CyBOK

CYBER-PHYSICAL SYSTEMS SECURITY KNOWLEDGE AREA

(DRAFT FOR COMMENT)

AUTHOR: Alvaro Cardenas – University of California, Santa Cruz

EDITOR: Emil Lupu – Imperial College, London

REVIEWERS:

Henrik Sandberg – KTH Royal Institute of Technology

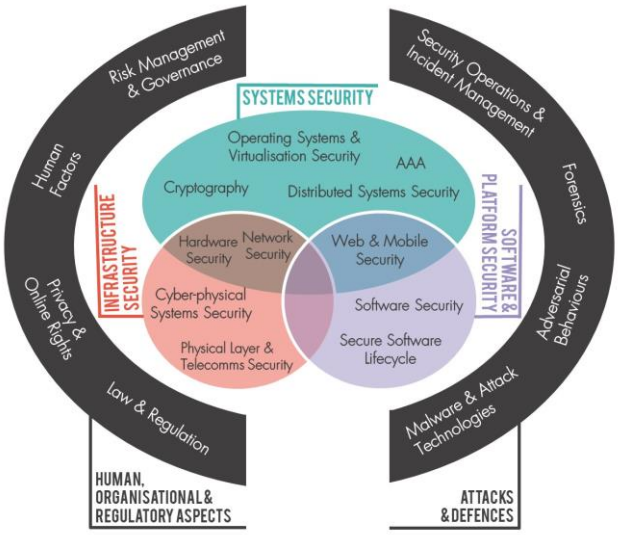
Marina Krotofil – Hamburg University of Technology

Mauro Conti – University of Padua

Nils Ole Tippenhauer – CISPA Helmholtz Center for Information Security

Rakesh Bobba – Oregon State University

Following wide community consultation with both academia and industry, 19 Knowledge Areas (KAs) have been identified to form the scope of the CyBOK as shown in the diagram below. The Scope document provides an overview of these top-level KAs and the sub-topics that should be covered under each and can be found on the project website: https://www.cybok.org/.



We are seeking comments within the scope of the individual KA; readers should note that important related subjects such as risk or human factors have their own knowledge areas.

It should be noted that a fully-collated CyBOK document which includes issue 1.0 of all 19 Knowledge Areas is anticipated to be released by the end of July 2019. This will likely include updated page layout and formatting of the individual Knowledge Areas.

Cyber-Physical Systems Security

Alvaro A. Cardenas

January 2019

INTRODUCTION

Cyber-Physical Systems (CPS) are engineered systems combining computation, communications, and physical resources. The purpose of this chapter is to provide an overview of the emerging field of CPS security. In contrast to the other chapters in this book, which can trace the roots of their fields back to several decades, the work on CPS security is relatively new, and our community has not yet developed the same consensus on best practices. Therefore, in this document we focus on providing an overview of the research trends and unique characteristics in this field.

CONTENT

1 Cyber-Physical Systems

The term Cyber-Physical Systems (CPS) emerged just over a decade ago as an attempt to unify the emerging application of embedded computer and communication technologies to a variety of physical domains, including aerospace, automotive, chemical production, civil infrastructure, energy, healthcare, manufacturing, materials, and transportation. The term CPS was coined in 2006 by Helen Gill from the National Science Foundation NSF in the United States [1].

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 of the fundamental intellectual problem of conjoining the engineering traditions of the cyber and physical worlds* [1].

In their program announcement, the NSF outlined their goal for considering these various industries under a unified lens: by abstracting from the particulars of specific applications in these domains, the goal of the CPS program is to reveal cross-cutting fundamental scientific and engineering principles that underpin the integration of cyber and physical elements across all application sectors.

Soon after the term CPS was coined, several research communities rallied to outline and understand how CPS *cyber security* research is fundamentally different compared to conventional Information Technology (IT) cyber security. Because of the cross-cutting nature of CPS, the background of early security position papers from 2006 to 2009 using the term CPS, ranged from real-time systems [2, 3], embedded systems [4, 5], control theory [6] and cyber-security [7, 8, 9].

While cyber security research had been considered in other physical domains prior to the rise of CPS—most notably in the Supervisory Control and Data Acquisition (SCADA) systems of the power grid [10]—these previous efforts focused on applying well-known IT security best practices to control systems; and what differentiates the early CPS security position papers was their cross-cutting nature focusing on a *multidisciplinary perspective* for CPS security. For example, while classical intrusion

detection systems monitor purely cyber-events (network headers, system calls, etc.), early CPS papers bringing control theory elements [6, 8] suggested that intrusion detection systems for CPS could also monitor the *physical* evolution of the process as a way to improve attack detection.

1.1 Characteristics of CPS

CPS are the result of several computing efforts in embedded systems, real-time systems, (wired and wireless) networking and control theory.

