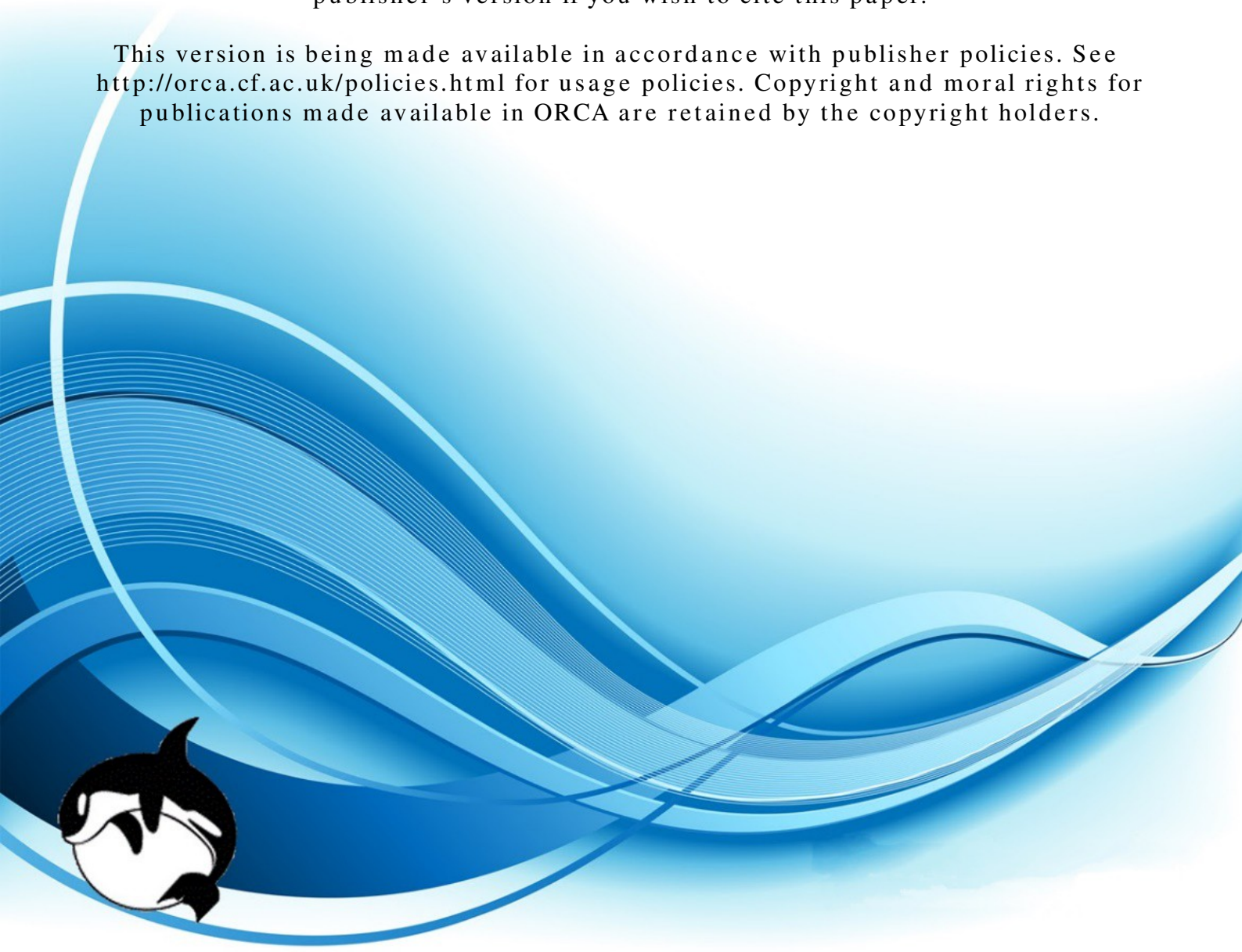


Cybersecurity of Industrial Cyber-Physical Systems: A Review

HAKAN KAYAN, Cardiff University, UK
MATTHEW NUNES, Cardiff University, UK
OMER RANA, Cardiff University, UK
PETE BURNAP, Cardiff University, UK
CHARITH PERERA, Cardiff University, UK

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. Although there are existing surveys in this context, very little is mentioned regarding the outputs of these reports. While these reports show that the most exploited vulnerabilities occur due to weak boundary protection, these vulnerabilities also occur due to limited or ill defined security policies. However, current literature focuses on intrusion detection systems (IDS), network traffic analysis (NTA) methods, or anomaly detection techniques. Hence, finding a solution for the problems mentioned in these reports is relatively hard. We bridge 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. Finally, we identify the general shortcomings and highlight the points that cause a gap in existing literature while defining future research directions.

CCS Concepts: • **Security and privacy → Security requirements**; **Distributed systems security**; Usability in security and privacy.

Additional Key Words and Phrases: Cyber-physical systems, industrial control systems, cybersecurity

ACM Reference Format:
Hakan Kayan, Matthew Nunes, Omer Rana, Pete Burnap, and Charith Perera. 2022. Cybersecurity of Industrial Cyber-Physical Systems: A Review. 1, 1 (February 2022), 35 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Industry 4.0 [94] and Industrial Internet [53] have accelerated integration of industrial cyber-physical systems (ICPSs) [139] with various industries, from manufacturing [96] to energy management [127], water treatment systems [177], and many more [29, 147, 186]. Critical infrastructures (CIs) [57] utilize ICPSs to perform and supervise industrial tasks in harsh industrial environments.

Authors' addresses: Hakan Kayan, Cardiff University, Queens Building, 5 The Parade, Roath, Cardiff, CF24 3AA, UK, kayanh@cardiff.ac.uk; Matthew Nunes, Cardiff University, Queens Building, 5 The Parade, Roath, Cardiff, CF24 3AA, UK, nunesma@cardiff.ac.uk; Omer Rana, Cardiff University, Queens Building, 5 The Parade, Roath, Cardiff, CF24 3AA, UK, RanaOF@cardiff.ac.uk; Pete Burnap, Cardiff University, Queens Building, 5 The Parade, Roath, Cardiff, CF24 3AA, UK, BurnapP@cardiff.ac.uk; Charith Perera, Cardiff University, Queens Building, 5 The Parade, Roath, Cardiff, CF24 3AA, UK, pererac@cardiff.ac.uk.

XXXX-XXXX/2022/2-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Significant research [37, 178, 187] exists on migration of air-gapped legacy ICS to their modern equivalents – often assisted by cloud technologies. These studies are also guided by community research organisations such as the Cloud Security Alliance (CSA) [144] to prevent insecure integration. This leads to several cybersecurity challenges due to: (i) high connectivity, (ii) increased attack surface, and (iii) heterogeneous infrastructure. Any disruption to availability resulting from the compromise of CIs can have a catastrophic impact. Particularly when those CIs support the fundamental needs of society. The survivability of the CIs depends on the security of ICPSs. Protection approaches that focus on CPSs security such as anomaly detection [151], secure routing [107], use of game theory & utility metrics [14], and watermarking [150], 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 and diversity makes it challenging to produce a unifying taxonomy, evaluation metrics, implementation techniques, and test environments.

The ICPS, ICS, Industrial Internet of Things (IIoT), and Industrial Wireless Sensor Networks (IWSN) are not mutually independent disciplines. There is however no unifying framework that explicitly describes the relationships of these different industrial disciplines. Surveys of ICS challenges based on cybersecurity management are presented in [27, 89]. Several surveys [55, 73, 116] classify IDS techniques, review security and privacy issues and describe the need for a security framework. Surveys of the current challenges for various ICPS architectures are covered in [99, 176, 185]. The technical review of control engineering tools is presented in [78] while review of the key enabling technologies and major applications of ICPSs can be found in [112]. ICPSs attack detection techniques are surveyed in [39, 40, 56, 71, 140]. Several proposals [33, 54, 103, 146, 180, 184] introduce IIoT, study state-of-the-art implementation, and give an outlook on possible solutions while mentioning future research directions. Other surveys [60, 111, 138] define principles, review technical challenges, and provide structured overview. We have classified the previous surveys according to their topics in Table 1. Based on this context, the main contributions of our paper are:

- We briefly define ICPSs, IWSN, IIoT, and ICS by identifying their unique environment characteristics and relationships. We identify the key components of an ICPS and describe a modern ICPS architecture (see §2). We analyze the differences between IT and OT and explain why ICPSs security is a unique field that requires particular attention (see §2.3).
- We provide a comprehensive review of industrial protocols and infrastructures (see §3).
- We review existing cyberattack taxonomies from both academia and industry, and provide ours which combines key aspects of these (see §4.1). We present key findings from several industrial reports [168, 169, 173] (see §4.3), and analyze cyber defense approaches that can be implemented to protect against the top ten most common vulnerabilities (see §4.4).
- We define ICPS security characteristics (see §4.5) and (v) review the latest trends on ICPS edge networks (see §4.6). Finally we share lessons learned (see §5), our recommendations (see §6) and (see §7) conclusions.

1.1 Scope of the Survey

The topic of CPS is indeed very popular in academia despite 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 [59]. However, although there are similarities, we believe CPS and ICPS security should be treated as distinct research areas due to attributes (based on the differences between Information Technology (IT) and Operational Technology (OT)) that are unique to industrial environments. This survey focuses on the cybersecurity solutions offered by

Table 1. Chronological Compariso of Previous Surveys

Year	Reference	I	CS	CPS	IoT	WSN	Cybersecurity
2009	Gungor and Hancke [60]	✓				✓	
2013	Cheminod et al. [27]	✓	✓				✓
2014	Da Xu et al. [33]	✓			✓		
	Mitchell and Chen [116]			✓			✓
2015	Lu et al. [111]	✓				✓	
	Sadeghi et al. [146]	✓			✓		✓
	Knowles et al. [89]	✓	✓				✓
2016	Leitao et al. [99]	✓		✓			
2017	Ding et al. [40]	✓		✓			✓
	Lu [112]	✓		✓			
	Queiroz et al. [138]	✓				✓	
	Humayed et al. [73]			✓			✓
	Giraldo et al. [55]			✓			✓
2018	Huang et al. [71]	✓		✓			✓
	Giraldo et al. [56]	✓		✓			✓
	Xu et al. [180]	✓			✓		✓
	Ramotsoela et al. [140]	✓				✓	✓
	Liao et al. [103]	✓			✓		
2019	Ding et al. [39]	✓		✓			✓
	Yu et al. [185]	✓		✓			
	Jbair et al. [78]	✓		✓			
	Younan et al. [184]	✓			✓		✓
2020	Gidlund et al. [54]	✓			✓		✓

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

academia for the most common vulnerabilities reported by three industrial cybersecurity reports [168, 169, 173] to find an answer to the question of what academia is offering against the most common ICPS vulnerabilities. It also analyzes these solutions based on several key features (e.g., used dataset, if machine learning (ML) is applied or not). We evaluate the real-life incidents based on the taxonomy that we developed as we believe that the previously developed taxonomies lack certain elements to examine these attacks. Then, we introduce the communication technologies and protocols. We also analyze the current situation of the ICPS edge networks as they are the main targets of cyberattacks that target ICPS. The cybersecurity perspective of the survey is limited to the offered solutions against the vulnerabilities determined by the cybersecurity reports [168, 169, 173], and surveys/papers that focus on edge security, datasets, and testbeds. Our selection criteria are based on the relevance of the papers to the above-mentioned topics and the publication years of these papers. We did not limit the survey to the papers that belong to certain journals/conferences.

