
CYBERSECURITY OF INDUSTRIAL CYBER-PHYSICAL SYSTEMS: A REVIEW

Hakan Kayan

School of Computer Science and Informatics
Cardiff University, UK
kayanh@cardiff.ac.uk

Matthew Nunes

School of Computer Science and Informatics
Cardiff University, UK
nunesma@cardiff.ac.uk

Omer Rana

School of Computer Science and Informatics
Cardiff University, UK
ranaof@cardiff.ac.uk

Pete Burnap

School of Computer Science and Informatics
Cardiff University, UK
burnapp@cardiff.ac.uk

Charith Perera

School of Computer Science and Informatics
Cardiff University, UK
pererac@cardiff.ac.uk

January 12, 2021

ABSTRACT

Industrial cyber-physical systems (ICPSs) manage critical infrastructures by controlling the processes based on the “physics” data gathered by edge sensor networks. Recent innovations in ubiquitous computing and communication technologies have prompted the rapid integration of highly interconnected systems to ICPSs. Hence, the “security by obscurity” principle provided by air-gapping is no longer followed. As the interconnectivity in ICPSs increases, so does the attack surface. Industrial vulnerability assessment reports have shown that a variety of new vulnerabilities have occurred due to this transition while the most common ones are related to weak boundary protection. Although there are existing surveys in this context, very little is mentioned regarding these reports. This paper bridges this gap by defining and reviewing ICPSs from a cybersecurity perspective. In particular, multi-dimensional adaptive attack taxonomy is presented and utilized for evaluating real-life ICPS cyber incidents. We also identify the general shortcomings and highlight the points that cause a gap in existing literature while defining future research directions.

Keywords: Security, Privacy, Usability, Industrial Cyber-Physical Systems

1 Introduction

Industry 4.0 [1] and Industrial Internet [2] have accelerated the integration of industrial cyber-physical systems (ICPSs) [3] to the various industries ranged from manufacturing [4] to energy management [5], water treatment systems [6], and many more [7, 8, 9]. Critical infrastructures (CIs) [10] utilize ICPSs to perform and supervise industrial tasks in harsh industrial environments. Plenty of research [11, 12, 13] has been done on how to facilitate the migration of air-gapped legacy ICS to the modern ones that are even assisted by cloud technologies. These studies are also guided by alliances/institutions such as the Cloud Security Alliance (CSA) [14] to prevent insecure integration. This rapid transformation of ICPSs does bring many cybersecurity challenges. There are three mutually inclusive primary reasons behind these challenges: (i) high connectivity, (ii) increased attack surface, and (iii) heterogeneous infrastructure.

The loss or compromise of CIs that supply fundamental needs may result in catastrophic impact. The survivability of the CIs depends on the security of ICPSs. The defence approaches that focus on CPSs security such as anomaly detection [15], secure routing [16], game theories [17, 18], and watermarking [19], cannot be directly applied to ICPSs that differ from CPSs in many aspects. The security challenges for ICPSs require unique solutions that consider harsh industrial environments. Even though there is a growing number of publications, the literature that focuses on ICPS security is quite diverse. This independent presentation and evaluation of complementary topics create an unnecessary diversity regarding taxonomies, evaluation metrics, implementation techniques, and test environments. This creates a challenging environment for the new proposals while limiting the discussion of research outputs in a more unified way.

Existing Surveys. The ICPS, ICS, Industrial Internet of Things (IIoT), and Industrial Wireless Sensor Networks (IWSN) are not mutually independent disciplines. Hence, we have also investigated surveys/reviews of them. However, it was challenging to decide research criteria as there is no framework that explicitly describes the relationships of different industrial disciplines studied by the academia. Surveys of ICS challenges from a security point of view based on cybersecurity management are presented in [20, 21]. Several surveys [22, 23, 24] classify IDS techniques, review security and privacy issues while systematizing CPSs security and providing a security framework. Surveys of the current challenges for various ICPS architectures are available in [25, 26, 27]. The technical review of control engineering tools is presented in [28] while review of the key enabling technologies and major applications of ICPSs is available in [29]. ICPSs attack detection techniques are surveyed in [30, 31, 32, 33, 34]. Several proposals [35, 36, 37, 38, 39, 40] introduce IIoT, study state-of-the-art implementation, and give an outlook on possible solutions while mentioning future research directions. Other surveys [41, 42, 43] define principles, review technical challenges, and provide structured overview. We classified the previous surveys according to their topics in Table 1. We consider all these existing reviews/surveys complementary to our work.

Table 1: Chronological Summary of Previous Surveys

Year	Reference	I	CS	CPS	IoT	WSN	Cybersecurity
2009	Gungor and Hancke [41]	✓				✓	
2013	Cheminod et al. [20]	✓	✓				✓
2014	Da Xu et al. [40]	✓			✓		
	Mitchell and Chen [22]			✓			✓
2015	Lu et al. [42]	✓				✓	
	Sadeghi et al. [35]	✓			✓		✓
	Knowles et al. [21]	✓	✓				✓
2016	Leitao et al. [26]	✓		✓			
2017	Ding et al. [30]	✓		✓			✓
	Lu [29]	✓		✓			
	Queiroz et al. [43]	✓				✓	
2018	Huang et al. [31]	✓		✓			✓
	Giraldo et al. [32]	✓		✓			✓
2018	Xu et al. [36]	✓			✓		✓
	Ramotsoela et al. [34]	✓				✓	✓
	Liao et al. [37]	✓			✓		
	Ding et al. [33]	✓		✓			✓
2019	Yu et al. [25]	✓		✓			
	Jbair et al. [28]	✓		✓			
	Younan et al. [38]	✓			✓		✓
2020	Gidlund et al. [39]	✓			✓		✓

I: Industrial, *CS*: Control Systems, *CPS*: Cyber-physical Systems, *IoT*: Internet of Things, *WSN*: Wireless Sensor Networks.

Scope of the survey. The topic of CPS is indeed very popular in academia even though being a fairly new term. This growing popularity is also recognized by the National Institute of Standards and Technology (NIST) that has published a CPS framework [44]. However, although there are similarities, we believe CPS and ICPS security should be treated as a distinct research areas due to attributes (based on the differences between Information Technology (IT) and Operational Technology (OT)) that are unique to industrial environments. Cyber incidents that occur in industrial environments might result in catastrophic failures. Therefore, we have focused on the ICPS security and organized our survey by taking these attributes into consideration.

Our contributions. (i) We briefly define ICPSs, IWSN, IIoT, and ICS by identifying their unique environment characteristics, relationships, and current positions in the literature. We have only investigated and compared the ones that we think as the most similar to ICPSs according to the way that they are studied in the literature. We define the fundamental components of an ICPS and present a modern ICPS architecture (see §2). (ii) We analyze the differences between IT and OT and explain why the security aspect of ICPSs is a unique field that requires particular interest (see §2.3). (iii) We provide a comprehensive review on industrial protocols and infrastructures (see §3). (iv) We review the present cyberattack taxonomies from both academic and industrial domains and provide ours which combines their strong aspects (see §4.1). Then we present key findings from several industrial reports [45, 46, 47] (see §4.3). Then we analyze the available cyber defense approaches that can be implemented against the top ten most common industrial vulnerabilities (see §4.4). (v) We define ICPS security characteristics (see §4.5) and (vi) review the latest trends on ICPS edge network (see §4.6). (vii) Finally we share the lessons learned (see §5) our recommendations (see §6) and (see §7) conclusions.

2 INDUSTRIAL SYSTEMS & INFRASTRUCTURES

We now briefly define each system, clarify their relationships, introduce ICPS components, and analyze the differences between IT and OT.

2.1 Industrial System Definitions

Industrial Wireless Sensor Networks. Wireless Sensors Networks (WSN) is made from a group of spatially distributed autonomous/self-processing sensors that simultaneously perform various tasks (e.g., monitoring, detecting, and recording) at a lower cost than wired systems [48] are deployed in various environments ranging from local (e.g. home, car) to industrial (e.g. military, and health) [49]. In WSN, the current main challenges are related to latency and security [50]. These two features are even more significant for IWSN as providing availability is the primary concern for industrial systems deployed to CIs. Thus, various expertise among different disciplines including but not limited to (i) industrial applications, (ii) sensor architectures, (iii) communication/transmission technologies, and (iv) network architectures are desired secure IWSNs [41]. Current IWSN technologies are supported by standardization organizations (e.g., ISA, IEC, IEEE) due to their adaptability to harsh environments [42]. IWSNs are being integrated into the internet via gateways [51] and even in the future, they may even have dedicated IPs [52].

Industrial Internet of Things. IIoT refers to a technology emerged from ICS (e.g., Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS)) with the integration of interconnected devices, networking architectures (i.e., IWSN), and services through the internet. Conventional manufacturing, automation, computing systems are started to utilize IIoT by implementing cloud infrastructures [35]. IIoT is composed of two main parts as ICPS: the cyber part (e.g., sensing, networking, computing) and the physical part (e.g., sensors, actuators). Thus, we can identify IIoT as a subsection of ICPS. The defining feature of IIoT is the internet connection provided via network nodes that offer remote management. Besides, the rapid development of cloud technology has made IIoT more attractive as it provides efficient processing and storage of big data [36]. The increasing heterogeneity of IIoT has led to the development of WoT [40] to solve interoperability problems. We believe in the future, the industrial Web of Things (IWoT) [53] will be a canonical research area as the connectivity grows within the industrial environments.

Industrial Control Systems. ICS is the common term that refers to control systems such as SCADA, DCS, Programmable Logic Controllers (PLC) systems that are located in various industrial sectors. Years ago, ICS was air-gapped while running proprietary protocols therefore being less prone to cyberattacks. Now, ICS adapted to changes that have come with Industry 4.0. Today's ICS are integrated with IWSN, IIoT, and new generation PLCs that evolves them into advanced ICPSs. SCADA and DCS also are converged together allowing the implementation of hybrid systems that generate new challenges [54]. ICS are also targeted by cyberattacks in a daily manner where a successful cyberattack may result in a devastating impact. Therefore, security management [21] is a key point for ICS that is guided by national/regional organizations including the National Institute of Standards and Technology (NIST) [55].

Industrial Cyber-Physical Systems. The rapid developments of embedded systems, sensors, and networks resulted in new kinds of mechanisms with multi-tasking capabilities. Thus, the solid line between the physical and cyber

environments are started to blur. The term of Cyber-Physical System (CPS) presents today’s advanced computing and networking technologies in a unified way [56]. Industrial Cyber-Physical System (ICPS) refer to CPS that is specifically designed for industrial appliances. ICPSs are deployed to various domains including manufacturing, transportation, healthcare, and energy. The factories belonging to these domains utilize modern ICPSs are called “smart factories”. Figure 1 summarizes the difference in hierarchies between old and modern ICPS.

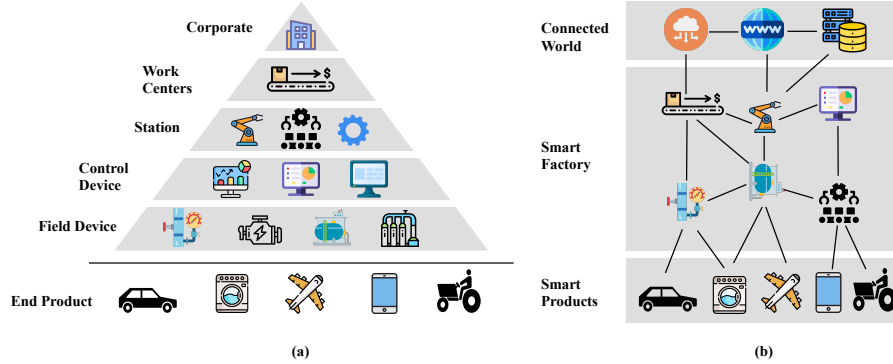


Figure 1: Illustrates the factory hierarchies [57] of Industry 3.0 (a) and Industry 4.0 (b). The increasing interconnectivity blurred the strict lines between ICPS levels and allowed the development of advanced heterogeneous systems which led to the emergence of the new term “smart factory”. Increasing overall efficiency is the main motivation behind this transition. However, organizations that tend to rush adopting new technologies without considering how to secure such a transition are prone to cyberattacks.

There are several CPS architectures present in the literature. The most basic one is 3C CPS architecture presented in [58, 59] where 3C means control, communication, and computation. Other available CPS architectures that classify the CPS domain in a more detailed way are 5C [4, 60], and 8C [61]. These processes are completed by a variety of interconnected components that are adapting to the latest technologies including real-time multiprocessing. Commercial-of-the-shelf (COTS) products [62] that perform the computation on the edge (via edge nodes) to forward already processed data to the cloud to minimize the system load/delay in industrial automation systems are such an example. The main components that are included in most of the ICPS architectures are sensors, actuators, controllers, and Human-Machine Interfaces (HMI). Figure 2 introduces the domain relationship of ICPS.

Sensors. Sensors are devices that convert the physical data to cyber data to monitor and forward events to designated components. Their application range varies from smart homes, transportation, manufacturing, medical systems to aviation. They can be grouped either according to their purposes such as temperature, proximity, light, ultrasonic and gas sensors, or their use cases such as industrial, residential, and commercial. As expected, industrial sensors have higher accuracy and durability thus cost higher than their peers while requiring periodic calibration to keep the data integrity. Industrial sensors are mostly utilized for ubiquitous monitoring purposes including human activity [63, 64], gas [65], and robotic arm [66].

Actuators. Actuators convert cyber data to a physical phenomenon therefore they are the complementary opposite of sensors. They are usually classified according to their working principles such as hydraulic, mechanical, electric, etc. Recent studies [42, 67] show that wireless actuators are very promising and even can be utilized for industrial

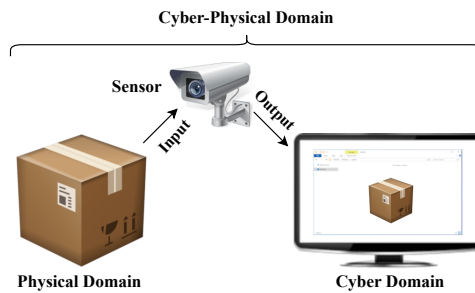
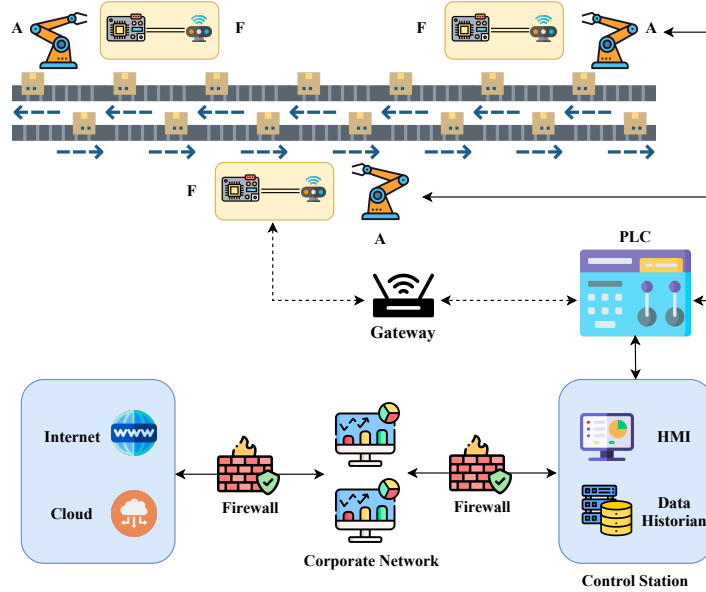


Figure 2: Illustrates the fundamental relationship between cyber and physical domain. To consider a domain as cyber-physical, it should at least include a cyber and physical phenomenon.



F: Fog Node *A*: Actuator *PLC*: Programmable Logic Controller *HMI*: Human-machine Interface

Figure 3: An example of modern manufacturing ICPS architecture. Actuators supervised by fog nodes contain embedded sensors. The data generated by sensors are processed at the edge and sent to PLC over a wireless communication channel. PLC automatically manages actuators based on the upcoming sensor data. Then the data sent to the control station. Here, the data stored in a database are accessible by the corporate network behind a firewall. The same is also applied when connecting outer networks.

environments where real-time applications take place. However, the new technologies and methods are required to overcome the existing challenges to accept wireless actuators as reliable for performing industrial tasks.

Controllers. The main control unit that gets inputs from sensors and sends outputs to actuators or central units is defined as the controller. The main controller types are Programmable Logic Controller (PLC), Distributed Control Systems (DCS), and Programmable Automation Controller (PAC). Controllers are evolved to the point where they can be utilized interchangeably [68] with the removal of technological limits that determines their design choices. Additionally, it is even possible to convert a microcontroller such as Raspberry Pi to a PLC via OpenPLC [69] to utilize for a low-cost simulation.

