Cyber-Physical Systems Security Knowledge Area

Version 1.0.1

Alvaro Cardenas | University of California Santa Cruz

EDITOR
Emil Lupu | Imperial College, London

REVIEWERS
Henrik Sandberg | KTH Royal Institute of Technology
Marina Krotofil | Hamburg University of Technology
Mauro Conti | University of Padua
Nils Ole Tippenhauer | CSIPA Helmholtz Center for Information
Rakesh Bobba | Oregon State University

COPYRIGHT

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at **contact@cybok.org** to let the project know how they are using CyBOK.

Version 1.0.1 is a stable public release of the Cyber-Physical Systems Security Knowledge Area.

CHANGELOG

Version date	Version number	Changes made
July 2021	1.0.1	Updated copyright statement; amended “issue” to “version”
October 2019	1.0	

INTRODUCTION

Cyber-Physical Systems (CPSs) are engineered systems that are built from, and depend upon, the seamless integration of computation, and physical components. While automatic control systems like the steam governor have existed for several centuries, it is only in the past decades that the automation of physical infrastructures like the power grid, water systems, or chemical reactions have migrated from analogue controls to embedded computer-based control, often communicating through computer-based networks. In addition, new advances in medical implantable devices, or autonomous self-driving vehicles are increasing the role of computers in controlling even more physical systems.

While computers give us new opportunities and functionalities for interacting with the physical world, they can also enable new forms of attacks. The purpose of this Knowledge Area is to provide an overview of the emerging field of CPS security.

In contrast with other Knowledge Areas within CyBOK that can trace the roots of their field back to several decades, the work on CPS security is relatively new, and our community has not developed yet the same consensus on best security practices compared to cyber security fields described in other KAs. Therefore, in this document, we focus on providing an overview of research trends and unique characteristics in this field.

CPSs are diverse and can include a variety of technologies, for example, industrial control systems can be characterised by a hierarchy of technology layers (the Purdue model [1]). However, the security problems in the higher layers of this taxonomy are more related to classical security problems covered in other KAs. Therefore, the scope of this document focuses on the aspects of CPSs more closely related to the sensing, control, and actuation of these systems (e.g., the lower layers of the Purdue model).

The rest of the Knowledge Area is organised as follows. In Section 1 we provide an introduction to CPSs and their unique characteristics. In Section 2, we discuss crosscutting security issues in CPSs generally applicable to several domains (e.g., the power grid or vehicle systems); in particular we discuss efforts for preventing, detecting, and responding to attacks. In Section 3, we summarise the specific security challenges in a variety of CPS domains, including the power grid, transportation systems, autonomous vehicles, robotics, and medical implantable devices. Finally, in Section 4, we examine the unique challenges CPS security poses to regulators and governments. In particular, we outline the role of governments in incentivising security protections for CPSs, and how CPS security relates to national security and the conduct of war.

CONTENT

1 CYBER-PHYSICAL SYSTEMS AND THEIR SECURITY RISKS

[2, 3, 4]

The term Cyber-Physical Systems (CPSs) emerged just over a decade ago as an attempt to unify the common research problems related to the application of embedded computer and communication technologies for the automation of physical systems, including aerospace, automotive, chemical production, civil infrastructure, energy, healthcare, manufacturing, new materials, and transportation. CPSs are usually composed of a set of networked agents interacting with the physical world; these agents include sensors, actuators, control processing units, and communication devices, as illustrated in Figure 1.

The term CPSs was coined in 2006 by Helen Gill from the National Science Foundation (NSF) in the United States [2]. In their program announcement, NSF outlined their goal for considering various industries (such as water, transportation, and energy) under a unified lens: by abstracting from the particulars of specific applications in these domains, the goal of the CPS program is to reveal crosscutting fundamental scientific and engineering principles that underpin the integration of cyber and physical elements across all application sectors.

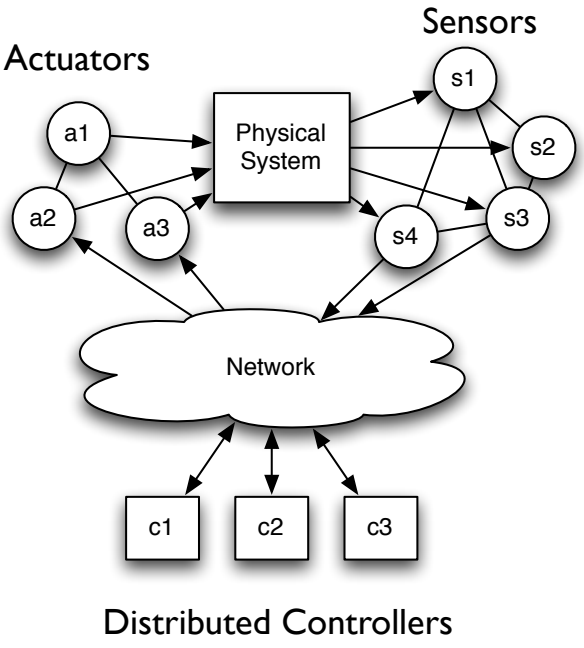

Figure 1: General architecture of cyber-physical systems [5].

Soon after the CPS term was coined, several research communities rallied to outline and understand how CPSs *cyber security* research is fundamentally different when compared to conventional IT cyber security. Because of the crosscutting nature of CPSs, the background of early security position papers from 2006 to 2009 using the term CPSs, ranged from real-time systems [6, 7], to embedded systems [8, 9], control theory [5], and cybersecurity [10, 11, 4, 12, 9].

While cyber security research had been previously considered in other physical domains—most

notably in the Supervisory Control and Data Acquisition (SCADA) systems of the power grid [13]—these previous efforts focused on applying well-known IT cyber security best practices to control systems. What differentiates the early CPS security position papers was their crosscutting nature focusing on a *multi-disciplinary perspective* for CPS security (going beyond classical IT security). For example, while classical intrusion detection systems monitor purely cyber-events (network packets, operating system information, etc.), early CPSs papers bringing control theory elements [4] suggested that intrusion detection systems for CPSs could also monitor the *physical* evolution of the system and then check it against a model of the expected dynamics as a way to improve attack detection.

CPS is related to other popular terms including the Internet of Things (IoT), Industry 4.0, or the Industrial Internet of Things, but as pointed out by Edward Lee, *the term "CPS" is more foundational and durable than all of these, because it does not directly reference either implementation approaches (e.g., "Internet" in IoT) nor particular applications (e.g., "Industry" in Industry 4.0). It focuses instead on the fundamental intellectual problem of conjoining the engineering traditions of the cyber and physical worlds* [2].

The rest of this section is organised as follows: in Section 1.1, we introduce general properties of CPS, then in Section 1.2, we discuss how physical systems have been traditionally protected from accidents and failures, and how these protections are not enough to protect the system against cyber-attacks. We finalise this section by discussing the security and privacy risks in CPSs along with summarising some of the most important real-world attacks on control systems in Section 1.3.

1.1 Characteristics of CPS

CPSs embody several aspects of embedded systems, real-time systems, (wired and wireless) networking, and control theory.

Embedded Systems: One of the most general characteristics of CPSs is that, because several of the computers interfacing directly with the physical world (sensors, controllers, or actuators) perform only a few specific actions, they do not need the general computing power of classical computers—or even mobile systems—and therefore they tend to have limited resources. Some of these embedded systems do not even run operating systems, but rather run only on *firmware*, which is a specific class of software that provides low-level control of the device hardware; devices without an operating systems are also known as *bare metal* systems. Even when embedded systems have an operating system, they often run a stripped-down version to concentrate on the minimal tools necessary for the platform.

Real-Time Systems: For safety-critical systems, the *time* in which computations are performed is important in order to ensure the correctness of the system [14]. Real-time programming languages can help developers specify timing requirements for their systems, and Real-Time Operating System (RTOS) guarantee the time to accept and complete a task from an application [15].

Network Protocols: Another characteristic of CPSs is that these embedded systems communicate with each other, increasingly over IP-compatible networks. While many critical infrastructures such as power systems have used serial communications to monitor remote operations in their SCADA systems, it is only in the past two decades that the information exchange between different parts of the system has migrated from serial communications to IP-compatible networks. For example, the serial communications protocol *Modbus* was

released by Modicon in 1979, and subsequent serial protocols with more capabilities included IEC 60870-5-101 and DNP3 in the 1990s. All these *serial* protocols were later adapted to support IP networks in the late 1990s and early 2000s with standards such as Modbus/TCP, and IEC 60870-5-104 [16, 17].

Wireless: While most of the long-distance communications are done over wired networks, wireless networks are also a common characteristic of CPSs. Wireless communications for embedded systems attracted significant attention from the research community in the early 2000s in the form of *sensor networks*. The challenge here is to build networks on top of low-powered and lossy wireless links, where traditional concepts for routing like the "hop distance" to a destination are no longer applicable, and other *link quality* metrics are more reliable, e.g., the expected number of times a packet has to be sent before a one-hop transmission is successful. While most of the research on wireless sensor networks was done in abstract scenarios, one of the first real-world successful applications of these technologies was in large process control systems with the advent of WirelessHART, ISA100, and ZigBee [18, 19]. These three communications technologies were developed on top of the IEEE 802.15.4 standard, whose original version defined frames sizes so small, that they could not carry the header of IPv6 packets. Since Internet-connected embedded systems are expected to grow to billions of devices in the next years, vendors and standard organisations see the need to create embedded devices compatible with IPv6. To be able to send IPv6 packets in wireless standards, several efforts tried to tailor IPv6 to embedded networks. Most notably the Internet Engineering Task Force (IETF) launched the 6LoWPAN effort, originally to define a standard to send IPv6 packets on top of IEEE 802.15.4 networks, and later to serve as an adaptation layer for other embedded technologies. Other popular IETF efforts include the RPL routing protocol for IPv6 sensor networks, and CoAP for application-layer embedded communications [20]. In the consumer IoT space some popular embedded wireless protocols include Bluetooth, Bluetooth Low Energy (BLE), ZigBee, and Z-Wave [21, 22].

Control: Finally, most CPSs observe and attempt to control variables in the physical world. Feedback control systems have existed for over two centuries, including technologies like the steam governor, which was introduced in 1788. Most of the literature in control theory attempts to model a physical process with differential equations and then design a controller that satisfies a set of desired properties such as stability and efficiency. Control systems were initially designed with analogue sensing and analogue control, meaning that the control logic was implemented in an electrical circuit, including a panel of relays, which usually encoded *ladder logic* controls. Analogue systems also allowed the seamless integration of control signals into a *continuous-time* physical process. The introduction of digital electronics and the microprocessor, led to work on **discrete-time control** [23], as microprocessors and computers cannot control a system in *continuous time* because sensing and actuation signals have to be sampled at discrete-time intervals. More recently, the use of computer networks allowed digital controllers to be further away from the sensors and actuators (e.g., pumps, valves, etc.), and this originated the field of **networked-controlled systems** [24]. Another recent attempt to combine the traditional models of physical systems (like differential equations) and computational models (like finite-state machines) is encapsulated in the field of **hybrid systems** [25]. Hybrid systems played a fundamental role in the motivation towards creating a CPS research program, as they were an example of how combining models of computation and models of physical systems can generate new theories that enable us to reason about the properties of cyber- and physical-controlled systems.

Having discussed these general characteristics of CPSs, one caveat is that CPSs are diverse, and they include modern vehicles, medical devices, and industrial systems, all with different

standards, requirements, communication technologies, and time constraints. Therefore, the general characteristics we associate with CPSs might not hold true in all systems or implementations.

Before we discuss cyber security problems, we describe how physical systems operating under automatic control systems have been protected from accidents and natural failures, and how these protections against non-malicious adversaries are not enough against strategic attackers (i.e., attackers that know that these protections are in place and try to either bypass them or abuse them).

1.2 Protections Against Natural Events and Accidents

Failures in the control equipment of physical infrastructures can cause irreparable harm to people, the environment, and other physical infrastructures. Therefore, engineers have developed a variety of protections against accidents and natural causes, including *safety systems, protection, fault-detection, and robustness*.

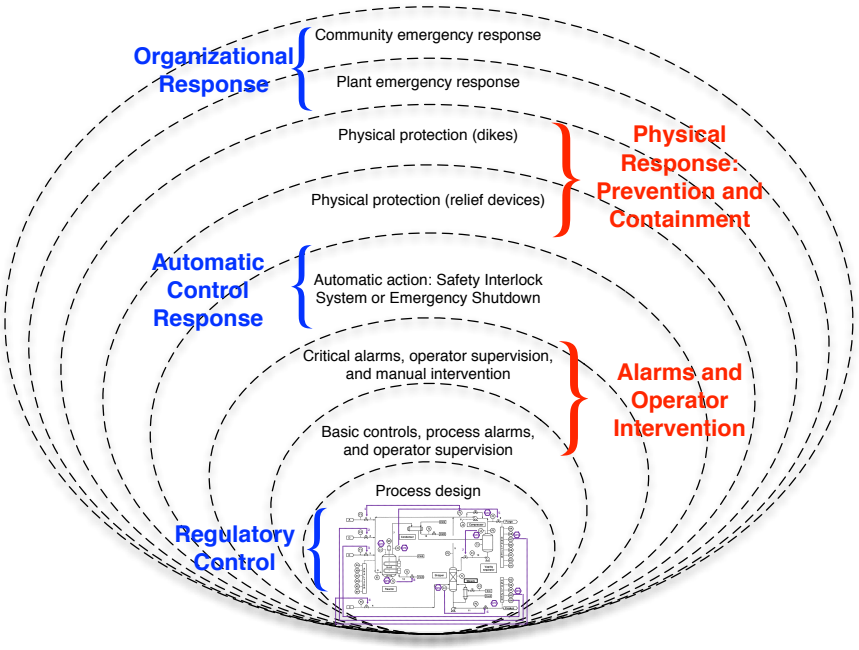

Figure 2: Layers of protection for safety-critical ICS.

Safety: The basic principle recommended by the general safety standard for control systems (IEC 61508) is to obtain requirements from a hazard and risk analysis including the likelihood of a given failure, and the consequence of the failure, and then design the system so that the safety requirements are met when all causes of failure are taken into account. This generic standard has served as the basis for many other standards in specific industries, for example, the process industry (refineries, chemical systems, etc.) use the IEC 61511 standard to design a Safety Instrumented System (SIS). The goal of a SIS is to prevent an accident by, e.g., closing a fuel valve whenever a high-pressure sensor raises an alarm. A more general defense-in-depth safety analysis uses *Layers of Protection* [26], where hazards are mitigated by a set of layers starting from (1) basic low priority alarms sent to a monitoring station, to (2) the activation of SIS systems, to (3) mitigation safeguards such as physical protection systems (e.g., dikes) and (4) organisational response protocols for a plant emergency response/evacuation. Figure 2 illustrates these safety layers of protection.

Protection: A related concept to safety is that of protection in electric power grids. These protection systems include,

- Protection of Generators: when the frequency of the system is too low or too high, the generator will be automatically disconnected from the power grid to prevent permanent damage to the generator.
- Under Frequency Load Shedding (UFLS): if the frequency of the power grid is too low, controlled load shedding will be activated. This disconnection of portions of the electric distribution system is done in a controlled manner, while avoiding outages in safety-critical loads like hospitals. UFLS is activated in an effort to increase the frequency of the power grid, and prevent generators from being disconnected.
- Overcurrent Protection: if the current in a line is too high, a protection relay will be triggered, opening the line, and preventing damage to equipment on each side of the lines.
- Over/Under Voltage Protection: if the voltage of a bus is too low or too high, a voltage relay will be triggered.

Reliability: While safety and protection systems try to prevent accidents, other approaches try to maintain operations even after failures in the system have occurred. For example, the electric system is designed and operated to satisfy the so-called N-1 security criterion, which means that the system could lose any one of its N components (such as one generator, substation, or transmission line) and continue operating with the resulting transients dying out to result in a satisfactory new steady-state operating condition, meaning that the reliable delivery of electric power will continue.

Fault Tolerance: A similar, but data-driven approach to detect and prevent failures falls under the umbrella of Fault Detection, Isolation, and Reconfiguration (FDIR) [27]. Anomalies are detected using either a model-based detection system, or a purely data-driven system; this part of the process is also known as *Bad Data Detection*. Isolation is the process of identifying which device is the source of the anomaly, and reconfiguration is the process of recovering from the fault, usually by removing the faulty sensor (if there is enough sensor redundancy in the system).

Robust Control: Finally, another related concept is *robust control* [28]. Robust control deals with the problem of uncertainty in the operation of a control system. These sources of unknown operating conditions can come from the environment (e.g., gusts of wind in the operation of planes), sensor noise, dynamics of the system not modelled by the engineers, or degradation of system components with time. Robust control systems usually take the envelope of least favourable operating conditions, and then design control algorithms so that the system operates safely, even in the worst-case uncertainty.

These mechanisms are not sufficient to provide security: Before *CPS security* was a mainstream field, there was a lot of confusion on whether safety, protection, fault-tolerance, and robust controls were enough to protect CPSs from cyber-attacks. However, as argued over a decade ago [5], these protection systems generally assume independent, non-malicious failures, and in security, incorrect model assumptions are the easiest way for the adversary to bypass any protection. Since then, there have been several examples that show why these mechanisms do not provide security. For example Liu et al. [29] showed how fault-detection (bad data detection) algorithms in the power grid can be bypassed by an adversary that sends incorrect data that is consistent with plausible power grid configurations, but at the same time

is erroneous enough from the real values to cause problems to the system. A similar example for dynamic systems (systems with a "time" component) considers *stealthy attacks* [30]. These are attacks that inject small false data in sensors so that the fault-detection system does not identify them as anomalies but, over a long-period of time, these attacks can drive the system to dangerous operating conditions. Similarly, the N-1 security criterion in the electric power grid assumes that if there is a failure, all protection equipment will react as configured, but an attacker can change the configuration of protection equipment in the power grid. In such a case, the outcome of an N-1 failure in the power grid will be completely unexpected, as equipment will react in ways that were unanticipated by the operators of the power grid, leading to potential cascading failures in the bulk power system. Finally, in Section 1.3.1, we will describe how real-world attacks are starting to target some of these protections against accidents; for example, the Triton malware specifically targeted safety systems in a process control system.