2 INDUSTRIAL SYSTEMS & INFRASTRUCTURES

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 [133] are deployed in various environments ranging from local (e.g. home, car) to industrial (e.g. military, and health) [4]. In WSN, the current main challenges are related to latency and security [129]. 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 [60].

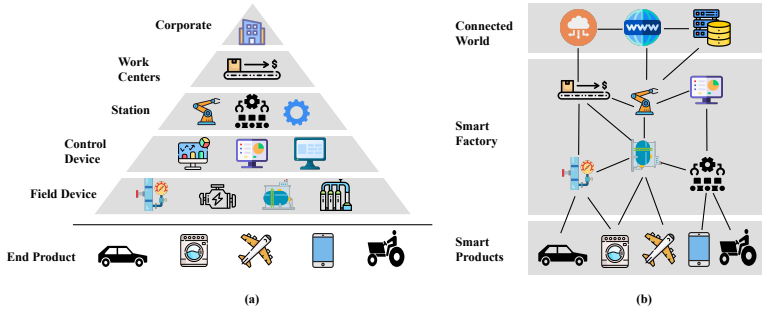


Fig. 1. Illustrates the factory hierarchies [152] of Industry 3.0 (a) and Industry 4.0 (b). The increasing interconnectivity has blurred the lines between ICPS levels and allowed the development of advanced heterogeneous systems which led to the emergence of the new term "smart factory".

Current IWSN technologies are supported by standardization organizations (e.g., ISA, IEC, IEEE) due to their adaptability to harsh environments [111]. IWSNs are being integrated into the internet via gateways [84] and even in the future, they may even have dedicated IPs.

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 [146]. 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 [180]. The increasing heterogeneity of IIoT has led to the development of WoT [33] to solve interoperability problems. We believe in the future, the industrial Web of Things (IWoT) [76] 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 and DCS that are located in various industrial sectors. Years ago, ICSs were air-gapped while running proprietary protocols. 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 [88]. ICS are also targeted by cyberattacks in a daily manner where a successful cyberattack may result in a devastating impact. Hence, security management [89] is a key point for ICS that is guided by national/regional organizations including the National Institute of Standards and Technology (NIST) [162].

Industrial Cyber-Physical Systems. The rapid developments of embedded systems, sensors, and networks resulted in new 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 [95]. 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.

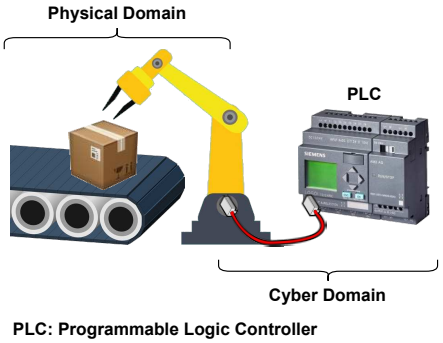
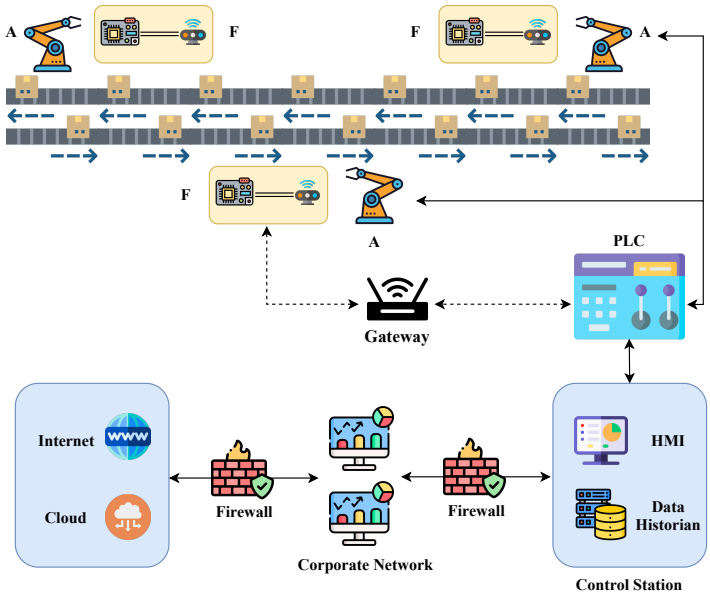


Fig. 2. Relationship between cyber and physical domain

There are several CPS architectures present in the literature. The most basic one is 3C CPS architecture presented in [18] where 3C means control, communication, and computation. Other available CPS architectures that classify the CPS domain in a more detailed way are 5C [96], and 8C [79]. These processes are completed by a variety of interconnected components that provide real-time multiprocessing. Commercial-off-the-shelf (COTS) products that perform the computation on the edge, and forward pre-processed data to the cloud (to minimize the system load/delay in industrial automation systems) are such an example. The main components included in 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 [143], gas [134], and robotic arm [91]. **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 [32, 111] show that wireless actuators are very promising and even can be utilized for industrial 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 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 [52] Additionally, microcontroller such as Raspberry Pi can be used as PLC via OpenPLC [7] 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 control purposes. HMI technology has already adopted touch screens, and mobile devices. In the future, the cloud-based mobile HMIs [157] 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



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

Fig. 3. An example of modern manufacturing ICPS architecture where fog nodes consist of an edge device (microcontroller or a single-board PC) that hosts several sensors (e.g., accelerometer, gyroscope, and magnetometer) to observe actuators – e.g. a robot arm. The data generated by sensors are processed at the edge and sent to a PLC over a wireless communication channel. This data is sent to the control station, stored in a database and accessible by the corporate network behind a firewall. The same is also applied when connecting outer networks.

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

In previous surveys Huang et al. [71], Jbair et al. [78], Leitao et al. [99], Mitchell and Chen [116] provide a CPS definition, but do not acknowledge its relationship with other technologies. Ding et al. [40], Lu et al. [111], Yue et al. [187] position ICPS suggest that IWSNs and industrial wireless sensor-actuator networks (IWSANs) can be referred to as subgroups of ICPSs. Lu [112] describe CPS as a technology that integrates the features of IoT and the Web of Things (WoT). Karnouskos [82] 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 their similarities & differences.

2.3 Information Technology vs Operational Technology

Whereas IT relates to information (data) processing, OT focuses on monitoring and controlling physical phenomenon via physical devices and processes. OT systems often operate and respond to events in real-time. The adoption of mobile devices in OT provides ubiquitous access to authorized personnel. Major ICPS suppliers such as Schneider Electric [126] and Rockwell Automation [142] have used mobile technologies for over 20 years now. ICPSs were also previously isolated from any

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

outer networks. Hence, 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) when in physical proximity to the system, as 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 the benefits [28] it brings. 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, as summarised in Table 2. 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 [31] and deployable for harsh industrial environments. We believe in the future, IT and OT will be integrated, and holistic approaches will form a base for future studies. Hence, while legacy ICPS components had obvious borders/differences, in today's systems this border is fading away. Hence, for example, it is possible to see a single device that can act as both PLC and HMI.

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 [2] 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 [153]. Wireless technologies are

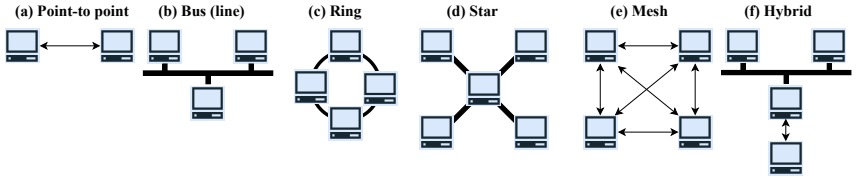


Fig. 4. Illustrates industrial communication network topologies. Each topology has unique pros and cons. For example, networks with mesh topology are more robust but cost higher, while bus topology costs less but is more prone to failures. Hybrid topologies are preferred in the existing ICPSs

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.

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 [122].

We can classify currently available industrial communication technologies according to their working principles: fieldbus [164], industrial ethernet [77], and wireless [101]. *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.