HMIs. Even though fully automated systems are getting popular, ICS that supervise CIs always requires human intervention at some point. HMI is the place where this intervention happens either for monitoring or controlling purposes. HMI technology has already adopted touch screens, and mobile devices. In the future, the cloud-based mobile HMIs [70] will be more widespread. There are also other ICPS components such as the Remote Terminal Unit (RTU), and data historian that are being integrated into main components to offer high connectivity with simple management. The future ICPSs will be only composed of components with multi-tasking capabilities. The modern manufacturing ICPS architecture contains aforementioned components is presented in Figure 3.

2.2 The Relationship Between Industrial Technologies

We believe the best way to understand the relationship between the aforementioned industrial technologies is to examine the work provided by previous surveys. While Mitchell and Chen [22], Leitao et al. [26], Huang et al. [31], Jbair et al. [28] provide a CPS definition, they do not acknowledge its relationship with other technologies. Ding et al. [30], Lu et al. [42], Yue et al. [13] position ICPS above other industrial terms and claim that IWSNs and industrial wireless sensor-actuator networks (IWSANs) can be referred to as subgroups of ICPSs. Lu [29] describes CPS as a technology that integrates the features of IoT and the Web of Things (WoT). Colombo et al. [71] describe ICPS as an industrial discipline that utilizes information communication technologies to integrate digital and physical elements to create intelligent systems. The authors also describe IoT and CPS as complementary disciplines by mentioning that IoT combines ubiquitous systems with CPS technologies. Karnouskos [72] mentions that SCADA relies on CPSs for monitoring purposes, hence defines them as complementary systems. While the most accepted opinion is that the ICPS is the combination of aforementioned disciplines, we could not find any framework that clearly outlines the similarities

and differences. We believe using these terms interchangeably results in an independent presentation of complementary works. Thus, there is a need for a framework that positions each term by clarifying their relationships.

2.3 Information Technology vs Operational Technology

We define IT as the technology of processing the information (data) while OT as the technology that focuses on monitoring and controlling physical phenomenon via physical devices and processes. This is why we see IT systems in nearly any kind of environment while we encounter with OT systems in only industrial ones. OT systems must operate in real-time due to being deployed in such an environment where the availability of the data is the primary concern. The adoption of mobile devices improves the availability of the system by providing ubiquitous access to authorized personnel [73]. Major ICPS suppliers such as Schneider Electric [74] and Rockwell Automation [75] already patented such mobile technologies nearly 20 years ago that also confirms how interconnected today’s technologies are.

ICPSs were air-gapped which means they were isolated from any outer networks. Therefore, they were automatically being protected from outsider threats. The only option for an adversary to attack a system was physically inserting data (i.e., via USB sticks) from the inside. Also, the IT and OT domains were kept separated. In today’s ICPS, OT has started to adopt IT-like technologies (e.g., TCP/IP protocol, Windows as an OS) because of its benefits [76]. However, controlling and monitoring OT devices via IT systems cause new vulnerabilities to appear as the “security through obscurity” approach is no longer applied. The implementation of new security measures requires the harmonization of IT and OT strategies and understanding of basic differences between two technologies. Table 2 summarizes the fundamental differences that we consider significant. Relatively new trends such as fog and cloud computing drive further convergence of IT and OT. In addition to these, wireless technology is also now more robust [77] and deployable for harsh industrial environments. We believe in the future the IT and OT will be integrated, and holistic approaches will form a base for future studies.

Table 2: Fundamental Differences Between IT and OT Domains

	Information Technology (IT)	Operational Technology (OT)
Protocols	HTTP, TCP/IP, FTP, UDP, SMTP	Modbus, Fieldbus, DNP3, BACnet
Operations	Stochastic	Deterministic
Patching(Updating)	Easy to patch	Hard to patch
Applications	Time-sharing	Real-time
Skilled Personnel	Available	Hardly Available
Deployment Cost	Low	High
Security Focus	Confidentiality	Availability
Authentication Method	Available	Barely available
Lifecycle	3 - 5 Years	Over 20 Years
Communication	User-centered	Machine-centered

3 ICPS Communication Technologies & Protocols

We classify the communication protocols according to standard availability, communication type, and network topology. There are two main communication protocol types in terms of standard availability: open, and proprietary protocols. Open protocols may be developed by a single or group of vendors and may require a license fee. They can be utilized with multiple vendors and also supported by a third-party software. On the other hand, proprietary protocols are developed and controlled by a single vendor. They are strictly restricted under legal terms. Legacy industrial systems had proprietary protocols therefore making manufacturer companies dependent on certain vendors. These protocols had been designed to achieve the best efficiency without considering security as a primary concern. The principle of security through obstruction was followed. However, even though there are still such systems, most of the ICPSs are no more air-gapped and even some of them are adopting cloud technologies. This makes open protocols more secure, and popular than the proprietary ones as they are developed by non-profit communities that keep them updated. Also, most companies prefer being more independent [78] when establishing their ICPS as they may integrate their systems with other components when needed.

The features of communication protocols for wireless and wired technologies differ from each other in many aspects. Legacy systems were mostly utilized wired communications technologies, unlike today’s ICPS which have a combination of both. Wired protocols such as Modbus and BACnet also compatible with many wireless technologies including Zigbee [79]. Wireless technologies are easy to deploy but may suffer from interference in an environment with high noise like electric distribution facilities. Wired communications are more reliable in terms of speed but harder to install and maintain. The systems that contain both can benefit from the advantages of each technology.

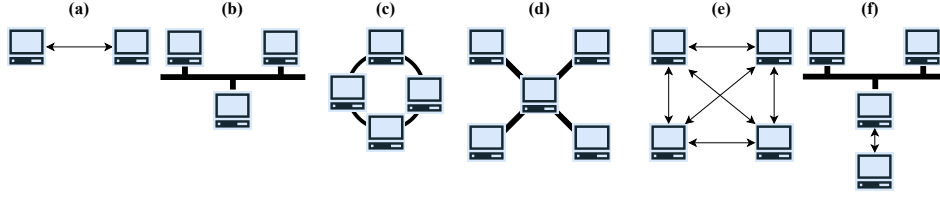


Figure 4: Illustrates industrial communication network topologies in the following order: (a) point-to-point, (b) bus (line), (c) ring, (d) star, (e) mesh, (f) hybrid. Each topology has unique pros and cons. For example, networks with mesh topology are more robust but cost higher, while bus topology costs less but more prone to failures. We can see these kinds of trade-offs for each network topology. Hybrid topologies are preferred in the latest ICPSs due to allowing more interconnectivity.

Data flow in the communication network may be one-way or bidirectional. Industrial manufacturers/vendors produce a variety of devices that comply with different topologies which determines the arrangement of nodes. These topologies either can be centralized (i.e., star) or decentralized (i.e., mesh). We illustrate the common topologies that are utilized in industrial environments in Figure 4. ICPS can benefit from the high number of nodes in terms of the computational power however it comes with an additional cost. Therefore, minimizing the number of nodes is one of the principles to consider when designing an ICPS. Research that examines this trade-off is presented in [80].

We can classify currently available industrial communication technologies according to their working principles: fieldbus [81], industrial ethernet [82], and wireless [83]. *Fieldbus*. End-user companies needed a real-time network model where they can connect all their industrial field assets (e.g., sensors, actuators) to increase production efficiency. This led to the development of fieldbus technology. The first ones came as proprietary protocols but later most of the major automation companies established groups/alliances and shared their licenses because the end-users required more heterogeneous production environments. *Industrial Ethernet*. The industrial communication technology started to shift to industrial ethernet from fieldbus because of the promises (i.e., very low latency) that ethernet offered. *Wireless*. The future industrial systems are expected to adopt more wireless technologies because they are easy to deploy and scalable. They also allow a low cost remote management without requiring additional setup. Early wireless systems lacked authentication schemes while having high latency which made them inadequate for industrial systems. Even though these issues are mostly resolved today, sustainability is still a big challenge, as wireless systems operate in resource-constrained environments. Figure 5 shows the market shares of deployed industrial network technologies respectively for 2019 and 2020.

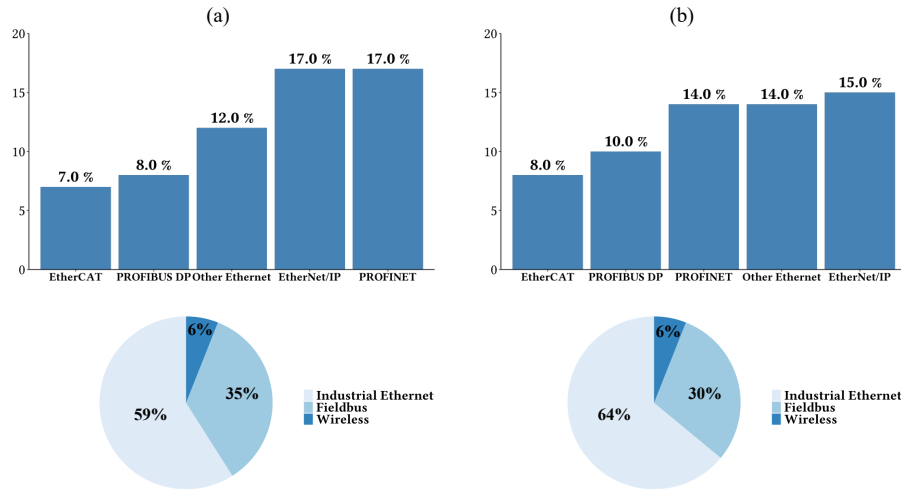


Figure 5: (a) Industrial network shares for top 5 protocols deployed in 2019 [84] including how the market shares differ per industrial network technology are shown. EtherNet/IP and Profinet led the industrial network market in 2019. Both of them are industrial ethernet standards while EtherNet/IP is popular in the USA, Profinet is widely accepted in Europe. In terms of overall market shares, Industrial Ethernet has a considerable lead. Increased bandwidth, high data transfer rate, and reliable real-time connection are the main reasons why companies favor industrial ethernet. (b) The same findings for 2020 [85] are shown. While the top 5 protocols do not show any significant changes, the Industrial Ethernet deployment rate is 5% increased while Fieldbus is 5% decreased which shows there is a transition from Fieldbus to Ethernet.

Fieldbus. *Modbus.* Open protocol developed and administered by Modbus Organization [86]. It is the most common industrial protocol that has several variants such as Modbus RTU (fieldbus) and Modbus TCP/IP (ethernet). It can be integrated with PLCs ranging from a variety of vendors. *DNP3.* Open protocol owned and developed by the DNP Users Group [87]. IEEE also standardized DNP3 [88] as it is one of the most common protocols that is utilized in power systems. It does not require additional setup to communicate with non-RTU units which makes it suitable for complex systems. *BACnet.* Open protocol mainly developed for building automation and control networks [89] also utilized in the heating ventilation and air conditioning (HVAC) industry. The protocol is maintained and developed by the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) [90]. Recently, BACnet Secure Connect (BACnet/SC) is proposed by ASHRAE to prevent problems when integrating IT systems into OT infrastructure for cloud-based applications [91]. *DeviceNet.* Open protocol invented by Rockwell Automation [92], now developed by ODVA [93]. The reduced number of wires with high flame resistance makes the DeviceNet network suitable for solar applications [94]. However, the increased number of nodes in DeviceNet causes an exponential increase in time delay [95] which may raise an issue for real-time complex networks.

Industrial Ethernet. *Profinet.* Open Industrial Ethernet Standard developed and administered by PROFINET International (PI) organization [96] that has around 1700 members. It provides a low response time that is ideal for real-time applications. The connection is provided by an ethernet jack that offers high flexibility. Profinet networks can easily interact with the IoT infrastructure [97]. *EtherCAT.* Ethernet-based open communication protocol designed for automation to minimize the delay within the industrial network. EtherCAT Technology Group [98] maintains the protocol. EtherCAT has a low implementation cost and also provides high-speed real-time communication [99] with low latency [100]. Thus, it is suitable for real-time robotic applications [101, 102]. *EtherNet/IP.* Open industrial protocol currently maintained and standardized by ODVA [103]. The EtherNet/IP network can be expanded by ethernet switches that theoretically enables connecting an unlimited number of nodes [104]. That also makes EtherNet/IP suitable easy to implement for highly interconnect ICPS. It offers several network structures including ring, star, and linear.

Wireless. *Zigbee.* One of the most popular open wireless communication protocol that is utilized in sectors ranging from industrial automation to smart homes/systems. It is administered and standardized by the Zigbee Alliance [105]. Being a low power solution and allowing remote management makes Zigbee suitable for environmental monitoring [106]. *Bluetooth.* Open wireless communication protocol that is designed as Personal Area Network (PAN), managed and standardized by Bluetooth Special Interest Group (SIG) [107]. Currently, the latest standardized version is Bluetooth 5.0. The rapid development of Bluetooth accelerates its integration into industrial applications. Not supporting mesh topology was a big downside of Bluetooth especially regarding industrial applications and led the proposal of academic solutions as seen in [108]. Therefore, Bluetooth SIG added this feature [109] and standardized it which is considered as a huge step in Bluetooth technology. *LoRaWAN.* Open wireless low-power wide-area network (LPWAN) protocol developed by Semtech maintained and standardized by LoRa Alliance [110]. It is arguably one of the most common LPWAN protocols utilized in many applications ranging from agricultural to home automation. LoRaWAN is suitable for smart home applications but for real-time monitoring, it should only be used where the application does not require a very low response time [111]. *WirelessHART.* Open wireless communication protocol based on the IEEE 802.15.4 standard developed by Field COMM Group [112] for industrial control applications. WirelessHART devices have the ability of bidirectional communication that is advantageous for mesh networks. A comprehension of WirelessHART with several wireless standards is presented in [113]. *ISA-100.11a.* Open wireless communication protocol based on IEEE 802.15.4 standard developed by ISA [114] to provide flexibility for industrial automation systems. ISA-100.11a supports mesh and star topologies. It can also communicate with multiple protocols via gateways thus allowing coexistence of wireless networks. *6LoWPAN.* IPv6 over Wireless Personal Area Networks (6LoWPAN) [115] is a wireless communication protocol based on IEEE 802.15.4 standard that is developed and standardized by Internet Engineering Task Force (IETF) [116]. The development of 6LoWPAN was a major stone for IIoT as it has provided an IP-based solution for a range of devices. However, IP-based solutions rise security concerns due to increased connectivity. We illustrate our security-oriented review of industrial communication protocols in Table 3.

4 ICPS Cybersecurity Analysis

ICPS is relatively a new term compared to IWSN, IIoT, ICS, DCS, and SCADA. Even though these systems are complementary to each other, there is an inadequate number of studies that examine the security of them under the ICPS roof. This leads to different study inputs such as taxonomies and evaluation metrics while making it harder to generate a common output for further research. Therefore, we have surveyed the studies that are also related to these systems and realized there is a need for multi-dimensional adaptive ICPS attack taxonomy. In this section, first we define ICPS attack taxonomy and evaluate real-life ICPS incidents. Then, we summarize key findings from several ICPS vulnerability assessment reports [46, 47, 45]. Finally, we define ICPS security characteristics and review proposed countermeasures against most common ICPS vulnerabilities.

Table 3: Comparison of communication protocols that can be deployed in ICPS.

Network Technology	Protocol	License	Maintainer	Network Topology [†]	Range(meters) [‡]
Fieldbus	Modbus-RTU	Open*	Modbus Organization [86]	Bus/Ring	1500
	DeviceNet	Open*	[93]	Bus/Ring	500
	BACnet	Open*	ASHRAE [90]	Bus	1200
	DNP3	Open*	DNP Users Group [87]	Bus/Ring/Point-to-Point	1200
Industrial Ethernet	Modbus-TCP	Open	Modbus Organization [86]	Bus/Star	100
	Profinet	Open	PROFINET International [96]	Bus/Ring/Star	100
	EtherCAT	Open	EtherCAT Technology Group [98]	Bus	100
	EtherNet/IP	Open	ODVA [93]	Star/Ring	100
Wireless	ZigBee	Open	Zigbee Alliance [105]	Mesh	30
	Bluetooth	Open	Bluetooth SIG [107]	Mesh	1k
	LoRaWAN	Open	LoRa Alliance [110]	Star	10k
	WirelessHART	Open	FieldCOMM Group [112]	Mesh	250
	ISA-100.11a	Open	ISA [114]	Star/Mesh	10
	6LoWPAN	Open	IETF [116]	Star/Mesh	100

*: The protocol converted to "open" from "proprietary". †: Most common network topologies are added, other versions might be available. ‡: For wired systems "Range" refers to a maximum cable length. Range values are estimated.