Safety vs. Security: The addition of new security defences may pose safety concerns, for example, a power plant was shutdown because a computer rebooted after a patch [31]. Software updates and patching might violate safety certifications, and preventing unauthorised users from accessing a CPS might also prevent first responders from access to the system in the case of an emergency (e.g., paramedics might need access to a medical device that prevents unauthorised connections). Security solutions should take these CPS safety concerns into account when designing and deploying new security mechanisms.

1.3 Security and Privacy Concerns

CPSs are at the core of health-care devices, energy systems, weapons systems, and transportation management. Industrial Control Systems systems, in particular, perform vital functions in critical national infrastructures, such as electric power distribution, oil and natural gas distribution, water and waste-water treatment, and intelligent transportation systems. The disruption of these CPSs could have a significant impact on public health, safety and lead to large economic losses.

For example, attacks on the power grid can cause blackouts, leading to interdependent cascading effects in other vital critical infrastructures such as computer networks, medical systems, or water systems creating potential catastrophic economic and safety effects in our society [32]. Attacks on ground vehicles can create highway accidents [33], attacks on GPS systems can mislead navigation systems and make drivers reach a destination desired by the attacker [34], and attacks on consumer drones can let attackers steal, cause accidents or surreptitiously turn on cameras and microphones to monitor victims [35].

1.3.1 Attacks Against CPSs

In general, a CPS has a physical process under its control, a set of sensors that report the state of the process to a controller, which in turn sends control signals to actuators (e.g., a valve) to maintain the system in a desired state. The controller often communicates with a supervisory and/or configuration device (e.g., a SCADA system in the power grid, or a medical device programmer) which can monitor the system or change the settings of the controller. This general architecture is illustrated in Figure 3.

Attacks on CPSs can happen at any point in the general architecture, as illustrated in Figure 4, which considers eight attack points.

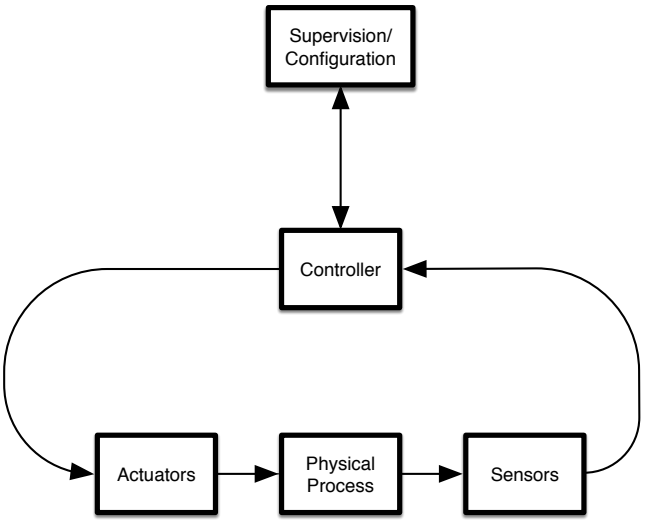

Figure 3: General Architecture of a CPS.

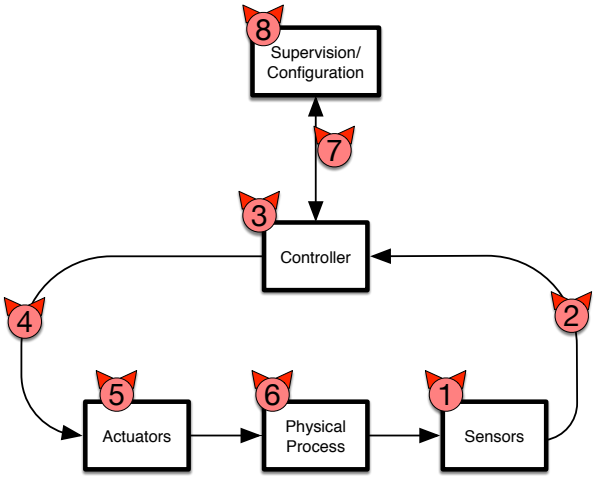

Figure 4: Attack Points in a CPS.

1. *Attack 1* represents an attacker who has compromised a sensor (e.g., if the sensor data is unauthenticated or if the attacker has the key material for the sensors) and injects false sensor signals, causing the control logic of the system to act on malicious data. An example of this type of attack is considered by Huang et al. [36].
2. *Attack 2* represents an attacker in the communication path between the sensor and the controller, who can delay or even completely block the information from the sensors to the controller, so the controller loses observability of the system (loss of view), thus causing it to operate with *stale data*. Examples of these attacks include denial-of-service attacks on sensors [37] and stale data attacks [38].
3. *Attack 3* represents an attacker who has compromised the controller and sends incorrect control signals to the actuators. An example of this attack is the threat model considered by McLaughlin [39].
4. *Attack 4* represents an attacker who can delay or block any control command, thus causing a denial of control to the system. This attack has been considered as a denial-of-service to the actuators [37].

5. *Attack 5* represents an attacker who can compromise the actuators and execute a control action that is different to what the controller intended. Notice that this attack is different to an attack that directly attacks the controller, as this can lead to *zero dynamics attacks*. These types of attacks are considered by Teixeira et al. [40].
6. *Attack 6* represents an attacker who can physically attack the system (e.g., physically destroying part of the infrastructure and combining this with a cyber-attack). This type of joint cyber and physical attack has been considered by Amin et al. [41].
7. *Attack 7* represents an attacker who can delay or block communications to and from the supervisory control system or configuration devices. This attack has been considered in the context of SCADA systems [42].
8. *Attack 8* represents an attacker who can compromise or impersonate the SCADA system or the configuration devices, and send malicious control or configuration changes to the controller. These types of attacks have been illustrated by the attacks on the power grid in Ukraine where the attackers compromised computers in the control room of the SCADA system [43] and attacks where the configuration device of medical devices has been compromised [44].

While traditionally most of the considered attacks on CPSs have been software-based, another property of CPSs is that the integrity of these systems can be compromised even without a computer-based exploit in what has been referred to as **transduction attacks** [45] (these attacks represent a physical way to inject false signals, as covered by Attack 1 in Figure 4). By targeting the way sensors capture real-world data, the attacker can inject a false sensor reading or even a false actuation action, by manipulating the physical environment around the sensor [45, 46]. For example attackers can use speakers to affect the gyroscope of a drone [47], exploit unintentional receiving antennas in the wires connecting sensors to controllers [48], use intentional electromagnetic interference to cause a servo (an actuator) to follow the attacker's commands [48], or inject inaudible voice commands to digital assistants [49].

In addition to security and safety-related problems, CPSs can also have profound privacy implications unanticipated by designers of new systems. Warren and Brandeis stated in their seminal 1890 essay *The right to privacy* [50] that they saw a growing threat from recent inventions, like "instantaneous photographs" that allowed people to be unknowingly photographed, and new media industries, such as newspapers, that would publish photographs without their subjects' consent. The rise of CPS technologies in general, and consumer IoT in particular, are similarly challenging cultural assumptions about privacy.

CPS devices can collect physical data of diverse human activities such as electricity consumption, location information, driving habits, and biosensor data at unprecedented levels of granularity. In addition, the *passive* manner of collection leaves people generally unaware of how much information about them is being gathered. Furthermore, people are largely unaware that such collection exposes them to possible surveillance or criminal targeting, as the data collected by corporations can be obtained by other actors through a variety of legal or illegal means. For example, automobile manufacturers are remotely collecting a wide variety of driving history data from cars in an effort to increase the reliability of their products. Data known to be collected by some manufacturers include speed, odometer information, cabin temperature, outside temperature, battery status, and range. This paints a very detailed map of driving habits that can be exploited by manufacturers, retailers, advertisers, auto insurers, law enforcement, and stalkers, to name just a few.

Having presented the general risks and potential attacks to CPSs we finalise our first section by

describing some of the most important real-world attacks against CPSs launched by malicious attackers.

1.3.2 High-Profile, Real-World Attacks Against CPSs

Control systems have been at the core of critical infrastructures, manufacturing and industrial plants for decades, and yet, there have been few confirmed cases of cyber-attacks (here we focus on attacks from malicious adversaries as opposed to attacks created by researchers for illustration purposes).

Non-targeted attacks are incidents caused by the same attacks that classical IT computers may suffer, such as the Slammer worm, which was indiscriminately targeting Windows servers but that inadvertently infected the Davis-Besse nuclear power plant [51] affecting the ability of engineers to monitor the state of the system. Another non-targeted attack example was a controller being used to send spam in a water filtering plant [52].

Targeted attacks are those where adversaries know that they are targeting a CPS, and therefore, *tailor their attack strategy with the aim of leveraging a specific CPS property*. We look in particular at attacks that had an effect in the physical world, and do not focus on attacks used to do reconnaissance of CPSs (such as Havex or BlackEnergy [53]).

The first publicly reported attack on an SCADA system was the 2000 attack on Maroochy Shire Council's sewage control system[1] in Queensland, Australia [55], where a contractor who wanted to be hired for a permanent position maintaining the system used commercially available radios and stolen SCADA software to make his laptop appear as a pumping station. During a 3-month period the attacker caused more than 750,000 gallons of untreated sewage water to be released into parks, rivers, and hotel grounds causing loss of marine life, and jeopardising public health. The incident cost the city council $176,000 in repairs, monitoring, clean-ups and extra security, and the contractor company spent $500,000 due to the incident [56].

In the two decades since the Maroochy Shire attack there have been other confirmed attacks on CPSs [57, 58, 59, 60, 61, 62, 63, 64, 65]. However, no other attack has demonstrated the new sophisticated threats that CPSs face like the Stuxnet worm (discovered in 2010) targeting the Nuclear enrichment program in Natanz, Iran [66]. Stuxnet intercepted requests to read, write, and locate blocks on a Programmable Logic Controller (PLC). By intercepting these requests, Stuxnet was able to modify the data sent to, and returned from, the PLC, without the knowledge of the PLC operator. The more popular attack variant of Stuxnet consisted in sending incorrect rotation speeds to motors powering centrifuges enriching Uranium, causing the centrifuges to break down so that they needed to be replaced. As a result, centrifuge equipment had to be replaced regularly, slowing down the amount of enriched Uranium the Natanz plant was able to produce.

Two other high-profile confirmed attacks on CPSs were the December 2015 and 2016 attacks against the Ukrainian power grid [67, 68]. These attacks caused power outages and clearly illustrate the evolution of attack vectors. While the attacks in 2015 leveraged a remote access program that attackers had on computers in the SCADA systems of the distribution power companies, and as such a human was involved trying to send malicious commands, the attacks in 2016 were more automated thanks to the Industroyer malware [69] which had

[1] There are prior reported attacks on control systems [54] but there is no public information corroborating these incidents and the veracity of some earlier attacks has been questioned.

knowledge of the industrial control protocols these machines use to communicate and could automatically craft malicious packets.

The most recent example in the arms race of malware creation targeting control systems is the Triton malware [70] (discovered in 2017 in the Middle-East) which targeted safety systems in industrial control systems. It was responsible for at least one process shutting down. Stuxnet, Industroyer, and Triton demonstrate a clear arms race in CPS attacks believed to be state sponsored. These attacks will have a profound impact on the way cyber-conflicts evolve in the future and will play an essential part in how wars may be waged, as we discuss in the last section of this chapter.

2 CROSSCUTTING SECURITY

[71, 72, 73]

The first step for securing CPS is to identify the risks that these systems may have, and then prioritise how to address these risks with a defence-in-depth approach. Risk assessment consists of identifying assets in a CPS [74], understanding their security exposure, and implementing countermeasures to reduce the risks to acceptable levels [13, 75, 76, 77, 78]. Penetration testing is perhaps the most common way to understand the level of risk of the system and can be used to design a vulnerability management and patching strategy. The supply chain is also another risk factor, discussed further in the Risk Management & Governance CyBOK Knowledge Area [79].

One new area in CPSs is to identify the actuators or sensors that give the attacker maximum controlability of the CPS if they are compromised [80, 30, 81, 82, 83] and then prioritise the protection of these devices.

Once the risks have been identified, a general defence-in-depth approach includes prevention, detection, and mitigation mechanisms. In this section we look at crosscutting security efforts to prevent, detect, and mitigate attacks, and the next section will look at specific CPS domains such as the power grid and intelligent transportation systems. This section is divided in three parts (1) preventing attacks (Section 2.1), (2) detecting attacks (Section 2.2), and (3) mitigating attacks (Section 2.3).

2.1 Preventing Attacks

The classical way to protect the first computer-based control systems was to have them isolated from the Internet, and from the corporate networks of the asset owners. As business practices changed, and efficiency reasons created more interconnections of control systems with other information technology networks, the concept of sub-network zone isolation was adopted by several CPS industries, most notably in the nuclear energy sector. This network isolation is usually implemented with the help of firewalls and *data diodes* [84].

On the other hand, there are several ways to break the air gap, including *insider attacks*, or adding new connectivity to the network via mobile devices. Therefore, to prevent attacks in modern CPSs, designers and developers have to follow the same best security practices as classical IT systems; i.e., they need to follow a secure development life cycle to minimise software vulnerabilities, implement access control mechanisms, and provide strong cryptographic protections along with a secure key management system [85].

While the best security practices of classical IT systems can give the *necessary* mechanisms for the security of control systems, these mechanisms alone are not *sufficient* for the defence-in-depth of CPSs. In this section we will discuss how, by understanding the interactions of the CPS system with the physical world, we should be able to

1. better understand the consequences of an attack.
2. design novel attack-detection algorithms.
3. design new attack-resilient algorithms and architectures.

In the rest of this subsection we will focus on illustrating the challenges for implementing classical IT security best practices in CPSs, including the fact that several CPSs are composed of legacy systems, are operated by embedded devices with limited resources, and face new vulnerabilities such as analogue attacks.

Securing Legacy Systems: The life cycle of CPS devices can be an order of magnitude larger than regular computing servers, desktops, or mobile systems. Consumers expect that their cars last longer than their laptops, hospitals expect medical equipment to last over a decade, the assets of most industrial control systems last for at least 25 years [86], and most of these devices will not be replaced until they are fully depreciated. Some of these devices were designed and deployed assuming a trusted environment that no longer exists. In addition, even if these devices were deployed with security mechanisms at the time, new vulnerabilities will eventually emerge and if the devices are no longer supported by the manufacturer, then they will not be patched. For example, after the Heartbleed vulnerability was discovered, major manufacturers pushed updates to mitigate this problem; however most embedded devices monitoring or controlling the physical world will not be patched (patching some safety-critical systems might even violate their safety certification). So even if a vendor used OpenSSL to create a secure communication channel between CPS devices originally, they also need to consider supporting the device over a long-time frame.

Therefore, to prevent attacks in CPSs we have to deal with (1) designing systems where security can be continuously updated, and (2) retrofitting security solutions for existing legacy systems [87].

Some devices cannot be updated with these new secure standards, and therefore a popular way to add security to legacy networks is to add a **bump-in-the-wire** [88]. Typically a bump-in-the-wire is a network appliance that is used to add integrity, authentication, and confidentiality to network packets exchanged between legacy devices. The legacy device thus sends un-encrypted and unauthenticated packets and the network appliance will tunnel them over a secure channel to another bump-in-the-wire system at the other end of the communication channel that then removes the security protections and gives the insecure packet to the final destination. Note that a bump-in-the-wire can only protect the system from untrusted parties on a network, but if the end-point is compromised, a bump-in-the-wire won't be effective.

A similar concept has been proposed for wireless devices like implantable medical devices. Because some of these wireless devices communicate over insecure channels, attackers can listen or inject malicious packets. To prevent this, a **wireless shield** [89] can be used near the vulnerable devices. The wireless shield will jam any communication attempt to the vulnerable devices except the ones from devices authorised by the owner of the shield. Wireless shields have also been proposed for other areas, such as protecting the privacy of consumers using BLE devices [90]. Because of their disruptive nature, it is not clear if wireless shields will find practical applications in consumer applications.

Lightweight Security: While several embedded devices support classical cryptography, for some devices the performance of cryptographic algorithms in terms of energy consumption, or latency, may not be acceptable [91]. For symmetric cryptography, NIST has plans for the standardisation of a portfolio of lightweight cryptographic algorithms [92] and the current CAESAR competition for an authenticated-encryption standard is evaluating the performance of their submissions in resource-constrained devices [93]. For public-key algorithms, Elliptic Curve Cryptography generally offers the best balance of performance and security guarantees, but other lightweight public-key algorithms might be more appropriate depending on the requirements of the system [94]. When it comes to exploit mitigation, the solutions are less clear. Most deeply embedded devices do not have support for data execution prevention, address space layout randomisation, stack canaries, virtual memory support, or cryptographically secure random number generators. In addition system-on-chip devices have no way to expand their memory, and real-time requirements might pose limitations on the use of virtual memory. However, there are some efforts to give embedded OS better exploit mitigation tools [95].