Fieldbus. *Modbus.* Open protocol developed and administered by Modbus Organization [118]. 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 [41]. 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 [22] 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) [13]. Recently, BACnet Secure Connect (BACnet/SC) is proposed by ASHRAE to prevent problems when integrating IT systems into OT infrastructure for cloud-based applications [51]. *DeviceNet.* Open protocol developed by ODVA [124]. The reduced number of wires with high flame resistance makes the DeviceNet network suitable for solar applications [154]. However, the

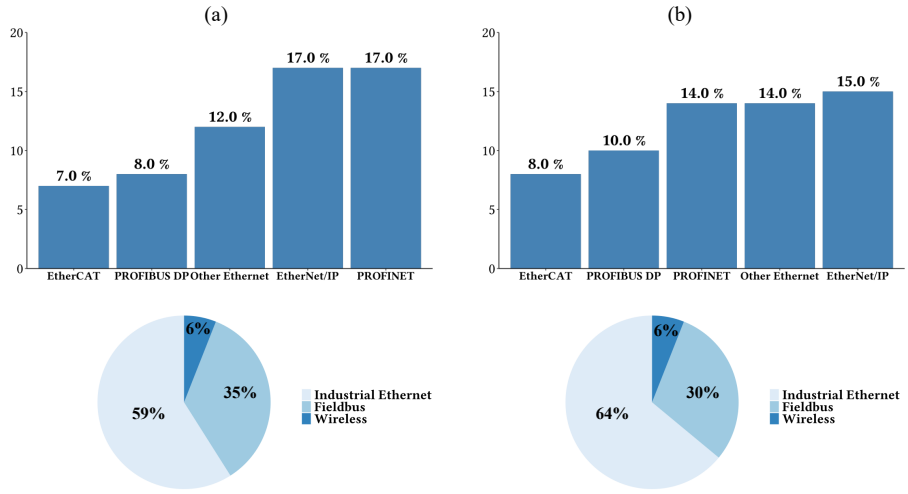


Fig. 5. (a) Industrial network shares for top 5 protocols deployed in 2019 [63] including how market share differ per industrial network technology. EtherNet/IP and Profinet led the industrial network market in 2019 – EtherNet/IP is popular in the USA, Profinet in Europe. Increased bandwidth, high data transfer rate, and reliable real-time connection are the main reasons why companies favour industrial ethernet. (b) The same findings for 2020 [64] are shown. While the top 5 protocols do not show any significant change, the Industrial Ethernet deployment rate is 5% increased while Fieldbus is 5% decreased which shows there is a transition from Fieldbus to Ethernet.

increased number of nodes in DeviceNet causes an exponential increase in time delay [12] which may raise an issue for real-time complex networks.

Industrial Ethernet. *Profinet.* Open Industrial Ethernet Standard developed and administrated by PROFINET International (PI) organization [136] 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 [16]. *EtherCAT.* Ethernet-based open communication protocol designed for automation to minimize the delay within the industrial network. EtherCAT Technology Group [48] maintains the protocol. EtherCAT has a low implementation cost and also provides high-speed real-time communication with low latency [123]. Thus, it is suitable for real-time robotic applications [36]. *EtherNet/IP.* Open industrial protocol currently maintained and standardized by ODVA [125]. 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 [188]. Being a low power solution and allowing remote management makes Zigbee suitable for environmental monitoring [26]. *Bluetooth.* Open wireless communication protocol that is designed as Personal Area Network (PAN), managed and standardized by Bluetooth Special Interest Group (SIG) [183]. 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 [34]. Therefore, Bluetooth SIG added this

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 [118]	Bus/Ring	1500
	DeviceNet	Open⋆	Something Here. [124]	Bus/Ring	500
	BACnet	Open⋆	ASHRAE [13]	Bus	1200
	DNP3	Open⋆	DNP Users Group [41]	Bus/Ring/Point-to-Point	1200
Industrial Ethernet	Modbus-TCP	Open	Modbus Organization [118]	Bus/Star	100
	Profinet	Open	PROFINET International [136]	Bus/Ring/Star	100
	EtherCAT	Open	EtherCAT Technology Group [48]	Bus	100
	EtherNet/IP	Open	ODVA [124]	Star/Ring	100
Wireless	ZigBee	Open	Zigbee Alliance [188]	Mesh	30
	Bluetooth	Open	Bluetooth SIG [183]	Mesh	1k
	LoRaWAN	Open	LoRa Alliance [109]	Star	10k
	WirelessHART	Open	FieldCOMM Group [49]	Mesh	250
	ISA-100.11a	Open	ISA [130]	Star/Mesh	10
	6LoWPAN	Open	IETF [74]	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.

feature 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 [109]. 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 [1]. *WirelessHART.* Open wireless communication protocol based on the IEEE 802.15.4 standard developed by Field COMM Group [49] 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 [62]. *ISA-100.11a.* Open wireless communication protocol based on IEEE 802.15.4 standard developed by ISA [130] 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) [120] is a wireless communication protocol based on IEEE 802.15.4 standard that is developed and standardized by Internet Engineering Task Force (IETF) [74]. 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.

In this section, first, we illustrated the network topologies. Then, we provided a deep analysis of communication technologies and protocols while describing their pros and cons according to the application domains. This evaluation shows that the industry now favors open protocols rather than proprietary ones. The Fieldbus is now less preferred as it is surpassed by the industrial ethernet. Also, wireless technologies are getting popular in industrial environments.

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 the 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

Table 4. Classification of the Currently Available Industrial Attack Taxonomies

Reference	IT	OT	Countermeasures	Vulnerabilities	Main Field
Simmons et al. [158]	●	◐	●	◐	General
Kim et al. [86]	◐	●	●	◐	Nuclear Power Plant
Loukas et al. [110]	●	◐	●	◐	Emergency Management
Chapman et al. [25]	◐	◐	○	○	General
Hu et al. [70]	●	◐	●	○	Smart Grids
Wu and Moon [179]	◐	●	○	◐	Manufacturing Systems
Sabillon et al. [145]	●	◐	○	○	General
Brar and Kumar [19]	◐	◐	○	○	General
Applegate and Stavrou [10]	◐	◐	●	○	General
Narwal et al. [121]	◐	◐	○	○	General
Yampolskiy et al. [182]	◐	●	○	●	CPS
Drias et al. [42]	◐	●	○	●	ICS Protocols
Berger et al. [17]	◐	●	○	●	IIoT
East et al. [44]	◐	●	○	○	DNP3
Elhabashy et al. [46]	◐	●	○	○	Manufacturing Systems
capec.mitre.org [24]	●	●	●	●	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.

from several ICPS vulnerability assessment reports [168, 169, 173]. Finally, we define ICPS security characteristics and review proposed countermeasures against most common ICPS vulnerabilities.

4.1 ICPS Attack Taxonomy

According to [67], 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 [24] 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) [58] that also complies with the standardization of the European Union [45] and the United Nations [166] in our taxonomy.
(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 [162] 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) [24] 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 [24] 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.

Maroochy Shire Sewage Spill [159]. 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.

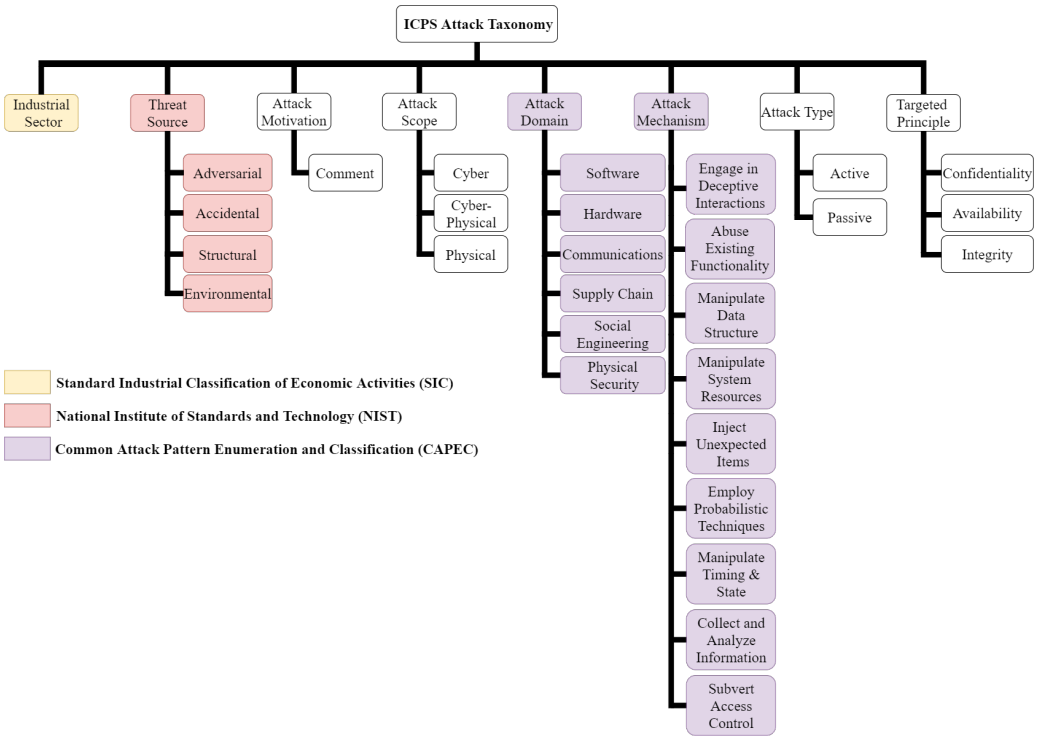


Fig. 6. Multi-dimensional adaptive ICPS attack taxonomy. We combine several strong aspects of other taxonomies to build efficient, multi-dimensional, and adaptive ICPS attack taxonomy. "Attack mechanism" and "attack domain" is taken from CAPEC [24] while "industrial sector" is from SIC [58], and "threat source" from NIST [162]. 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. Outsourced parts are color-coded.

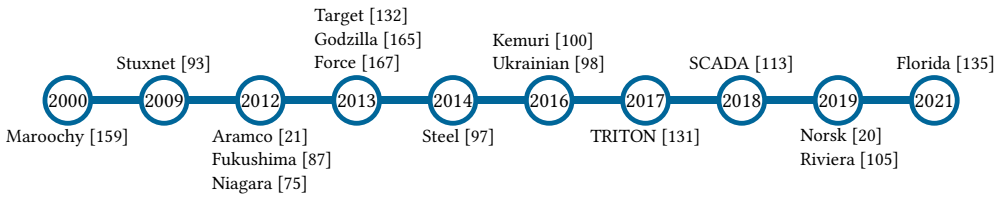


Fig. 7. The timeline of the significant ICPS attacks.

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 [93]. 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 [30] 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 [21]. 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 [87]. 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 [75]. 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 [132]. 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! [165]. 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 [167]. 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 [97]. 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 [100]. 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 [98]. 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 [131]. 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 [113]. 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 [20]. 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 [105]. 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 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.

Florida Water Treatment Poisoning Attack[135] On February 8, 2021, an adversary tried to poison of Oldsmar, a city in Florida, USA. The adversary accessed the computer that host the water treatment control software via remote access program (TeamViewer), then increased the amount of sodium hydroxide to above normal level. The water concentration change was seen by an operator and immediately reversed. Then, the remote access was disabled. How computer credentials were

captured is still unknown. In this incident, having 24/7 IT staff (which is not a case for most of the industrial systems) to supervise the system prevented the possible disaster from happening. Also, adversary did not fake the sensor readings hence the unexpected change was detected.

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 [58] 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 [92].