4.1 ICPS Attack Taxonomy

According to [117], a well-designed taxonomy should have the following attributes: mutually exclusive, exhaustive, unambiguous, repeatable, accepted, and useful. We believe taxonomies that follow these principles and mention countermeasures and vulnerabilities are more applicable to real-life applications. We have evaluated the available security taxonomies based on their contents and summarized our findings in Table 4. We have observed that most of the current taxonomies mainly focus on the IT field and the taxonomies that address OT mostly consider a certain characteristic (e.g., environment, application) which makes them non-usable for different OT systems. We have considered the aforementioned when developing our taxonomy. Also, industrial environments are adapting new ubiquitous technologies hence being more dynamic and heterogeneous. This makes non-adaptive attack taxonomies invalid for future cyber incidents. For this reason, multi-dimensional adaptive taxonomy that is specifically designed for a certain environment is more effective in terms of describing sophisticated cyberattacks. Thus, we have developed such a taxonomy where some of the key features are outsourced to an online attack taxonomy [118] that is regularly updated. We now present this taxonomy in Figure 6 that contains the following major attributes:

- (1) *Industrial Sector*: It is significant to define the sector to gain an initial opinion about cyberattacks in general. A food company that operates in two different sectors; food production (manufacturing), and delivery (transportation), may be subject to a cyberattack that targets both. We use the UK's Standard Industrial Classification (SIC) [134] that also complies with the standardization of the European Union [135] and the United Nations [136] in our taxonomy.

Table 4: Classification of the Currently Available Industrial Attack Taxonomies

Reference	IT	OT	Countermeasures	Vulnerabilities	Main Field
Simmons et al. [119]	●	●	●	●	General
Kim et al. [120]	●	●	●	●	Nuclear Power Plant
Loukas et al. [121]	●	●	●	●	Emergency Management
Chapman et al. [122]	●	●	○	○	General
Hu et al. [123]	●	●	●	○	Smart Grids
Wu and Moon [124]	●	●	○	●	Manufacturing Systems
Sabillon et al. [125]	●	●	○	○	General
Brar and Kumar [126]	●	●	○	○	General
Applegate and Stavrou [127]	●	●	●	○	General
Narwal et al. [128]	●	●	○	○	General
Yampolskiy et al. [129]	●	●	○	●	CPS
Drias et al. [130]	●	●	○	●	ICS Protocols
Berger et al. [131]	●	●	○	●	IIoT
East et al. [132]	●	●	○	○	DNP3
Elhabashy et al. [133]	●	●	○	○	Manufacturing Systems
capec.mitre.org [118]	●	●	●	●	General

Legend: ● : The aspect is explicitly stated and examined, ● : The aspect is not explicitly stated but partially included by authors, ○ : The aspect is not examined.

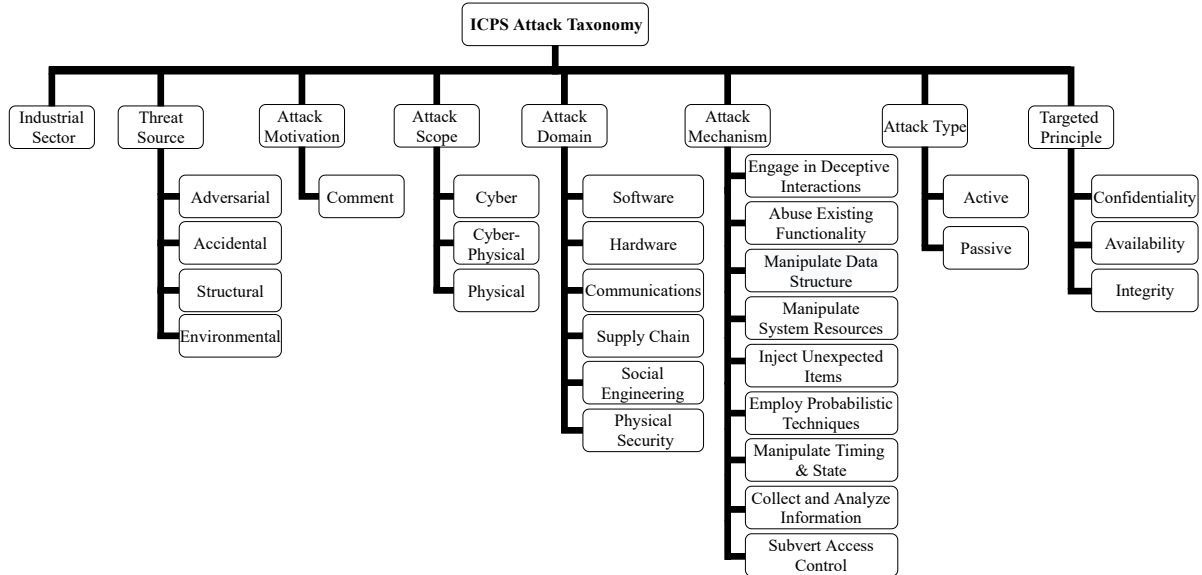


Figure 6: Multi-dimensional adaptive ICPS attack taxonomy. We combine several strong aspects of other taxonomies to build efficient, multi-dimensional, and adaptive ICPS attack taxonomy. "Attack mechanism" and "attack domain" is taken from CAPEC [118] while "industrial sector" is from SIC [134], and "threat source" from NIST [55]. The only downside of the proposed taxonomy is its dependence on CAPEC. As long as the CAPEC keeps their database up to date, we believe the proposed taxonomy will be sufficient. Even though we claim our taxonomy is suitable and efficient for ICPS attacks in general, we believe application-specific (e.g., manufacturing, transportation) taxonomies have a higher potential to describe industrial attacks more accurately. Only major classes of multi-dimensional branches are shown due to space constraints.

- (2) *Threat Source*: Who or what is behind the incident. It is necessary to identify the threat source to provide further protection for future attacks. In some cases, the threat source might compromise someone else's cyber source to hide its identity which is a very common case for distributed denial-of-service (DDoS) attacks. In that case, it is significant to distinguish them from victims. We utilize the threat source definition of NIST [55] in our taxonomy.
- (3) *Attack Motivation*: Recognizing the main reason that is directly related to the threat source behind the attack is crucial to determine what you may face in the aftermath of the incident. As the motive can be many things (e.g. financial gain, political opinion), categorizing attack motivation may result in an excessive amount of terms. Therefore, we believe commenting on this issue with a few sentences/words is more practical and informative.
- (4) *Attack Scope*: ICPS is a combination of cyber and physical systems. The attack may target not only the cyber but also the physical domain or both. For example, if the attacker accesses the network and steals data, that attack is cyber only. However, if the attacker gains control of the actuator via unauthorized network access, the attacks become cyber-physical. The only physical attacks are also possible such as physical theft or physically damaging an ICPS equipment. Thus, the scope is divided into three: cyber, physical, and cyber-physical.
- (5) *Attack Domain*: Describes the attack pattern. Defining the attacked domain is significant because similar attacks may require similar countermeasures and categorizing them hierarchically supports developing an adequate security plan. We include the multi-dimensional attack domain taxonomy of Common Attack Pattern Enumeration and Classification (CAPEC) [118] which is sufficient, detailed, and up to date. There are six main attack domains defined by CAPEC: software, hardware, communications, supply chain, social engineering, and physical security. For example, a common "e-mail injection" attack goes into the following categories in order as follows: software, and parameter injection.
- (6) *Attack Mechanism*: It defines the attack technique. Classifying the attack mechanism helps to figure out the vulnerability of the exploited system. One attack may contain several attack mechanisms (techniques) as mostly seen in Advanced Persistent Threat (APT) attacks where the attacker remains undetected for an extended period. We also utilize the multi-dimensional attack mechanism taxonomy of CAPEC [118] in this case.

- (7) *Attack Type*: The cyberattacks are divided into two categories in general: active, and passive. Imagine an attack scenario where the attacker has gained unauthorized access to the edge data (the data that is driven by sensors) in ICPS. If the attacker just extorts the sensor data without modifying, it is a passive attack. However, if the attacker falsifies the sensor data to further malicious activities the attack turns into an active attack.
- (8) *Targeted Principle*: There are three main information security principles: confidentiality, availability, and integrity. Confidentiality refers to the protection of data from unauthorized third parties. Availability refers to the data being accessible by authorized parties whenever needed. Integrity refers to the data being complete and uncorrupted. These three are defined as the CIA triad. One attack may target one or more principles at the same time. For example, while ransomware attacks mostly target availability, malware such as Trojan may target both confidentiality and integrity.

4.2 Evaluation of Real-life ICPS Incidents Based on ICPS Attack Taxonomy

ICPS incidents gain lots of industrial and academic interest as they are discovered. Academia, industry, and even sometimes government entities provide a deep analysis of the incident and publish report/article to inform related communities. Successful attacks with higher impacts subject to more research due to encompassing a variety of aspects including threat actor, attack method, and impact. We have evaluated 15 ICPS incidents (see Table 5 for evaluation and Figure 7 for timeline) based on our multi-dimensional adaptive attack taxonomy.

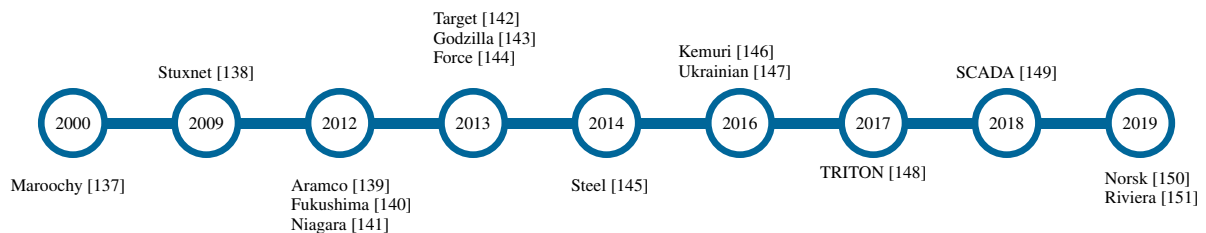


Figure 7: The timeline of the significant ICPS attacks.

Maroochy Shire Sewage Spill [137]. In 2000, a former employee of Maroochy Water Services hacked 142 sewage pumping stations and caused spilling around one million liters of sewage to local water systems. The attack was carried out with just a laptop, compact PC, and radio transmitter. The disgruntled employee accessed the system with stolen system assets and acted as an insider. He actively drove around pumping stations with a car with the hacking tools in it and manipulated the system values. Maroochy Shire Sewage Spill incident is a good example in terms of showing us how using the same credentials that are known by former employees might cause incidents. Industrial organizations must rearrange these credentials to prevent unauthorized access.

Stuxnet [138]. In 2009, the nuclear facility of Iran was targeted by the most complex attack known to date. Stuxnet infected more than 100,000 hosts in 25 countries where around 60% of infected hosts were located in Iran. It specifically targets the vulnerabilities that exist in Microsoft OS and Siemens PLCs while remaining hidden and aiming to generate physical anomalies in CIs. It is claimed [152] that the Stuxnet was developed by the US and Israel to sabotage Iran’s uranium enrichment program. However, there was no official confirmation from any sides.

Saudi Aramco Attack [139]. In 2012, the oil and gas manufacturer Saudi Aramco was targeted by a malware attack later named as Shamoon. Attackers accessed the enterprise network and deployed the malware which deleted data related to production. It is believed that the attackers also had insider help as deploying that kind of malware requires physical access to internal computers. The attack failed to access the industrial network. The hacker group named “The Cutting Sword of Justice” announced that they were behind the attack for political reasons.

Fukushima Daiichi Nuclear Disaster [140]. In 2011, the earthquake disrupted Fukushima Daiichi nuclear power station by damaging power systems that cool the reactors which resulted in radioactive contamination and followed by the evacuation of around 100,000 residents. Natural disasters are predictable only to some extent. Usually, the risks that may occur due to these events are ignored when designing ICPS. Fukushima Daiichi nuclear disaster incident led to the re-examination of similar facilities to question how safe they are against natural disasters.

Tridium Niagara Framework Attack [141]. In 2012, attackers infiltrated the HVAC system of a company located in the USA. The company was using an older version of Tridium Niagara ICS that contains several vulnerabilities that allow backdoor access. These vulnerabilities were already published and analyzed by several cybersecurity organizations. However, the victim company was unaware of the issue. The ICS was connected to the internet with password protection set up. Attackers gained administration privileges without knowing the password by exploiting the

already known vulnerability. The attackers did not access any significant document and the motivation behind the attack is unknown.

Target Attack [142]. In 2013, the anomalies in the IT system of TARGET were discovered by a third-party forensic team. The attackers had accessed the personal information of more than 1,000,000 customers. The list of third-party vendors that work with Target was already available in Target's Supplier Portal. The attackers chose Fazio Mechanical (HVAC manufacturer) and sent a phishing e-mail to one of the employees. They injected malware via a phishing e-mail and stole the login credentials of Fazio Mechanical. Then, they accessed the enterprise network and stole personal information with the motivation of financial gain. This incident is unique in a way that the attackers accessed the IT network by comprising the OT network first.

Godzilla Attack! Turn Back! [143]. In 2013, the electronic road signs in San Francisco, USA were hacked and instead of essential messages, they were showing "Godzilla Attack!" and "Turn Back!". The signs were controlled by a third-party company that was still using default credentials to access the network. The incident did not cause any significant problems. The company responsible for the signs claimed that the attack was done by someone who already knew the credentials. It is believed that the motivation behind the attack was just personal entertainment.

Brute Force Attacks on Internet-Facing Control Systems [144]. In 2013, a gas compressor station owner in the USA alerted ICS-CERT regarding detected increased number of brute force attack attempts on their systems. They were done from 49 different IP addresses. The threat actors and motivation behind the attacks are still unknown. None of the attacks were successful. This case is a good example to show how early detection of intrusion attempts prevents further damage to industrial systems by increasing the possibility of an effective response.

German Steel Mill Cyberattack [145]. In 2014, the blast furnace of a German steel mill was attacked. The attack resulted in massive physical damage since the furnace could not be shut down. Attackers accessed to the enterprise network via phishing e-mail then moved into an industrial network and performed malicious code execution to reprogram several PLCs to compromise the functions of the furnace. They exploited the vulnerabilities resulting from weak boundary protection between established networks due to lack of DMZ. The attack has been defined as an APT and believed to be executed by a group that aims intellectual property theft.

Kemuri Water Company Attack [146]. In 2016, Verizon published a report of an attack on a water treatment company (Verizon named the company as Kemuri to hide its real identity). The company had stored operational control system credentials on the front-end web server. The adversaries accessed those credentials via SQL injection and phishing. They managed control actuators but failed to cause any harm due to a lack of expertise on SCADA systems. However, it is believed that the personal information of around 2,500,000 users was stolen.

Ukrainian Power Grid Attack [147]. In 2015, the electricity distribution company Ukrainian Kyivoblenergo was subjected to attack resulted in the power outage that affected 225,000 customers. The attackers accessed the IT network via phishing e-mails, then seized the credentials, and infiltrated the industrial network to execute malware named BlackEnergy 3. They kept attacking the system with 30-minute intervals to prevent mitigation techniques to be deployed.

TRITON [148]. In 2017, the Safety Instrumented System (SIS) of a Middle Eastern oil and gas utility company was shut down due to the successful execution of malware named TRITON. SIS controller that prevents OT assets from malfunctioning made by Schneider Electric SE connected to a Windows PC was deactivated due to TRITON leaving whole utility vulnerable to OT incidents. The attackers first infiltrated the IT network then moved to the OT that shows there was weak boundary protection between these networks.

Cryptocurrency Malware Attack on SCADA [149]. In 2018, a malware was discovered on the OT system of a European water utility company. The malware was designed to mine Monero cryptocurrency by utilizing the HMI and SCADA servers of the victim. It was able to run in stealth mode, but increased CPU and bandwidth usage were detected by the IDS. Updating OT systems requires advanced techniques and thus most of the systems cannot get the latest updates on time. In this case, HMI applications that were not up-to-date were connected to the internet to allow remote management. Attackers exploited these applications to access the system.

Norsk Hydro Ransomware Attack [150]. In 2019, aluminum manufacturing company Norsk Hydro suffered from a ransomware attack later named as LockerGoga. The adversaries accessed and encrypted the critical data resulting in the shutdown of the enterprise network and halt of many operations including order processing. The motivation of the attack is estimated as disrupting the production and reputation of the company rather than financial gain as the adversaries chose to execute a previously known ransomware attack after gaining access to the system.