Secure Microkernels: Another OS security approach is to try to formally prove the security of the kernel. The design of secure operating systems with formal proofs of security is an effort dating back to the *Orange Book* [96]. Because the increasing complexity of code in monolithic kernels makes it hard to prove that operating systems are free of vulnerabilities, microkernel architectures that provide a minimal core of the functionality of an operating system have been on the rise. One example of such a system is the seL4 microkernel, which is notable because several security properties have been machine-checked with formal proofs of security [97]. DARPA's HACMS program [98] used this microkernel to build a quadcopter with strong safety and security guarantees [98].

Preventing Transduction Attacks: As introduced in the previous section, *transduction attacks* represent one of the novel ways in which CPS security is different from classical IT security. Sensors are transducers that translate a physical signal into an electrical one, but these sensors sometimes have a coupling between the property they want to measure, and another analogue signal that can be manipulated by the attacker. For example, sound waves can affect accelerometers in wearable devices and make them report incorrect movement values [99], and radio waves can trick pacemakers into disabling pacing shocks [100]. Security countermeasures to prevent these attacks include the addition of better filters in sensors, improved shielding from external signals, anomaly detection, and sensor fusion [46]. Some specific proposals include: drilling holes differently in a circuit board to shift the resonant frequency out of the range of the sensor, adding physical trenches around boards containing speakers to reduce mechanical coupling, using microfiber cloths for acoustic isolation, implementing low-pass filters that cut-off coupled signals, and secure amplifiers that prevent signal clipping [99, 45].

2.2 Detecting Attacks

Detecting attacks can be done by observing the internal state of a CPS device, by monitoring the interaction among devices to spot anomalous activities, or even using out-of-band channels.

In the first category, **Remote Attestation** is a field that has received significant attention for detecting malware in embedded systems because they usually do not have strong malware protections themselves [101, 102, 103, 104]. Remote attestation relies on the verification of the current internal state (e.g., RAM) of an untrusted device by a trusted verifier. There are three variants of remote attestation: software-based attestation, hardware-assisted attestation, and

hybrid attestation. Software-based attestation does not rely on any special security hardware in the device, but it has weak security guarantees and usually requires wireless range between the verifier and the device being checked. In contrast, hardware-based attestation (e.g., attestation with the support from a TPM, TrustZone or SGX) provides stronger security, but requires dedicated secure hardware in CPSs devices, which in turn increases their cost, which might not be affordable in some low-end embedded systems. Hybrid approaches attempt to find a middle ground by reducing the secure hardware requirements while overcoming the security limitations of pure software-based approaches [105, 106]. The minimal secure hardware requirements include a secure place to store the secret key, and safe code that has exclusive access to that key. A challenge for hybrid attestation is the fact that it needs to be non-interruptible and atomic (it has to run from the beginning to the end), and the (so far) relatively long (5-7 seconds [105, 106]) secure measurement of embedded memory might not be applicable for safety-critical real-time applications. In addition to academic work, industry is also developing standards to enhance the security of embedded systems with minimal silicon requirements. For example, the Trusted Computing Group (TCG) Device Identifier Composition Engine (DICE) is working on combining simple hardware capabilities to establish strong identity, attest software, and security policy, and assist in deploying software updates. We finalise our description of attestation by pointing out that most of the practical proposals for attestation work for initialisation, but building practical run-time attestation solutions remains a difficult challenge.

Network Intrusion Detection: The second category of solutions for detecting attacks relies on monitoring the interactions of CPS devices. In contrast with classical IT systems, where simple Finite-State models of network communications will fail, CPSs exhibit comparatively simpler network behaviour: servers change less frequently, there is a more stable network topology, a smaller user population, regular communication patterns, and networks host a smaller number of protocols. Therefore, intrusion detection systems, anomaly detection algorithms, and white listing access controls are easier to design and deploy than in classical IT systems [107]. If the CPS designer can give a specification of the intended behaviour of the network, then any non-specified traffic can be flagged as an anomaly [108]. Because most of the communications in CPS networks are between machines (with no human intervention), they happen automatically and periodically, and given their regularity, these communication patterns may be captured by finite state models like Deterministic Finite Automata [109, 110] or via Discrete-Time Markov Chains [111, 112]. While network specification is in general easier in CPS environments when compared to IT, it is still notoriously difficult to maintain.

Physics-Based Attack Detection: The major distinction of control systems with respect to other IT systems is the interaction of the control system with the physical world. In contrast to work in CPS intrusion detection that focuses on monitoring “cyber” patterns, another line of work studies how monitoring sensor (and actuation) values from physical observations, and control signals sent to actuators, can be used to detect attacks; this approach is usually called *physics-based* attack detection [72]. The models of the physical variables in the system (their correlations in time and space) can be purely data-driven [113], or based on physical models of the system [30]. There are two main classes of physical anomalies: **historical anomalies** and **physical-law anomalies**.

Historical Anomalies: identify physical configuration we have not seen before. A typical example is to place limits on the observed behaviour of a variable [114]. For example if during the learning phase, a water level in a tank is always between 1m and 2m, then if the water level ever goes above or below these values we can raise an alert. Machine learning models of the historical behaviour of the variables can also capture historical correlations of these

variables. For example, they can capture the fact that when the tank of a water-level is high, the water level of a second tank in the process is always low [115]. One problem with historical anomalies is that they might generate a large number of false alarms.

Physical-Law Anomalies: A complementary approach to historical observations that may have fewer false alarms, is to create models of the physical evolution of the system. For example we have a sensor that monitors the height of a bouncing ball, then we know that this height follows the differential equations from Newton's laws of mechanics. Thus, if a sensor reports a trajectory that is not plausible given the laws of physics, we can immediately identify that something is not right with the sensor (a fault or an attack). Similarly, the physical properties of water systems (fluid dynamics) or the power grid (electromagnetic laws) can be used to create time series models that we can then use to confirm that the control commands sent to the field were executed correctly and that the information coming from sensors is consistent with the expected behaviour of the system. For example, if we open an intake valve we should expect that the water level in the tank should rise, otherwise we may have a problem with the control, actuator, or the sensor. Models of the physical evolution of the system have been shown to be better at limiting the short-term impact of stealthy attacks (i.e., attacks where the attacker creates a malicious signal that is within the margin of error of our physical models) [116]. However, if the attack persists for a long time and drives the system to an unsafe region by carefully selecting a physically plausible trajectory, then historical models can help in detecting this previously unseen state [117].

In addition to the physics of the system being controlled, devices (such as actuators) have dynamics as well, and these physical properties can also be used to monitor the proper behaviour of devices [118].

Out-of-band Detection: Another way to passively monitor the physical system is through out-of-band channels [119]. For example, Radio Frequency-based Distributed Intrusion Detection [120] monitors radio frequency emissions from a power grid substation in order to check if there are malicious circuit breaker switching, transformer tap changes, or any activation of protecting relays without the direct request sent from the SCADA server. The basic idea is to correlate control commands sent by the SCADA server, with the radio frequency emissions observed in the substation. A potential drawback with this approach is that attackers can launch RF attacks mimicking the activation of a variety of electric systems, which can lead to security analysts losing confidence in the veracity of the alerts.

Active Detection: In addition to passively monitoring a CPS, an intrusion detection system can actively query devices to detect anomalies in how devices respond to these requests [121]. In addition to a network query, the intrusion detection system can also send a *physical challenge* to change the system's physical behaviour. This approach is also known as **physical attestation** [122, 123, 115], where a control signal is used to alter the physical world, and in response, it expects to see the changes done in the physical world reflected in the sensor values. For example, we can send signals to change the network topology of the power grid to see if the sensors report this expected change [124], use a change in the field of vision of a camera to detect hacked surveillance cameras [125], or use a watermarking signal in a control algorithm [126]. The concept of active detection is related to research on *moving target defence* applied to cyber-physical systems [127, 128, 129, 130]. However, both active detection and moving target defence might impose unnecessary perturbations in a system by their change of the physical world for security purposes. Therefore, these techniques might be too invasive and costly. Consequently, the practicality of some of these approaches is uncertain.

2.3 Mitigating Attacks

Most of the efforts for mitigating faults in CPSs have focused on safety and reliability (the protection of the system against random and/or independent faults). Attack mitigation is an extension of safety and reliability protections for when the faults in the systems are not created at random by nature, but by an adversary.

Attack mitigation is related to the concept of **resilient control systems**, defined as those that maintain state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature [131].

There are two main types of mitigating technologies: i) proactive and ii) reactive. Proactive mitigation considers design choices deployed in the CPS prior to any attack. On the other hand, reactive responses only take effect once an attack has been detected, and they reconfigure the system online in order to minimise the impact of the attack. We first describe proactive approaches.

Conservative Control: One of the first ideas for mitigating the impact of attacks was to operate the system with enough safety margins so that if an attack ever occurred, it would be harder for the attacker to reach an unsafe region. One intuitive idea for this type of control algorithm is to use Model Predictive Control (MPC) to design a control strategy that predicts that an attack will happen starting at the next time step [37], and therefore plans an optimal control action that will attempt to keep the system safe if the attack happens. Operating a CPS conservatively usually comes at the cost of suboptimal operation and extra costs when the system is not under attack.

Resilient Estimation: Resilient estimation algorithms attempt to obtain this state of a system, even if a subset of sensors is compromised [132, 133]. The basic idea is to use the knowledge of a CPS and the correlations of all sensor values. With enough redundancy in sensor measurements, a resilient estimation algorithm can reject attempted attacks and still obtain an accurate state estimate. This idea is similar to error correcting codes in information theory, where a subset of the bits transmitted can be corrupted, but the error correcting code reconstructs the original message. The drawback, however, is that not all CPSs will have a variety of correlated sensors to check the consistency of others, so this approach depends on the properties of the system.

Sensor Fusion: Resilient estimation algorithms usually assume a variety of multi-modal sensors to achieve their security guarantees. This is also the idea behind sensor fusion, where sensors of different types can help "confirm" the measurement of other sensors [134, 135, 136]. A basic example of sensor fusion in automotive systems is to verify that both the LiDAR readings and the camera measurements report consistent observations.

Virtual Sensors: When we use *physical-laws* anomaly detection systems, we have, in effect, a model of the physical evolution of the system. Therefore, one way to mitigate attacks on the sensors of a CPS is to use a physical model of the system to come up with the expected sensor values that can then be provided to the control algorithm [30, 137, 117]. By removing a sensor value with its expected value obtained from the system model, we are effectively controlling a system using open-loop control, which might work in the short-term, but may be risky as a long-term solution, as all physical models are not perfect, and the error between the real-world and the model simulation can increase over time. Another important consideration when designing virtual sensors as an attack-response mechanism, is to evaluate the safety of the system whenever the system is activated due to a false alarm [30].

Constraining Actuation: A similar principle of operating conservatively is to physically constrain the actuators of a CPS so that if the attacker ever succeeds in gaining access to the system, it is restricted in how fast it can change the operation of the system. This approach can guarantee, for example, the safety of vehicle platooning systems, even when the attacker has complete control of one of the vehicles [138].

Inertial Resets: Another idea to mitigate attacks is to reset and diversify the system as frequently as possible so that attackers are unable to gain persistent control of the system [139, 140]. The basic idea is that a full software reset of the system will make the system boot again in a trusted state, eliminating the presence of an attacker. This requires the system to have a trusted computing base that can boot the system in a secure state where the malware is not loaded yet. However, turning off a system that is in operation is a potentially dangerous action, and it is not clear if this proposal will be practical.

Reactive Control Compensation: When sensors or controllers are under attack, new actions are generated in order to maintain the safety of the system. Inspired by the literature on *fault-tolerant control*, one idea is to attempt to estimate the attack signal, and then generate a compensating action to eliminate it [141]. The problem with this approach is that it does not consider strategic adversaries; however game-theoretic approaches can address that limitation. In game-theoretic models, an attacker compromises a set of control signals $u_k^a \in R^{ma}$ and the defender uses the remaining controllers $u_k^d \in R^{md}$ to deploy a defence action. The game between the attacker and the defender can be simultaneous (zero-sum or minimax game) [142, 143, 144] or sequential (e.g., Stackelberg game) [145, 146, 147]. One of the challenges with game theory is that, in order to model and prove results, the formulation needs to be simplified, and in addition, models need to add a number of extra assumptions that might not hold in practice.

Safe Control Actions: Another reactive approach is to change or even prevent a potentially malicious control action from acting on the system. The idea of having a High Assurance Controller (HAC) as a backup to a High Performance Controller (HPC) predates work on CPS security, and was proposed as a safety mechanism to prevent complex and hard-to verify HPCs from driving the system to unsafe states [148]. A more recent and security-oriented approach is to use the concept of a *reference monitor* to check if the control action will result in any unsafe behaviour before it is allowed to go into the field [39]. The proposed approach depends on a controller of controllers (C^2), which mediates all control signals sent by the controller to the physical system. In particular, there are three main properties that C^2 attempts to hold: 1) *safety* (the approach must not introduce new unsafe behaviours, i.e., when operations are denied the 'automated' control over the plant, it should not lead the plant to an unsafe behaviour); 2) *security* (mediation guarantees should hold under all attacks allowed by the threat model); and 3) *performance* (control systems must meet real-time deadlines while imposing minimal overhead).

All the security proposals for preventing, detecting, and responding to attacks presented in this section are generally applicable to CPSs. However, there are unique properties of each CPS application that can make a difference in how these solutions are implemented. Furthermore, some unique properties of a particular CPS domain can lead to new solutions (such as the *touch-to-access* principle proposed for implantable medical devices [149]). In the next section we change focus from general and abstract CPS descriptions, to domain-specific problems and solutions.

3 CPS DOMAINS

[150, 151, 152, 153, 154, 155, 156, 71]

Having presented general principles for securing CPSs, in this section we discuss domain-specific security problems for CPSs. In particular we focus on industrial control systems, electrical power grids, transportation systems, vehicles, robots, medical devices, and consumer IoT.

3.1 Industrial Control Systems

Industrial control systems represent a wide variety of networked information technology systems connected to the physical world [157]. Depending on the application, these control systems are also called Process Control Systems (PCSs) in the chemical industry, or Distributed Control Systems (DCSs) if the devices used for supervision and control are procured using a monolithic architecture.

Control systems are usually composed of a set of networked agents, consisting of sensors, actuators, control processing units such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and communication devices. For example, the oil and gas industry uses integrated control systems to manage refining operations at plant sites, remotely monitor the pressure and flow of gas pipelines, and control the flow and pathways of gas transmission. Water utilities can remotely monitor well levels and control the wells' pumps; monitor flows, tank levels, or pressure in storage tanks; monitor pH, turbidity, and chlorine residual; and control the addition of chemicals to the water.

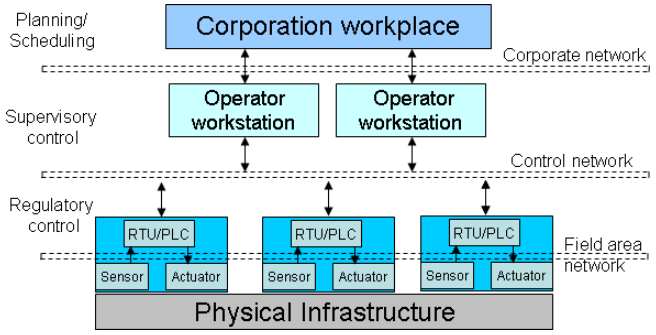

Figure 5: Bottom Layers of Industrial Control Systems [4].

Control systems have a layered hierarchy [1], which can be used for network segmentation and to ensure access control. Figure 5 shows an illustration of the lower layers of this hierarchy.

The top layers operate using mostly traditional Information Technology: computers, operating systems, and related software. They control the business logistic system, which manages the basic plant production schedule, material use, shipping and inventory levels, and also plant performance, and keep data historians for data-driven analytics (e.g., predictive maintenance).

The supervisory control layer is where the Supervisory Control and Data Acquisition (SCADA) systems and other servers communicate with remote control equipment like Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). The communication between servers in a control room and these control equipment is done via a Supervisory Control Network (SCN).

Regulatory control is done at the lower layer, which involves instrumentation in the field, such as sensors (thermometers, tachometers, etc.) and actuators (pumps, valves, etc.). While traditionally this interface has been analogue (e.g., 4-20 milliamperes), the growing numbers of sensors and actuators as well as their increased intelligence and capabilities, has given rise to new Field Communication Networks (FCNs) where the PLCs and other types of controllers interface with remote Input/Output boxes or directly with sensors and actuators using new Ethernet-based industrial protocols like ENIP and PROFINET, and wireless networks like WirelessHART. Several ring topologies have also been proposed to avoid a single point of failure for these networks, such as the use of Device Level Ring (DLR) over ENIP.

SCN and FCN networks represent Operational Technology (OT) networks, and they have different communication requirements and different industrial network protocols. While SCN can tolerate delays of up to the order of seconds, FCN typically require an order of magnitude of lower communication delays, typically enabling communications between devices with a period of 400 us.

Intrusion detection is a popular research topic for protecting control systems, and this includes using network security monitors adapted to industrial protocols [107, 109, 158, 110, 111, 159, 112], and physics-based anomaly detection [30, 114, 116, 160, 113, 161]. The layer where we monitor the physics of the system can have a significant impact on the types of attacks that can be detected [162].

In particular the adversary can compromise and launch attacks from (1) SCADA servers [163], (2) controllers/PLCs [164], (3) sensors [29], and (4) actuators [165], and each of these attacks can be observable at different layers of the system.