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [170] 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) [50]. Their industrial vulnerability assessment reports respectively for 2015 [168] and 2016 [169] 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) [114] is one way to mitigate such a problem. Table 6 illustrates the key findings from these reports.

Cyber Kill Chain (CKC) [108] is a widely accepted framework created by Lockheed Martin in 2011 that identifies the stages of a successful cyberattack. The CKC developed by SANS [11] 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 [173] 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).

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 [169]. 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 [168, 169, 173] 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

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
2021	Florida Water Treatment Poisoning Attack	E	Adversarial/Group	Sabotage	Cyber	Software Hardware	Inject Unexpected Items	Active	Confidentiality

Table 6. Comparison of ICS-CERT Industrial System Vulnerability Assessment Reports [169]

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%

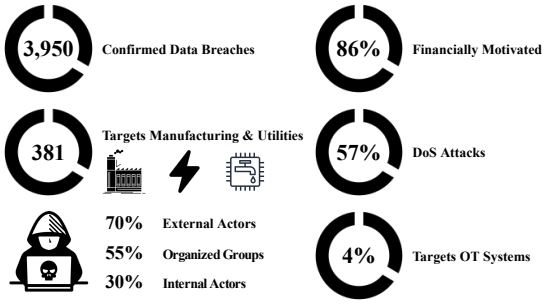


Fig. 8. Key findings from Verizon's 2020 data breach report [173]. 381 data breaches (10% of total) are against industrial control systems – although not all of these target OT equipment. Financial gain is the main reason behind 86% of attacks, carried out by organized groups which form 55% of total threat actors. DoS is the most preferred attack method, as seen in the Mirai Botnet [9] incident.

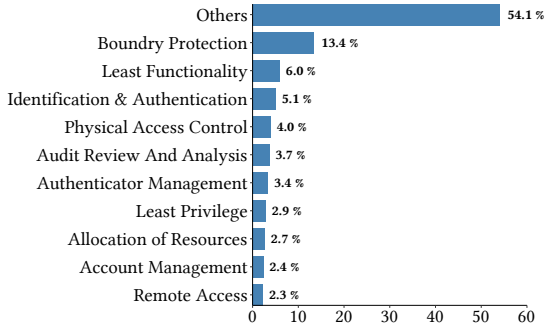


Fig. 9. Top 10 vulnerabilities seen in industrial environments. Vulnerabilities are not isolated from each other. Providing boundary protection when integrating IT & OT technologies and lack of enforcement of security policies remain key challenges.

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 [162]. 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 [97, 100, 105]. 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 [90]. Mazur et al. [114] defines the requirements of a DMZ while discussing if it is needed for mining applications.

Jiang et al. [80] simulate a DMZ using Riverbed Modeler to evaluate performance factors regarding defense-in-depth strategy. Hassan et al. [61] develop IDS based on a semi-supervised deep learning model to provide 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. [23] 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. [106] 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. [102] 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. [47] 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. [35] 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. [65] 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. [119] 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. [117] 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. [148] 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. [163] 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. [72] 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 [159] 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. [149] 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. [90] 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 [162] 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 [83] 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 [172] evaluates the use of Software-defined networking (SDN) switches to implement the least principle scheme for ICPS. Authors address the cybersecurity requirements on [162] 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 [160] 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 [175]. 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. [161] 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 [171] 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. [141] 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 a security-oriented access control strategy/model before enabling remote access. The main access control models that are implemented in industrial environments are discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC). Custom models are developed to provide the domain-specific features required by application domains such as IoT [43], and cloud [38].

Alcaraz et al. [6] 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. [146] 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 [8] 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.

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. [114] Jiang et al. [80] Hassan et al. [61]	Boundary Protection	✓		✓	✓		✓
Cao et al. [23] Ling et al. [106]	Least Functionality				✓ ✓	✓ ✓	
Li et al. [102] Esfahani et al. [47] Das et al. [35]	Identification and Authentication				✓ ✓ ✓	✓ ✓	
Ho et al. [65] Mudholkar et al. [119] Mock et al. [117]	Physical Access Control	✓		✓ ✓		✓ ✓	✓
Sancho et al. [148] Tao et al. [163] Huang et al. [72]	Audit Review and Analysis	✓ ✓ ✓	✓		✓ ✓ ✓	✓	✓
Sarkar et al. [149] Korman et al. [90]	Authenticator Management				✓		
Kern and Anderl [83] Venugopal et al. [172]	Least Privilege	✓		✓	✓		
Smeraldi and Malacaria [160] Wang [175] Srinidhi et al. [161]	Allocation of Resources				✓ ✓		
Valenzano [171] Ren et al. [141]	Account Management				✓ ✓	 ✓	
Alcaraz et al. [6] Sadeghi et al. [146] Anand and Regi [8]	Remote Access			✓		✓ ✓	

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

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 [174] such as Netflix's Simian Army approach [69] 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 long does it take for the system to fully recover after an anomaly. SDN [5] 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 [81].

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 [93, 97, 131]. 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 [169, 173] 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. [56] 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. [140] 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 [155] 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. [115] 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. [181] 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. [66] review 30 ICS testbeds based on the evaluation metrics defined by Siaterlis et al. [156] 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 [162]. 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 [116] 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. [85] 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. [3] 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. [189] 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

Unlike IT security, industrial security still lacks maturity. Integration of IT systems with 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 a 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, WSAN, SCADA, DCS, and IWoT) with the other complementary industrial disciplines. Aside from ICPS, we have only defined ICS, IIoT and IWSN since these were the terms for which we found the most 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

The vulnerability assessment reports we analyzed have shown that ICPS cyber incidents (as reported in [113]) occur due to the use of out of date security mechanisms. These non-adaptive cybersecurity mechanisms are prone to fail, as attacks often utilise the newest methods (e.g., zero-day attacks,

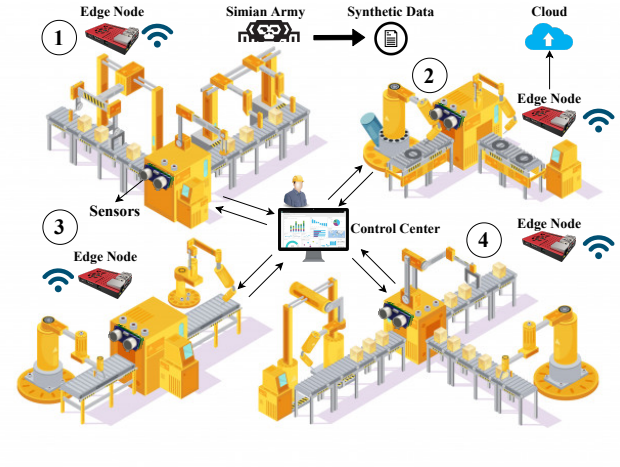


Fig. 10. Example of an ideal ICPS evaluation environment. Four testbeds with different contexts are present. Each testbed is supervised by context-aware sensors connected to the main network and edge nodes deployed on an isolated network connected to the cloud. The control center monitors and manages each testbed. Simian Army [69] approach is applied to conduct attacks so we can generate a robust synthetic dataset that contains mixed network traffic. Adaptability is achieved by using context-aware sensors/edge nodes while edge nodes also provide redundancy.

Advanced Persistent Threats (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. We propose an adaptive ICPS attack taxonomy, the validity of which depends on CAPEC [24].

Context-awareness [128] is a promising feature that we expect to see in further adaptive ICPS edge security. AI/ML algorithms are utilized to develop models that consist of several steps including data gathering, parsing, and training. Current ML models/workflows are automated using workflows based on open-source frameworks or cloud ML services to simulate an interconnected environment and achieve realistic results. To carry out these processes in an accessible cyber environment, these models are prone to adversarial machine learning techniques [137] (e.g., model exploratory, data poisoning attacks) that aim to sabotage the training process. Thus, precautions should be taken during the ML process to prevent such attacks. An adversarial machine learning can be adapted to Simian Army [69] 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 [97] is such an example of to 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 [105] 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 [168, 169, 173]. 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 [30]. 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 [169] 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. Experimenting on real and active ICPS is often limited due to possible disruption in CIs. Hence, use of *realistic* testbeds and synthetic datasets [15] that benefit from being privacy-free (the reason behind the lack of efficient publicly available datasets) and safe to gather are the most feasible options. We believe the development of advanced industrial simulation environments [68] that can generate robust synthetic datasets to be utilized with machine learning models is a significant future direction to be considered. To generate such a dataset where the privacy of the data is out of concern, and that contains both malicious and normal traffic, either we can conduct attacks (a similar approach to the Simian Army [69] may be applied) or deploy honeypot to the ICPS testbed network. However, achieving a suitable sized dataset is still a challenge when 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 actual incidents based on 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.

ACKNOWLEDGMENTS

This work is partially supported by EPSRC PETRAS (EP/S035362/1) and GCHQ National Resilience Fellowship. We would like to acknowledge the scholarship and support provided by Republic of Turkey Ministry of National Education.

REFERENCES

[1] Ferran Adelantado, Xavier Vilajosana, Pere Tuset-Peiro, Borja Martinez, Joan Melia-Segui, and Thomas Watteyne. 2017. Understanding the Limits of LoRaWAN. *IEEE Commun. Mag.* 55, 9 (2017), 34–40.

[2] Jai Agaram, John Andary, Douglas Effenberger, Kent Peterson, Steven Strauss, and Steve Taylor. 2018. Building Automation System Procurement Guide. Retrieved August 13, 2020 from 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

[3] Mohiuddin Ahmed, Abdun Naser Mahmood, and Jiankun Hu. 2016. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications* 60 (2016), 19–31.

[4] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. 2002. Wireless Sensor Networks: A Survey. *Comput. Netw.* 38, 4 (2002), 393–422.

[5] Saba Al-Rubaye, Ekhlas Kadhum, Qiang Ni, and Alagan Anpalagan. 2019. Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency. *IEEE Internet Things J.* 6, 1 (Feb. 2019), 267–277.

[6] Cristina Alcaraz, Rodrigo Roman, Pablo Najera, and Javier Lopez. 2013. Security of Industrial Sensor Network-Based Remote Substations in the Context of the Internet of Things. *Ad Hoc Netw.* 11, 3 (May 2013), 1091–1104.