Riviera Beach Ransomware Attack [151]. In 2019, the water utilities of Riviera Beach (a small city located in Florida, USA) were subjected to a ransomware attack. Attackers sent a phishing e-mail to the police department where the employee opened a malicious link triggered the immediate lockdown of the department computer. The attack spread to all city networks including water utility systems due to being interconnected to the IT network without any bound

Table 5: Evaluation of Real-Life ICPS Incidents

Year	Name	Industrial Sector	Threat Source	Attack Motivation	Attack Scope	Attack Domain	Attack Mechanism	Attack Type	Targeted Principle
2000	Maroochy Shire Sewage Spill	E	Adversarial/Outsider	Revenge	Cyber-Physical	Software Communications	Subvert Access Control	Active	Confidentiality
2009	Stuxnet	C	Adversarial/Nation-State	Sabotage	Cyber-Physical	Software Hardware Communications	Engage in Deceptive Interactions Manipulate System Resources Inject Unexpected Items	Active	Integrity
2012	Saudi Aramco Attack	D	Adversarial/Group/Established	Political Reasons	Cyber	Software Supply Chain	Manipulate Data Structures Subvert Access Control	Active	Integrity
2012	Tridium Niagara Framework Attack	D	Adversarial/Individual	N/A	Cyber	Software	Abuse Existing Functionality	Active	Confidentiality
2012	Fukushima Daiichi Nuclear Disaster	C	Environmental/Natural Disaster	N/A	Physical	N/A	N/A	N/A	N/A
2013	Target Attack	G	Adversarial/Group/Established	Financial Gain	Cyber	Software Social Engineering	Inject Unexpected Items Subvert Access Control	Active	Confidentiality
2013	Godzilla Attack! Turn Back!	H	Adversarial/Individual	Personal Entertainment	Cyber	Software	Subvert Access Control	Active	Integrity
2013	Brute Force Attacks on Control Systems	D	Adversarial/Outsider	N/A	Cyber	Software	Employ Probabilistic Techniques	Active	Confidentiality
2014	German Steel Mill Cyber Attack	C	Adversarial/Group/Competitor	Theft	Cyber-Physical	Social Engineering Software	Inject Unexpected Items Manipulate System Resources	Active	Integrity
2016	Kemuri Water Company Attack	E	Adversarial/Nation-State	Sabotage	Cyber-Physical	Software Social Engineering	Inject Unexpected Items Engage in Deceptive Interactions	Active	Integrity
2016	Ukrainian Power Grid Attack	D	Adversarial/Nation-State	Sabotage	Cyber-Physical	Software Hardware Communications Supply Chain	Manipulate System Resources Inject Unexpected Items	Active	Integrity
2017	TRITON	C	Adversarial/Nation-State	Sabotage	Cyber-Physical	Software Hardware	Inject Unexpected Items Manipulate System Resources	Active	Integrity
2018	Cryptocurrency Malware Attack on SCADA	E	Adversarial/Group/Established	Financial Gain	Cyber	Software	Inject Unexpected Items	Active	Integrity
2019	Norsk Hydro Ransomware Attack	C	Adversarial/Organization	Reputation	Cyber	Software	Inject Unexpected Items	Active	Availability
2019	Riviera Beach Ransomware Attack	E	Adversarial/Group	Financial Gain	Cyber	Software	Inject Unexpected Items	Active	Availability

protection mechanisms. The city council agreed to pay the ransom which was 65 Bitcoins (around \$600,000 due that date) however attackers did not send the decryption key. Then the city council decided to change outdated hardware that was deployed on attacked systems.

Table 5 demonstrates the evaluation of major ICPS incidents based on the ICPS attack taxonomy that we developed. Our findings have shown that the most targeted industrial sectors [134] are manufacturing and electricity, gas, steam and air conditioning supply. Most ICPS attacks are active and organized by nation/state established groups while aiming to disrupt the data integrity. Also, there are no physical-only attacks among major cases.

The attacks against ICPS mostly include more than one stage while the advanced ones may execute the whole CKC. Integrating IT and OT networks without providing robust and secure boundary protection is the most exploited case that has been encountered in ICPS incidents. Attackers mostly target companies that lack security personnel with industrial security expertise via phishing e-mails. Most of the companies that subject to data breach reject publishing a public report on incidents to hide their identities. The information on incidents is mostly available through news agencies or cybersecurity bloggers where they claim getting information via whistle-blowers (e.g., former or current employee with a pseudonym) that makes further examination harder.

4.3 ICPS Vulnerability Assessment Reports

ICPSs should be treated as if they will be subject to cyberattack any moment. Security professionals need to discover all vulnerabilities while knowing only one may be enough for an adversary to damage the system. Risk assessment is required to design an efficient security plan. Risk assessment plans vary for each ICPS as they contain different assets that are rapidly evolving due to the integration of new technologies. Such research that considers this change and proposes a risk assessment method for modern smart grids is presented in [153].

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [154] analyses vulnerabilities of CIs ranged from small and medium-sized businesses (SMBs) to large corporations that are located in the USA. The vulnerabilities are ranked based on The Common Vulnerability Scoring System (CVSS) [155]. Their industrial vulnerability assessment reports respectively for 2015 [46] and 2016 [47] outline that the integration of IT to OT causes new vulnerabilities while most of them are related to weak boundary protection. Weak boundaries between OT and IT (enterprise) networks may result in unauthorized access. Establishing an industrial demilitarized zone (IDMZ) [156] is one way to mitigate such a problem. Table 6 illustrates the key findings from these reports.

Table 6: Comparison of ICS-CERT Industrial System Vulnerability Assessment Reports [46, 47]

Year	Number of Assessments	Found Weaknesses	Weakness Per Asset	Boundary Protection
2015	112	638	5.7	13.00%
2016	130	700	5.4	13.40%

Cyber Kill Chain (CKC) [157] is a widely accepted framework created by Lockheed Martin in 2011 that identifies the stages of a successful cyberattack. The CKC developed by SANS [158] is more precise and applicable for ICPS in general. Successful delivery of CKC to ICPS results in a data breach that may trigger catastrophic failures. Figure 8 illustrates the key findings from Verizon’s [45] data breach report where only 4% of the total confirmed breaches belonged to the OT systems. However, the results of 4% may have a bigger impact than the rest (96% IT-related breaches).

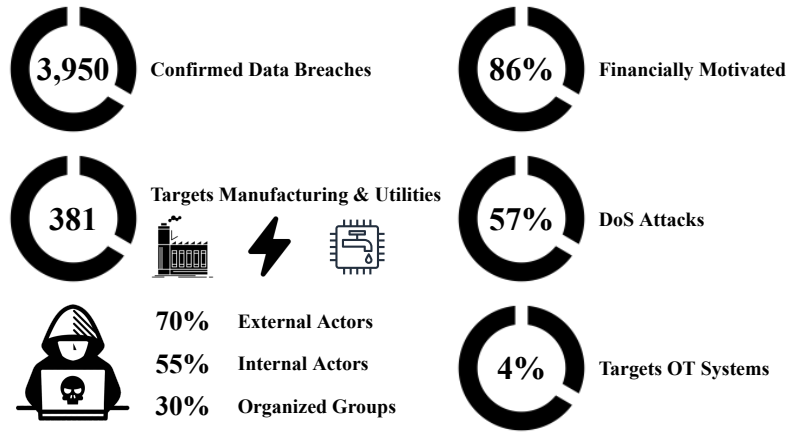


Figure 8: Key findings from Verizon’s 2020 data breach report [45]. 381 data breaches (10% of total) are against industrial systems where not all of them target OT equipment. Financial gain is the main reason behind 86% of attacks where most likely they are carried out by organized groups which form 55% of total threat actors. DoS is the most preferred attack method due to the availability of unsupervised many IoT devices as seen in the Mirai Botnet [159] incident.

4.4 Countermeasures Against Most Common ICPS Vulnerabilities

Figure 9 displays the top ten ICPS vulnerabilities accounting for 45.90% of the total in 2016 [47]. While boundary protection is the most common vulnerability, it is followed by weak authentication mechanisms. Integrating IT systems to OT by utilizing the latest available technologies to increase the processing efficiency of factories without properly preparing and complying with security plans, policies, and procedures cause new vulnerabilities that can be exploited by threat actors. The industrial cybersecurity reports [46, 47, 45] we have examined determine the direction of cybersecurity studies being funded by security companies, research councils, and state establishments. This allows the rapid development of security techniques that provide the deployment of new defence mechanisms. Now, we review academic studies that present such techniques as a solution to the top ten common vulnerabilities (see Figure 9) identified by ICS-CERT based on the NIST classification [55]. We evaluate related studies in the literature based on several characteristics illustrated in Table 7 that increase the industrial practicality of these proposals.

4.4.1 Boundary Protection

The boundary between IT and OT networks in ICPS is fading away due to increased connectivity. Weak boundaries pose a great risk as seen in the past cyber incidents [145, 146, 151]. Establishing a DMZ that contains protection mechanisms including a firewall is the first step to strengthen these boundaries. However, even DMZ itself is prone to attacks. [160]. Mazur et al. [156] defines the requirements of a DMZ while discussing if it is needed for mining applications. Jiang et al. [161] simulate a DMZ using Riverbed Modeler to evaluate performance factors regarding defense-in-depth strategy. Hassan et al. [162] develop IDS based on a semi-supervised deep learning model to provide

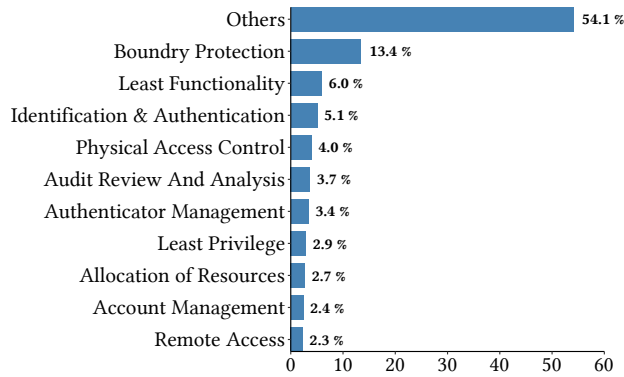


Figure 9: Illustrates the top ten vulnerabilities seen in industrial environments. Vulnerabilities are not isolated from each other. One weakness of ICPS may be a reason for several vulnerabilities. Attacks against CIs target altering the integrity of data first compromise the confidentiality. Therefore, an adversary checks for confidentiality vulnerabilities before engaging in malicious activity. While the current most significant issue is providing boundary protection when integrating new IT technologies to OT, others are mostly present due to a lack of enforcement of well-designed security policies.

boundary protection while proposing a framework of attack strategies that target IIoT networks. They evaluate their model on a real-life IIoT network testbed.

4.4.2 Least Functionality

The interconnected heterogeneous industrial network contains a variety of system functions (e.g., port, protocol, and services) that keep the main processing units running. Least functionality refers to prohibiting and restricting the usage of these to prevent potential abuse. The industrial companies tend to ignore security due to focusing on reducing cost, hence, resulting in the least functionality vulnerabilities. Cao et al. [163] discuss this issue and propose the random multipath routing model that minimizes the required number of paths to reduce the least functionality vulnerabilities. They utilize that model to provide a security-oriented node deployment framework optimized by a distributed parallel algorithm. Particle swarm optimization (PSO) is another method that addresses optimized node deployment. Ling et al. [164] propose such an enhanced PSO method that may be utilized for real-world industrial systems to improve efficiency and security aspects. They apply 17 benchmarking tests to evaluate the proposed model and compare it with previously developed PSO methods while also evaluating their performance on economic load dispatch (ELD) that schedules power generator outputs according to load demands.

4.4.3 Identification and Authentication

Applying proper authentication mechanisms in an industrial environment prevents unauthorized access while easing data circulation. Authenticating human-to-machine or machine-to-machine (M2M) communications requires prior identification. Unidentified entities in such environments are prohibited from acting. By faking sensor data, an adversary can damage the ICPS while preventing intrusion detection. Authentication mechanisms are deployed to the edge to prevent such an act. Li et al. [165] discuss that deploying traditional authentication mechanisms to the resource-constrained environment of sensor nodes poses a challenge and propose a privacy-preserving secure biometrics-based authentication scheme for IIoT. They do the testing via simulation by considering authentication based security properties (e.g., password change, wrong password detection). Esfahani et al. [166] emphasize that and proposes a lightweight authentication scheme for M2M protocols. Their scheme has two steps: each sensor is registered to the system via an authentication server, then mutual authentication is provided. Das et al. [167] propose a biometrics-based user authentication scheme for a cloud-based IIoT model that deployed in manufacturing sites while preserving privacy.

4.4.4 Physical Access Control

Access to industrial facilities is provided via keys, electronic cards, and mobile technologies. While physical keys are subject to theft, electronic cards and mobile technologies (i.e., smart locks) are prone to forging. Ho et al. [168] discuss the security of smart locks by modeling with different threat models. They address how current COTS smart locks

are vulnerable to state consistency and relay attacks. They propose a touch-based authentication scheme where the communication is provided via bone conduction. Mudholkar et al. [169] briefly introduce biometrics and propose a fingerprint-based authentication mechanism. They claim access to a computer can be provided via fingerprint scanners instead of a password to improve overall security. Mock et al. [170] address that the real-time continuous authentication mechanisms provide better security. They develop an iris recognition authentication model based on a commercial eye tracker and claim the current error rate is too high to be used as a standalone mechanism.

4.4.5 Audit Review and Analysis

Organizations should adopt Security Information and Event Management (SIEM) system as an operational whole log management mechanism. However, the adversary can organize decoy attacks to occupy SIEM. Thus, prioritizing alerts is an important task. Sancho et al. [171] propose a threat level rating model that evaluates the SIEM output. The authors classify threats and assign four priority levels: critical, important, moderate, and low. First, they perform a data balancing to real-life datasets and then evaluate the proposed model on balanced datasets. They compare the proposed model with commercial software to validate. Due to available limited processing power, an in-depth analysis of ICPS edge data is challenging. Tao et al. [172] discuss these issues and proposes a secure event detection scheme for ICPS while providing a data validation algorithm. They test their system on a real-world dataset and claim that the proposed scheme is adequate to secure data transmission in ICPSs. Huang et al. [173] propose a data historian based on the IBM Informix database for Big Data management. The authors develop an IIoT data management benchmark (named as IOT-X) by utilizing two relational databases to evaluate their design. They claim the proposed system offers high efficiency compared to traditional historians.

4.4.6 Authenticator Management

Three essential principles that must be regulated by password enforcement policies are password change, removal, and encryption. *Password change*. COTS ICPS devices like PLCs come with a default password that is assigned by the vendor. Thus, it poses a great risk and a new password should be set (see [137] for real-life incident example) before device deployment while being reset at random intervals. *Password removal*. Due to the severity of the operations and availability concerns memorizing a password is not feasible in industrial environments. Therefore, the passwords belong to operational devices are stored in a local/cloud database. When an employee is no longer associated with the organization, the linked password should be removed from the database to prevent possible abuse. *Password encryption*. Strong encryption mechanisms need to be applied to secure passwords starting from the authentication step. If the password is transmitted or kept as plain text, an adversary can access it in case of an intrusion. Sarkar et al. [174] address that the password policies for traditional IT networks can be applied to ICPS where the environment contains unique devices such as PLC and RTU. They propose a security-oriented password policy for ICPS with a detailed password creating guideline. Korman et al. [160] evaluate the effectiveness of several ICPS cybersecurity countermeasures including password policy enforcement. Authors analyze the available CPS security assessment tools based on three techniques: network segregation, strengthened access control, and patch management. They claim password policy enforcement complement network segmentation to secure CPSs.

4.4.7 Least Privilege

NIST [55] suggests applying the least privilege principle as a part of the defense-in-depth strategy for ICPS. It provides minimal access to a software/user required for essential tasks when needed, while the task number is being kept at the minimum. This provides easy to analyze systems with higher overall security. Least privilege can be provided via the application of role-based access control (RBAC) that assigns certain access rights to dedicated roles. Such a work is presented in [175] where authors implement RBAC to the industrial remote maintenance system. They evaluate the proposed system on Raspberry Pi 3 by setting up virtual hosts. They claim such an implementation as a standalone security mechanism can be implemented to remote maintenance systems as a countermeasure against zero-day attacks. Another work [176] evaluates the use of Software-defined networking (SDN) switches to implement the least principle scheme for ICPS. Authors address the cybersecurity requirements on [55] as a motivation of their work while discussing how to implement NIST suggested mitigation techniques via SDN switches. They test the proposed system via two different SDN switches (real-life testbed) and claim ICPS can benefit in terms of least privilege networking from such an implementation.

4.4.8 Allocation of Resources

Due to increasing interconnectivity, providing a secure environment for ICPS is becoming more resource-demanding. Smeraldi and Malacaria [177] discuss the question of how to optimize the cybersecurity budget spending. They apply the knapsack problem and develop an optimization model for two different cases: multiple targets and separate

resources, multiple targets and shared resources. They claim such a combinational optimization can be applied for resource allocation. Another model for this issue is presented by Wang [178]. The author utilizes mathematical cyber breach probability models to develop a function as a solution to the resource allocation problem. They address that the organizations can benefit if they apply the least privilege principle and access authentication schemes before allocating security resources. Srinidhi et al. [179] analyze the resource allocation problem from the manager's perspective and claim that managers tend to over-invest specific security methods that are effective in the short run due to financial distress that they are faced with while investors prefer more productive ways that are more effective in the long run. They propose a resource allocation decision-support model for managers and investors utilized in case of a breach.