Most of the work on network security monitoring for industrial control systems has deployed network intrusion detection systems at the SCN. However, if an anomaly detection system is only deployed in the supervisory control network then a compromised PLC can send manipulated data to the field network, while pretending to report that everything is normal back to the supervisory control network. In the Stuxnet attack, the attacker compromised a PLC (Siemens 315) and sent a manipulated control signal u^a (which was different from the original u, i.e., $u^a \neq u$). Upon reception of u^a, the frequency converters periodically increased and decreased the rotor speeds well above and below their intended operation levels. While the status of the frequency converters y was then relayed back to the PLC, the compromised PLC reported a manipulated value $y_a \neq y$ to the control centre (claiming that devices were operating normally). A similar attack was performed against the Siemens 417 controller [164], where attackers captured 21 seconds of valid sensor variables at the PLC, and then replayed them continuously for the duration of the attack, ensuring that the data sent through the SCN to the SCADA monitors would appear normal [164]. A systematic study of the detectability of various ICS attacks (controller, sensor, or actuator attacks) was given by Giraldo et al. [162], and the final recommendation is to deploy system monitors at the field network, as well as at the supervisory network, and across different loops of the control system.

In addition to attack detection, preventing the system from reaching unsafe states is also an active area of research [39, 166, 167, 168, 169]. The basic idea is to identify that a control action can cause a problem in the system, and therefore a reference monitor will prevent this control signal from reaching the physical system. Other research areas include the retrofitting of security in legacy systems [170, 87], and malware in industrial control devices [171, 172]. A concise survey of *research* in ICS security was given by Krotofil and Gollmann [173], and reviews of state-of-the-art practices in the field of ICS security include the work of Knowles et al. and Cherdantseva et al. [174, 78].

A problem for studying industrial control systems is the diversity of platforms, including the diversity of devices (different manufacturers with different technologies) and applications (water, chemical systems, oil and gas, etc.). Therefore one of the big challenges in this space is the reproducibility of results and the generality of industrial control testbeds [175].

3.2 Electric Power Grids

At the turn of the century, the US National Academy of Engineering selected the top 20 engineering achievements of the twentieth century (the achievements that most improved people's quality of life) and at the top of this list, was the power grid [176]. In the approximately 140 years since their inception, electric grids have extended transmission lines to 5 billion people around the world, bringing light, refrigeration, and many other basic services to people across the globe.

The power grid has three major parts: (1) generation, (2) transmission, and (3) distribution. Electric power is generated wherever it is convenient and economical, and then it is transmitted at high voltages (100kV-500kV) in order to minimise energy losses—electrical power is equal to voltage times electrical current ($P = VI$), (and given a constant power, high voltage lines have less electrical current), and therefore there is less energy lost as heat as the current moves through the transmission lines. Geographically, a distribution system is located in a smaller region thereby energy losses are less of a concern while safety (preventing accidents, fires, electrocutions, etc.) is more important, therefore they are operated at lower voltages.

The transmission system is an interconnected, redundant network that spans large regions (usually one country). Large generation plants and the transmission network (the first two parts of the power grid) are usually referred to as the **Bulk Power System**, and this bulk power system is responsible for the reliable delivery of electricity to large areas. A disruption in the bulk power grid can cause a country-level blackout that would require several days of a blackstart period to restart the system. In contrast, distribution systems (the third part of the grid) are much smaller, their networks are radial (non-redundant), and a failure in their system usually only causes a localised outage (e.g., a blackout in a neighborhood). This is the reason most government and industry efforts have prioritised the creation of standards for security in the bulk power system [152].

One of the most popular lines of work related to the security of power systems is the study of false data injection attacks in order to cause the algorithms in the power grid to misbehave. The most popular of this type of attacks are the false data injection attacks against state estimation. In the power grid, operators need to estimate the phase angles x_k from the measured power flow y_k in the transmission grid. As mentioned in the section about CPS safety, bad data detection algorithms were meant to detect random sensor faults, not strategic attacks, and as Liu et al. [29, 177] showed, it is possible for an attacker to create false sensor signals that will not raise an alarm (experimental validation in software used by the energy sector was later confirmed [178]). There has been a significant amount of follow up research focusing on false data injection for state estimation in the power grid, including the work of Dán and Sandberg[179], who study the problem of identifying the best k sensors to protect in order to minimise the impact of attacks, and Kosut et al. [180], who consider attackers trying to minimise the error introduced in the estimate, and defenders with a new detection algorithm that attempts to detect false data injection attacks. Further work includes [124, 81, 181, 182, 183].

3.2.1 Smart Grids

While the current power grid architecture has served well for many years, there is a growing need to modernise the world's electric grids to address new requirements and to take advantage of the new technologies. This modernisation includes the integration of renewable sources of energy, the deployment of smart meters, the exchange of electricity between consumers and the grid, etc. Figure 6 illustrates some of these concepts. The rationale for modernising the power grid includes the following reasons:

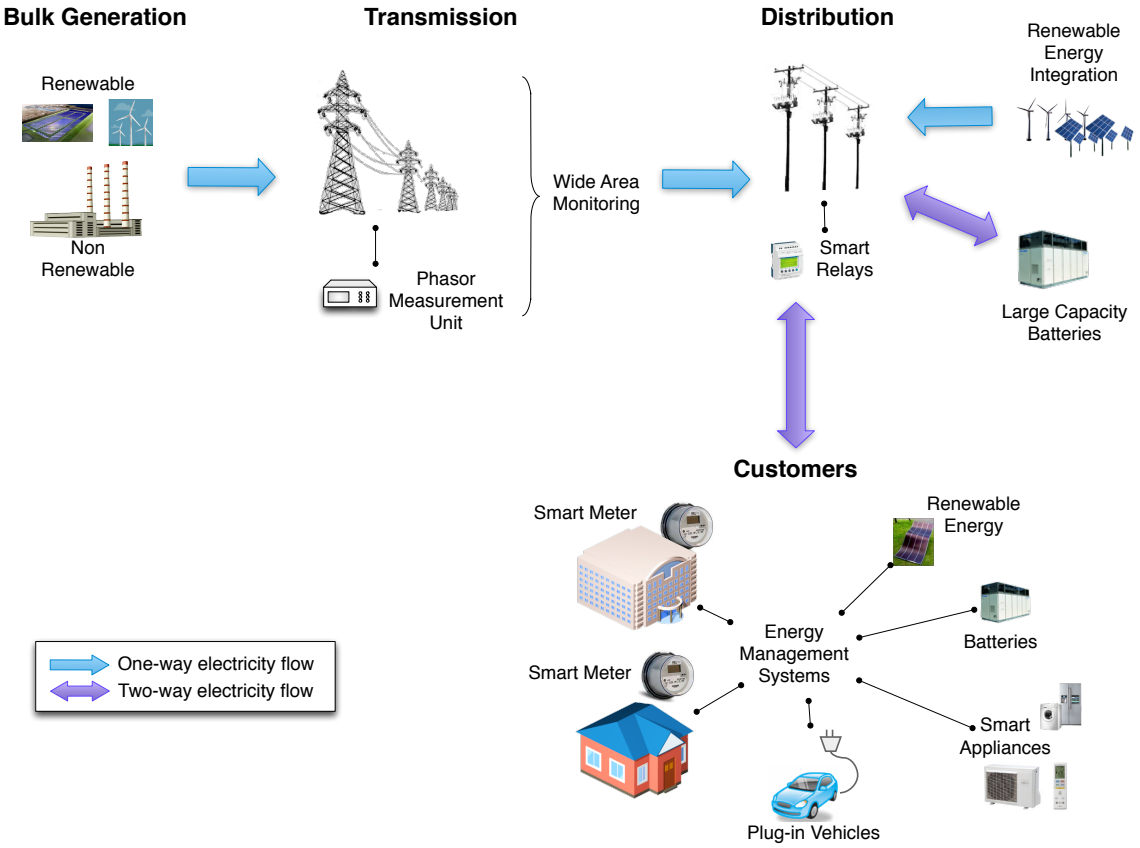

Figure 6: Modernization of the power grid [184].

Efficiency: One of the main drivers of the smart grid programs is the need to make more efficient use of the current assets. The peak demand for electricity is growing every year and so utility companies need to spend more money each year in new power plants and their associated infrastructures. However, the peak demand is only needed 16% of the time and so the equipment required to satisfy this peak demand will remain idle for the rest of the time.

One of the goals for the smart grid is to change the grid from *load following* to *load shaping* by giving incentives to consumers for reducing electricity consumption at the times of peak demand. Reducing peak demand – in addition to increasing the grid stability – can enable utilities to postpone or avoid the construction of new power stations. The control or incentive actions used to shape the load is usually called *Demand Response*.

Efficiency also deals with the integration of the new and renewable generation sources, such as wind and solar power with the aim of reducing the carbon footprint.

Reliability: The second main objective of modernising the power grid is reliability, especially at the distribution layer (the transmission layer is more reliable). By deploying new sensors and

actuators throughout the power grid, operators can receive real-time, fine-grained data about the status of the power grid, that enables better situational awareness, faster detection of faults (or attacks), and better control of the system, resulting in fewer outages. For example, the deployment of smart meters is allowing distribution utilities to automatically identify the location and source of an outage.

Consumer choice: The third objective is to address the lack of transparency the current power grid provides to consumers. Currently, most consumers receive only monthly updates about their energy usage. In general, consumers do not know their electricity consumption and prices that they are paying at different times of the day. They are also not informed about other important aspect of their consumption such as the proportion of electricity that was generated through renewable resources. Such information can be used to shape the usage pattern (i.e., the load). One of the goals of the smart grid is to offer consumers real-time data and analytics about their energy use. Smart appliances and energy management systems will automate homes and businesses according to consumer preferences, such as cost savings or by making sure more renewable energy is consumed.

To achieve these objectives, the major initiatives associated with the smart grid are the advanced metering infrastructure, demand response, transmission and distribution automation, distributed energy resources, and the integration of electric vehicles.

While modernising the power grid will bring many advantages, it can also create new threat vectors. For example, by increasing the amount of collected consumer information, new forms of attack will become possible [185]. Smart grid technologies can be used to infer the location and behaviour of users including if they are at home, the amount of energy that they consume, and the type of devices they own [186, 187]).

In addition to new privacy threats, another potential new attack has been referred to as *load-altering attack*. Load-altering attacks have been previously studied in demand-response systems [188, 189, 190, 191, 192, 193]. Demand-response programs provide a new mechanism for controlling the demand of electricity to improve power grid stability and energy efficiency. In their basic form, demand-response programs provide incentives (e.g., via dynamic pricing) for consumers to reduce electricity consumption during peak hours. Currently, these programs are mostly used by large commercial consumers and government agencies managing large campuses and buildings, and their operation is based on informal incentive signals via phone calls by the utility or by the demand-response provider (e.g., a company such as Enel X) asking the consumer to lower their energy consumption during the peak times. As these programs become more widespread (targeting residential consumers) and automated (giving utilities or demand-response companies the ability to directly control the load of their customers remotely) the attack surface for load-altering attacks will increase. The attacks proposed consider that the adversary has gained access to the company controlling remote loads and can change a large amount of the load to affect the power system and cause either inefficiencies to the system, economic profits for the attacker, or potentially cause enough load changes to change the frequency of the power grid and cause large-scale blackouts. Demand-response systems can be generalised by transactive energy markets, where *prosumers* (consumers with energy generation and storage capabilities) can trade energy with each other, bringing their own privacy and security challenges [194].

More recently Soltan et al. [195] studied the same type of load-altering attacks but when the attacker creates a large-scale botnet with hundreds of thousands of high-energy IoT devices (such as water heaters and air conditioners). With such a big botnet the attacker can cause (i) frequency instabilities, (ii) line failures, and (iii) increased operating costs. A followup work by

Huang et al. [196] showed that creating a system blackout—which would require a black start period of several days to restart the grid—or even a blackout of a large percentage of the bulk power grid can be very difficult in part because the power grid has several protections to load changes, including under-frequency load shedding.

3.3 Transportation Systems and Autonomous Vehicles

Modern vehicular applications leverage ubiquitous sensing and actuation capabilities to improve transportation operations [197] thanks to technologies such as smart phones [198], participatory sensing [199], and wireless communication networks [200]. Modern functionalities include *Traffic flow control* with ramp metering at freeway on-ramps and signal timing plans at signalised intersections to reduce congestion; *Demand management* which focuses on reducing the excess traffic during peak hours; *Incident management* which targets resources to alleviate incident hot spots; and *Traveler information* which is used to reduce traveler buffer time, i.e., the extra time the travelers must account for, when planning trips.

While this large-scale collection of sensor data can enable various societal advantages, it also raises significant privacy concerns. To address these emerging privacy concerns from sensor data, many techniques have been proposed, including differential privacy [201].

Although privacy is an important concern for these systems, it is unfortunately not the only one. Widespread vulnerabilities such as those from traffic sensors [202, 65, 203] can be readily exploited [204, 205, 206, 207]. For example, Wang et al. [206] showed that attackers can inject false data in crowdsourced services to cause false traffic congestion alarms and fake accidents, triggering the services to automatically reroute traffic.

Similar problems can be found on commercial flights. Not only are airplanes being modernised while introducing potentially new attack vectors by attempting to attack avionic systems through the entertainment network [208] but air traffic systems might also be vulnerable to attacks. A new technology complementing (or potentially replacing) radar systems is the Automatic Dependent Surveillance-Broadcast (ADS-B) system. ADS-B consists of airplanes sharing their GPS coordinates with each other and with air traffic control systems, but these systems are currently unauthenticated and unencrypted, posing security and privacy problems [209].

3.3.1 Ground, Air, and Sea Vehicles

Software problems in the sensors of vehicles can cause notorious failures, as the Ariane 5 rocket accident [210], which was caused by software in the inertial navigation system shut down causing incorrect signals to be sent to the engines. With advances in manufacturing and modern sensors, we are starting to see the proliferation of Unmanned Vehicles (UVs) in the consumer market as well as across other industries. Devices that were only available to government agencies have diversified their applications ranging from agricultural management to aerial mapping and freight transportation [211]. Out of all the UVs available in the commercial market (aerial, ground and sea vehicles) unmanned aerial vehicles seem to be the most popular kind with a projected 11.2 billion dollar global market by 2020 [212].

The expansion of unmanned aerial vehicles has increased security and privacy concerns. In general, there is a lack of security standards for drones and it has been shown that they are vulnerable to attacks that target either the cyber and/or physical elements [154, 213]. From

the point of view of privacy, drones can let users spy on neighbours [214, 215], and enable literal *helicopter parenting* [216].

Attacks remotely accessing someone else's drone (e.g., a neighbour) to take photos or videos, stealing drones wirelessly (e.g., an attacker in a vehicle can take over a drone and ask it to follow the vehicle), and taking down a drone operated by someone else (which can lead to charges like mishandling a drone in public, which in turn has resulted in reckless endangerment convictions) [35].

UVs have multiple sensors that aid them to assess their physical environments such as accelerometers, gyroscopes, barometers, GPS and cameras. While reliance on sensor data without any form of validation has proven to be an effective trade-off in order to maintain the efficiency demands of real-time systems, it is not a sustainable practice as UVs become more pervasive. *Transduction attacks* on sensors have shown that accelerometers, gyroscopes, and even cameras used by drones for stabilisation can be easily attacked, causing the drone to malfunction, crash, or even be taken over by the attacker [47, 99, 217].

Even on many operational warships, remote monitoring of equipment is now done with a hardwired LAN by systems such as the Integrated Condition Assessment System (ICAS) [218]. ICAS are generally installed with connections to external Programmable Logic Controllers (PLCs), which are used in Supervisory Control and Data Acquisition (SCADA) systems to direct the movement of control equipment that performs actual manipulation of physical devices in the ship such as propulsion and steering (rudder) devices [218, 219]. Therefore, the secure operation of ships is highly related to the security of industrial control systems.

For ground vehicles, one of the areas of interest is the security of the Controller Area Network (CAN). The CAN system is a serial broadcast bus designed by Bosch in 1983 to enable the communication of Electronic Control Units (ECUs) in cars. Examples of ECUs include brake systems, the central timing module, telematic control units, gear control, and engine control. The CAN protocol, however, does not have any security mechanism, and therefore an attacker who can enter the CAN bus in a vehicle (e.g., through a local or remote exploit) can spoof any ECU to ignore the input from drivers, and disable the brakes or stop the engine [220]. Therefore, research has considered ways to retrofit lightweight security mechanisms for CAN systems [221], or how to detect spoofed CAN messages based on the physical-layer characteristics of the signal [222] (voltage level profiles, timing, frequency of messages, etc.). However, the security of some of these systems remains in question [223].

Autonomous vehicles will also face new threats, for example, a malicious vehicle in an automated platoon can cause the platoon to behave erratically, potentially causing accidents [224]. Finally, new functionalities like a remote kill-switch can be abused by attackers, for example, an attacker remotely deactivated hundreds of vehicles in Austin, Texas, leaving their owners without transportation [225].

3.4 Robotics and Advanced Manufacturing

Security in manufacturing has been for many years a part of critical infrastructure security but, as the manufacturing process became more sophisticated, the threats have increased. Wells et al. [155] give a high-level view about the concerns of this industry. They also mention that quality control techniques traditionally used in the manufacturing industry can be leveraged to detect attacks.

Attacks can target the structural integrity (scale, indent, or vertex) or material integrity (strength, roughness, or color) of the manufactured products [226]. Physical tests, for example, non-destructive tests such as visual inspection, weight measure, dimension measure, 3D laser scanning, interferometry, X-ray, CT, and destructive mechanical tests like employing the tensile and yield properties of the material can help us in detecting attacks.