[7] Thiago Alves and Thomas Morris. 2018. OpenPLC: An IEC 61,131–3 Compliant Open Source Industrial Controller for Cyber Security Research. *Comput. Secur.* 78 (Sept. 2018), 364–379.

[8] Sharath Anand and Riya Regi. 2018. Remote Monitoring of Water Level in Industrial Storage Tanks Using NB-IoT. In *2018 Int. Conf. Commun. Inf. Comput. Technol. (ICCICT)*. IEEE, Mumbai, 1–4.

[9] 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. 2017. Understanding the Mirai Botnet. In *26th {USENIX} security symposium ({USENIX} Security 17)*. USENIX, Vancouver, BC, Canada, 1093–1110.

[10] Scott D Applegate and Angelos Stavrou. 2013. Towards a cyber conflict taxonomy. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*. IEEE, Tallinn, Estonia, 1–18.

[11] Michael J Assante and Robert M Lee. 2015. The Industrial Control System Cyber Kill Chain. Retrieved August 15, 2020 from https://scadahacker.com/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf

[12] Smak Azad and K. Srinivasan. 2017. Delay Analysis of ControlNet and DeviceNet in Distributed Control System. In *Proceedings of 2nd Int. Conference on Intelligent Computing and Applications*, P. Deiva Sundari, Subhransu Sekhar Dash, Swagatam Das, and Bijaya Ketan Panigrahi (Eds.). Vol. 467. Springer Singapore, Singapore, 617–626. Series Title: Advances in Intelligent Systems and Computing.

[13] bacnet.org. 2020. BACnet. Retrieved August 22, 2020 from http://www.bacnet.org/

[14] Craig Bakker, Arnab Bhattacharya, Samrat Chatterjee, and Draguna L. Vrabie. 2020. Hypergames and Cyber-Physical Security for Control Systems. *ACM Trans. Cyber-Physical Syst.* 4, 4 (Aug. 2020), 1–41.

[15] Viacheslav Belenko, Vasiliy Krundyshev, and Maxim Kalinin. 2018. Synthetic datasets generation for intrusion detection in VANET. In *Proceedings of the 11th International Conference on Security of Information and Networks*. 1–6.

[16] Paolo Bellagente, Paolo Ferrari, Alessandra Flammini, Stefano Rinaldi, and Emiliano Sisinni. 2016. Enabling PROFINET Devices to Work in IoT: Characterization and Requirements. In *IEEE International Instrumentation and Measurement Technology Conference Proceedings*. IEEE, Taipei, Taiwan, 1–6.

[17] Stephan Berger, Olga Bürger, and Maximilian Röglinger. 2020. Attacks on the Industrial Internet of Things – Development of a Multi-Layer Taxonomy. *Comput. Secur.* 93 (June 2020), 101790.

[18] Naoufel Boulila. 2019. *Cyber-Physical Systems and Industry 4.0: Properties, Structure, Communication, and Behavior*. Technical Report. Siemens Corporate Technology.

[19] Harmandeep Singh Brar and Gulshan Kumar. 2018. Cybercrimes: A Proposed Taxonomy and Challenges. *J. Comput. Netw. Commun.* 2018 (2018), 1–11.

[20] Bill Briggs. 2019. Hackers Hit Norsk Hydro With Ransomware. the Company Responded With Transparency. Retrieved August 27, 2020 from https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/
[21] Christopher Bronk and Eneken Tikk-Ringas. 2013. The Cyber Attack on Saudi Aramco. *Survival* 55, 2 (May 2013), 81–96.
[22] Steven T. Bushby and H. Michael Newman. 2002. BACnet Today. *ASHRAE Journal* 10 (2002), 10–18.
[23] Bin Cao, Jianwei Zhao, Yu Gu, Shanshan Fan, and Peng Yang. 2020. Security-Aware Industrial Wireless Sensor Network Deployment Optimization. *IEEE Trans. Ind. Inform.* 16, 8 (Aug. 2020), 5309–5316.
[24] capec.mitre.org. 2019. CAPEC - CAPEC List Version 3.3. Retrieved August 21, 2020 from http://capec.mitre.org/data/index.html
[25] Ian M. Chapman, Sylvain P. Leblanc, and Andrew Partington. 2011. Taxonomy of Cyber Attacks and Simulation of Their Effects. In *Proceedings of the 2011 Military Modeling & Simulation Symposium* (Boston, Massachusetts) *(MMS '11)*. Society for Computer Simulation Int., San Diego, CA, USA, 73–80.
[26] Abdellah Chehri and Rachid Saadane. 2019. Zigbee-Based Remote Environmental Monitoring for Smart Industrial Mining. In *Proceedings of the 4th International Conference on Smart City Applications* (Casablanca, Morocco) *(SCA '19)*. Association for Computing Machinery, New York, NY, USA, Article 111, 6 pages.
[27] Manuel Cheminod, Luca Durante, and Adriano Valenzano. 2013. Review of Security Issues in Industrial Networks. *IEEE Trans. Ind. Inform.* 9, 1 (Feb. 2013), 277–293.
[28] A Chemudupati, S Kaulen, M Mertens, and S Zimmermann. 2012. The Convergence of It and Operational Technology. Retrieved August 11, 2020 from https://fieldcommgroup.org/services/product-testing-registration
[29] Rui-Yang Chen. 2017. An Intelligent Value Stream-Based Approach to Collaboration of Food Traceability Cyber Physical System by Fog Computing. *Food Control* 71 (Jan. 2017), 124–136.
[30] Thomas M. Chen. 2010. Stuxnet, the Real Start of Cyber Warfare? [Editor's Note]. *IEEE Netw.* 24, 6 (Nov. 2010), 2–3.
[31] CISCO. 2018. *IT/OT Convergence: Moving Digital Manufacturing Forward.* Technical Report. CISCO. 9 pages.
[32] Daniel-Ioan Curiac. 2016. Towards Wireless Sensor, Actuator and Robot Networks: Conceptual Framework, Challenges and Perspectives. *J. Netw. Comput. Appl.* 63 (March 2016), 14–23.
[33] Li Da Xu, Wu He, and Shancang Li. 2014. Internet of Things in Industries: A Survey. *IEEE Trans. Ind. Inform.* 10, 4 (Nov. 2014), 2233–2243.
[34] Seyed Mahdi Darroudi and Carles Gomez. 2017. Bluetooth Low Energy Mesh Networks: A Survey. *Sensors* 17, 7 (June 2017), 1467.
[35] Ashok Kumar Das, Mohammad Wazid, Neeraj Kumar, Athanasios V. Vasilakos, and Joel J. P. C. Rodrigues. 2018. Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment. *IEEE Internet Things J.* 5, 6 (Dec. 2018), 4900–4913.
[36] Raimarius Delgado, Shin-Young Kim, Bum-Jae You, and Byoung-Wook Choi. 2016. An EtherCAT-Based Real-Time Motion Control System in Mobile Robot Application. In *2016 13th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*. IEEE, Xian, China, 710–715.
[37] Jerker Delsing, Fredrik Rosenqvist, Oscar Carlsson, Armando W. Colombo, and Thomas Bangemann. 2012. Migration of Industrial Process Control Systems Into Service Oriented Architecture. In *IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society*. IEEE, Montreal, QC, Canada, 5786–5792.
[38] Yuri Demchenko, Canh Ngo, Cees De Laat, and Craig Lee. 2014. Federated access control in heterogeneous intercloud environment: Basic models and architecture patterns. In *2014 IEEE International Conference on Cloud Engineering*. IEEE, 439–445.
[39] Derui Ding, Qing-Long Han, Zidong Wang, and Xiaohua Ge. 2019. A Survey on Model-Based Distributed Control and Filtering for Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Inform.* 15 (May 2019), 2483–2499.
[40] Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, and Xian-Ming Zhang. 2018. A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems. *Neurocomputing* 275 (Jan. 2018), 1674–1683.
[41] dnp.org. 2004. DNP Users Group. Retrieved June 11, 2020 from https://www.dnp.org/About/DNP-Users-Group
[42] Zakarya Drias, Ahmed Serhrouchni, and Olivier Vogel. 2015. 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)*. IEEE, Paris, France, 1–6.
[43] Chethana Dukkipati, Yunpeng Zhang, and Liang Chieh Cheng. 2018. Decentralized, blockchain based access control framework for the heterogeneous internet of things. In *Proceedings of the Third ACM Workshop on Attribute-Based Access Control*. 61–69.
[44] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. 2009. A Taxonomy of Attacks on the DNP3 Protocol. In *International Conference on Critical Infrastructure Protection*, Charles Palmer and Sujeet Shenoi (Eds.). Vol. 311. Springer Berlin Heidelberg, Berlin, Heidelberg, 67–81. Series Title: IFIP Advances in Information and Communication Technology.

[45] ec.europa.eu. 2020. RAMON - Reference and Management of Nomenclatures. Retrieved August 27, 2020 from https://ec.europa.eu/eurostat/ramon/nomenclatures/index.cfm?TargetUrl=LST_CLS_DLD&StrNom=NACE_REV2&StrLanguageCode=EN&StrLayoutCode=HIERARCHIC

[46] Ahmad E. Elhabashy, Lee J. Wells, Jaime A. Camelio, and William H. Woodall. 2019. A Cyber-Physical Attack Taxonomy for Production Systems: A Quality Control Perspective. *J. Intell. Manuf.* 30, 6 (Aug. 2019), 2489–2504.

[47] Alireza Esfahani, Georgios Mantas, Rainer Matischek, Firooz B. Saghezchi, Jonathan Rodriguez, Ani Bicaku, Silia Maksuti, Markus G. Tauber, Christoph Schmittner, and Joaquim Bastos. 2019. A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment. *IEEE Internet Things J.* 6, 1 (Feb. 2019), 288–296.

[48] ethercat.org. 2020. EtherCAT Technology Group. Retrieved September 03, 2020 from https://www.ethercat.org/en/tech_group.html

[49] fieldcommgroup.org. 2016. Product Testing & Registration. Retrieved August 27, 2020 from https://fieldcommgroup.org/services/product-testing-registration

[50] first.org. 2019. Common Vulnerability Scoring System SIG. Retrieved June 02, 2020 from https://www.first.org/cvss/specification-document

[51] David Fisher, Bernhard Isler, and Michael Osborne. 2019. BACnet Secure Connect: A Secure Infrastructure for Building Automation. Retrieved June 21, 2020 from http://www.bacnet.org/Bibliography/B-SC-Whitepaper-v15_Final_20190521.pdf

[52] Brendan Galloway and Gerhard P. Hancke. 2012. Introduction to Industrial Control Networks. *IEEE Commun. Surveys Tut.* 15, 2 (2012), 860–880.