4.4.9 Account Management

Additional accounts in ICPS networks are used in exceptional (e.g., error, intrusion) situations. These temporary/emergency accounts may have access to critical assets. Hence, they need to be removed/disabled once their use is completed. Such an action should be regulated by an access control policy. Valenzano [180] proposes a role-based twofold access control policy model for industrial systems. The author emphasizes the difficulty of validating access policy enforcement. Thus, most solutions in this context either assume that the policy is either enforced or propose an additional software/hardware extensions. The model proposed by the author clearly outlines the usage conditions on edge mechanisms. Ren et al. [181] utilize blockchain technology to implement identity management and access control to edge IIoT mechanisms. The access control policy is defined by the edge network terminal, hence automated. Their evaluation shows that the proposed model can efficiently work in the IIoT edge which is a resource-constrained environment.

4.4.10 Remote Access

The integration of cloud technology to OT and rapid advancements in IWSNs have been a huge steppingstone for IIoT and allowed feasible remote monitoring/management within the ICPS. RTUs that gather data from edge sensors are converted to remote substations with the integration of IWSN where the data is accessed and forwarded to a designated point via remote management. However, providing an additional access point increases the attack surface thus new security measures should be set based on security-oriented integration strategy before or when enabling remote access. Alcaraz et al. [182] discuss how to securely integrate IWSN with the internet to provide ubiquitous management for ICPS. Authors address two main challenges: available limited local access options, and the trade-off between real-time performance and security. They analyze the integration strategies and mechanisms from both efficiency and security perspective while addressing internet connection is not required to build remote accessible IWSN. Sadeghi et al. [35] discuss that security has become a hot topic after the integration of IT systems to IIoT that offers remote monitoring and control. They mention future management of IIoT will be challenging due to rapidly increasing heterogeneity that will generate large data. They claim only cloud-based services are capable of processing large data in real-time. However, using cloud services for industrial tasks may raise privacy concerns. Anand and Regi [183] propose a remote water level monitoring design. Authors discuss how current remote access technologies lack modern security mechanisms. They claim existing security measurements for GSM and LTE may be a solution for these issues and can be utilized for remote monitoring while being adapted to IIoT. They also mention that the security of remote access concepts depends on the communication protocol choice.

4.5 ICPS Cybersecurity Characteristics

The most sophisticated cyber attacks (e.g., Stuxnet, TRITON) in history targets CIs that are managed by ICPS. Therefore, the concept of defense-in-depth must be applied to all assets contained in CIs. Defense-in-depth can be provided via establishing several defense layers where each layer serves for a certain purpose while the main objective is to provide a secure environment. These layers may differ for technical assets (e.g., hardware, software) while showing similarities in terms of personnel and procedures. Secure industrial environment that is designed based on defense-in-depth approach should contain the following characteristics that complement each other:

Robustness. All systems are prone to fail. Robustness determines how much a system can endure before failing. This is a significant security feature for each asset in industrial environments due to the cascading effect observed in highly interconnected ICPS. The robustness of a system should be tested whenever a change is made to the system. Even though there are not any known changes, periodically testing is required as some of the components may degrade over time. Fuzz testing [184] such as Netflix's Simian Army approach [185] can be implemented to evaluate ICPS robustness.

Resilience. We can shut down IT systems whenever an anomaly is detected. However, this is not valid for OT systems as they are supervising CIs, they need to be kept operating even when there is an intrusion. Resilience determines how

Table 7: The Evaluation of Proposed Countermeasures Against Most Common ICPS Vulnerabilities Based on Dataset Availability, Evaluation Method, Privacy, and Utilization of AI/ML Techniques

	ICPS Vulnerability	Dataset		Evaluated Method		Privacy	AI/ML
		Pre-obtained	Generated	CPS Testbed	Others*		
Mazur et al. [156] Jiang et al. [161] Hassan et al. [162]	Boundary Protection	✓		✓	✓		✓
Cao et al. [163] Ling et al. [164]	Least Functionality				✓ ✓	✓ ✓	
Li et al. [165] Esfahani et al. [166] Das et al. [167]	Identification and Authentication				✓ ✓ ✓	✓ ✓	
Ho et al. [168] Mudholkar et al. [169] Mock et al. [170]	Physical Access Control	✓		✓ ✓		✓ ✓	✓
Sancho et al. [171] Tao et al. [172] Huang et al. [173]	Audit Review and Analysis	✓ ✓ ✓	✓		✓ ✓ ✓	✓	✓
Sarkar et al. [174] Korman et al. [160]	Authenticator Management				✓		
Kern and Anderl [175] Venugopal et al. [176]	Least Privilege	✓		✓	✓		
Smeraldi and Malacaria [177] Wang [178] Srinidhi et al. [179]	Allocation of Resources				✓ ✓		
Valenzano [180] Ren et al. [181]	Account Management				✓ ✓	✓	
Alcaraz et al. [182] Sadeghi et al. [35] Anand and Regi [183]	Remote Access			✓		✓ ✓	

*: Others include evaluation via benchmarking tests, simulations, or proof of concept.

long does it take for the system to fully recover after an anomaly. SDN [186, 187] is one of the techniques that may be utilized to develop models that contain routing algorithms to increase resiliency in ICPSs.

Redundancy. If we can answer the question of what happens when one sensor fails during the manufacturing process with the back-up sensor activates and keeps reporting, that means we designed a redundant system. The edge monitoring mechanism of ICPS consists of a sensor that supervises production line assets such as robotic arm, conveyor belt, gas tank, and oven. The data taken from these are either sent to the command and control (C&C) center to be checked by the control engineer or handled by autonomous control units. The final phase of the attack against ICPS includes faking sensor values to delay the activation of SIS. This can be prevented via deploying additional layers of sensors under the context of increasing redundancy. Therefore, even though it is not directly mentioned when designing optimized systems, redundancy is one of the main factors that is considered. Such an example is presented in [188].

4.6 Securing ICPS Edge Network

The real-life ICPS incident evaluation (see §4.2) has shown that most adversaries target edge network/mechanisms by either exploiting weak boundary protection mechanisms (i.e., accessing OT assets from IT domain) (see §4.4.1) or infiltrating other ICPS elements (e.g., HMIs, PLCs) as the main motivation behind the attacks to maximize given damage by disrupting actuator behaviours [137, 138, 145, 148]. Therefore, their first step after breaching the system is to fake sensor readings to bypass deployed anomaly detection mechanisms. Thus, even though the vulnerability assessment reports [46, 47, 45] show that the most common ICPS vulnerabilities based on weak boundary protection mechanisms, as the final aim of the adversary to disrupt ICPS edge network, efficient security mechanisms that feature key cybersecurity characteristics (see §4.5 and detect the anomalies in physical behaviours (e.g., change in the temperature, pressure, fan behaviour) should be deployed to the edge. The evaluation based on real-life testbeds and datasets generate the most realistic results for such research. Now we briefly summarize the latest research related to ICPS edge security based on the findings of previous surveys/works (see Table 1).

Edge Anomaly Detection. Giraldo et al. [32] survey the physics-based attack detection techniques in cyber-physical systems and propose a taxonomy to evaluate related research. Their key findings include: (i) the vast majority of papers

do not share common evaluation metrics and do not simultaneously utilize simulation, testbed, and real-world data, (ii) the cases when adversaries in control are ignored. The authors emphasize that the anomaly detection monitor should be deployed to the edge and not just to the central network while proposing new evaluation metrics that can be applied to a variety of anomaly detection algorithms. Ramotsoela et al. [34] survey the anomaly detection methods utilized for IWSNs. The authors mention that the trade-off between detection accuracy and power consumption is one of the main issues to be considered while the other one is the lack of training data. They emphasize the high cost and inability to evaluate complex ML algorithms are the main drawbacks of IWSN testbeds. Besides, many papers utilize simulation programs, hence, we can conclude that the access to these testbeds is also questionable. Shah and Tiwari [189] apply anomaly detection by utilizing several machine learning techniques on data gathered from real-life industrial machines. The authors conclude that while in some use cases the anomalies can be detected via statistical analysis, others require machine learning techniques. They mention the data deviation due to external reasons (e.g., at the start, malfunctioning, being idle, degradation) occurs more than expected so should be considered when training the ML model.

ICPS Testbeds. McLaughlin et al. [190] summarize the required features of an efficient ICPS testbed and emphasize that the hardware is a must for an ICPS testbed, hence, hardware-in-the-loop (HIL) testbeds are better at simulating real-world cases. The authors also mention that the HIL testbeds are becoming standard for vulnerability assessment thanks to their increasing numbers and allowing the testing of cyber-physical components. Yamin et al. [191] propose an extensive survey regarding security testbeds. The authors confirm that the interest in security testbeds (emulation, simulation, hybrid, or real) is increasing. However, the efficiency of these testbeds is questionable due to the lack of quantitative and qualitative analysis. Holm et al. [192] review 30 ICS testbeds based on the evaluation metrics defined by Siaterlis et al. [193] which are *fidelity*, *repeatability*, *measurement accuracy*, and *safe execution of tests*. The authors describe fidelity is the most key characteristic as it defines the accuracy of the testbed. However, only 4 of the works discuss the fidelity of the testbeds based on the standards [55]. Also, the objectives of the testbeds are defined in detail. Hence, the authors emphasize the need for a comprehensive evaluation framework to be utilized to compare the available ICS testbeds.

ICPS Datasets. Mitchell and Chen [22] survey 28 papers that propose IDS for CPS based on the detection technique and audit material. 24 out of 28 papers utilize datasets while 22 of them do not share them. 6 papers use simulated datasets rather than operational ones. The authors also define physical process monitoring is one of the key aspects of intrusion detection. Khraisat et al. [194] review the IDS datasets. The authors mention that the utilization of older datasets accepted as benchmarks results in inaccurate claims due to their lack of current sophisticated malware. Thus, there is a need for an up-to-date publicly available dataset. Ahmed et al. [195] also propose such a survey. The authors claim that the real reason behind the lack of publicly available datasets is privacy-related issues. They also find the usage of older datasets problematic. They emphasize the importance of dual optimization to achieve simpler datasets. Zolanvari et al. [196] study the place of ML techniques in IIoT. The authors emphasize that the anomalies correspond to around 1% of the total data in real-life cases, hence causing the generation of imbalanced datasets. However, training ML models via imbalanced datasets cause generation of inaccurate security mechanisms and the techniques (e.g., oversampling, undersampling) used to overcome this issue have their drawbacks.

The utilization of ML techniques to detect anomalies in industrial systems is favored by academia. However, there are still many challenges to be addressed including operating in resource-constrained environments, and dealing with anomalies resulted from non-adversary events. The increase in the number of testbeds (e.g, physical, simulation, HIL, emulation and virtualisation) is another positive development, however the access to cyber-physical testbeds that provide the most realistic results is questionable as more research is done via simulation only testbeds. The older datasets that are accepted as benchmarks are still widely used even though they do not present the current cybersecurity environment. Privacy is the main concern behind the lack of up-to-date public datasets. Besides, evaluating works that do not release the utilized dataset is more challenging.

5 LESSONS LEARNED

Dissimilar to IT security, industrial security is still in early development and gradually adapting to scientific research. Integration of IT systems and the rapid development of technologies based on ubiquitous computing (e.g., IIoT, IWSN) that increases the overall efficiency, heterogeneity, and interconnectivity of industrial systems makes the currently available security measures inadequate. We make the following observations based on our review: (i) the relationship between emerging new industrial technologies requires clarification, (ii) industrial cybersecurity policy based solutions lack common evaluation framework, (iii) non-adaptive cybersecurity solutions lose validity over time, (iv) security policies and redundant solutions are overlooked, (v) inefficient realistic testbed and up-to-date dataset utilization. We now examine these in detail.

Confusion over lack of classification. New terms emerge from new technologies. To prevent confusion and overlapping, we need to clarify the relationship of such terms (e.g., ICS, IIoT, IWSN, WSN, SCADA, DCS, and IWoT) with the other complementary industrial disciplines. We only have defined the ICS, IIoT, and IWSN other than ICPS because we find relevant studies in the literature. However, we have not provided a clear distinction as it requires further study. The classification framework that explicitly states the relationship of terms that are used to define systems located in industrial environments will prevent the diversion of complementary future industrial research.

Industrial cybersecurity policy-based solutions lack common evaluation ground and framework. While the top industrial cybersecurity vulnerabilities occur due to weak boundary protection, they are followed by security policy-based weaknesses (e.g., least functionality, identification and authentication, physical access control, authenticator management, least privilege) that can be evaluated under the access control policies. Implementing such a policy on a real ICPS environment while simulating attacks and observing for a certain period may be the most realistic way to evaluate, however, disrupting an ICPS is not acceptable due to supervision of critical tasks. Several proposed solutions apply hardware extensions to enforce these policy-based models but the efficiency of these methods is questionable due to the lack of an evaluation framework.

Non-adaptive cybersecurity solutions/taxonomies lose validity. Legacy air-gapped ICPS had a static structure that was built from components expected to work at least 15 years without any significant changes. However, current ICPS are dynamic due to constantly adopting new components/technologies. Besides, suitable components (e.g., PLC, HMI) are updated when a vulnerability is discovered to prevent further abuse. Our real-life incident evaluation has shown that outdated security mechanisms are the main reason for the data breach. However, redeploying is not feasible as they are obliged to non-stop monitor critical tasks. Thus, we need flexible, adaptive solutions that can continue to operate with minimum human intervention. Such solutions can only be produced via utilizing testbed, dataset, and machine learning algorithms.

Inefficient realistic testbed and up-to-date dataset utilization. Even though there are many realistic testbeds available, the evaluation that shows how close they mimic their real-life counterparts is hard to find. Besides, the vast majority of research that focus on ICPS, and CPS anomaly detection prefer simulation only testbeds and the evaluation phase mostly contain only one type of testbed rather than combining several ones. Hence, we can question the accessibility of these realistic testbeds. The issue regarding datasets is the lack of publicly available ones that include network traffic containing latest malware. Also, many research do not release the dataset they utilize, hence, making it hard to compare with similar works.

A lack of security policy studies and redundant solutions. Humans are the weakest link in the information security chain. Enforcing security policies is the most feasible solution to prevent human-centric errors/misuses. However, our study has shown while academia heavily favors developing intrusion detection systems (post-attack), it lacks in terms of security policy based studies (pre-attack). On the other hand, redundant systems are also overlooked. We have realized while most papers focus on resilience and robustness while slightly mentioning redundancy.

6 Research Challenges and Directions

In this section, we identify the research challenges derived from the evaluation of this survey. Our findings show that there are challenges in the field of ICPS cybersecurity that are based on the lack of adequate evaluation/test environments that utilize up-to-date datasets, variety of testbeds while adapting unified evaluation methods. Thus, novel techniques should be employed to provide adequate solutions for these unique challenges where the "uniqueness" comes from being in an "industrial" environment adopting recent ubiquitous computing and communication technologies. We illustrate an ideal ICPS evaluation environment as a solution to these challenges that are based on the future directions derived from our survey in Figure 10.

6.1 Adaptability and Context Awareness

Cybersecurity is now one of the most dynamic disciplines due to the high interest of large entities (i.e., states/nations) in cybercrime. The vulnerability assessments reports we analyzed have shown that ICPS cyber incidents (as similar in [149]) occur due to the utilization of out of date security mechanisms. These non-adaptive cybersecurity mechanisms are prone to fail before attacks utilizing the newest methods (e.g., zero-day attacks, APTs). ICPSs that consist of continuous processes require real-time supervision (by sensors) without human intervention. Hence, the deployed cybersecurity mechanisms should provide adaptive, autonomous, and non-stop protection. These challenges are also valid for cyberattack taxonomies. Hence, we have proposed an adaptive ICPS attack taxonomy. However, the validity of our taxonomy depends on CAPEC [118] and it may not reflect all characteristics of specific industrial applications.