Robotic systems in automated assembly lines can also be used to create damaged parts or cause safety problems [227]. Safety accidents with robots date back to 1979, when a worker at Ford motor company was killed by a robot. As pointed out by P.W. Singer, the Ford worker might have been the first, but he would be far from the last, as robots have killed various other people [228]. Beyond manufacturing, robotic weapons also pose significant challenges. For example, in 2007 a software glitch in an antiaircraft system sporting two cannons began firing hundreds of high-explosive rounds, and by the time they were emptied, nine soldiers were dead, and fourteen seriously injured [228]. We will discuss later in this document how new advances in CPSs may change the way nations wage future wars.

3.5 Medical Devices

Due to their safety and privacy risks, embedded medical devices are another CPS domain that has received significant attention in the literature.

While not an attack, the software error of the Therac-25 is one of the most well-known classical examples of how software problems can harm and even kill people. The Therac-25 was a computer-controlled radiation therapy machine that gave massive radiation overdoses to patients resulting in deaths and injuries [229]. Our concern here is if these problems are not accidental but malicious?

Modern Implantable Medical Devices (IMDs) include pacemakers, defibrillators, neurostimulators, and drug delivery systems. These devices can usually be queried and reprogrammed by a doctor, but this also opens these devices up to security and privacy threats, in particular when an attacker can impersonate the device used by the doctor to modify the settings of IMDs.

Rushanan et al. [156] and Camara et al. [230] describe the types of adversaries that medical devices will be subject to, including the ability to eavesdrop all communication channels (passive) or read, modify and inject data (active). In order to mitigate possible attacks in the telemetry interface, they propose authentication (e.g., biometric, distance bounding, out of band channels, etc.), and the use of an external wearable device that allows or denies access to the medical device depending on whether this extra wearable device is present. In addition to prevention, they also discuss attack detection by observing patterns to distinguish between safe and unsafe behaviour.

In particular, a novel proposal to study proper authentication of the programmer with the IMD is the *touch-to-access* principle [149, 231]. The basic idea is that the patient has a biometric

signal (such as the time between heart beats) that should only be available to other devices in direct contact with the patient. This "secret" information is then used by the programmer and the IMD as a fuzzy password to bootstrap their security association.

A key challenge is to make sure that the biometric signal being used to give access via *touch-to-access*, is not remotely observable. However, heart beats can be inferred with side information including a webcam [232], and an infrared laser [233].

Security goes beyond implantable devices. As healthcare computer and software infrastructure introduces new technology, the industry will need to increase its security efforts. Medical data is a prime target for theft and privacy violations, and denial of service attacks in the form of ransomware [234].

3.6 The Internet of Things

Consumer Internet of Things (IoT) devices are found everywhere: in our houses as voice-assistant devices, home automation smart devices, smart appliances, and surveillance systems; in healthcare as wearable technology including fitness devices and health-monitoring devices; in education including Internet-connected educational children toys; and for entertainment including remote controlled Wi-Fi devices.

As our lives become more dependent on these systems, their security has become an important, growing concern. The security of these devices depends on the integrity of the software and firmware they execute and the security mechanisms they implement.

New attack vectors make IoT devices attractive to criminals, like bad actors using vulnerable IoT devices to orchestrate massive Distributed Denial of Service (DDoS) attacks (the Mirai botnet) [235, 236], attackers who compromised a fish tank to penetrate the internal network of a casino [237], or attackers demanding ransomware from a hotel so they could let their guests enter their rooms [58].

A large number of the IoT devices included in large IoT botnets [235, 236] include Internet-connected cameras. Internet-connected cameras have given rise to multiple reports of unauthorised access by attackers [238], and video feeds of multiple cameras are openly available online and discoverable through IoT web indexing platforms like Shodan [239], potentially compromising the privacy of consumers who do not check the default configuration mechanisms. The threats to IoT go beyond privacy fears and DDoS attacks. Vulnerabilities in consumer IoT products including drones, IoT cameras, smart toys for children, and intimate devices can lead not only to privacy invasions but also to physical damages (drones being used to harm people), abuse, and harassment [240]. Understanding the consequences of these new type of physical and mental abuses will require the involvement of more social scientists and legal scholars to help us define a framework on how to reason about them.

An area that has attracted significant attention from the research community is the security of voice-activated digital assistants. For example, researchers leveraged microphone non-linearities to inject inaudible voice commands to digital assistants [49]. Other recent work includes the use of new attacks like "voice squatting" or "voice masquerading" to take over voice-controlled applications [241]. For example the consumer might want to open the application "Capital One", but an attacker can make an application available called "Capital Won" and the voice-controlled personal assistant might open the second functionality. In the "voice masquerading" attack, an attacker application might remain in control of the system

and pretend to be following the consumer's commands to open other functionalities, while in reality it is impersonating the desired functionalities.

Several of the security solutions for consumer IoT have proposed the idea of having a centralised IoT secure hub that mediates the communications between IoT devices in a home, and the Internet [242]. One of the problems of relying on an external device to mediate IoT communications is that the connections between IoT device and the cloud servers may be encrypted, and therefore this hub will need to make security decisions with encrypted traffic [243]. On the other hand, end-to-end encrypted communications can also prevent consumers from auditing their IoT devices to make sure they are not violating their privacy expectations. One option to address this problem is to ask the vendor of the IoT device to disclose their key (and rotate their key) to a trusted third party (called "auditor") that can decrypt and show the results to the owners of the data [244].

In short, the proliferation of vulnerable IoT devices is raising new security and privacy concerns, while making IoT devices attractive to attackers. Insecurities in these devices range from insecure-by-design implementations (e.g., devices that have backdoors for troubleshooting) to their inability to apply software updates to patch vulnerable firmware. One of the biggest problems for improving the security of IoT and CPSs is that market forces do not incentivise vendors to compete for better security. In the next section we will discuss the causes of this lack of security and some potential solutions.

4 POLICY AND POLITICAL ASPECTS OF CPS SECURITY

[245, 228, 246]

In this final section of the paper we summarise some of the industry- and government-led efforts to try to improve the security of CPSs, and how to leverage the new field of CPS security for attacks and wars.

4.1 Incentives and Regulation

Most industries in the CPS domain have rarely seen attacks sabotaging their physical process, in part because CPS attacks are hard to monetise by criminals. In addition to being rare, attacks on CPSs are not openly reported, and this lack of actuarial data leads to low quality risk estimates; as the US Department of Energy (DoE) stated in their Energy Delivery Systems Cyber Security Roadmap [247]: "Making a strong business case for cyber security investments is complicated by the difficulty of quantifying risk in an environment of (1) rapidly changing, (2) unpredictable threats, (3) with consequences that are hard to demonstrate."

In summary, market incentives alone are insufficient to improve the security posture of CPSs, and as a result, our CPS infrastructures remain fairly vulnerable to computer attacks and with security practices that are decades behind the current security best practices used in enterprise IT domains. This market failure for improving the security of CPSs has resulted in several calls for government intervention [248, 249, 250].

Regulation: Mandating cyber security standards that the CPS industries have to follow is a possible government intervention, and there is some precedent for this idea. Before 2003, the North American Electric Reliability Corporation (NERC) merely suggested standards to the power systems operators in the US but after the August 2003 blackout, regulations that were

once optional are now mandatory [151]. However, CPS industries have pushed back against regulation, arguing that regulations (e.g., mandating compliance to specific security standards) will stifle innovation, and that more regulation tends to create a culture of *compliance* instead of a culture of *security*.

Some states in the US are starting to take regulation into their hands; for example, the recently proposed California Senate Bill SB-327 will make California the first state in the US with an IoT cyber security law—starting in 2020, any manufacturer of a device that connects "directly or indirectly" to the Internet must equip it with "reasonable" security features, designed to prevent unauthorised access, modification, or information disclosure.

The European Union Agency for cyber security proposed the EU Network and Information Security directive [251] as the first piece of EU-wide cyber security legislation, where operators of essential services such as those outlined in this KA have to comply with these new sets of standards.

Another alternative to imposing regulation broadly, is to use the governments' "power of the purse" by mandating cyber security standards only to companies that want to do business with the government. The goal would be that once the best security practices are developed to meet the standards for working with the government, then they will spread to other markets and products. This approach is a reasonable balance between incentives and regulation. Only CPS and IoT vendors working with the Federal government will have to follow specific security standards, but once they are implemented, the same security standards will benefit other markets where they reuse the technologies.

One of the notable exceptions to the lack of regulation is the nuclear energy industry. Because of the highly safety-critical nature of this industry, nuclear energy is highly regulated in general, and in cyber security standards in particular, with processes such as the Office for Nuclear Regulation (ONR) Security Assessment Principles in the UK [252].

Incentives: A complementary way to nudge companies to improve their cyber security posture is for governments to nurture a cyber-insurance market for CPS protection. So, instead of asking companies to follow specific standards, governments would demand firms to have cyber-insurance for their operations [253, 254, 255, 256]. There is a popular view that under certain conditions, the insurance industry can incentivise investments in protection [257]. The idea is that premiums charged by the insurance companies would reflect the cyber security posture of CPS companies; if a company follows good cyber security practices, the insurance premiums would be low, otherwise, the premiums would be very expensive (and this would in principle incentivise the company to invest more in cyber security protections). It is not clear if this cyber-insurance market will grow organically, or if it would need to be mandated by the government.

It is unclear if government incentives to improve security in CPSs will require first a catastrophic cyber-attack, but it appears that, in the future, the choice will no longer be between government regulation and no government regulation, but between *smart government regulation and stupid regulation* [245].

4.2 Cyber-Conflict

Computer networks enable an extension to the way we interact with others, and any conflict in the *real-world*, will have its representation in cyberspace; including (cyber-)crime, activism, bullying, espionage, and war [12].

Cybercriminals compromise computers anywhere they can find them (even in control systems). These attacks may not be targeted (i.e., they do not have the intention of harming control systems), but may cause negative side effects: control systems infected with malware may operate inappropriately. The most famous non-targeted attack on control systems occurred in 2003, when the Slammer worm affected the computerised safety monitoring system at the Davis-Besse nuclear power plant in the US. While the plant was not connected to the Internet, the worm entered the plant network via a contractor's infected computer connected by telephone directly to the plant's network, thereby bypassing the firewall [51]. A more recent example of a non-targeted attack occurred in 2006, when a computer system that managed the water treatment operations of a water filtering plant near Harrisburgh Pensylvania, was compromised and used to send spam and redistribute illegal software [52]. More recently, ransomware has also been used to attack CPSs, like the attack on the Austrian hotel [58], where guests were unable to get their room keys activated until the hotel paid the ransom.

Disgruntled employees are a major source of targeted computer attacks against control systems [258, 57, 60]. These attacks are important from a security point of view because they are caused by insiders: individuals with authorised access to computers and networks used by control systems. So, even if the systems had proper authentication and authorisation, as well as little information publicly available about them, attacks by insiders would still be possible. Because disgruntled employees generally act alone, the potential consequences of their attacks may not be as damaging as the potential harm caused by larger organised groups such as terrorists and nation states.

Terrorists, and activists are another potential threat to control systems. While there is no concrete evidence that terrorists or activists have targeted control systems via cyber-attacks, there is a growing threat of such an attack in the future.

Nation states are establishing military units with computer security expertise for any future conflicts. For example, the US established Cyber Command [259] to conduct full spectrum *operations* (offensive capabilities) in 2009, and several other countries also announced similar efforts around the same time. The role of computer networks in warfare has been a topic of academic discussion since 1998 [260], and CPSs are playing a foundational difference on how wars are waged, from robotic units and unmanned vehicles supporting soldiers in the field, to discussions of cyberwar [261].

In addition to land, air, sea and space, cyberspace is now considered by many nations as an additional theatre of conflict. International treaties have developed public international law concerning two main principles in the law of war (1) *jus ad bellum* the right to wage a war, and (2) *jus in bellum* acceptable wartime conduct. Two sources have considered how the law of war applies to cyberspace [246]: (1) The Tallinn Manual, and (2) the Koh Speech.

The Tallinn manual is a non-binding study by NATO's cooperative cyber-defence center of excellence, on how the law of war applies to cyber conflicts, and the Koh Speech was a speech given by Harold Koh, a US State Department legal advisor, which explained how the US interprets international law applied to cyberspace. Both of these sources agree that a key reason to authorise the use of force (*jus ad bellum*) as a response to a cyber operation, is

when the physical effects of a cyber-attack are comparable to kinetic effects of other armed conflicts, for example, when a computer attack triggers a nuclear plant meltdown, opens a dam upriver, or disables air-traffic control. The argument is that the effects of any of these attacks are similar to what a missile strike from an enemy would look like. In contrast, when there is no physical harm, the problem of determining when a cyber-attack can be considered a *use of force* by the enemy is unresolved, so cyber-attacks to the financial, or election infrastructure of a nation may not clear the bar to be considered an act of war.

Once nations are engaged in war, the question is how to leverage computer attacks in a way that is consistent with acceptable wartime conduct (*jus in bellum*). The conventional norm is that attacks must distinguish between military and non-military objectives. Military objectives can include war-fighting, war-supporting, and war-sustaining efforts. The problem in attacking critical infrastructures is that some of the infrastructures supporting these efforts are in dual-use by the military as well as by the civilian population. For example, a large percentage of military communications in the US use civilian networks at some stage, and the power grid supports military as well as civilian infrastructures.

Another factor to consider in designing CPS attacks is that the "law of war" in general prohibits uncontrollable or unpredictable attacks, in particular those that deny the civilian population of indispensable objects, such as food or water. While physical weapons have a limited geographical area of impact, cyberweapons can have more uncontrollable side-effects; for example, worms can replicate and escape their intended target network and infect civilian infrastructures. Therefore, nations will have to extensively test any cyberweapon to minimise unpredictable consequences.

In short, any future conflict in the physical world will have enabling technologies in the cyber-world, and computer attacks may be expected to play an integral part in future conflicts. There is a large grey area regarding what types of computer attacks can be considered an act of force, and a future challenge will be to design cyber-attacks that only target military objectives and minimise civilian side effects. At the same time, attack attribution in cyber-space will be harder, and nation-states might be able to get away with sabotage operations without facing consequences. It is a responsibility of the international community to design new legal frameworks to cover cyber-conflicts, and for nation states to outline new doctrines covering how to conduct cyber-operations with physical side effects.

Finally, cyberwar is also related to the discussion in the last section about cyber-insurance. For example, after the NotPetya cyberattack in 2017 [262], several companies who had purchased cyber-insurance protections sought to get help from their insurance companies to cover part of their loses. However, some insurance companies denied the claims citing a *war exclusion* which protects insurers from being saddled with costs related to damage from war. Since then insurers have been applying the war exemption to avoid claims related to digital attacks [2]. This type of collateral damage from cyber-attacks might be more common in the future, and presents a challenge for insurance industries in their quest to quantify the risk of correlated large-scale events.

[2] **https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html**

4.3 Industry Practices and Standards

We finalise the CPS Security KA by referencing various industry and government efforts for improving the security of CPSs. There are several industrial and government-led efforts to improve the security of control systems. One of the most important security standards in this space started with the International Society of Automation (ISA) standard ISA 99, which later became a US standard with ANSI 62443 and finally an international cyber security standard for control systems known as IEC 62443 [263].

The US National Institute of Standards and Technology (NIST) has guidelines for security best practices for general IT in Special Publication 800-53. US Federal agencies must meet NIST SP 800-53, but industry in general (and industry dealing with the US government in particular) uses these recommendations as a basis for their security posture. To address the security of control systems in particular, NIST has also published a Guide to Industrial Control System (ICS) Security [150], a guideline to smart grid security in NIST-IR 762 [264], and a guideline for IoT security and privacy [71]. Although these recommendations are not enforceable, they can provide guidance for analysing the security of most utility companies. A more recent effort is the NIST cyber security framework for protecting critical infrastructure, which was initiated by an Executive Order from then US President Obama [265], as an effort to improve the security posture of critical infrastructures.

Another notable industry-led effort for protecting critical infrastructures is the North American Electric Reliability Corporation (NERC) cyber security standards for control systems [152]. NERC is authorised to enforce compliance to these standards, and it is expected that all electric utilities operating the bulk power system in North America are fully compliant with these standards.

All of these standards are general and flexible. Instead of prescribing specific technology solutions, they give a high-level overview of the variety of security technologies available (e.g., authentication, access control, network segmentation, etc.), and then give a set of general procedures for protecting systems, starting with (1) gathering data to identify the attack surface of a given system (this includes a basic network enumeration procedure that seeks to enumerate all devices and services available in the network of the asset owner), (2) building a security policy based on the attack surface of the system, and (3) deploy the security countermeasures, including network segmentation, or network security monitoring.

In addition to these general security standards for control systems, the industries that develop and maintain specific industrial control protocols, such as those used for SCADA, e.g., IEC 104, or those in the process industry, e.g., PROFINET, have also released standards and documentation for securing industrial networks. Recall that most of these industrial protocols were developed before security was a pressing concern for industrial control systems, therefore the communication links were not authenticated or encrypted. The new standard IEC 62351 is meant to guide asset owners on how to deploy a secure network to authenticate and encrypt network links, and other organisations have released similar support, such as, providing security extensions for PROFINET[3]. Instead (or in addition) to using these end-to-end application layer security recommendations, some operators might prefer to use lower-layer security protections of IP networks, including TLS and IPSec.

In the IoT domain, ETSI, the European Standards Organisation developed the first globally-applicable security standard for consumer IoT. ETSI TS 103 645 establishes a security baseline

[3] https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/

for Internet-connected consumer products and provide a basis for future IoT certification. This standard builds closely on the UK's Code of Practice for Consumer IoT Security [266]. Another more specific IoT standard by the Internet Engineering Task Force (IETF) for IoT devices is the Manufacturer Usage Description (MUD) standard [267]. The goal of this standard is to automate the creation of network *white lists*, which are used by network administrators to block any unauthorised connection by the device. Other IoT security standards being developed by the IETF include protocols for communications security, access control, restricting communications, and firmware and software updates [268].