One of the most general characteristics of CPS 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 full operating systems, but rather run only on *firmware*, which is a specific class of software that provides low-level control of device hardware. Even when embedded systems have an operating system, they run a stripped-down version of it to concentrate on the minimal tools necessary for the platform; for example, a fairly popular operating system in IoT consumer devices is Busybox [11], and another popular operating system for embedded devices that provides networking functionalities is OpenWrt [12].

For safety-critical systems, the *time* in which computations are performed is important in order to ensure the correctness of the system [13]. Real-time programming languages can help developers specify timing requirements for their systems, and Real-Time Operating Systems (RTOS) guarantee the time to accept and complete a task from an application [14].

Another characteristic of CPS is that these embedded systems communicate with each other, usually over IP-compatible networks. While many critical infrastructures such as power systems have used radio communications to monitor operations in their SCADA systems remotely, it is only in the past two decades that the information exchanged between different parts of the system have migrated from serial communications to IP-compatible networks. Modern SCADA systems are interconnected through a variety of network industrial protocols such as DNP3, Modbus/TCP, EtherNet/IP, PROFINET, ICCP, and IEC 60870-5-104 (IEC 104) [15, 16].

While most of the long-distance communications are done over wired networks, wireless networks are also a fundamental characteristic of CPS. 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 networks, where traditional concepts for routing like the hop distance to a destination is no longer a good metric, and other link quality metrics like the probability of a successful one-hop transmission are more reliable. While most research into wireless sensor networks was done in abstract scenarios, one of the first real-world successful applications of these technologies was in the supervision of large industrial systems with the advent of WirelessHART, ISA100 and ZigBee [17, 18]. These three communications technologies were developed on top of the IEEE 802.15.4 standard, whose original version defined frame sizes so small, that they could not carry the header of IPv6 packets. As Internet-connected embedded systems are expected to grow to billions of devices in the next few years, vendors and standard organisations see the need to create embedded devices compatible with IPv6 [19]. To be able to send IPv6 packets in wireless standards, there have some attempts 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 to 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]

Finally, most CPS observe and attempt to control variables in the physical world. Feedback control

systems have existed for over two centuries, including technologies like the engine centrifugal steam governor, which was introduced in 1788. Most of the literature on control theory attempts to model a physical process with differential (or difference) equations and then design a controller that satisfies a set of desired properties like stability, safety, and performance criteria. Control systems were originally designed with analogue sensing and control, which allows the seamless integration of control signals into a *continuous-time* physical process; however, microprocessors and computers cannot control a system in *continuous time* because sensing and actuation signals have to be sampled at discrete-time intervals. This gave rise to the study of *discrete-time* control [23]. More recently, the rise of computer networks has allowed digital controllers to be further away from the sensors and actuators (e.g., pumps, valves, etc.), and this also gave rise to 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) has given rise to the field of *hybrid systems* [25]. Hybrid systems played a fundamental role in the motivation for creating a CPS research program, as they were an example of how combining models of computation and physical systems can give way to new theories that enable us to reason about the properties of cyber and physical-controlled systems.

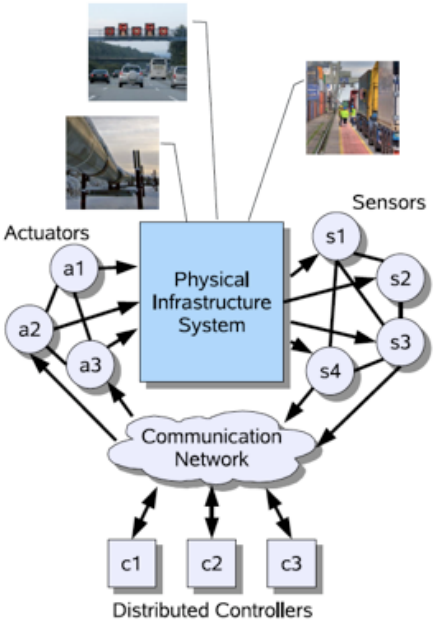


Figure 1: Representation of a general CPS.

Figure 1 illustrates a general CPS architecture. Having stated these general characteristics of CPS, we should point out that CPS are very diverse, including modern vehicles, medical devices, and industrial systems, all with different standards, requirements, communication technologies, and time constraints. Therefore, the general characteristics we associated with CPS might not hold true in all systems or implementations.

1.2 Security and Privacy Concerns

Several CPS can be labelled *safety-critical*, i.e., their failure can cause irreparable harm to the physical system being controlled and to the people who depend on it. SCADA systems, in particular, perform vital functions in national critical infrastructures, such as electric power distribution, oil and natural gas distribution, water and waste-water treatment, and intelligent transportation systems. They are also at the core of health-care devices, weapons systems, and transportation management. Disruption to these CPS could have a significant impact on public health and safety, and could lead to large economic losses.