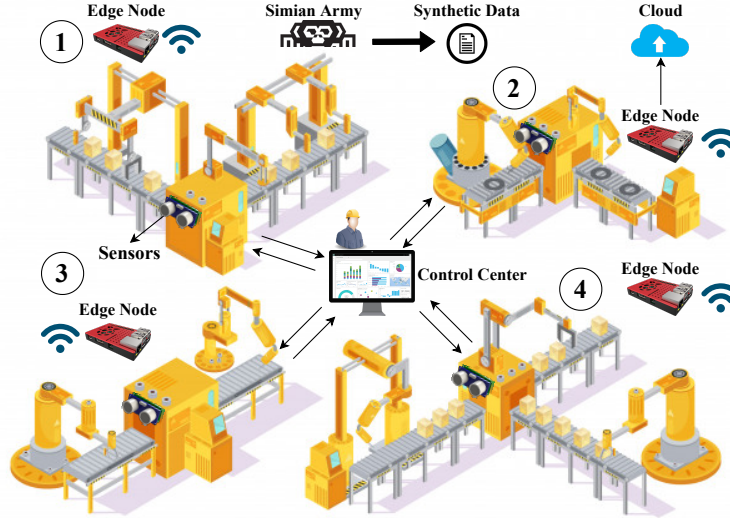


Figure 10: Example of an ideal ICPS evaluation environment. Four testbeds with different contexts are present. Each testbed is supervised by context-aware sensors connected to the main network and edge nodes deployed on an isolated network connected to the cloud. The control center monitors and manages each testbed. Simian Army [185] approach is applied to conduct attacks so we can generate a robust synthetic dataset that contains mixed network traffic. The adaptability is present thanks to context-aware sensors/edge nodes while edge nodes also provide redundancy.

Context-awareness [197] is a promising feature that we expect to see in further adaptive ICPS edge security related studies. The AI/ML algorithms are utilized to develop ML models that consist several steps including data gathering, parsing, and training. Current ML models/workflows are automated via machine learning pipelines based on open-source frameworks or cloud ML services to simulate interconnected environment and achieve realistic results. Due to carrying out these processes in an accessible cyber environment, these models are prone to adversarial machine learning techniques [198] (e.g., model exploratory, data poisoning attacks) that aim to sabotage training process. Thus, the required precautions should be taken during the ML process to prevent such attacks. We also believe adversarial machine learning can be adapted to Simian Army [185] approach in the context of attack generation.

6.2 Redundancy and Resilience

Among the characteristics that determine the overall security of an ICPS, the most overlooked one is a redundancy (see §4.5) that also directly contributes to the resilience of the system. The German Steel Mill incident [145] is such an example of a lack of redundancy where the incident could have been prevented if there was an additional system to shut down the furnace. Regarding resilience, imagine the rotating speed of the fan is altered by an adversary to cause a fire in the manufacturing line. If the fan can go back to a normal state without causing fire we can define that system as resilient. In industrial environments, only the most significant elements (i.e., electricity) are considered from these perspectives where cyber-physical edge security mechanisms subject to replacement when they fail which makes the ICPS vulnerable during the replacement process. Deploying an alternative system for each process is not a feasible option (in most situations, the cost will be too high) due to the heterogeneity of an industrial environment. The same is also applied to industrial networks. As we mentioned in §2, ICPSs may benefit from a highly interconnected network that also increases the attack surface (see [151] for real-life incident example). This case becomes more significant when there is inadequate boundary protection (see §4.4) as we have also seen from the vulnerability assessment reports [47, 45, 46]. Thus, two main challenges arise: (i) how can we determine the industrial assets that require back-up systems, (ii) how should we implement them. The risk assessment has to be done to analyze available options. Regarding ICPS edge resources, we may question the abandonment of air-gapping policy in ICPSs. Deploying supervision/security mechanisms to the same network allows the adversary to bypass them by manipulating their outputs forwarded to the control center [152]. Thus, deploying edge security mechanisms on an air-gapped secondary network seems like a promising further research topic.

6.3 Testbeds and Synthetic Datasets

The survey revealed that most of the proposals targeting the top ten identified industrial weaknesses [47] utilize benchmarking tests, simulations, or proof of concepts to evaluate their proposals. To achieve the most realistic results, real-life datasets and testbeds are required. This is a well-known challenge for industrial studies that exist from the beginning. Experimenting on real and active ICPS is out of the question due to the chance of possible disruption in CIs. Hence, aiming for the utilization of the most realistic testbeds and synthetic datasets [199, 200] that benefit from being privacy-free (the reason behind the lack of efficient publicly available datasets) and safe to gather is the most feasible option. We believe the development of advanced industrial simulation environments [201] that can generate robust synthetic datasets to be utilized with machine learning models is one of the significant future directions to be considered. To generate such a dataset where the privacy of the data is out of concern that contains both malicious and normal traffic, either we can conduct attacks (a similar approach to the Simian Army [185] may be applied) or deploy honeypot to the ICPS testbed network. However, achieving big data is still a challenge with in terms of generating synthetic datasets. On the other hand, realistic evaluation becomes more challenging if we consider the studies regarding industrial security policies where the efficiency of the policy is mostly determined by the aftermath of the real attacks. Possible directions include simulating real-life incidents based on the choices of developed policies and the development of an evaluation framework that differs according to industrial environments.

7 Conclusions

The industrial cyber-physical systems (ICPS) are adopting new communication, computation based technologies, and becoming more interconnected, heterogeneous, and dynamic. Even though ICPS benefits from this rapid integration, providing cybersecurity is becoming a primary concern due to increased attack surface. In this paper, we reviewed the overall ICPS cybersecurity to understand what the current challenges are and how they are treated by the academia. We analyzed the ICPS architecture by defining its components and emphasizing the unique characteristic of OT systems. We provided an analysis of ICPS communication protocols. We proposed an adaptive attack taxonomy then evaluated real-life ICPS cyber incidents. We analyzed the latest trends on ICPS edge security. Then, we surveyed the growing ICPS cybersecurity literature to determine how academia approaches against ICPS vulnerabilities. We evaluated studies that propose ICPS security mechanisms based on the evaluation metrics that aim for continuity. We argued about the datasets, testbeds, machine learning techniques, security policies that will shape the future of ICPS security. In all papers we surveyed, no paper proposes a framework that explains the relationship with complementary industrial systems. The less utilization of realistic testbeds, lack of up-to-date datasets, and evaluation framework to compare AI/ML techniques are also among major challenges. Besides, the most common vulnerabilities are either due to weak boundary protection or lack of enforcement of well-designed security policy. We hope that our review and suggestions will motivate further research while closing the gap between academia and industry in this field and lead unified studies that focus on adaptive security mechanisms based on strong policies.

References

- [1] Heiner Lasi, Peter Fettke, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. Industry 4.0. *Bus. Inf. Syst. Eng.*, 6(4):239–242, August 2014.
- [2] ge.com. Everything you need to know about the industrial internet of things, May 2020. URL <https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-internet-things>.
- [3] Ragunathan (Raj) Rajkumar, Insup Lee, Lui Sha, and John Stankovic. Cyber-physical systems: The next computing revolution. In *Design Automation Conference*, pages 731–736, Anaheim, California, 2010. IEEE.
- [4] Jay Lee, Behrad Bagheri, and Hung-An Kao. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manuf. Lett.*, 3:18–23, January 2015.
- [5] Luca Parolini, Niraj Tolia, Bruno Sinopoli, and Bruce H. Krogh. A cyber-physical systems approach to energy management in data centers. In *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems - ICCPS '10*, pages 168–177, Stockholm, Sweden, 2010. ACM Press.
- [6] Zhaohui Wang, Houbing Song, David W. Watkins, Keat Ghee Ong, Pengfei Xue, Qing Yang, and Xianming Shi. Cyber-physical systems for water sustainability: Challenges and opportunities. *IEEE Commun. Mag.*, 53(5): 216–222, May 2015.
- [7] Xinghuo Yu and Yusheng Xue. Smart Grids: A Cyber-Physical Systems Perspective. *Proc. IEEE*, 104(5): 1058–1070, May 2016.

- [8] Rui-Yang Chen. An intelligent value stream-based approach to collaboration of food traceability cyber physical system by fog computing. *Food Control*, 71:124–136, January 2017.
- [9] Krishna Sampigethaya and Radha Poovendran. Aviation Cyber-Physical Systems: Foundations for Future Aircraft and Air Transport. *Proc. IEEE*, 101(8):1834–1855, August 2013.
- [10] gov.uk. Public summary of sector security and resilience plans, February 2019. URL https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf.
- [11] Jerker Delsing, Fredrik Rosenqvist, Oscar Carlsson, Armando W. Colombo, and Thomas Bangemann. Migration of industrial process control systems into service oriented architecture. In *IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society*, pages 5786–5792, Montreal, QC, Canada, October 2012. IEEE.
- [12] Dazhong Wu, Matthew John Greer, David W. Rosen, and Dirk Schaefer. Cloud manufacturing: Strategic vision and state-of-the-art. *J. Manuf. Syst.*, 32(4):564–579, October 2013.
- [13] Xuejun Yue, Hu Cai, Hehua Yan, Caifeng Zou, and Keliang Zhou. Cloud-assisted industrial cyber-physical systems: an insight. *Microprocessors Microsystems*, 39(8):1262–1270, November 2015.
- [14] Michael Roza, William Ho, Sabri Khemissa, and Darnell Washington. Cloud industrial internet of things (iiot) - industrial control systems security glossary. Technical report, Cloud Security Alliance, may 2020.
- [15] Peter Schneider and Konstantin Böttinger. High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy - CPS-SPC '18*, pages 1–12, Toronto, Canada, 2018. ACM Press.
- [16] Yuxin Liu, Xiao Liu, Anfeng Liu, Neal N. Xiong, and Fang Liu. A Trust Computing-based Security Routing Scheme for Cyber Physical Systems. *ACM Trans. Intell. Syst. Tech.*, 10(6):1–27, December 2019.
- [17] Craig Bakker, Arnab Bhattacharya, Samrat Chatterjee, and Draguna L. Vrabie. Hypergames and Cyber-Physical Security for Control Systems. *ACM Trans. Cyber-Physical Syst.*, 4(4):1–41, August 2020.
- [18] Kun Wang, Miao Du, Dejun Yang, Chunsheng Zhu, Jian Shen, and Yan Zhang. Game-Theory-Based Active Defense for Intrusion Detection in Cyber-Physical Embedded Systems. *ACM Trans. Embedded Comput. Syst.*, 16(1):1–21, November 2016.
- [19] Bharadwaj Satchidanandan and Panganamala R Kumar. Dynamic Watermarking: Active Defense of Networked Cyber-Physical Systems. *Proc. IEEE*, 105(2):219–240, February 2017.
- [20] Manuel Cheminod, Luca Durante, and Adriano Valenzano. Review of Security Issues in Industrial Networks. *IEEE Trans. Ind. Inform.*, 9(1):277–293, February 2013.
- [21] William Knowles, Daniel Prince, David Hutchison, Jules Ferdinand Pagna Disso, and Kevin Jones. A survey of cyber security management in industrial control systems. *Int. J. Crit. Infrastructure Protection*, 9:52–80, June 2015.
- [22] Robert Mitchell and Ing-Ray Chen. A survey of intrusion detection techniques for cyber-physical systems. *ACM Comput. Surv.*, 46(4):1–29, April 2014.
- [23] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. Cyber-Physical Systems Security—A Survey. *IEEE Internet Things J.*, 4(6):1802–1831, December 2017.
- [24] Jairo Giraldo, Esha Sarkar, Alvaro A. Cardenas, Michail Maniatakos, and Murat Kantarcioglu. Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE Des. Test*, 34(4):7–17, August 2017.
- [25] Wenjin Yu, Tharam Dillon, Fahed Mostafa, Wenny Rahayu, and Yuehua Liu. Implementation of Industrial Cyber Physical System: Challenges and Solutions. In *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, pages 173–178, Taipei, Taiwan, May 2019. IEEE.
- [26] Paulo Leitao, Stamatis Karnouskos, Luis Ribeiro, Jay Lee, Thomas Strasser, and Armando W. Colombo. Smart Agents in Industrial Cyber-Physical Systems. *Proc. IEEE*, 104(5):1086–1101, May 2016.
- [27] Yunbo Wang, Mehmet C. Vuran, and Steve Goddard. Cyber-physical systems in industrial process control. *ACM SIGBED Rev.*, 5(1):1–2, January 2008.
- [28] Mohammad Jbair, Bilal Ahmad, Mus’ab H. Ahmad, and Robert Harrison. Industrial cyber physical systems: a survey for control-engineering tools. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pages 270–276, St. Petersburg, May 2018. IEEE, IEEE.
- [29] Yang Lu. Cyber Physical System (CPS)-Based Industry 4.0: A Survey. *J. Ind. Integration Manage.*, 02(03):1750014, September 2017.

- [30] Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, and Xian-Ming Zhang. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275:1674–1683, January 2018.
- [31] Kaixing Huang, Chunjie Zhou, Yu-Chu Tian, Shuanghua Yang, and Yuanqing Qin. Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Electronics*, 65(10):8153–8162, October 2018.
- [32] Jairo Giraldo, David Urbina, Alvaro Cardenas, Junia Valente, Mustafa Faisal, Justin Ruths, Nils Ole Tippenhauer, Henrik Sandberg, and Richard Candell. A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. *ACM Comput. Surv.*, 51(4):1–36, September 2018.
- [33] Derui Ding, Qing-Long Han, Zidong Wang, and Xiaohua Ge. A Survey on Model-Based Distributed Control and Filtering for Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Inform.*, 15:2483–2499, May 2019.
- [34] Daniel Ramotsoela, Adnan Abu-Mahfouz, and Gerhard Hancke. A Survey of Anomaly Detection in Industrial Wireless Sensor Networks with Critical Water System Infrastructure as a Case Study. *Sensors*, 18(8):2491, August 2018.
- [35] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. Security and privacy challenges in industrial internet of things. In *Proceedings of the 52nd Annual Design Automation Conference on - DAC '15*, pages 1–6, San Francisco, California, 2015. IEEE, ACM Press.
- [36] Hansong Xu, Wei Yu, David Griffith, and Nada Golmie. A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. *IEEE Access*, 6:78238–78259, 2018.
- [37] Yongxin Liao, Eduardo de Freitas Rocha Loures, and Fernando Deschamps. Industrial Internet of Things: A Systematic Literature Review and Insights. *IEEE Internet Things J.*, 5(6):4515–4525, December 2018.
- [38] Mina Younan, Essam H. Houssein, Mohamed Elhoseny, and Abdelmgeid A. Ali. Challenges and recommended technologies for the industrial internet of things: a comprehensive review. *Meas.*, 151:107198, February 2020.
- [39] M. Gidlund, G. P. Hancke, M. H. Eldefrawy, and J. Akerberg. Guest Editorial: Security, Privacy, and Trust for Industrial Internet of Things. *IEEE Trans. Ind. Inform.*, 16(1):625–628, January 2020.
- [40] Li Da Xu, Wu He, and Shancang Li. Internet of Things in Industries: A Survey. *IEEE Trans. Ind. Inform.*, 10(4):2233–2243, November 2014.
- [41] Vehbi C Gungor and Gerhard P Hancke. Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches. *IEEE Trans. Ind. Electronics*, 56(10):4258–4265, October 2009.
- [42] Chenyang Lu, Abusayeed Saifullah, Bo Li, Mo Sha, Humberto Gonzalez, Dolvara Gunatilaka, Chengjie Wu, Lanshun Nie, and Yixin Chen. Real-Time Wireless Sensor-Actuator Networks for Industrial Cyber-Physical Systems. *Proc. IEEE*, 104(5):1013–1024, May 2016.
- [43] Diego V. Queiroz, Marcelo S. Alencar, Ruan D. Gomes, Iguatemi E. Fonseca, and Cesar Benavente-Peces. Survey and systematic mapping of industrial Wireless Sensor Networks. *J. Netw. Comput. Appl.*, 97:96–125, November 2017.
- [44] Edward R Griffor, Chris Greer, David A Wollman, and Martin J Burns. Framework for cyber-physical systems: volume 1, overview. Technical report, National Institute of Standards and Technology, June 2017.
- [45] verizon.com. 2020 Data Breach Investigations Report, 2020. URL <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>.
- [46] us cert.cisa.gov. NCCIC/ICS-CERT Industrial Control Systems Assessment Summary Report, 2015. URL https://us-cert.cisa.gov/sites/default/files/Annual_Reports/FY2015_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf.
- [47] us cert.cisa.gov. ICS-CERT Annual Assessment Report FY2016, 2016. URL https://us-cert.cisa.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf.
- [48] Gregory J Pottie and William J Kaiser. Wireless integrated network sensors. *Commun. ACM*, 43(5):51–58, May 2000.
- [49] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. Wireless sensor networks: A survey. *Comput. Netw.*, 38(4):393–422, 2002.
- [50] Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. *Commun. ACM*, 47(6):53–57, June 2004.