All these industry efforts and standards have essentially three goals: (1) create awareness of security issues in control systems, (2) help operators of control systems and security officers design a security policy, and (3) recommend basic security mechanisms for prevention (authentication, access controls, etc), detection, and response to security breaches. For the most part industry efforts for protecting CPSs are based on the same technical principles from general Information Technology systems. Therefore, industry best practices are behind general IT security best practices and the most recent CPS security research discussed in this KA. We hope that in the next decade CPS security research becomes mature enough to start having an impact on industry practices.

CONCLUSIONS

As technology continues to integrate computing, networking, and control elements in new cyber-physical systems, we also need to train a new generation of engineers, computer scientists, and social scientists to be able to capture the multidisciplinary nature of CPS security, like transduction attacks. In addition, as the technologies behind CPS security mature, some of them will become industry-accepted best practices while others might be forgotten. In 2018, one of the areas with greatest momentum is the industry for network security monitoring (intrusion detection) in cyber-physical networks. Several start-up companies in the US, Europe, and Israel offer services for profiling and characterising industrial networks, to help operators better understand what is allowed and what should be blocked. On the other hand, there are other CPS security research areas that are just starting to be analysed, like the work on attack mitigation, and in particular, the response to alerts from intrusion detection systems.

We are only at the starting point for CPS security research, and the decades to come will bring new challenges as we continue to integrate physical things with computing capabilities.

CROSS-REFERENCE OF TOPICS VS REFERENCE MATERIAL

	[269]	*Other*
1 Cyber-Physical Systems and their Security Risks		
1.1 Characteristics of CPS	c1	[2]
1.2 Protections Against Natural Events and Accidents		[3]
1.3 Security and Privacy Concerns		[4]
2 Crosscutting Security		
2.1 Preventing Attacks	c6,c9	[71]
2.2 Detecting Attacks	c18	[72]
2.3 Mitigating Attacks		[73]
3 CPS Domains		
3.1 Industrial Control Systems		[150]
3.2 Electric Power Grids	c25	[151, 152]
3.3 Transportation Systems and Autonomous Vehicles	c26, c29	[153, 154]
3.4 Robotics and Advanced Manufacturing		[155]
3.5 Medical Devices	c27	[156]
3.6 The Internet of Things		[71]
4 Policy and Political Aspects of CPS Security		
4.1 Incentives and Regulation		[245]
4.2 Cyber-Conflict		[228, 246]
4.3 Industry Practices and Standards		[150]

REFERENCES

[1] T. J. Williams, "The Purdue enterprise reference architecture," *Computers in industry*, vol. 24, no. 2, pp. 141–158, 1994.

[2] E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," *Sensors*, vol. 15, no. 3, pp. 4837–4869, 2015.

[3] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability engineering & system safety*, vol. 139, pp. 156–178, 2015.

[4] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems." in *Proceedings of the 3rd Conference on Hot Topics in Security*. USENIX Association, 2008, pp. 1–6.

[5] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops*. IEEE, 2008, pp. 495–500.

[6] F. Mueller, "Challenges for cyber-physical systems: Security, timing analysis and soft error protection," in *High-Confidence Software Platforms for Cyber-Physical Systems (HCSP-CPS) Workshop, Alexandria, Virginia*, 2006, p. 4.

[7] M. Sun, S. Mohan, L. Sha, and C. Gunter, "Addressing safety and security contradictions in cyber-physical systems," in *Proceedings of the 1st Workshop on Future Directions in Cyber-Physical Systems Security (CPSSW'09)*, 2009.

[8] E. A. Lee, "Cyber-physical systems-are computing foundations adequate," in *Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, vol. 2. Citeseer, 2006.

[9] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, "Security challenges in

next generation cyber physical systems," in *Proceedings of Beyond SCADA: Networked Embedded Control for Cyber Physical Systems*. Academic Press, 2006, pp. 1–4.

[10] H. Tang and B. M. McMillin, "Security property violation in CPS through timing," in *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*. IEEE, 2008, pp. 519–524.

[11] C. Neuman, "Challenges in security for cyber-physical systems," in *DHS Workshop on Future Directions in Cyber-Physical Systems Security*. CPS-VO, 2009, pp. 22–24.

[12] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Workshop on future directions in cyber-physical systems security*, 2009, p. 5.

[13] P. Oman, E. Schweitzer, and D. Frincke, "Concerns about intrusions into remotely accessible substation controllers and scada systems," in *Proceedings of the Twenty-Seventh Annual Western Protective Relay Conference*, vol. 160, 2000.

[14] L. Sha, T. Abdelzaher, K.-E. Årzén, A. Cervin, T. Baker, A. Burns, G. Buttazzo, M. Caccamo, J. Lehoczky, and A. K. Mok, "Real time scheduling theory: A historical perspective," *Real-time systems*, vol. 28, no. 2-3, pp. 101–155, 2004.

[15] J. A. Stankovic and R. Rajkumar, "Real-time operating systems," *Real-Time Systems*, vol. 28, no. 2-3, pp. 237–253, 2004.

[16] M. Felser, "Real-time ethernet-industry prospective," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1118–1129, 2005.

[17] C. Alcaraz and S. Zeadally, "Critical control system protection in the 21st century," *Computer*, vol. 46, no. 10, pp. 74–83, 2013.

[18] J. Song, S. Han, A. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, "Wirelesshart: Applying wireless technology in real-time industrial process control," in *IEEE real-time and embedded technology and applications symposium*. IEEE, 2008, pp. 377–386.

[19] V. C. Gungor, G. P. Hancke *et al.*, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches." *IEEE Trans. Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, 2009.

[20] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, "A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 91–98, 2013.

[21] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *The Journal of Supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.

[22] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology," *Sensors*, vol. 12, no. 9, pp. 11 734–11 753, 2012.

[23] K. Ogata, *Discrete-time control systems*. Prentice Hall Englewood Cliffs, NJ, 1995, vol. 2.

[24] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, 2007.

[25] R. Goebel, R. G. Sanfelice, and A. R. Teel, "Hybrid dynamical systems," *IEEE Control Systems*, vol. 29, no. 2, pp. 28–93, 2009.

[26] A. E. Summers, "Introduction to layers of protection analysis," *Journal of Hazardous Materials*, vol. 104, no. 1-3, pp. 163–168, 2003.

[27] I. Hwang, S. Kim, Y. Kim, and C. E. Seah, "A survey of fault detection, isolation, and reconfiguration methods," *IEEE transactions on control systems technology*, vol. 18, pp. 636–653, 2009.

[28] K. Zhou and J. C. Doyle, *Essentials of robust control*. Prentice hall Upper Saddle River,

NJ, 1998, vol. 104.
[29] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the conference on Computer and communications security (CCS)*. ACM, 2009, pp. 21–32.
[30] A. A. Cardenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proceedings of the ACM symposium on information, computer and communications security*, 2011, pp. 355–366.
[31] B. Krebs. (2008, June) Cyber incident blamed for nuclear power plant shutdown. http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html.
[32] Lloyds, "Business blackout: The insurance implications of a cyber attack on the us power grid," Lloyd's, Tech. Rep., 2015. [Online]. Available: http://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout
[33] A. Greenberg, "Hackers remotely kill a jeep on the highway?with me in it," *Wired*, vol. 7, p. 21, 2015.
[34] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, "All your GPS are belong to us: Towards stealthy manipulation of road navigation systems," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1527–1544.
[35] J. Valente and A. A. Cardenas, "Understanding security threats in consumer drones through the lens of the discovery quadcopter family," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. ACM, 2017, pp. 31–36.
[36] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 3, pp. 73–83, 2009.
[37] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2009, pp. 31–45.
[38] M. Krotofil, A. Cardenas, J. Larsen, and D. Gollmann, "Vulnerabilities of cyber-physical systems to stale data?determining the optimal time to launch attacks," *International journal of critical infrastructure protection*, vol. 7, no. 4, pp. 213–232, 2014.
[39] S. McLaughlin, "CPS: Stateful policy enforcement for control system device usage," in *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*. New York, NY, USA: ACM, 2013, pp. 109–118.
[40] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, Oct 2012, pp. 1806–1813.
[41] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—Part I: analysis and experimentation of stealthy deception attacks," *Control Systems Technology, IEEE Transactions on*, vol. 21, no. 5, pp. 1963–1970, 2013.
[42] A. Jakaria, W. Yang, B. Rashidi, C. Fung, and M. A. Rahman, "VFence: A defense against distributed denial of service attacks using network function virtualization," in *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual*, vol. 2. IEEE, 2016, pp. 431–436.
[43] K. Zetter. (2016, mar) Inside the cunning, unprecedented hack of ukraine's power grid. WIRED magazine. [Online]. Available: http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[44] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software

radio attacks and zero-power defenses," in *IEEE Symposium on Security and Privacy*, 2008.
[45] K. Fu and W. Xu, "Risks of trusting the physics of sensors," *Communications of the ACM*, vol. 61, no. 2, pp. 20–23, 2018.
[46] I. Giechaskiel and K. B. Rasmussen, "SoK: Taxonomy and challenges of out-of-band signal injection attacks and defenses," *CoRR*, vol. abs/1901.06935, 2019. [Online]. Available: http://arxiv.org/abs/1901.06935
[47] Y. M. Son, H. C. Shin, D. K. Kim, Y. S. Park, J. H. Noh, K. B. Choi, J. W. Choi, and Y. D. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," in *24th USENIX Security symposium*. USENIX Association, 2015.
[48] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, M. Mina *et al.*, "Electromagnetic induction attacks against embedded systems," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. ACM, 2018, pp. 499–510.
[49] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "DolphinAttack: Inaudible voice commands," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 103–117.
[50] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard law review*, pp. 193–220, 1890.
[51] R. J. Turk, "Cyber incidents involving control systems," Idao National Laboratory, Tech. Rep. INL/EXT-05-00671, October 2005.
[52] R. Esposito. (2006, October) Hackers penetrate water system computers. [Online]. Available: https://www.computerworld.com/article/2547938/hackers-break-into-water-system-network.html
[53] K. Hemsley and R. Fisher, "A history of cyber incidents and threats involving industrial control systems," in *International Conference on Critical Infrastructure Protection*. Springer, 2018, pp. 215–242.
[54] T. Reed, *At the Abyss: An Insider's History of the Cold War*. Presidio Press, March 2004.
[55] M. Abrams and J. Weiss, "Malicious control system cyber security attack case study–maroochy water services, australia," The MITRE Corporation, Tech. Rep., 2008.
[56] N. Sayfayn and S. Madnick, "Cybersafety analysis of the Maroochy shire sewage spill," Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, Massachusetts Institute of Technology, Working Paper CISL#2017-09, 2017.
[57] AP, "Revenge hacker: 34 months, must repay Georgia-Pacific $1m," February 2017. [Online]. Available: https://www.usnews.com/news/louisiana/articles/2017-02-16/revenge-hacker-34-months-must-repay-georgia-pacific-1m
[58] D. Bilefsky. (2017, January) Hackers use new tactic at Austrian hotel: Locking the doors. The New York Times.
[59] B. Krebs, "FBI: smart meter hacks likely to spread," April 2012. [Online]. Available: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/
[60] M. Dalli, *Enemalta employees suspended over 1,000 tampered smart meters*. https://www.maltatoday.com.mt/news/national/35650/enemalta-employees-suspended-over-1-000-tampered-smart-meters-20140211: Malta Today, February 2014.
[61] R. M. Lee, M. J. Assante, and T. Conway, "German steel mill cyber attack," *Industrial Control Systems*, vol. 30, p. 62, 2014.
[62] "United States Attorney, Eastern District of California. Willows man arrested for hacking into Tehama Colusa Canal Authority computer system," November 2007. [Online]. Available: https://www.computerworld.com/article/2540235/insider-charged-with-hacking-california-canal-system.html

[63] "United States Attorney, Eastern District of California. Sacramento man pleads guilty to attempting ot shut down california's power grid," November 2007. [Online]. Available: http://www.usdoj.gov/usao/cae/press_releases/docs/2007/12-14-07DenisonPlea.pdf
[64] D. Kravets. (2009, March) Feds: Hacker disabled offshore oil platform leak-detection system. http://www.wired.com/threatlevel/2009/03/feds-hacker-dis/.
[65] J. Leyden. (2008, 11th Jan) Polish teen derails tram after hacking train network. http://www.theregister.co.uk/2008/01/11/tram_hack/.
[66] K. Zetter, *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Broadway books, 2014.
[67] Booz Allen Hamilton, "When the lights went out: Ukraine cybersecurity threat briefing," p. 20, 2016. [Online]. Available: http://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-wentout
[68] A. Greenberg, "'Crash override': The malware that took down a power grid," *Wired Magazine*, pp. 09–20, 2017.
[69] A. Cherepanov, "Win32/industroyer, a new threat for industrial control systems," *White Paper. ESET*, 2017.
[70] M. Giles, "Triton is the world's most murderous malware, and it's spreading," 2019. [Online]. Available: https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/
[71] K. Boeckl, M. Fagan, W. Fisher, N. Lefkovitz, K. Megas, E. Nadeau, B. Piccarreta, D. G. O'Rourke, and K. Scarfone, "Considerations for managing internet of things (IoT) cybersecurity and privacy risks," *National Institute of Standards and Technology, NISTIR 8228*, 2018.
[72] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, p. 76, 2018.
[73] R. Langner, *Robust Control System Networks: How to Achieve Reliable Control After Stuxnet*. Momentum Press, 2011.
[74] R. Antrobus, B. Green, S. Frey, and A. Rashid, "The forgotten I in IIoT: A vulnerability scanner for industrial internet of things," in *Living in the Internet of Things 2019*, 4 2019.
[75] P. Ralston, J. Graham, and J. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA transactions*, vol. 46, no. 4, pp. 583–594, 2007.
[76] P. Craig, J. Mortensen, and J. Dagle, "Metrics for the National SCADA Test Bed Program," PNNL-18031, Pacific Northwest National Laboratory (PNNL), Richland, WA (US), Tech. Rep., 2008.
[77] G. Hamoud, R. Chen, and I. Bradley, "Risk assessment of power systems SCADA," in *IEEE Power Engineering Society General Meeting, 2003*, vol. 2, 2003.
[78] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & security*, vol. 56, pp. 1–27, 2016.
[79] P. Burnap, *The Cyber Security Body of Knowledge*. University of Bristol, 2021, ch. Risk Management & Governance, version 1.1.1. [Online]. Available: https://www.cybok.org/
[80] J. H. Castellanos, M. Ochoa, and J. Zhou, "Finding dependencies between cyber-physical domains for security testing of industrial control systems," in *Proceedings of the 34th Annual Computer Security Applications Conference*. ACM, 2018, pp. 582–594.
[81] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, Stockholm, Sweden*, 2010.
[82] U. Vaidya and M. Fardad, "On optimal sensor placement for mitigation of vulnerabilities

to cyber attacks in large-scale networks," in *Proceedings of the 2013 European Control Conference (ECC)*, July 2013, pp. 3548–3553.

[83] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1108–1118, July 2012.

[84] H. Okhravi and F. T. Sheldon, "Data diodes in support of trustworthy cyber infrastructure," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*. ACM, 2010, p. 23.

[85] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 147–159, 2011.

[86] R. Anderson and S. Fuloria, "Security economics and critical national infrastructure," in *Economics of Information Security and Privacy*. Springer, 2010, pp. 55–66.

[87] J. H. Castellanos, D. Antonioli, N. O. Tippenhauer, and M. Ochoa, "Legacy-compliant data authentication for industrial control system traffic," in *International Conference on Applied Cryptography and Network Security*. Springer, 2017, pp. 665–685.

[88] P. P. Tsang and S. W. Smith, "YASIR: A low-latency high-integrity security retrofit for lecacy SCADA systems," in *23rd International Information Security Conference (IFIC SEC)*, September 2008, pp. 445–459.

[89] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proceedings of the ACM SIGCOMM 2011 Conference*, ser. SIGCOMM '11. New York, NY, USA: ACM, 2011, pp. 2–13.

[90] K. Fawaz, K.-H. Kim, and K. G. Shin, "Protecting privacy of BLE device users." in *USENIX Security Symposium*, 2016, pp. 1205–1221.

[91] R. Roman, C. Alcaraz, and J. Lopez, "A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes," *Mobile Networks and Applications*, vol. 12, no. 4, pp. 231–244, 2007.

[92] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, "Nistir 8114: Draft report on lightweight cryptography," *Available on the NIST website: http://csrc. nist. gov/publications/drafts/nistir-8114/nistir_8114_draft. pdf*, 2016.

[93] S. Koteshwara and A. Das, "Comparative study of authenticated encryption targeting lightweight IoT applications," *IEEE Design & Test*, vol. 34, no. 4, pp. 26–33, 2017.

[94] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577–601, 2016.

[95] A. Abbasi, J. Wetzels, T. Holz, and S. Etalle, "Challenges in designing exploit mitigations for deeply embedded systems," in *Proceedings of the 2019 IEEE European Symposium on Security and Privacy*. IEEE, 2019.

