. In Machine-To-Machine (M2M) Communications; Woodhead Publishing: Sawston, UK, 2015; pp. 207–226. [**Google Scholar**] [**CrossRef**]

[4]. Farkas, J.; Varga, B.; Miklós, G.; Sachs, J. 5G-TSN Integration Meets Networking Requirements for Industrial Automation; Ericsson: Stockholm, Sweden, 2019; ISBN 0014-0171. [**Google Scholar**]

[5]. Leander, B.; Čaušević, A.; Hansson, H. Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019. [**Google Scholar**] [**CrossRef**]

[6]. Gurtov, A.; Liyanage, M.; Korzun, D. Secure Communication and Data Processing Challenges in the Industrial Internet. Balt. J. Mod. Comput. **2016**, 4. [**Google Scholar**] [**CrossRef**]

[7]. Rak, J.; Hutchison, D. Guide to Disaster-Resilient Communication Networks; (Computer Communications and Networks); Springer: Cham, Switzerland, 2020. [**Google Scholar**] [**CrossRef**]

[8]. Martinez, B.; Cano, C.; Vilajosana, X. A Square Peg in a Round Hole: The Complex Path for Wireless in the Manufacturing Industry. IEEE Commun. Mag. **2019**, 57, 109–115. [**Google Scholar**] [**CrossRef**][**Green Version**]

[9]. Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. J. Netw. Comput. Appl. **2020**, 149, 102481. [**Google Scholar**] [**CrossRef**]

[10]. Hameed, S.; Khan, F.; Hameed, B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. J. Comput. Netw. Commun. **2019**, 2019, 1–14. [**Google Scholar**] [**CrossRef**][**Green Version**]

[11]. Riahi Sfar, A.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. Digit. Commun. Netw. **2018**, 4, 118–137. [**Google Scholar**] [**CrossRef**]

[12]. Anand, P.; Singh, Y.; Selwal, A.; Alazab, M.; Tanwar, S.; Kumar, N. IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. IEEE Access **2020**, 8, 168825–168853. [**Google Scholar**] [**CrossRef**]

[13]. Panchiwala, S.; Shah, M. A Comprehensive Study on Critical Security Issues and Challenges of the IoT World. J. Data, Inf. Manag. **2020**, 2, 257–278. [**Google Scholar**] [**CrossRef**]

[14]. Gopstein, A.; Nguyen, C.; O'Fallon, C.; Hastings, N.; Wollman, D. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0; Special Publication (NIST SP)—1108rev4; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021. [**Google Scholar**] [**CrossRef**]

[15]. Eden, P.; Blyth, A.; Jones, K.; Soulsby, H.; Burnap, P.; Cherdantseva, Y.; Stoddart, K. SCADA System Forensic Analysis within IIoT. In Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing; Springer Series in Advanced Manufacturing; Springer: Berlin/Heidelberg, Germany, 2017; pp. 73–101. [**Google Scholar**] [**CrossRef**]

[16]. Kelly, S.; Kumar, D.K. Top U.S. Fuel Pipeline Remains Days from Reopening after Cyberattack. Available online: **https://www.reuters.com/business/energy/us-govt-top-fuel-supplier-work-secure-pipelines-closure-enters-4th-day-2021-05-10/** (accessed on 15 May 2021).

[17]. Deloitte. Examining the Industrial Control System Cyber Risk Gap. Available online: **https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ics-white-paper.pdf** (accessed on 4 March 2021).

[18]. Bhattacharjee, S. Industrial Internet of Things Security; Packt: Birmingham, UK, 2019. [**Google Scholar**]

[19]. McAllister, J. Industrial IoT Security: Cybersecurity Implications for IT-OT Convergence. 2019. Available online: **https://teskalabs.com/blog/industrial-iot-it-ot-convergence** (accessed on 24 November 2020).
[20]. Lekidis, A. Trends and Security from the IT/OT Convergence. 1st Global Cybersecurity Observatory. 2020. Available online: **https://cyberstartupobservatory.com/trends-and-security-challenges-from-the-it-ot-convergence/** (accessed on 14 March 2021).
[21]. Active Cyber. Active Cyber Surveys the Standards Landscape for OT and IoT Systems Security. Available online: **https://www.activecyber.net/active-cyber-surveys-the-standards-landscape-for-ot-and-iot-systems-security/** (accessed on 3 March 2021).
[22]. Peters, J. MITRE ATT&CK Framework, Everything You Need to Know. Varonis. 2020. Available online: **https://www.varonis.com/blog/mitre-attck-framework-complete-guide** (accessed on 17 February 2021).
[23]. IBM X-Force Threat Intelligence Index. Available online: **https://www.ibm.com/security/data-breach/threat-intelligence** (accessed on 25 February 2021).
[24]. Evans, J. Be Prepared for the Security Challenges of Industry 4.0. Available online: **https://www.orange-business.com/en/blogs/be-prepared-security-challenges-industry-40** (accessed on 10 January 2021).