- [51] Nacer Khalil, Mohamed Riduan Abid, Driss Benhaddou, and Michael Gerndt. Wireless sensors networks for Internet of Things. In *2014 IEEE Ninth Int. Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, pages 1–6, Singapore, April 2014. IEEE, IEEE.
- [52] Jonathan W. Hui and David E. Culler. IP is dead, long live IP for wireless sensor networks. In *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems - SenSys '08*, pages 15–28, Raleigh, NC, USA, 2008. ACM Press.
- [53] Sohail Jabbar, Murad Khan, Bhagya Nathali Silva, and Kijun Han. A Rest-based industrial web of things' framework for smart warehousing. *J. Supercomputing*, 74(9):4419–4433, September 2018.
- [54] Keith Kirkpatrick. Protecting industrial control systems. *Commun. ACM*, 62(10):14–16, October 2019.
- [55] Keith Stouffer, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams, and Adam Hahn. Guide to industrial control systems (ics) security supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc). Technical report, National Institute of Standards and Technology, May 2014.
- [56] Edward A. Lee. Cyber Physical Systems: Design Challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pages 363–369, Orlando, FL, USA, May 2008. IEEE.
- [57] Karsten Schweichhart. Reference Architectural Model Industrie 4.0 (RAMI 4.0), April 2016. URL <https://www.wapz.net/down/remi-4/f4f.pdf>.
- [58] Garrison Greenwood, John Gallagher, and Eric Matson. Cyber-Physical Systems: The Next Generation of Evolvable Hardware Research and Applications. In Hisashi Handa, Hisao Ishibuchi, Yew-Soon Ong, and Kay Chen Tan, editors, *Proceedings of the 18th Asia Pacific Symposium on Intelligent and Evolutionary Systems, Volume 1*, volume 1, pages 285–296. Springer Int. Publishing, Cham, 2015. Series Title: Proceedings in Adaptation, Learning and Optimization.
- [59] Naoufel Boulila. Cyber-Physical Systems and Industry 4.0: Properties, Structure, Communication, and Behavior. Technical report, Siemens Corporate Technology, apr 2019.
- [60] Behrad Bagheri, Shanhu Yang, Hung-An Kao, and Jay Lee. Cyber-physical Systems Architecture for Self-Aware Machines in Industry 4.0 Environment. *IFAC-PapersOnLine*, 48(3):1622–1627, 2015.
- [61] Jehn-Ruey Jiang. An improved cyber-physical systems architecture for Industry 4.0 smart factories. *Advances Mech. Eng.*, 10(6):1–15, June 2018.
- [62] mh monitoringcontrol.com. Edge Computing in Industrial Automation, April 2018. URL https://mh-monitoringcontrol.com/sites/default/files/downloads/mh_edge_computing_in_industrial_automation.pdf.
- [63] Kai Lin, Wenjian Wang, Yuanguo Bi, Meikang Qiu, and Mohammad Mehedi Hassan. Human localization based on inertial sensors and fingerprints in the Industrial Internet of Things. *Comput. Netw.*, 101:113–126, June 2016.
- [64] Alina Roitberg, Nikhil Somani, Alexander Perzylo, Markus Rickert, and Alois Knoll. Multimodal human activity recognition for industrial manufacturing processes in robotic workcells. In *Proceedings of the 2015 ACM on International Conference on Multimodal Interaction, ICMI '15*, page 259–266, New York, NY, USA, 2015. Assoc. Comput. Machinery.
- [65] Radislav A. Potyrailo. Multivariable Sensors for Ubiquitous Monitoring of Gases in the Era of Internet of Things and Industrial Internet. *Chem. Rev.*, 116(19):11877–11923, October 2016.
- [66] Shitij Kumar, Celal Savur, and Ferat Sahin. Dynamic Awareness of an Industrial Robotic Arm Using Time-of-Flight Laser-Ranging Sensors. In *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 2850–2857, Miyazaki, Japan, October 2018. IEEE.
- [67] Daniel-Ioan Curiac. Towards wireless sensor, actuator and robot networks: Conceptual framework, challenges and perspectives. *J. Netw. Comput. Appl.*, 63:14–23, March 2016.
- [68] Brendan Galloway and Gerhard P. Hancke. Introduction to Industrial Control Networks. *IEEE Commun. Surveys Tut.*, 15(2):860–880, 2012.
- [69] Thiago Alves and Thomas Morris. OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research. *Comput. Secur.*, 78:364–379, September 2018.
- [70] Waqas Ahmed Siddique, Muhammad Farhan Siddiqui, and Awais Khan. Controlling and Monitoring of Industrial Parameters Through Cloud Computing and HMI Using OPC Data Hub Software. *Indian J. Sci. Tech.*, 13(2): 114–126, March 2020.

- [71] Armando W Colombo, Stamatis Karnouskos, Okayay Kaynak, Yang Shi, and Shen Yin. Industrial cyberphysical systems: A backbone of the fourth industrial revolution. *IEEE Industrial Electronics Magazine*, 11(1):6–16, 2017.
- [72] Stamatis Karnouskos. Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society*, pages 4490–4494. IEEE, 2011.
- [73] Adam Hahn. Operational Technology and Information Technology in Industrial Control Systems. In Edward J. M. Colbert and Alexander Kott, editors, *Cyber-Security of SCADA and Other Industrial Control Systems*, volume 66, pages 51–68. Springer Int. Publishing, Cham, 2016. Series Title: Advances in Information Security.
- [74] A Dean Papadopoulos, Newton Center, and West Newbury. System for remotely accessing an industrial control system over a commercial communications network, may 2000. URL <https://patents.google.com/patent/US6061603A/en>. US Patent 6,061,603.
- [75] Robert J. Kretschmann. Mobile human/machine interface for use with industrial control systems for controlling the operation of process executed on spatially separate machines, December 26 2000. URL <https://patents.google.com/patent/US6167464A/en>. US Patent 6,167,464.
- [76] A Chemudupati, S Kaulen, M Mertens, and S Zimmermann. The convergence of it and operational technology, nov 2012. URL <https://fieldcommgroup.org/services/product-testing-registration>.
- [77] CISCO. IT/OT Convergence: Moving Digital Manufacturing Forward. Technical report, CISCO, 2018.
- [78] Jai Agaram, John Andary, Douglas Effenberger, Kent Peterson, Steven Strauss, and Steve Taylor. Building Automation System Procurement Guide, July 2018. URL <https://www2.calstate.edu/csu-system/doing-business-with-the-csu/capital-planning-design-construction/operations-center/Documents/guidelines/Controls-Procurement-Guide-12-Dec-2018%20.pdf>.
- [79] se.com. Guide to Open Protocols in Building Automation, November 2015. URL https://blog.se.com/wp-content/uploads/2015/11/SE-Protocols-Guide_A4_v21.pdf.
- [80] Angelia Nedić, Alex Olshevsky, and Michael G Rabbat. Network Topology and Communication-Computation Tradeoffs in Decentralized Optimization. *Proc. IEEE*, 106(5):953–976, May 2018.
- [81] J.-P. Thomesse. Fieldbus Technology in Industrial Automation. *Proc. IEEE*, 93(6):1073–1101, June 2005.
- [82] Juergen Jasperneite, Markus Schumacher, and Karl Weber. Limits of increasing the performance of Industrial Ethernet protocols. In *2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007)*, pages 17–24, Patras, Greece, September 2007. IEEE.
- [83] Xiaomin Li, Di Li, Jiafu Wan, Athanasios V. Vasilakos, Chin-Feng Lai, and Shiyong Wang. A review of industrial wireless networks in the context of Industry 4.0. *Wireless Netw.*, 23(1):23–41, January 2017.
- [84] hms networks.com. Industrial network market shares 2019 according to HMS, May 2019. URL <https://www.hms-networks.com/news-and-insights/news-from-hms/2019/05/07/industrial-network-market-shares-2019-according-to-hms>.
- [85] hms networks.com. Industrial network market shares 2020 according to HMS Networks, May 2020. URL <https://www.hms-networks.com/news-and-insights/news-from-hms/2020/05/29/industrial-network-market-shares-2020-according-to-hms-networks>.
- [86] modbus.org. About Modbus Organization, oct 2005. URL https://www.modbus.org/about_us.php.
- [87] dnp.org. Dnp users group, 2004. URL <https://www.dnp.org/About/DNP-Users-Group>.
- [88] IEEE Standards Association et al. Ieee standard for electric power systems communications-distributed network protocol(dnp3), 2014. URL <https://standards.ieee.org/standard/1815-2012.html>.
- [89] Steven T. Bushby and H. Michael Newman. Bacnet today. *ASHRAE Journal*, 10:10–18, 2002.
- [90] bacnet.org. Bacnet, August 2020. URL <http://www.bacnet.org/>.
- [91] David Fisher, Bernhard Isler, and Michael Osborne. Bacnet secure connect: A secure infrastructure for building automation, 22 2019. URL http://www.bacnet.org/Bibliography/B-SC-Whitepaper-v15_Final_20190521.pdf.
- [92] rockwellautomation.com. Devicenet network, August 2020. URL <https://www.rockwellautomation.com/en-us/products/hardware/allen-bradley/networks-and-communications/devicenet-networks.html>.
- [93] odva.org. Devicenet, 2020. URL <https://www.odva.org/technology-standards/key-technologies/devicenet/>.

- [94] Abraham Serhane, Mohammad Shraif, Hassan Chehadi, Adnan Harb, and Ali Mohsen. Optimizing solar systems using DeviceNET. In *2017 29th International Conference on Microelectronics (ICM)*, pages 1–4, Beirut, Lebanon, December 2017. IEEE.
- [95] Smak Azad and K. Srinivasan. Delay Analysis of ControlNet and DeviceNet in Distributed Control System. In P. Deiva Sundari, Subhransu Sekhar Dash, Swagatam Das, and Bijaya Ketan Panigrahi, editors, *Proceedings of 2nd Int. Conference on Intelligent Computing and Applications*, volume 467, pages 617–626. Springer Singapore, Singapore, 2017. Series Title: Advances in Intelligent Systems and Computing.
- [96] profibus.com. Profinet - the leading industrial ethernet standard, September 2009. URL <https://www.profibus.com/technology/profinet/>.
- [97] Paolo Bellagente, Paolo Ferrari, Alessandra Flammini, Stefano Rinaldi, and Emiliano Sisinni. Enabling PROFINET devices to work in IoT: Characterization and requirements. In *IEEE International Instrumentation and Measurement Technology Conference Proceedings*, pages 1–6, Taipei, Taiwan, May 2016. IEEE.
- [98] ethercat.org. Ethercat technology group, September 2020. URL https://www.ethercat.org/en/tech_group.html.
- [99] Kevin Langlois, Tom van der Hoeven, David Rodriguez Cianca, Tom Verstraten, Tomislav Bacek, Bryan Convens, Carlos Rodriguez-Guerrero, Victor Grosu, Dirk Lefebber, and Bram Vanderborght. EtherCAT Tutorial: An Introduction for Real-Time Hardware Communication on Windows [Tutorial]. *IEEE Robot. Automat. Mag.*, 25(1):22–122, March 2018.
- [100] Vinh Quang Nguyen and Jae Wook Jeon. Ethercat network latency analysis. In *2016 International Conference on Computing, Communication and Automation (ICCCA)*, pages 432–436, Noida, India, 2016. IEEE.
- [101] Felix Sygulla, Robert Wittmann, Philipp Seiwald, Tobias Berninger, Arne-Christoph Hildebrandt, Daniel Wahrmann, and Daniel Rixen. An EtherCAT-Based Real-Time Control System Architecture for Humanoid Robots. In *2018 IEEE 14th International Conference on Automation Science and Engineering (CASE)*, pages 483–490, Munich, August 2018. IEEE.
- [102] Raimarius Delgado, Shin-Young Kim, Bum-Jae You, and Byoung-Wook Choi. An EtherCAT-based real-time motion control system in mobile robot application. In *2016 13th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*, pages 710–715, Xian, China, August 2016. IEEE.
- [103] odva.org. Ethernet/ip, 2020. URL <https://www.odva.org/technology-standards/key-technologies/ethernet-ip/>.
- [104] Zhihong Lin and Stephanie Pearson. An inside look at industrial ethernet communication protocols. Technical report, Texas Instruments, 2013.
- [105] zigbeealliance.org. Zigbee alliance, 2010. URL <https://zigbeealliance.org/solution/zigbee/>.
- [106] Abdellah Chehri and Rachid Saadane. Zigbee-based remote environmental monitoring for smart industrial mining. In *Proceedings of the 4th International Conference on Smart City Applications, SCA '19*, New York, NY, USA, 2019. Association for Computing Machinery.
- [107] Junjie Yin, Zheng Yang, Hao Cao, Tongtong Liu, Zimu Zhou, and Chenshu Wu. A survey on bluetooth 5.0 and mesh: New milestones of iot. *ACM Trans. Sensor Netw.*, 15(3):1–29, 2019.
- [108] Seyed Mahdi Darroudi and Carles Gomez. Bluetooth Low Energy Mesh Networks: A Survey. *Sensors*, 17(7):1467, June 2017.
- [109] Seyed Mahdi Darroudi, Raül Caldera-Sánchez, and Carles Gomez. Bluetooth mesh energy consumption: A model. *Sensors*, 19(5):1238, 2019.
- [110] lora alliance.org. Lora alliance, January 2015. URL <https://lora-alliance.org/>.
- [111] Ferran Adelantado, Xavier Vilajosana, Pere Tuset-Peiro, Borja Martinez, Joan Melia-Segui, and Thomas Watteyne. Understanding the limits of lorawan. *IEEE Commun. Mag.*, 55(9):34–40, 2017.
- [112] fieldcommgroup.org. Product Testing & Registration, March 2016. URL <https://fieldcommgroup.org/services/product-testing-registration>.
- [113] Sabo Miya Hassan, Rosdiazli Ibrahim, Kishore Bingi, Tran Duc Chung, and Nordin Saad. Application of wireless technology for control: A wirelesshart perspective. *Procedia Comput. Sci.*, 105(supplement C):240–247, 2017.
- [114] Stig Petersen and Simon Carlsen. Wirelesshart versus isa100. 11a: The format war hits the factory floor. *IEEE Ind. Electronics Mag.*, 5(4):23–34, 2011.

- [115] Geoff Mulligan. The 6LoWPAN architecture. In *Proceedings of the 4th Workshop on Embedded Networked Sensors - EmNets '07*, pages 78–82, Cork, Ireland, 2007. ACM Press.
- [116] ietf.org. Ipv6 over networks of resource-constrained nodes (6lo), December 2019. URL <https://datatracker.ietf.org/wg/6lo/about/>.
- [117] John D Howard and Thomas A Longstaff. A common language for computer security incidents. Technical Report SAND98-8667, 751004, Office of Scientific and Technical Information (OSTI), October 1998.
- [118] capec.mitre.org. CAPEC - CAPEC List Version 3.3, September 2019. URL <http://capec.mitre.org/data/index.html>.
- [119] Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, and Qishi Wu. AVOIDIT: A cyber attack taxonomy. In *9th Annual Symposium on Information Assurance (ASIA'14)*, pages 2–12, Albany, NY, USA, 2014.
- [120] Seungmin Kim, Gyunyoung Heo, Enrico Zio, Jinsoo Shin, and Jae-gu Song. Cyber attack taxonomy for digital environment in nuclear power plants. *Nucl. Eng. Tech.*, 52(5):995–1001, May 2020.
- [121] George Loukas, Diane Gan, and Tuan Vuong. A taxonomy of cyber attack and defence mechanisms for emergency management networks. In *2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pages 534–539, San Diego, CA, March 2013. IEEE.
- [122] Ian M. Chapman, Sylvain P. Leblanc, and Andrew Partington. Taxonomy of cyber attacks and simulation of their effects. In *Proceedings of the 2011 Military Modeling & Simulation Symposium, MMS '11*, page 73–80, San Diego, CA, USA, 2011. Society for Computer Simulation Int.
- [123] Jiankun Hu, Hemanshu R. Pota, and Song Guo. Taxonomy of Attacks for Agent-Based Smart Grids. *IEEE Trans. Parallel Distrib. Syst.*, 25(7):1886–1895, July 2013.
- [124] Mingtao Wu and Young B. Moon. Taxonomy of Cross-Domain Attacks on CyberManufacturing System. *Procedia Comput. Sci.*, 114:367–374, 2017.
- [125] Regner Sabillon, Victor Cavaller, Jeimy Cano, and Jordi Serra-Ruiz. Cybercriminals, cyberattacks and cybercrime. In *2016 IEEE International Conference on Cybercrime and Computer Forensic*, pages 1–9, Vancouver, BC, Canada, June 2016. IEEE.
- [126] Harmandeep Singh Brar and Gulshan Kumar. Cybercrimes: A Proposed Taxonomy and Challenges. *J. Comput. Netw. Commun.*, 2018:1–11, 2018. ISSN 2090-7141, 2090-715X.
- [127] Scott D Applegate and Angelos Stavrou. Towards a cyber conflict taxonomy. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, pages 1–18, Tallinn, Estonia, 2013. IEEE.
- [128] Bhawna Narwal, Amar Kumar Mohapatra, and Kaleem Ahmed Usmani. Towards a taxonomy of cyber threats against target applications. *J. Statist. Manage. Syst.*, 22(2):301–325, February 2019.
- [129] Mark Yampolskiy, Peter Horvath, Xenofon D. Koutsoukos, Yuan Xue, and Janos Sztipanovits. Taxonomy for description of cross-domain attacks on CPS. In *Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems - HiCoNS '13*, page 135, Philadelphia, Pennsylvania, USA, 2013. ACM Press.
- [130] Zakarya Drias, Ahmed Serhrouchni, and Olivier Vogel. Taxonomy of attacks on industrial control protocols. In *2015 International Conference on Protocol Engineering (ICPE) and Int. Conference on New Technologies of Distributed Systems (NTDS)*, pages 1–6, Paris, France, July 2015. IEEE.
- [131] Stephan Berger, Olga Bürger, and Maximilian Röglinger. Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy. *Comput. Secur.*, 93:101790, June 2020.
- [132] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. A Taxonomy of Attacks on the DNP3 Protocol. In Charles Palmer and Sujeet Shenoi, editors, *International Conference on Critical Infrastructure Protection*, volume 311, pages 67–81. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009. Series Title: IFIP Advances in Information and Communication Technology.
- [133] Ahmad E. Elhabashy, Lee J. Wells, Jaime A. Camelio, and William H. Woodall. A cyber-physical attack taxonomy for production systems: A quality control perspective. *J. Intell. Manuf.*, 30(6):2489–2504, August 2019.
- [134] gov.uk. Nature of business: Standard Industrial Classification (SIC) codes, July 2020. URL <http://resources.companieshouse.gov.uk/sic/>.
- [135] ec.europa.eu. Ramon - reference and management of nomenclatures, 2020. URL https://ec.europa.eu/eurostat/ramon/nomenclatures/index.cfm?TargetUrl=LST_CLS_DLD&StrNom=NACE_REV2&StrLanguageCode=EN&StrLayoutCode=HIERARCHIC.