[96] United States Department of Defense, *Department of Defense, Trusted Computer System Evaluation Criteria*, ser. Rainbow Series. Dept. of Defense, 1985, no. 5200.28-STD. [Online]. Available: https://books.google.nl/books?id=-KBPAAAAMAAJ

[97] G. Klein, K. Elphinstone, G. Heiser, J. Andronick, D. Cock, P. Derrin, D. Elkaduwe, K. Engelhardt, R. Kolanski, M. Norrish, T. Sewell, H. Tuch, and S. Winwood, "seL4: formal verification of an OS kernel," in *Proceedings of the ACM SIGOPS 22Nd Symposium on Operating Systems Principles*, ser. SOSP '09. New York, NY, USA: ACM, 2009, pp. 207–220. [Online]. Available: http://doi.acm.org/10.1145/1629575.1629596

[98] K. Fisher, J. Launchbury, and R. Richards, "The HACMS program: using formal methods to eliminate exploitable bugs," *Phil. Trans. R. Soc. A*, vol. 375, no. 2104, p. 20150401, 2017.

[99] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on*. IEEE, 2017, pp. 3–18.

[100] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost Talk: Mitigating EMI signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy*, May 2013, pp. 145–159.

[101] X. Carpent, K. Eldefrawy, N. Rattanavipanon, A.-R. Sadeghi, and G. Tsudik, "Reconciling remote attestation and safety-critical operation on simple iot devices," in *2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC)*. IEEE, 2018, pp. 1–6.

[102] M. Ambrosin, M. Conti, A. Ibrahim, G. Neven, A.-R. Sadeghi, and M. Schunter, "SANA: secure and scalable aggregate network attestation," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 731–742.

[103] V. P. Illiano, R. V. Steiner, and E. C. Lupu, "Unity is strength!: Combining attestation and measurements inspection to handle malicious data injections in WSNs," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2017, pp. 134–144.

[104] R. V. Steiner and E. Lupu, "Attestation in wireless sensor networks: A survey," *ACM Computing Surveys (CSUR)*, vol. 49, no. 3, p. 51, 2016.

[105] K. Eldefrawy, G. Tsudik, A. Francillon, and D. Perito, "SMART: secure and minimal architecture for (establishing dynamic) root of trust," in *19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5-8, 2012*, 2012.

[106] K. Eldefrawy, N. Rattanavipanon, and G. Tsudik, "Hydra: hybrid design for remote attestation (using a formally verified microkernel)," in *Proceedings of the 10th ACM Conference on Security and Privacy in wireless and Mobile Networks*. ACM, 2017, pp. 99–110.

[107] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using model-based intrusion detection for SCADA networks," in *Proceedings of the SCADA Security Scientific Symposium*, Miami Beach, FL, USA, 2007.

[108] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *Proceedings of Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE, 2011, pp. 184–193.

[109] N. Goldenberg and A. Wool, "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems," *International Journal of Critical Infrastructure Protection*, vol. 6, pp. 63–75, 2013.

[110] C. Markman, A. Wool, and A. A. Cardenas, "Temporal phase shifts in SCADA networks," in *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*. ACM, 2018, pp. 84–89.

[111] M. Caselli, E. Zambon, and F. Kargl, "Sequence-aware intrusion detection in industrial control systems," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, 2015, pp. 13–24.

[112] M. Faisal, A. A. Cardenas, and A. Wool, "Modeling Modbus TCP for intrusion detection," in *Communications and Network Security (CNS), 2016 IEEE Conference on*. IEEE, 2016, pp. 386–390.

[113] W. Aoudi, M. Iturbe, and M. Almgren, "Truth will out: Departure-based process-level detection of stealthy attacks on control systems," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 817–831.

[114] D. Hadžiosmanović, R. Sommer, E. Zambon, and P. H. Hartel, "Through the eye of the

PLC: semantic security monitoring for industrial processes," in *Proceedings of the 30th Annual Computer Security Applications Conference*. ACM, 2014, pp. 126–135.

[115] Y. Chen, C. M. Poskitt, and J. Sun, "Learning from mutants: Using code mutation to learn and monitor invariants of a cyber-physical system," *IEEE Symposium on Security and Privacy*, 2018.

[116] D. I. Urbina, J. A. Giraldo, A. A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg, "Limiting the impact of stealthy attacks on industrial control systems," in *Proceedings of the Conference on Computer and Communications Security (CCS)*. ACM, 2016, pp. 1092–1105.

[117] K. Paridari, N. O'Mahony, A. E.-D. Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg, "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 113–128, 2018.

[118] Q. Gu, D. Formby, S. Ji, H. Cam, and R. Beyah, "Fingerprinting for cyber-physical system security: Device physics matters too," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 49–59, 2018.

[119] A. Petropulu, K. I. Diamantaras, Z. Han, D. Niyato, and S. Zonouz, "Contactless monitoring of critical infrastructure [from the guest editors]," *IEEE Signal Processing Magazine*, vol. 36, no. 2, pp. 19–21, 2019.

[120] T. Shekari, C. Bayens, M. Cohen, L. Graber, and R. Beyah, "RFDIDS: Radio frequency-based distributed intrusion detection system for the power grid." in *NDSS*, 2019.

[121] W. Jardine, S. Frey, B. Green, and A. Rashid, "Senami: Selective non-invasive active monitoring for ics intrusion detection," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*. ACM, 2016, pp. 23–34.

[122] T. Roth and B. McMillin, "Physical attestation of cyber processes in the smart grid," in *International Workshop on Critical Information Infrastructures Security*. Springer, 2013, pp. 96–107.

[123] J. Valente, C. Barreto, and A. A. Cárdenas, "Cyber-physical systems attestation," in *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*. IEEE, 2014, pp. 354–357.

[124] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proceedings of Workshop on Secure Control Systems*, 2010.

[125] J. Valente and A. A. Cárdenas, "Using visual challenges to verify the integrity of security cameras," in *Proceedings of the 31st Annual Computer Security Applications Conference*. ACM, 2015, pp. 141–150.

[126] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs," *Control Systems, IEEE*, vol. 35, no. 1, pp. 93–109, 2015.

[127] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proceedings of the First ACM Workshop on Moving Target Defense*. ACM, 2014, pp. 59–68.

[128] J. Rowe, K. N. Levitt, T. Demir, and R. Erbacher, "Artificial diversity as maneuvers in a control theoretic moving target defense," in *National Symposium on Moving Target Research*, 2012.

[129] J. Giraldo and A. A. Cardenas, "Moving target defense for attack mitigation in multi-vehicle systems," in *Proactive and Dynamic Network Defense*. Springer, 2019, pp. 163–190.

[130] J. Giraldo, A. Cardenas, and R. G. Sanfelice, "A moving target defense to reveal cyber-attacks in CPS and minimize their impact," in *American Control Conference*, 2019.

[131] C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: Next generation design research," in *2009 2nd Conference on Human System Interactions*. IEEE, 2009, pp. 632–636.
[132] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *Automatic Control, IEEE Transactions on*, vol. 60, no. 4, pp. 1145–1151, April 2015.
[133] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.
[134] D. Wijayasekara, O. Linda, M. Manic, and C. Rieger, "FN-DFE: Fuzzy-neural data fusion engine for enhanced resilient state-awareness of hybrid energy systems," *IEEE transactions on cybernetics*, vol. 44, no. 11, pp. 2065–2075, 2014.
[135] E. P. Blasch, D. A. Lambert, P. Valin, M. M. Kokar, J. Llinas, S. Das, C. Chong, and E. Shahbazian, "High level information fusion (HLIF): Survey of models, issues, and grand challenges," *IEEE Aerospace and Electronic Systems Magazine*, vol. 27, no. 9, pp. 4–20, 2012.
[136] E. Blasch, I. Kadar, J. Salerno, M. M. Kokar, S. Das, G. M. Powell, D. D. Corkill, and E. H. Ruspini, "Issues and challenges of knowledge representation and reasoning methods in situation assessment (level 2 fusion)," in *Signal Processing, Sensor Fusion, and Target Recognition XV*, vol. 6235. International Society for Optics and Photonics, 2006, p. 623510.
[137] A. F. M. Piedrahita, V. Gaur, J. Giraldo, A. A. Cardenas, and S. J. Rueda, "Virtual incident response functions in control systems," *Computer Networks*, vol. 135, pp. 147–159, 2018.
[138] S. H. Kafash, J. Giraldo, C. Murguia, A. A. Cardenas, and J. Ruths, "Constraining attacker capabilities through actuator saturation," in *2018 Annual American Control Conference (ACC)*. IEEE, 2018, pp. 986–991.
[139] M. Arroyo, H. Kobayashi, S. Sethumadhavan, and J. Yang, "FIRED: frequent inertial resets with diversification for emerging commodity cyber-physical systems," *arXiv preprint arXiv:1702.06595*, 2017.
[140] F. Abdi, C.-Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Guaranteed physical security with restart-based design for cyber-physical systems," in *Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems*. IEEE Press, 2018, pp. 10–21.
[141] L. F. Combita, J. A. Giraldo, A. A. Cardenas, and N. Quijano, "Dddas for attack detection and isolation of control systems," in *Handbook of Dynamic Data Driven Applications Systems*. Springer, 2018, pp. 407–422.
[142] A. Farraj, E. Hammad, A. A. Daoud, and D. Kundur, "A game-theoretic control approach to mitigate cyber switching attacks in smart grid systems," in *Proceedings of the IEEE Smart Grid Communications*, Venice, Italy, 2014, pp. 958–963.
[143] C. Barreto, A. A. Cárdenas, and N. Quijano, "Controllability of dynamical systems: Threat models and reactive security," in *Decision and Game Theory for Security*. Springer, 2013, pp. 45–64.
[144] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2015, pp. 747–755.
[145] Y. Yuan, F. Sun, and H. Liu, "Resilient control of cyber-physical systems against intelligent attacker: a hierarchal stackelberg game approach," *To appear on International Journal of Systems Science*, 2015.
[146] A. Barth, B. Rubinstein, M. Sundararajan, J. Mitchell, D. Song, and P. Bartlett, "A learning-based approach to reactive security," *IEEE Transactions on Dependable and Secure Com-*

puting, vol. 9, no. 4, pp. 482–493, July 2012.

[147] D. Shelar and S. Amin, "Analyzing vulnerability of electricity distribution networks to der disruptions," in *American Control Conference (ACC), 2015*, 2015, pp. 2461–2468.

[148] L. Sha, "Using simplicity to control complexity," *IEEE Software*, vol. 18, no. 4, pp. 20–28, Jul 2001.

[149] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): authentication for implanted medical devices," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 1099–1112.

[150] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, "Guide to industrial control systems (ICS) security: Supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (plc)," NIST, Tech. Rep. Special Publication 800-82: Revision 2, May 2015.

[151] T. Koppel, *Lights out: a cyberattack, a nation unprepared, surviving the aftermath*. Broadway Books, 2016.

[152] NERC-CIP, *Critical Infrastructure Protection*. North American Electric Reliability Corporation, 2008. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[153] F. Sakiz and S. Sen, "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[154] B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, "Sok-security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps," *arXiv preprint arXiv:1903.05155*, 2019.

[155] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," *Manufacturing Letters*, vol. 2, no. 2, pp. 74–77, 2014.

[156] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *Security and Privacy (SP), 2014 IEEE Symposium on*. IEEE, 2014, pp. 524–539.

[157] C. Alcaraz, G. Fernandez, and F. Carvajal, "Security aspects of SCADA and DCS environments," in *Critical Infrastructure Protection*. Springer, 2012, pp. 120–149.

[158] M. Iturbe, I. Garitano, U. Zurutuza, and R. Uribeetxeberria, "Towards large-scale, heterogeneous anomaly detection systems in industrial networks: A survey of current trends," *Security and Communication Networks*, vol. 2017, 2017.

[159] I. Garitano, C. Siaterlis, B. Genge, R. Uribeetxeberria, and U. Zurutuza, "A method to construct network traffic models for process control systems," in *Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012)*. IEEE, 2012, pp. 1–8.

[160] C. Feng, V. R. Palleti, A. Mathur, and D. Chana, "A systematic framework to generate invariants for anomaly detection in industrial control systems." in *NDSS*, 2019.

[161] C. M. Ahmed, J. Zhou, and A. P. Mathur, "Noise matters: Using sensor and process noise fingerprint to detect stealthy cyber attacks and authenticate sensors in CPS," in *Proceedings of the 34th Annual Computer Security Applications Conference*. ACM, 2018, pp. 566–581.

[162] J. Giraldo, D. Urbina, A. A. Cardenas, and N. O. Tippenhauer, "Hide and seek: An architecture for improving attack-visibility in industrial control systems," in *International Conference on Applied Cryptography and Network Security*. Springer, 2019, pp. 175–195.

[163] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," SANS Industrial Control Systems, Tech. Rep., 03 2016. [Online]. Available:

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[164] R. Langner, "To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve," *Arlington, VA: Langner Group*, vol. 7, p. 21, 2013. [Online]. Available: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
[165] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2012, pp. 1806–1813.
[166] M. Parvania, G. Koutsandria, V. Muthukumary, S. Peisert, C. McParland, and A. Scaglione, "Hybrid control network intrusion detection systems for automated power distribution systems," in *Proceedings of Conference on Dependable Systems and Networks (DSN)*, June 2014, pp. 774–779.
[167] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParland, and A. Scaglione, "A hybrid network IDS for protective digital relays in the power transmission grid," in *Proceedings of Conference on Smart Grid Communications (SmartGridComm)*, 2014.
[168] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Semantic security analysis of SCADA networks to detect malicious control commands in power grids," in *Proceedings of the first ACM workshop on Smart energy grid security*. ACM, 2013, pp. 29–34.
[169] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in SCADA systems," *Industrial Informatics, IEEE Transactions on*, vol. 7, no. 2, pp. 179–186, 2011.
[170] A. Le, U. Roedig, and A. Rashid, "Lasarus: Lightweight attack surface reduction for legacy industrial control systems," in *International Symposium on Engineering Secure Software and Systems*. Springer, 2017, pp. 36–52.
[171] A. Keliris and M. Maniatakos, "ICSREF: A framework for automated reverse engineering of industrial control systems binaries," *NDSS*, 2018.
[172] S. McLaughlin, S. Zonouz, D. Pohly, and P. McDaniel, "A trusted safety verifier for process controller code," in *Proceedings of the ISOC Network and Distributed Systems Security Symposium (NDSS)*, 2014.
[173] M. Krotofil and D. Gollmann, "Industrial control systems security: What is happening?" in *2013 11th IEEE International Conference on Informatics (INDIN)*, July 2013, pp. 670–675.
[174] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *International journal of critical infrastructure protection*, vol. 9, pp. 52–80, 2015.
[175] B. Green, A. Lee, R. Antrobus, U. Roedig, D. Hutchison, and A. Rashid, "Pains, gains and PLCs: ten lessons from building an industrial control systems testbed for security research," in *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*, 2017.
[176] G. Constable and B. Somerville, Eds., *A Century of Innovation: Twenty Engineering Achievements that Transformed our Lives*. Washington, DC: The National Academies Press, 2003. [Online]. Available: https://www.nap.edu/catalog/10726/a-century-of-innovation-twenty-engineering-achievements-that-transformed-our
[177] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.
[178] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," in *Proceedings of IFAC World Congress*, vol. 18, no. 1, 2011, pp. 11 271–11 277.
[179] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *First IEEE Smart Grid Commnunications Conference (SmartGrid-*

Comm), October 2010.

[180] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," in *First IEEE Smart Grid Communications Conference (SmartGridComm)*, October 2010.

[181] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proceedings of Conference on Decision and Control (CDC)*. IEEE, 2010, pp. 5991–5998.

[182] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures$^{\pi}$," in *Proceedings of Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2011, pp. 232–237.

[183] M. A. Rahman, E. Al-Shaer, M. Rahman *et al.*, "A formal model for verifying stealthy attacks on state estimation in power grids," in *Proceedings of Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2013, pp. 414–419.

[184] A. A. Cárdenas and R. Safavi-Naini, "Security and privacy in the smart grid," *Handbook on Securing Cyber-Physical Critical Infrastructure.*, pp. 637–654, 2012.

[185] Government Accountability Office, "Electricity grid modernization. progress being made on cybersecurity guidelines, but key challenges remain to be addressed," January 2011. [Online]. Available: https://www.gao.gov/new.items/d11117.pdf

[186] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *IEEE Security & Privacy Magazine*, vol. 8, no. 1, pp. 11–20, January/February 2010.

[187] X. Liao, D. Formby, C. Day, and R. A. Beyah, "Towards secure metering data analysis via distributed differential privacy," in *44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2014, Atlanta, GA, USA, June 23-26, 2014*, 2014, pp. 780–785. [Online]. Available: http://dx.doi.org/10.1109/DSN.2014.82

[188] R. Tan, V. Badrinath Krishna, D. K. Yau, and Z. Kalbarczyk, "Impact of integrity attacks on real-time pricing in smart grids," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 439–450.

[189] C. Barreto, A. A. Cárdenas, N. Quijano, and E. Mojica-Nava, "CPS: Market analysis of attacks against demand response in the smart grid," in *Proceedings of the 30th Annual Computer Security Applications Conference*. ACM, 2014, pp. 136–145.

[190] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862–2872, 2018.

[191] J. Giraldo, A. Cárdenas, and N. Quijano, "Integrity attacks on real-time pricing in smart grids: impact and countermeasures," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2249–2257, 2016.

[192] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[193] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, "Implementing attacks for Modbus/TCP protocol in a real-time cyber physical system test bed," in *Communications Quality and Reliability (CQR), 2015 IEEE International Workshop Technical Committee on*. IEEE, 2015, pp. 1–6.

[194] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers," in *Proceedings of the Seventh International Conference on the Internet of Things*. ACM, 2017, p. 13.