[53] ge.com. 2020. Everything You Need to Know About the Industrial Internet of Things. Retrieved August 13, 2020 from https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-internet-things

[54] M. Gidlund, G. P. Hancke, M. H. Eldefrawy, and J. Akerberg. 2020. Guest Editorial: Security, Privacy, and Trust for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* 16, 1 (Jan. 2020), 625–628.

[55] Jairo Giraldo, Esha Sarkar, Alvaro A. Cardenas, Michail Maniatakos, and Murat Kantarcioglu. 2017. Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE Des. Test* 34, 4 (Aug. 2017), 7–17.

[56] Jairo Giraldo, David Urbina, Alvaro Cardenas, Junia Valente, Mustafa Faisal, Justin Ruths, Nils Ole Tippenhauer, Henrik Sandberg, and Richard Candell. 2018. A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. *ACM Comput. Surv.* 51, 4 (Sept. 2018), 1–36.

[57] gov.uk. 2019. Public Summary of Sector Security and Resilience Plans. Retrieved August 13, 2020 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf

[58] gov.uk. 2020. Nature of Business: Standard Industrial Classification (SIC) Codes. Retrieved August 27, 2020 from http://resources.companieshouse.gov.uk/sic/

[59] Edward R Griffor, Chris Greer, David A Wollman, and Martin J Burns. 2017. *Framework for cyber-physical systems: volume 1, overview.* Technical Report. National Institute of Standards and Technology.

[60] Vehbi C Gungor and Gerhard P Hancke. 2009. Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches. *IEEE Trans. Ind. Electronics* 56, 10 (Oct. 2009), 4258–4265.

[61] Mohammad Hassan, Shamsul Huda, Shaila Sharmeen, Jemal Abawajy, and Giancarlo Fortino. 2020. An Adaptive Trust Boundary Protection for IIoT Networks Using Deep-Learning Feature Extraction Based Semi-Supervised Model. *IEEE Trans. Ind. Inform.* (2020), 1–1.

[62] Sabo Miya Hassan, Rosdiazli Ibrahim, Kishore Bingi, Tran Duc Chung, and Nordin Saad. 2017. Application of Wireless Technology for Control: A WirelessHART Perspective. *Procedia Comput. Sci.* 105, supplement C (2017), 240–247.

[63] hms networks.com. 2019. Industrial Network Market Shares 2019 According to HMS. Retrieved July 16, 2020 from https://www.hms-networks.com/news-and-insights/news-from-hms/2019/05/07/industrial-network-market-shares-2019-according-to-hms

[64] hms networks.com. 2020. Industrial Network Market Shares 2020 According to HMS Networks. Retrieved July 16, 2020 from https://www.hms-networks.com/news-and-insights/news-from-hms/2020/05/29/industrial-network-market-shares-2020-according-to-hms-networks

[65] Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. 2016. 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*. ACM Press, Xi'an, China, 461–472.

[66] Hannes Holm, Martin Karresand, Arne Vidström, and Erik Westring. 2015. A survey of industrial control system testbeds. In *Nordic Conference on Secure IT Systems*. Springer, 11–26.

[67] John D Howard and Thomas A Longstaff. 1998. *A common language for computer security incidents.* Technical Report SAND98-8667, 751004. Office of Scientific and Technical Information (OSTI). SAND98–8667, 751004 pages.

[68] https://airbus-cyber security.com/. 2020. OT Simulation Platform. Retrieved June 22, 2020 from https://airbus-cybersecurity.com/wp-content/uploads/2020/01/Airbus-CyberSecurity_Brochure-OT-Simulation-Platform.pdf

[69] https://netflixtechblog.com/. 2018. The Netflix Simian Army. Retrieved September 03, 2020 from https://netflixtechblog.com/the-netflix-simian-army-16e57fbab116
[70] Jiankun Hu, Hemanshu R. Pota, and Song Guo. 2013. Taxonomy of Attacks for Agent-Based Smart Grids. *IEEE Trans. Parallel Distrib. Syst.* 25, 7 (July 2013), 1886–1895.
[71] Kaixing Huang, Chunjie Zhou, Yu-Chu Tian, Shuanghua Yang, and Yuanqing Qin. 2018. Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Electronics* 65, 10 (Oct. 2018), 8153–8162.
[72] Sheng Huang, Yaoliang Chen, Xiaoyan Chen, Kai Liu, Xiaomin Xu, Chen Wang, Kevin Brown, and Inge Halilovic. 2014. 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*. ACM Press, Snowbird, Utah, USA, 169–176.
[73] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. 2017. Cyber-Physical Systems Security—A Survey. *IEEE Internet Things J.* 4, 6 (Dec. 2017), 1802–1831.
[74] ietf.org. 2019. IPv6 over Networks of Resource-constrained Nodes (6lo). Retrieved August 25, 2020 from https://datatracker.ietf.org/wg/6lo/about/
[75] info.publicintelligence.net. 2012. *Situational Information Report Federal Bureau of Investigation*. Technical Report. FEDERAL BUREAU OF INVESTIGATION. Retrieved August 17, 2020 from https://info.publicintelligence.net/FBI-AntisecICS.pdf
[76] Sohail Jabbar, Murad Khan, Bhagya Nathali Silva, and Kijun Han. 2018. A Rest-Based Industrial Web of Things' Framework for Smart Warehousing. *J. Supercomputing* 74, 9 (Sept. 2018), 4419–4433.
[77] Juergen Jasperneite, Markus Schumacher, and Karl Weber. 2007. Limits of Increasing the Performance of Industrial Ethernet Protocols. In *2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007)*. IEEE, Patras, Greece, 17–24.
[78] Mohammad Jbair, Bilal Ahmad, Mus'ab H. Ahmad, and Robert Harrison. 2018. Industrial Cyber Physical Systems: a Survey for Control-Engineering Tools. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, IEEE, St. Petersburg, 270–276.
[79] Jehn-Ruey Jiang. 2018. An Improved Cyber-Physical Systems Architecture for Industry 4.0 Smart Factories. *Advances Mech. Eng.* 10, 6 (June 2018), 1–15.
[80] Ning Jiang, Hu Lin, Zhenyu Yin, and Liaomo Zheng. 2018. Performance Research on Industrial Demilitarized Zone in Defense-in-Depth Architecture. In *2018 IEEE International Conference on Information and Automation (ICIA)*. IEEE, Wuyishan, China, 534–537.
[81] Ezgi Karabulut, Necati Aras, and İ Kuban Altınel. 2017. Optimal Sensor Deployment to Increase the Security of the Maximal Breach Path in Border Surveillance. *European J. Oper. Res.* 259, 1 (May 2017), 19–36.
[82] Stamatis Karnouskos. 2011. Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 4490–4494.
[83] Alexander Kern and Reiner Anderl. 2018. 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*. IEEE, Valencia, 107–114.
[84] Nacer Khalil, Mohamed Riduan Abid, Driss Benhaddou, and Michael Gerndt. 2014. Wireless Sensors Networks for Internet of Things. In *2014 IEEE Ninth Int. Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*. IEEE, IEEE, Singapore, 1–6.
[85] Ansam Khraisat, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. 2019. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity* 2, 1 (2019), 20.
[86] Seungmin Kim, Gyunyoung Heo, Enrico Zio, Jinsoo Shin, and Jae-gu Song. 2020. Cyber Attack Taxonomy for Digital Environment in Nuclear Power Plants. *Nucl. Eng. Tech.* 52, 5 (May 2020), 995–1001.
[87] Younghwan Kim, Minki Kim, and Wonjoon Kim. 2013. Effect of the Fukushima Nuclear Disaster on Global Public Acceptance of Nuclear Energy. *Energy Policy* 61 (Oct. 2013), 822–828.
[88] Keith Kirkpatrick. 2019. Protecting Industrial Control Systems. *Commun. ACM* 62, 10 (Oct. 2019), 14–16.
[89] William Knowles, Daniel Prince, David Hutchison, Jules Ferdinand Pagna Disso, and Kevin Jones. 2015. A Survey of Cyber Security Management in Industrial Control Systems. *Int. J. Crit. Infrastructure Protection* 9 (June 2015), 52–80.
[90] Matus Korman, Margus Välja, Gunnar Björkman, Mathias Ekstedt, Alexandre Vernotte, and Robert Lagerström. 2017. 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*. ACM Press, Pittsburgh, PA, USA, 73–78.
[91] Shitij Kumar, Celal Savur, and Ferat Sahin. 2018. 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)*. IEEE, Miyazaki, Japan, 2850–2857.
[92] Lucie Langer, Florian Skopik, Paul Smith, and Markus Kammerstetter. 2016. From Old to New: Assessing Cybersecurity Risks for an Evolving Smart Grid. *Comput. Secur.* 62 (2016), 165–176.
[93] Ralph Langner. 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Secur. Privacy Mag.* 9, 3 (May 2011), 49–51.