- [136] unstats.un.org. UNSD — ISIC, 2020. URL <https://unstats.un.org/unsd/classifications/Econ/ISIC.cshtml#:~:text=The%20International%20Standard%20Industrial%20Classification,statistics%20according%20to%20such%20activities>.
- [137] Jill Slay and Michael Miller. Lessons Learned from the Maroochy Water Breach. In Eric Goetz and Sujeet Sheno, editors, *Critical Infrastructure Protection*, volume 253, pages 73–82. Springer US, Boston, MA, 2007. Series Title: IFIP Int. Federation for Information Processing.
- [138] Ralph Langner. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Secur. Privacy Mag.*, 9(3):49–51, May 2011.
- [139] Christopher Bronk and Eneken Tikk-Ringas. The Cyber Attack on Saudi Aramco. *Survival*, 55(2):81–96, May 2013.
- [140] Younghwan Kim, Minki Kim, and Wonjoon Kim. Effect of the fukushima nuclear disaster on global public acceptance of nuclear energy. *Energy Policy*, 61:822–828, October 2013.
- [141] info.publicintelligence.net. Situational Information Report Federal Bureau of Investigation. Technical report, FEDERAL BUREAU OF INVESTIGATION, July 2012. URL <https://info.publicintelligence.net/FBI-AntisecICS.pdf>.
- [142] Miloslova Plachkinova and Chris Maurer. Security breach at target. *J. Inf. Syst. Educ.*, 29(1):7, 2019.
- [143] Ted Thornhill. San francisco pranksters hack road sign to warn drivers of godzilla attack, May 2014. URL <https://www.dailymail.co.uk/news/article-2632556/Godzilla-Attack-Turn-Pranksters-hack-San-Francisco-road-sign-warn-drivers-just-movie-makes-monster.html>.
- [144] us cert.cisa.gov. ICS-CERT MONITOR, June 2013. URL https://us-cert.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf.
- [145] Robert M. Lee, Michael J. Assante, and Tim Conway. German steel mill cyber attack. *Ind. Control Syst.*, 30:62, 2014.
- [146] John Leyden. Water treatment plant hacked, chemical mix changed for tap supplies, mar 2016. URL https://www.theregister.com/2016/03/24/water_utility_hacked/.
- [147] Robert M. Lee, Michael J. Assante, and Tim Conway. Analysis of the cyber attack on the ukrainian power grid, mar 2016. URL https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- [148] Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. Triton: The first ics cyber attack on safety instrument systems, 2018. URL <https://i.blackhat.com/us-18/Wed-August-8/us-18-Carcano-TRITON-How-It-Disrupted-Safety-Systems-And-Changed-The-Threat-Landscape-Of-Industrial-ICS.pdf>.
- [149] NJ Mahwah. Radiflow reveals first documented cryptocurrency malware attack on a scada network, February 2020. URL <https://radiflow.com/news/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network/>.
- [150] Bill Briggs. Hackers hit norsk hydro with ransomware. the company responded with transparency, Dec 2019. URL <https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/>.
- [151] Lindsey O’Donnell. Post-Ransomware Attack, Florida City Decides to Pay \$600K, May 2020. URL <https://threatpost.com/ransomware-florida-city-pays-600k-ransom/145869/>.
- [152] Thomas M. Chen. Stuxnet, the real start of cyber warfare? [Editor’s Note]. *IEEE Netw.*, 24(6):2–3, November 2010.
- [153] Lucie Langer, Florian Skopik, Paul Smith, and Markus Kammerstetter. From old to new: Assessing cybersecurity risks for an evolving smart grid. *Comput. Secur.*, 62:165–176, 2016.
- [154] us cert.cisa.gov. Industrial control systems, 2020. URL <https://us-cert.cisa.gov/ics>.
- [155] first.org. Common vulnerability scoring system sig, June 2019. URL <https://www.first.org/cvss/specification-document>.
- [156] David C. Mazur, Rob A. Entzminger, Pete A. Morell, John A. Kay, and Erik Syme. Defining the Industrial Demilitarized Zone and Its Benefits for Mining Applications. *IEEE Trans. Ind. Appl.*, 52(3):2731–2736, May 2016.
- [157] lockheedmartin.com. The cyber kill chain, 2018. URL <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.

- [158] Michael J Assante and Robert M Lee. The industrial control system cyber kill chain, oct 2015. URL https://scadahacker.com/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf.
- [159] Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the Mirai Botnet. In *26th {USENIX} security symposium ({USENIX} Security 17)*, pages 1093–1110, Vancouver, BC, Canada, 2017. USENIX.
- [160] Matus Korman, Margus Välja, Gunnar Björkman, Mathias Ekstedt, Alexandre Vernotte, and Robert Lagerström. Analyzing the Effectiveness of Attack Countermeasures in a SCADA System. In *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids - CPSR-SG'17*, pages 73–78, Pittsburgh, PA, USA, 2017. ACM Press.
- [161] Ning Jiang, Hu Lin, Zhenyu Yin, and Liaomo Zheng. Performance research on industrial demilitarized zone in defense-in-depth architecture. In *2018 IEEE International Conference on Information and Automation (ICIA)*, pages 534–537, Wuyishan, China, August 2018. IEEE.
- [162] Mohammad Hassan, Shamsul Huda, Shaila Sharmeen, Jemal Abawajy, and Giancarlo Fortino. An adaptive trust boundary protection for IIoT networks using deep-learning feature extraction based semi-supervised model. *IEEE Trans. Ind. Inform.*, pages 1–1, 2020.
- [163] Bin Cao, Jianwei Zhao, Yu Gu, Shanshan Fan, and Peng Yang. Security-Aware Industrial Wireless Sensor Network Deployment Optimization. *IEEE Trans. Ind. Inform.*, 16(8):5309–5316, August 2020.
- [164] Sai Ho Ling, Kit Yan Chan, Frank Hung Fat Leung, Frank Jiang, and Hung Nguyen. Quality and robustness improvement for real world industrial systems using a fuzzy particle swarm optimization. *Eng. Appl. Artif. Intell.*, 47:68–80, January 2016.
- [165] Xiong Li, Jianwei Niu, Md Zakirul Alam Bhuiyan, Fan Wu, Marimuthu Karuppiah, and Saru Kumari. A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. *IEEE Trans. Ind. Inform.*, 14(8):3599–3609, August 2017.
- [166] Alireza Esfahani, Georgios Mantas, Rainer Matischek, Firooz B. Saghezchi, Jonathan Rodriguez, Ani Bicaku, Silia Maksuti, Markus G. Tauber, Christoph Schmittner, and Joaquim Bastos. A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment. *IEEE Internet Things J.*, 6(1):288–296, February 2019.
- [167] Ashok Kumar Das, Mohammad Wazid, Neeraj Kumar, Athanasios V. Vasilakos, and Joel J. P. C. Rodrigues. Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment. *IEEE Internet Things J.*, 5(6):4900–4913, December 2018.
- [168] Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. Smart Locks: Lessons for Securing Commodity Internet of Things Devices. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security - ASIA CCS '16*, pages 461–472, Xi'an, China, 2016. ACM Press. ISBN 978-1-4503-4233-9.
- [169] Smita S. Mudholkar, Pradnya M. Shende, and Milind V. Sarode. Biometrics Authentication Technique for Intrusion Detection Systems Using Fingerprint Recognition. *Int. J. Comput. Sci. Eng. Inf. Tech.*, 2(1):57–65, February 2012.
- [170] Kenrick Mock, Bogdan Hoanca, Justin Weaver, and Mikal Milton. Real-time continuous iris recognition for authentication using an eye tracker. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security - CCS '12*, pages 1007–1009, Raleigh, North Carolina, USA, 2012. ACM Press.
- [171] José Carlos Sancho, Andrés Caro, Mar Ávila, and Alberto Bravo. New approach for threat classification and security risk estimations based on security event management. *Future Gener. Comput. Syst.*, 113:488–505, December 2020.
- [172] Hai Tao, Md Zakirul Alam Bhuiyan, Md Arafatur Rahman, Tian Wang, Jie Wu, Sinan Q. Salih, Yafeng Li, and Thayer Hayajneh. TrustData: Trustworthy and Secured Data Collection for Event Detection in Industrial Cyber-Physical System. *IEEE Trans. Ind. Inform.*, 16(5):3311–3321, May 2019.
- [173] Sheng Huang, Yaoliang Chen, Xiaoyan Chen, Kai Liu, Xiaomin Xu, Chen Wang, Kevin Brown, and Inge Halilovic. The next generation operational data historian for IoT based on informix. In *Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data - SIGMOD '14*, pages 169–176, Snowbird, Utah, USA, 2014. ACM Press.

- [174] Sajal Sarkar, Sudip Sarkar, Kajal Sarkar, and Soumalya Ghosh. Cyber security password policy for industrial control networks. In *2015 1st International Conference on Next Generation Computing Technologies (NGCT)*, pages 408–413, Dehradun, India, September 2015. IEEE.
- [175] Alexander Kern and Reiner Anderl. Using RBAC to Enforce the Principle of Least Privilege in Industrial Remote Maintenance Sessions. In *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, pages 107–114, Valencia, October 2018. IEEE.
- [176] Varsha Venugopal, Jim Alves-Foss, and Sandeep Gogineni Ravindrababu. Use of an SDN Switch in Support of NIST ICS Security Recommendations and Least Privilege Networking. In *Proceedings of the Fifth Annual Industrial Control System Security (ICSS) Workshop*, pages 11–20, San Juan PR USA, December 2019. ACM.
- [177] Fabrizio Smeraldi and Pasquale Malacaria. How to spend it: Optimal investment for cyber security. In *Proceedings of the 1st International Workshop on Agents and CyberSecurity - ACySE '14*, pages 1–4, Paris, France, 2014. ACM Press.
- [178] Shaun Wang. Optimal Level and Allocation of Cybersecurity Spending: Model and Formula. *SSRN Electron. J.*, page 12, 2017.
- [179] Bin Srinidhi, Jia Yan, and Giri Kumar Tayi. Allocation of resources to cyber-security: the effect of misalignment of interest between managers and investors. *Decis. Support Syst.*, 75:49–62, July 2015.
- [180] Adriano Valenzano. Industrial cybersecurity: improving security through access control policy models. *IEEE Industrial Electronics Magazine*, 8(2):6–17, 2014.
- [181] Yongjun Ren, Fujian Zhu, Jian Qi, Jin Wang, and Arun Kumar Sangaiah. Identity management and access control based on blockchain under edge computing for the industrial internet of things. *Applied Sciences*, 9(10):2058, 2019.
- [182] Cristina Alcaraz, Rodrigo Roman, Pablo Najera, and Javier Lopez. Security of industrial sensor network-based remote substations in the context of the Internet of Things. *Ad Hoc Netw.*, 11(3):1091–1104, May 2013.
- [183] Sharath Anand and Riya Regi. Remote monitoring of water level in industrial storage tanks using NB-IoT. In *2018 Int. Conf. Commun. Inf. Comput. Technol. (ICCICT)*, pages 1–4, Mumbai, February 2018. IEEE.
- [184] Artemios G. Voyiatzis, Konstantinos Katsigiannis, and Stavros Koubias. A Modbus/TCP Fuzzer for testing internetworked industrial systems. In *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, pages 1–6, Luxembourg, September 2015. IEEE.
- [185] <https://netflixtechblog.com/>. The netflix simian army, Sep 2018. URL <https://netflixtechblog.com/the-netflix-simian-army-16e57fbab116>.
- [186] Radu F. Babiceanu and Remzi Seker. Cyber resilience protection for industrial internet of things: a software-defined networking approach. *Comput. Ind.*, 104:47–58, January 2019. ISSN 01663615.
- [187] Saba Al-Rubaye, Ekhlas Kadhum, Qiang Ni, and Alagan Anpalagan. Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency. *IEEE Internet Things J.*, 6(1):267–277, February 2019.
- [188] Ezgi Karabulut, Necati Aras, and İ Kuban Altinel. Optimal sensor deployment to increase the security of the maximal breach path in border surveillance. *European J. Oper. Res.*, 259(1):19–36, May 2017.
- [189] Gauri Shah and Aashis Tiwari. Anomaly detection in iiot: A case study using machine learning. In *Proceedings of the ACM India Joint International Conference on Data Science and Management of Data*, pages 295–300, 2018.
- [190] Stephen McLaughlin, Charalambos Konstantinou, Xueyang Wang, Lucas Davi, Ahmad-Reza Sadeghi, Michail Maniatakos, and Ramesh Karri. The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5):1039–1057, 2016.
- [191] Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88:101636, 2020.
- [192] Hannes Holm, Martin Karresand, Arne Vidström, and Erik Westring. A survey of industrial control system testbeds. In *Nordic Conference on Secure IT Systems*, pages 11–26. Springer, 2015.
- [193] Christos Siaterlis, Andres Perez Garcia, and Béla Genge. On the use of emulab testbeds for scientifically rigorous experiments. *IEEE Communications Surveys & Tutorials*, 15(2):929–942, 2012.
- [194] Ansam Khraisat, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2(1):20, 2019.
- [195] Mohiuddin Ahmed, Abdun Naser Mahmood, and Jiankun Hu. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60:19–31, 2016.

- [196] Maede Zolanvari, Marcio A Teixeira, and Raj Jain. Effect of imbalanced datasets on security of industrial iot using machine learning. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 112–117. IEEE, 2018.
- [197] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Context Aware Computing for The Internet of Things: A Survey. *IEEE Commun. Surveys Tut.*, 16(1):414–454, 2014.
- [198] Bin Qian, Jie Su, Zhenyu Wen, Devki Nandan Jha, Yin hao Li, Yu Guan, Deepak Puthal, Philip James, Renyu Yang, Albert Y Zomaya, et al. Orchestrating the development lifecycle of machine learning-based iot applications: A taxonomy and survey. *ACM Computing Surveys (CSUR)*, 53(4):1–47, 2020.
- [199] Viacheslav Belenko, Vasiliy Krundyshev, and Maxim Kalinin. Synthetic datasets generation for intrusion detection in vanet. In *Proceedings of the 11th International Conference on Security of Information and Networks*, pages 1–6, 2018.
- [200] Juan Vanerio and Pedro Casas. Ensemble-learning approaches for network security and anomaly detection. In *Proceedings of the Workshop on Big Data Analytics and Machine Learning for Data Communication Networks*, pages 1–6, 2017.
- [201] <https://airbus-cyber-security.com/>. Ot simulation platform, January 2020. URL https://airbus-cyber-security.com/wp-content/uploads/2020/01/Airbus-CyberSecurity_Brochure-OT-Simulation-Platform.pdf.