[195] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can

disrupt the power grid," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 15–32.

[196] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against IoT demand attacks," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019.

[197] R. Herring, A. Hofleitner, S. Amin, T. Nasr, A. Khalek, and A. Bayen, "Using mobile phones to forecast arterial traffic through statistical learning," in *Proc. of the 89th Annual Meeting of the Transportation Research Board (TRB)*, 2010, pp. 1–22.

[198] Texas Transportation Institute, "Annual Urban Mobility Report." 2010, http://mobility.tamu.edu/ums.

[199] E. De Cristofaro and C. Soriente, "Participatory privacy: Enabling privacy in participatory sensing," *IEEE Network*, vol. 27, no. 1, pp. 32–36, 2013.

[200] C.-L. Huang, Y. Fallah, R. Sengupta, and H. Krishnan, "Intervehicle transmission rate control for cooperative active safety system," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 12, no. 3, pp. 645 –658, sept. 2011.

[201] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 901–914.

[202] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: analyzing the security of traffic infrastructure," in *8th USENIX Workshop on Offensive Technologies (WOOT 14)*, 2014.

[203] (2014, October 28) Sensys networks traffic sensor vulnerabilities (Update A). https://ics-cert.us-cert.gov/advisories/ICSA-14-247-01A.

[204] (2014, March 31) Israeli students spoof waze app with fake traffic jam. http://www.popsci.com/article/gadgets/israeli-students-spoof-waze-app-fake-traffic-jam.

[205] M. T. Garip, M. E. Gursoy, P. Reiher, and M. Gerla, "Congestion attacks to autonomous cars using vehicular botnets," in *NDSS Workshop on Security of Emerging Networking Technologies (SENT), San Diego, CA*, 2015.

[206] G. Wang, B. Wang, T. Wang, A. Nika, H. Zheng, and B. Y. Zhao, "Defending against sybil devices in crowdsourced mapping services," in *Accepted in the 14th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'16)*, 2016.

[207] (2016, June 5) Traffic-weary homeowners and waze are at war, again. guess who?s winning? https://www.washingtonpost.com/local/traffic-weary-homeowners-and-waze-are-at-war-again-guess-whos-winning/2016/06/05/c466df46-299d-11e6-b989-4e5479715b54_story.html.

[208] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty, "Future e-enabled aircraft communications and security: The next 20 years and beyond," *Proceedings of the IEEE*, vol. 99, no. 11, pp. 2040–2055, 2011.

[209] A. Costin and A. Francillon, "Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," *Black Hat USA*, pp. 1–12, 2012.

[210] E. J. Weyuker, "Testing component-based software: A cautionary tale," *IEEE software*, vol. 15, no. 5, pp. 54–59, 1998.

[211] D. Jenkins and B. Vasigh, *The economic impact of unmanned aircraft systems integration in the United States*. Association for Unmanned Vehicle Systems International (AUVSI), 2013.

[212] (2017) Gartner predicts 3 million drones to be shipped in 2017. [Online]. Available: https://dronelife.com/2017/02/10/gartner-predicts-3-million-drones-shipped-2017/

[213] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A

survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, p. 7, 2016.
[214] R. J. Rosen, "So this is how it begins: Guy refuses to stop drone-spying on seattle woman," 2013. [Online]. Available: https://www.theatlantic.com/technology/archive/2013/05/so-this-is-how-it-begins-guy-refuses-to-stop-drone-spying-on-seattle-woman/275769/
[215] B. Schneier, "Is it OK to shoot down a drone over your backyard?" 2015. [Online]. Available: https://www.cnn.com/2015/09/09/opinions/schneier-shoot-down-drones/
[216] O. B. Waxman, "World's most embarrassing dad has drone follow daughter to school," 2015. [Online]. Available: https://time.com/3831431/dad-daughter-drone-school/
[217] D. Davidson, H. Wu, R. Jellinek, T. Ristenpart, and V. Singh, "Controlling UAVs with sensor input spoofing attacks," in *Proceedings of the 10th USENIX Conference on Offensive Technologies*, ser. WOOT'16. Berkeley, CA, USA: USENIX Association, 2016, pp. 221–231.
[218] M. Diulio, C. Savage, B. Finley, and E. Schneider, "Taking the integrated condition assessment system to the year 2010," in *13th Int. Ship Control Systems Symposium, Orlando, FL*, 2003.
[219] M. Diulio, R. Halpin, M. Monaco, H. Chin, T. Hekman, and F. Dugie, "Advancements in equipment remote monitoring programs–providing optimal fleet support in a cyber-safe environment," *Naval Engineers Journal*, vol. 127, no. 3, pp. 109–118, 2015.
[220] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010, pp. 447–462.
[221] S. Nürnberger and C. Rossow, "–vatiCAN–vetted, authenticated CAN bus," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2016, pp. 106–124.
[222] K.-T. Cho and K. G. Shin, "Viden: Attacker identification on in-vehicle networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 1109–1123.
[223] S. U. Sagong, X. Ying, A. Clark, L. Bushnell, and R. Poovendran, "Cloaking the clock: emulating clock skew in controller area networks," in *Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems*. IEEE Press, 2018, pp. 32–42.
[224] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ACM, 2015, pp. 167–178.
[225] K. Poulsen. (2010, March) Hacker disables more than 100 cars remotely. WIRED. [Online]. Available: https://www.wired.com/2010/03/hacker-bricks-cars/
[226] Y. Pan, J. White, D. C. Schmidt, A. Elhabashy, L. Sturm, J. Camelio, and C. Williams, "Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems," *International Journal of Interactive Multimedia and Artificial Inteligence*, vol. 4, no. Special Issue on Advances and Applications in the Internet of Things and Cloud Computing, 2017.
[227] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin, and S. Zanero, "An experimental security analysis of an industrial robot controller," in *2017 38th IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 268–286.
[228] P. W. Singer, *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin, 2009.
[229] N. G. Leveson and C. S. Turner, "An investigation of the Therac-25 accidents," *IEEE computer*, vol. 26, no. 7, pp. 18–41, 1993.
[230] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable

medical devices: A comprehensive survey," *Journal of biomedical informatics*, vol. 55, pp. 272–289, June 2015.

[231] E. Marin, D. Singelée, B. Yang, V. Volski, G. A. Vandenbosch, B. Nuttin, and B. Preneel, "Securing wireless neurostimulators," in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*. ACM, 2018, pp. 287–298.

[232] M.-Z. Poh, D. J. McDuff, and R. W. Picard, "Advancements in noncontact, multiparameter physiological measurements using a webcam," *IEEE transactions on biomedical engineering*, vol. 58, no. 1, pp. 7–11, 2010.

[233] D. Hambling, "The Pentagon has a laser that can identify people from a distance by their heartbeat," *MIT Technology Review*, 2019.

[234] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[235] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[236] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the Mirai botnet," in *USENIX Security Symposium*, 2017, pp. 1092–1110.

[237] L. Mathews, "Criminals Hacked A Fish Tank To Steal Data From A Casino," 2017. [Online]. Available: https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/#5dba8c4632b9

[238] K. Albrecht and L. Mcintyre, "Privacy nightmare: When baby monitors go bad [opinion]," *IEEE Technology and Society Magazine*, vol. 34, no. 3, pp. 14–19, 2015.

[239] D. Goldman, "Shodan: The scariest search engine," Apr. 2013. [Online]. Available: https://money.cnn.com/2013/04/08/technology/security/shodan/

[240] J. Valente, M. A. Wynn, and A. A. Cardenas, "Stealing, spying, and abusing: Consequences of attacks on internet of things devices," *IEEE Security Privacy*, vol. 17, no. 5, pp. 10–21, Sep. 2019.

[241] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, and F. Qian, "Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems," in *Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems*. IEEE, 2019, p. 0.

[242] A. K. Simpson, F. Roesner, and T. Kohno, "Securing vulnerable home IoT devices with an in-hub security manager," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 2017, pp. 551–556.

[243] W. Zhang, Y. Meng, Y. Liu, X. Zhang, Y. Zhang, and H. Zhu, "Homonit: Monitoring smart home apps from encrypted traffic," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 1074–1088.

[244] J. Wilson, R. S. Wahby, H. Corrigan-Gibbs, D. Boneh, P. Levis, and K. Winstein, "Trust but verify: Auditing the secure internet of things," in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2017, pp. 464–474.

[245] B. Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. WW. Norton & Company, September 2018.

[246] M. Schmitt, "International law in cyberspace: The Koh Speech and the Tallinn manual juxtaposed," *Harvard International Law Journal Online*, vol. 13, 2012.

[247] Energy Sector Control Systems Working Group, "Roadmap to achieve energy delivery systems cybersecurity," U.S. Department of Energy, Tech.

Rep., 2011. [Online]. Available: https://www.energy.gov/ceser/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011
[248] B. Schneier, "The internet of things will upend our industry," *IEEE Security and Privacy*, vol. 15, no. 2, pp. 108–108, 2017.
[249] K. Fu. (2016) Infrastructure disruption: Internet of things security. U.S. House of Representatives. [Online]. Available: http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-FuK-20161116.pdf
[250] M. Y. Vardi, "Cyber insecurity and cyber libertarianism," *Communications of the ACM*, vol. 60, no. 5, pp. 5–5, 2017.
[251] M. Schallbruch, "The european network and information security directive–a cornerstone of the digital single market," in *Digital Marketplaces Unleashed*. Springer, 2018, pp. 287–295.
[252] "Security assessment principles for the civil nuclear industry," 2017.
[253] M. Daniel. (2013) Incentives to support adoption of the cybersecurity framework. https://obamawhitehouse.archives.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.
[254] Department of Homeland Security Integrated Task Force, "Executive order 13636: Improving critical infrastructure cybersecurity," https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf, Department of Homeland Security, Tech. Rep., 2013.
[255] (2014) Protection of critical infrastructure. European Commission. [Online]. Available: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en
[256] T. Augustinos, L. Bauer, A. Cappelletti, J. Chaudhery, I. Goddijn, L. Heslault, N. Kalfigkopoulos, V. Katos, N. Kitching, M. Krotofil *et al.*, "Cyber insurance: recent advances, good practices & challenges," *European Union Agency For Network and Information Security (ENISA)*, 2016.
[257] I. Ehrlich and G. S. Becker, "Market insurance, self-insurance, and self-protection," *Journal of political Economy*, vol. 80, no. 4, pp. 623–648, 1972.
[258] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," in *Critical Infrastructure Protection*, vol. 253/2007. Springer Boston, November 2007, pp. 73–82.
[259] P. J. Denning and D. E. Denning, "Discussing cyber attack," *Communications of the ACM*, vol. 53, no. 9, pp. 29–31, 2010.
[260] A. K. Cebrowski and J. J. Garstka, "Network-centric warfare: Its origin and future," in *US Naval Institute Proceedings*, vol. 124, no. 1, 1998, pp. 28–35.
[261] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Computers & security*, vol. 49, pp. 70–94, 2015.
[262] A. Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history, august 2018," *From the book Sandworm published on Security wired website.*, 2019. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[263] R. Piggin, "Development of industrial cyber security standards: IEC 62443 for SCADA and industrial control system security," in *IET Conference on Control and Automation 2013: Uniting Problems and Solutions*. IET, 2013, pp. 1–6.
[264] NIST, US, "Guidelines for smart grid cyber security (vol. 1 to 3)," *NIST IR-7628, Aug*, 2010.
[265] B. Obama, "Executive order 13636: Improving critical infrastructure cybersecurity," *Federal Register*, vol. 78, no. 33, p. 11739, 2013.
[266] L. Tanczer, I. Brass, M. Elsden, M. Carr, and J. J. Blackstock, "The United Kingdom's emerging internet of things (IoT) policy landscape," *Tanczer, LM, Brass, I., Elsden, M.,*

Carr, M., & Blackstock, J.(2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance, pp. 37–56, 2019.

[267] E. Lear, R. Droms, and D. Romascanu, "Manufacturer usage description specification," IETF Network Working Group, Tech. Rep. draft-ietf-opsawg-mud-11, 2018.

[268] H. Tschofenig and E. Baccelli, "Cyberphysical security for the masses: A survey of the internet protocol suite for internet of things security," *IEEE Security Privacy*, vol. 17, no. 5, pp. 47–57, Sep. 2019.

[269] S. K. Das, K. Kant, and N. Zhang, *Handbook on securing cyber-physical critical infrastructure*. Elsevier, 2012.

[270] Techopedia. [Online]. Available: https://www.techopedia.com/dictionary

[271] Cyber-physical systems. [Online]. Available: https://www.nsf.gov/pubs/2019/nsf19553/nsf19553.htm

[272] V. R. Segovia and A. Theorin, "History of control history of PLC and DCS," *University of Lund*, 2012.

[273] Industrial Internet Consortium, "The Industrial Internet Vocabulary Technical Report V 2.1 ," IIconsortium, Tech. Rep., May 2018.

[274] W. Wahlster, "From industry 1.0 to industry 4.0: towards the 4th industrial revolution (forum business meets research)," *3rd European Summit on Future Internet Towards Future Internet International Collaborations Espoo, Finland*, vol. 31, 2012.

[275] K. Stouffer, T. Zimmerman, C. Tang, J. Lubell, J. Cichonski, and J. McCarthy, "Cybersecurity framework manufacturing profile," National Institute of Standards and Technology, Tech. Rep. NISTIR 8183, 2017.

[276] A. Siemens, F. O. L. TID, A. S. Segura, V. Toubiana, J. W. Walewski, and S. Haller, "Internet-of-things architecture IoT-a project deliverable D1.2—initial architectural reference model for IoT," EU Commission Seventh Framework Programme, Tech. Rep., 2011.

[277] J. A. Simpson and E. S. C. Weiner, Eds., *Oxford English Dictionary*. Oxford University Press, 1989.

ACRONYMS

ADS-B Automatic Dependent Surveillance-Broadcast.

BLE Bluetooth Low Energy.

CAN Controller Area Network.

CPS Cyber-Physical System.

DCS Distributed Control System.

DDoS Distributed Denial of Service.

DICE Device Identifier Composition Engine.

DLR Device Level Ring.

DoE Department of Energy.

ECU Electronic Control Unit.

ETSI European Telecommunications Standards Institute.

FCN Field Communication Network.

FDIR Fault Detection, Isolation, and Reconfiguration.

GPS Global Positioning System.

HAC High Assurance Controller.

HACMS High Assurance Cyber Military Systems.

HPC High Performance Controller.

ICAS Integrated Condition Assessment System.

ICS Industrial Control System.

IEC International Electrotechnical Commission.

IETF Internet Engineering Task Force.

IMD Implantable Medical Device.

IoT Internet of Things.

ISA International Society of Automation.

KA Knowledge Area.

LAN Local Area Network.

MPC Model Predictive Control.

MUD Manufacturer Usage Description.

NERC North American Electric Reliability Corporation.

NIST National Institute of Standards and Technology.

NSF National Science Foundation.

ONR Office for Nuclear Regulation.

OS Operating System.

OT Operational Technology.

PCS Process Control System.

PLC Programmable Logic Controller.

RAM Random Access Memory.

RF Radio Frequency.

RPL Routing Protocol for Low-Power and Lossy Networks.

RTOS Real-Time Operating System.

RTU Remote Terminal Unit.

SCADA Supervisory Control and Data Acquisition.

SCN Supervisory Control Network.

SGX Software Guard Extensions.

SIS Safety Instrumented System.

TCG Trusted Computing Group.

TCP Transmission Control Protocol.

TLS Transport Layer Security.

TPM Trusted Platform Module.

UFLS Under Frequency Load Shedding.

UV Unmanned Vehicle.

GLOSSARY

Actuator An actuator is a device that moves or controls some mechanism. An actuator turns a control signal into mechanical action such as an electric motor. Actuators may be based on hydraulic, pneumatic, electric, thermal or mechanical means, but are increasingly being driven by software. An actuator ties a control system to its environment [270].

Cyber-Physical System Engineered systems that are built from, and depend upon, the seamless integration of computation, and physical components [271].

CyBOK Refers to the Cyber Security Body of Knowledge.

Distributed Control System A control system that combines supervised control of several individual computer-based controllers in different control-loop throughout a process. In contrast to SCADA systems, the supervision of these systems tends to be onsite rather than remote [272].

Industrial Control Systems General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy) [150].

Industrial Internet of Things System that connects and integrates industrial control systems with enterprise systems, business processes, and analytics [273].

Industry 4.0 Industry 4.0 refers to the modernization of manufacturing with Internet of Things services, which provide the basis for the fourth industrial revolution. The first industrial revolution was enabled by the introduction of mechanical production facilities powered by water and steam, the second revolution was enabled by mass production powered by electrical energy, and the third revolution was enabled by the introduction of electronics and information technology [274].

Internet of Things Network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with the manufacturer, operator and/or other connected devices. The IoT refers to devices, that are often constrained in communication and computation capabilities, now becoming more commonly connected to the Internet, and to various services that are built on top of the capabilities these devices jointly provide[4].

Operational Technology Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise [275].

Programmable Logic Controller (PLC) An industrially hardened computer-based unit that performs discrete or continuous control functions in a variety of processing plant and factory environments. It was originally intended as a relay replacement equipment for the automotive industry. As opposed to DCS, they can be sold as stand-alone equipment (instead of an integrated system as DCS) [272].

Sensor A device that perceives certain characteristics of the real world and transfers them into a digital representation [276].

Transducer A device that converts variations in a physical quantity, such as pressure or brightness, into an electrical signal, or vice versa [277].

[4] **https://www.ietf.org/topics/iot/**

INDEX