[94] Heiner Lasi, Peter Fettke, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. 2014. Industry 4.0. *Bus. Inf. Syst. Eng.* 6, 4 (Aug. 2014), 239–242.
[95] Edward A. Lee. 2008. Cyber Physical Systems: Design Challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*. IEEE, Orlando, FL, USA, 363–369.
[96] Jay Lee, Behrad Bagheri, and Hung-An Kao. 2015. A Cyber-Physical Systems Architecture for Industry 4.0-Based Manufacturing Systems. *Manuf. Lett.* 3 (Jan. 2015), 18–23.
[97] Robert M. Lee, Michael J. Assante, and Tim Conway. 2014. German Steel Mill Cyber Attack. *Ind. Control Syst.* 30 (2014), 62.
[98] Robert M. Lee, Michael J. Assante, and Tim Conway. 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid. Retrieved August 17, 2020 from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[99] Paulo Leitao, Stamatis Karnouskos, Luis Ribeiro, Jay Lee, Thomas Strasser, and Armando W. Colombo. 2016. Smart Agents in Industrial Cyber–Physical Systems. *Proc. IEEE* 104, 5 (May 2016), 1086–1101.
[100] John Leyden. 2016. *Water Treatment Plant Hacked, Chemical MIX Changed for Tap Supplies.* (March 2016). Retrieved August 17, 2020 from https://www.theregister.com/2016/03/24/water_utility_hacked/
[101] Xiaomin Li, Di Li, Jiafu Wan, Athanasios V. Vasilakos, Chin-Feng Lai, and Shiyong Wang. 2017. A Review of Industrial Wireless Networks in the Context of Industry 4.0. *Wireless Netw.* 23, 1 (Jan. 2017), 23–41.
[102] Xiong Li, Jianwei Niu, Md Zakirul Alam Bhuiyan, Fan Wu, Marimuthu Karuppiah, and Saru Kumari. 2017. A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* 14, 8 (Aug. 2017), 3599–3609.
[103] Yongxin Liao, Eduardo de Freitas Rocha Loures, and Fernando Deschamps. 2018. Industrial Internet of Things: A Systematic Literature Review and Insights. *IEEE Internet Things J.* 5, 6 (Dec. 2018), 4515–4525.
[104] Zhihong Lin and Stephanie Pearson. 2013. *An inside look at industrial Ethernet communication protocols.* Technical Report. Texas Instruments.
[105] Lindsey O'Donnell. 2020. Post-Ransomware Attack, Florida City Decides to Pay $600K. Retrieved August 22, 2020 from https://threatpost.com/ransomware-florida-city-pays-600k-ransom/145869/
[106] Sai Ho Ling, Kit Yan Chan, Frank Hung Fat Leung, Frank Jiang, and Hung Nguyen. 2016. Quality and Robustness Improvement for Real World Industrial Systems Using a Fuzzy Particle Swarm Optimization. *Eng. Appl. Artif. Intell.* 47 (Jan. 2016), 68–80.
[107] Yuxin Liu, Xiao Liu, Anfeng Liu, Neal N. Xiong, and Fang Liu. 2019. A Trust Computing-based Security Routing Scheme for Cyber Physical Systems. *ACM Trans. Intell. Syst. Tech.* 10, 6 (Dec. 2019), 1–27.
[108] lockheedmartin.com. 2018. The Cyber Kill Chain. Retrieved August 26, 2020 from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[109] lora alliance.org. 2015. LoRa Alliance. Retrieved August 22, 2020 from https://lora-alliance.org/
[110] George Loukas, Diane Gan, and Tuan Vuong. 2013. 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)*. IEEE, San Diego, CA, 534–539.
[111] Chenyang Lu, Abusayeed Saifullah, Bo Li, Mo Sha, Humberto Gonzalez, Dolvara Gunatilaka, Chengjie Wu, Lanshun Nie, and Yixin Chen. 2016. Real-Time Wireless Sensor-Actuator Networks for Industrial Cyber-Physical Systems. *Proc. IEEE* 104, 5 (May 2016), 1013–1024.
[112] Yang Lu. 2017. Cyber Physical System (CPS)-Based Industry 4.0: A Survey. *J. Ind. Integration Manage.* 02, 03 (Sept. 2017), 1750014.
[113] NJ Mahwah. 2020. Radiflow Reveals First Documented Cryptocurrency Malware Attack on a SCADA Network. Retrieved August 17, 2020 from https://radiflow.com/news/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network/
[114] David C. Mazur, Rob A. Entzminger, Pete A. Morell, John A. Kay, and Erik Syme. 2016. Defining the Industrial Demilitarized Zone and Its Benefits for Mining Applications. *IEEE Trans. Ind. Appl.* 52, 3 (May 2016), 2731–2736.
[115] Stephen McLaughlin, Charalambos Konstantinou, Xueyang Wang, Lucas Davi, Ahmad-Reza Sadeghi, Michail Maniatakos, and Ramesh Karri. 2016. The cybersecurity landscape in industrial control systems. *Proc. IEEE* 104, 5 (2016), 1039–1057.
[116] Robert Mitchell and Ing-Ray Chen. 2014. A Survey of Intrusion Detection Techniques for Cyber-Physical Systems. *ACM Comput. Surv.* 46, 4 (April 2014), 1–29.
[117] Kenrick Mock, Bogdan Hoanca, Justin Weaver, and Mikal Milton. 2012. 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*. ACM Press, Raleigh, North Carolina, USA, 1007–1009.
[118] modbus.org. 2005. About Modbus Organization. https://www.modbus.org/about_us.php
[119] Smita S. Mudholkar, Pradnya M. Shende, and Milind V. Sarode. 2012. Biometrics Authentication Technique for Intrusion Detection Systems Using Fingerprint Recognition. *Int. J. Comput. Sci. Eng. Inf. Tech.* 2, 1 (Feb. 2012), 57–65.

[120] Geoff Mulligan. 2007. The 6LoWPAN Architecture. In *Proceedings of the 4th Workshop on Embedded Networked Sensors - EmNets '07*. ACM Press, Cork, Ireland, 78–82.

[121] Bhawna Narwal, Amar Kumar Mohapatra, and Kaleem Ahmed Usmani. 2019. Towards a Taxonomy of Cyber Threats Against Target Applications. *J. Statist. Manage. Syst.* 22, 2 (Feb. 2019), 301–325.

[122] Angelia Nedić, Alex Olshevsky, and Michael G Rabbat. 2018. Network Topology and Communication-Computation Tradeoffs in Decentralized Optimization. *Proc. IEEE* 106, 5 (May 2018), 953–976.

[123] Vinh Quang Nguyen and Jae Wook Jeon. 2016. Ethercat Network Latency Analysis. In *2016 International Conference on Computing, Communication and Automation (ICCCA)*. IEEE, Noida, India, 432–436.

[124] odva.org. 2020. DeviceNet. Retrieved August 21, 2020 from https://www.odva.org/technology-standards/key-technologies/devicenet/

[125] odva.org. 2020. EtherNet/IP. Retrieved August 21, 2020 from https://www.odva.org/technology-standards/key-technologies/ethernet-ip/

[126] A Dean Papadopoulos, Newton Center, and West Newbury. 2000. System for Remotely Accessing an Industrial Control System Over a Commercial Communications Network. , 11 pages. Retrieved August 21, 2020 from https://patents.google.com/patent/US6061603A/en US Patent 6,061,603.

[127] Luca Parolini, Niraj Tolia, Bruno Sinopoli, and Bruce H. Krogh. 2010. 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*. ACM Press, Stockholm, Sweden, 168–177.

[128] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. 2014. Context Aware Computing for The Internet of Things: A Survey. *IEEE Commun. Surveys Tut.* 16, 1 (2014), 414–454.

[129] Adrian Perrig, John Stankovic, and David Wagner. 2004. Security in Wireless Sensor Networks. *Commun. ACM* 47, 6 (June 2004), 53–57.

[130] Stig Petersen and Simon Carlsen. 2011. WirelessHART versus ISA100. 11a: The Format War Hits the Factory Floor. *IEEE Ind. Electronics Mag.* 5, 4 (2011), 23–34.

[131] Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. 2018. TRITON: The first ICS cyber attack on safety instrument systems. Retrieved July 02, 2020 from 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-Control-Systems-Forever-wp.pdf

[132] Miloslova Plachkinova and Chris Maurer. 2019. Security Breach at Target. *J. Inf. Syst. Educ.* 29, 1 (2019), 7.

[133] Gregory J Pottie and William J Kaiser. 2000. Wireless Integrated Network Sensors. *Commun. ACM* 43, 5 (May 2000), 51–58.

[134] Radislav A. Potyrailo. 2016. Multivariable Sensors for Ubiquitous Monitoring of Gases in the Era of Internet of Things and Industrial Internet. *Chem. Rev.* 116, 19 (Oct. 2016), 11877–11923.

[135] Associated Press. 2021. *Hacker tries to poison water supply in Florida city.* Retrieved May 3, 2021 from https://www.telegraph.co.uk/news/2021/02/09/hacker-tries-poison-water-supply-florida-city/

[136] profibus.com. 2009. PROFINET - The Leading Industrial Ethernet Standard. Retrieved August 18, 2020 from https://www.profibus.com/technology/profinet/

[137] Bin Qian, Jie Su, Zhenyu Wen, Devki Nandan Jha, Yinhao Li, Yu Guan, Deepak Puthal, Philip James, Renyu Yang, Albert Y Zomaya, et al. 2020. Orchestrating the development lifecycle of machine learning-based iot applications: A taxonomy and survey. *ACM Computing Surveys (CSUR)* 53, 4 (2020), 1–47.

[138] Diego V. Queiroz, Marcelo S. Alencar, Ruan D. Gomes, Iguatemi E. Fonseca, and Cesar Benavente-Peces. 2017. Survey and Systematic Mapping of Industrial Wireless Sensor Networks. *J. Netw. Comput. Appl.* 97 (Nov. 2017), 96–125.

[139] Ragunathan (Raj) Rajkumar, Insup Lee, Lui Sha, and John Stankovic. 2010. Cyber-Physical Systems: The Next Computing Revolution. In *Design Automation Conference*. IEEE, Anaheim, California, 731–736.

[140] Daniel Ramotsoela, Adnan Abu-Mahfouz, and Gerhard Hancke. 2018. A Survey of Anomaly Detection in Industrial Wireless Sensor Networks with Critical Water System Infrastructure as a Case Study. *Sensors* 18, 8 (Aug. 2018), 2491.

[141] Yongjun Ren, Fujian Zhu, Jian Qi, Jin Wang, and Arun Kumar Sangaiah. 2019. Identity management and access control based on blockchain under edge computing for the industrial Internet of Things. *Applied Sciences* 9, 10 (2019), 2058.

[142] Robert J. Kretschmann. 2000. Mobile Human/Machine Interface for Use With Industrial Control Systems for Controlling the Operation of Process Executed on Spatially Separate Machines. Retrieved August 21, 2020 from https://patents.google.com/patent/US6167464A/en US Patent 6,167,464.

[143] Alina Roitberg, Nikhil Somani, Alexander Perzylo, Markus Rickert, and Alois Knoll. 2015. Multimodal Human Activity Recognition for Industrial Manufacturing Processes in Robotic Workcells. In *Proceedings of the 2015 ACM on International Conference on Multimodal Interaction* (Seattle, Washington, USA) *(ICMI '15)*. Assoc. Comput. Machinery, New York, NY, USA, 259–266.

[144] Michael Roza, William Ho, Sabri Khemissa, and Darnell Washington. 2020. *Cloud Industrial Internet of Things (IIoT) - Industrial Control Systems Security Glossary.* Technical Report. Cloud Security Alliance.
[145] Regner Sabillon, Victor Cavaller, Jeimy Cano, and Jordi Serra-Ruiz. 2016. Cybercriminals, Cyberattacks and Cybercrime. In *2016 IEEE International Conference on Cybercrime and Computer Forensic*. IEEE, Vancouver, BC, Canada, 1–9.
[146] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. 2015. Security and Privacy Challenges in Industrial Internet of Things. In *Proceedings of the 52nd Annual Design Automation Conference on - DAC '15*. IEEE, ACM Press, San Francisco, California, 1–6.
[147] Krishna Sampigethaya and Radha Poovendran. 2013. Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport. *Proc. IEEE* 101, 8 (Aug. 2013), 1834–1855.
[148] José Carlos Sancho, Andrés Caro, Mar Ávila, and Alberto Bravo. 2020. New Approach for Threat Classification and Security Risk Estimations Based on Security Event Management. *Future Gener. Comput. Syst.* 113 (Dec. 2020), 488–505.
[149] Sajal Sarkar, Sudip Sarkar, Kajal Sarkar, and Soumalya Ghosh. 2015. Cyber Security Password Policy for Industrial Control Networks. In *2015 1st International Conference on Next Generation Computing Technologies (NGCT)*. IEEE, Dehradun, India, 408–413.
[150] Bharadwaj Satchidanandan and Panganamala R Kumar. 2017. Dynamic Watermarking: Active Defense of Networked Cyber–Physical Systems. *Proc. IEEE* 105, 2 (Feb. 2017), 219–240.
[151] Peter Schneider and Konstantin Böttinger. 2018. 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*. ACM Press, Toronto, Canada, 1–12.
[152] Karsten Schweichhart. 2016. Reference Architectural Model Industrie 4.0 (RAMI 4.0). Retrieved September 05, 2020 from https://www.wapz.net/down/remi-4/f4f.pdf
[153] se.com. 2015. Guide to Open Protocols in Building Automation. Retrieved August 26, 2020 from https://blog.se.com/wp-content/uploads/2015/11/SE-Protocols-Guide_A4_v21.pdf
[154] Abraham Serhane, Mohammad Shraif, Hassan Chehadi, Adnan Harb, and Ali Mohsen. 2017. Optimizing Solar Systems Using DeviceNET. In *2017 29th International Conference on Microelectronics (ICM)*. IEEE, Beirut, Lebanon, 1–4.
[155] Gauri Shah and Aashis Tiwari. 2018. 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*. 295–300.
[156] Christos Siaterlis, Andres Perez Garcia, and Béla Genge. 2012. On the use of Emulab testbeds for scientifically rigorous experiments. *IEEE Communications Surveys & Tutorials* 15, 2 (2012), 929–942.
[157] Waqas Ahmed Siddique, Muhammad Farhan Siddiqui, and Awais Khan. 2020. Controlling and Monitoring of Industrial Parameters Through Cloud Computing and HMI Using OPC Data Hub Software. *Indian J. Sci. Tech.* 13, 2 (March 2020), 114–126.
[158] Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, and Qishi Wu. 2014. AVOIDIT: A Cyber Attack Taxonomy. In *9th Annual Symposium on Information Assurance (ASIA'14)*. Albany, NY, USA, 2–12.
[159] Jill Slay and Michael Miller. 2007. Lessons Learned from the Maroochy Water Breach. In *Critical Infrastructure Protection*, Eric Goetz and Sujeet Shenoi (Eds.). Vol. 253. Springer US, Boston, MA, 73–82. Series Title: IFIP Int. Federation for Information Processing.
[160] Fabrizio Smeraldi and Pasquale Malacaria. 2014. How to Spend It: Optimal Investment for Cyber Security. In *Proceedings of the 1st International Workshop on Agents and CyberSecurity - ACySE '14*. ACM Press, Paris, France, 1–4.
[161] Bin Srinidhi, Jia Yan, and Giri Kumar Tayi. 2015. Allocation of Resources to Cyber-Security: the Effect of Misalignment of Interest Between Managers and Investors. *Decis. Support Syst.* 75 (July 2015), 49–62.
[162] Keith Stouffer, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams, and Adam Hahn. 2014. *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. 255 pages.
[163] Hai Tao, Md Zakirul Alam Bhuiyan, Md Arafatur Rahman, Tian Wang, Jie Wu, Sinan Q. Salih, Yafeng Li, and Thaier Hayajneh. 2019. TrustData: Trustworthy and Secured Data Collection for Event Detection in Industrial Cyber-Physical System. *IEEE Trans. Ind. Inform.* 16, 5 (May 2019), 3311–3321.
[164] J.-P. Thomesse. 2005. Fieldbus Technology in Industrial Automation. *Proc. IEEE* 93, 6 (June 2005), 1073–1101.
[165] Ted Thornhill. 2014. San Francisco Pranksters Hack Road Sign to Warn Drivers of Godzilla Attack. Retrieved August 21, 2020 from https://www.dailymail.co.uk/news/article-2632556/Godzilla-Attack-Turn-Pranksters-hack-San-Francisco-road-sign-warn-drivers-just-movie-makes-monster-93-2million-box-office.html
[166] unstats.un.org. 2020. UNSD — ISIC. Retrieved August 29, 2020 from https://unstats.un.org/unsd/classifications/Econ/ISIC.cshtml#:~:text=The%20International%20Standard%20Industrial%20Classification,statistics%20according%20to%20such%20activities.

[167] us cert.cisa.gov. 2013. ICS-CERT MONITOR. Retrieved August 01, 2020 from https://us-cert.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf
[168] us cert.cisa.gov. 2015. NCCIC/ICS-CERT Industrial Control Systems Assessment Summary Report. , 25 pages. Retrieved August 26, 2020 from https://us-cert.cisa.gov/sites/default/files/Annual_Reports/FY2015_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf
[169] us cert.cisa.gov. 2016. ICS-CERT Annual Assessment Report FY2016. , 24 pages. Retrieved August 23, 2020 from https://us-cert.cisa.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf
[170] us cert.cisa.gov. 2020. Industrial Control Systems. Retrieved August 26, 2020 from https://us-cert.cisa.gov/ics
[171] Adriano Valenzano. 2014. Industrial cybersecurity: improving security through access control policy models. *IEEE Industrial Electronics Magazine* 8, 2 (2014), 6–17.
[172] Varsha Venugopal, Jim Alves-Foss, and Sandeep Gogineni Ravindrababu. 2019. 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*. ACM, San Juan PR USA, 11–20.
[173] verizon.com. 2020. 2020 Data Breach Investigations Report. Retrieved August 21, 2020 from https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
[174] Artemios G. Voyiatzis, Konstantinos Katsigiannis, and Stavros Koubias. 2015. A Modbus/TCP Fuzzer for Testing Internetworked Industrial Systems. In *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*. IEEE, Luxembourg, 1–6.
[175] Shaun Wang. 2017. Optimal Level and Allocation of Cybersecurity Spending: Model and Formula. *SSRN Electron. J.* (2017), 12.
[176] Yunbo Wang, Mehmet C. Vuran, and Steve Goddard. 2008. Cyber-Physical Systems in Industrial Process Control. *ACM SIGBED Rev.* 5, 1 (Jan. 2008), 1–2.
[177] Zhaohui Wang, Houbing Song, David W. Watkins, Keat Ghee Ong, Pengfei Xue, Qing Yang, and Xianming Shi. 2015. Cyber-Physical Systems for Water Sustainability: Challenges and Opportunities. *IEEE Commun. Mag.* 53, 5 (May 2015), 216–222.
[178] Dazhong Wu, Matthew John Greer, David W. Rosen, and Dirk Schaefer. 2013. Cloud Manufacturing: Strategic Vision and State-of-the-Art. *J. Manuf. Syst.* 32, 4 (Oct. 2013), 564–579.
[179] Mingtao Wu and Young B. Moon. 2017. Taxonomy of Cross-Domain Attacks on CyberManufacturing System. *Procedia Comput. Sci.* 114 (2017), 367–374.
[180] Hansong Xu, Wei Yu, David Griffith, and Nada Golmie. 2018. A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. *IEEE Access* 6 (2018), 78238–78259.
[181] Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos. 2020. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security* 88 (2020), 101636.
[182] Mark Yampolskiy, Peter Horvath, Xenofon D. Koutsoukos, Yuan Xue, and Janos Sztipanovits. 2013. Taxonomy for Description of Cross-Domain Attacks on CPS. In *Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems - HiCoNS '13*. ACM Press, Philadelphia, Pennsylvania, USA, 135.
[183] Junjie Yin, Zheng Yang, Hao Cao, Tongtong Liu, Zimu Zhou, and Chenshu Wu. 2019. A survey on Bluetooth 5.0 and mesh: New milestones of IoT. *ACM Trans. Sensor Netw.* 15, 3 (2019), 1–29.
[184] Mina Younan, Essam H. Houssein, Mohamed Elhoseny, and Abdelmgeid A. Ali. 2020. Challenges and Recommended Technologies for the Industrial Internet of Things: a Comprehensive Review. *Meas.* 151 (Feb. 2020), 107198.
[185] Wenjin Yu, Tharam Dillon, Fahed Mostafa, Wenny Rahayu, and Yuehua Liu. 2019. Implementation of Industrial Cyber Physical System: Challenges and Solutions. In *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*. IEEE, Taipei, Taiwan, 173–178.
[186] Xinghuo Yu and Yusheng Xue. 2016. Smart Grids: A Cyber–Physical Systems Perspective. *Proc. IEEE* 104, 5 (May 2016), 1058–1070.
[187] Xuejun Yue, Hu Cai, Hehua Yan, Caifeng Zou, and Keliang Zhou. 2015. Cloud-Assisted Industrial Cyber-Physical Systems: an Insight. *Microprocessors Microsystems* 39, 8 (Nov. 2015), 1262–1270.
[188] zigbeealliance.org. 2010. Zigbee Alliance. Retrieved August 19, 2020 from https://zigbeealliance.org/solution/zigbee/
[189] Maede Zolanvari, Marcio A Teixeira, and Raj Jain. 2018. Effect of imbalanced datasets on security of industrial IoT using machine learning. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 112–117.