For example, attacks on a power grid could cause blackouts, leading to interdependent cascading effects in other vital critical infrastructures such as computer networks, medical systems or water systems perhaps having a catastrophic effect on the economy and public safety in our society [26]. Attacks on ground vehicles could cause road traffic accidents [27], attacks on GPS systems could mislead navigation systems and make drivers reach destinations desired by the attackers [28], and attacks on consumer drones could let attackers steal, cause accidents or surreptitiously turn on cameras and microphones to monitor their victims [29].

In addition to security, CPS are socio-technical systems and, as such, they could also have profound privacy implications unanticipated by the designers of new systems. Warren and Brandeis stated in their seminal 1890 essay *The right to privacy* [30] 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 are similarly challenging cultural assumptions about privacy.

CPS have a variety of sensors that can collect more information about the world around them than previously possible. This ability of CPS devices to passively sense surrounding activity makes the privacy issues they raise distinct from the privacy issues raised by traditional computing systems as they collect physical data about diverse human activities such as electricity consumption, location information, driving habits, and biosensor data at unprecedented levels of granularity. In addition, their passive manner of collection leaves people generally unaware of how much information about them is being gathered. People are also mostly unaware that this 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 remotely collect 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 picture of driving habits that can be exploited by manufacturers, retailers, advertisers, auto insurers, law enforcement, and stalkers, to name just a few.

To tackle these problems, we need a multidisciplinary perspective on the security and privacy implications of CPS that bridges the understanding of their social, economic, cultural, and regulatory context with an understanding of their technical workings. Such a multidisciplinary perspective will allow us to identify the new challenges and possible new methods of addressing these problems.

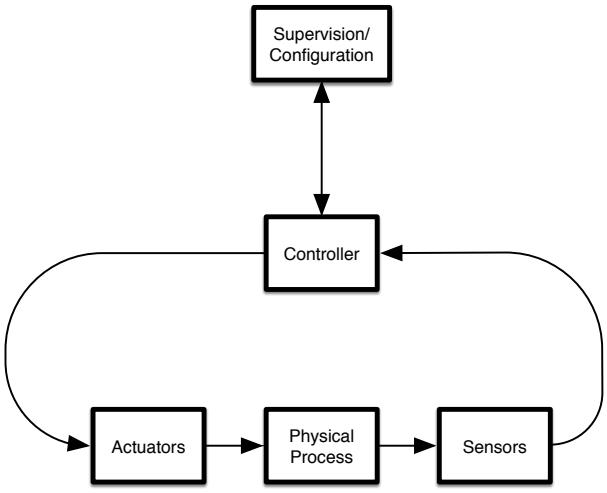


Figure 2: General Architecture of a CPS.

1.3 Attacks Against CPS

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 2.

Attacks on CPS can happen at any point in the general architecture, as illustrated in Figure 3: (1) an attacker can inject false data into the system by faking sensor data (e.g., if the sensor data is unauthenticated or if the attacker has the key material for the sensors) and cause the control logic of the system to act on malicious data [31]. (2) The attacker can delay or even completely block the information from the sensors to the controller, so the controller loses observability of the system [32], thus causing it to operate with *stale data* [33]. (3) The attacker may be able to compromise the controller and send incorrect control signals to the actuators [34]. (4) The attacker can delay or block any control command, thus causing a denial of control to the system [32]. (5) The attacker can compromise the actuators and execute a control action that is different to what the controller intended [35]. (6) The attacker may be able to physically attack the system (e.g., physically destroying part of the infrastructure and combining this with a cyberattack) [36]. (7) The attacker can delay or block communications to the supervisory or configuration devices [37], and (8) the attacker can compromise or impersonate the supervisor [38] or configuration [39] devices, and send malicious control or configuration changes to the controller.

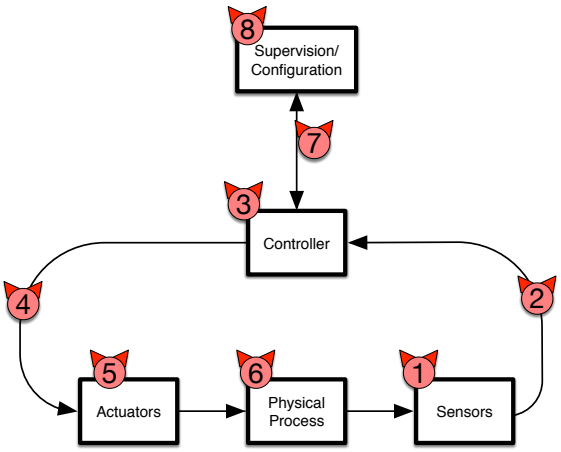


Figure 3: Attack Points in a CPS.

Launching successful attacks on CPS depends on the Attacker Model [40, 41]. Attackers may differ in their experience, knowledge of the system they are attacking, their motivation and their resources. For example, cybercriminals who are only interested in monetary profits from spam, mining of cryptocurrencies, stealing personal information etc. might launch non-targeted attacks on CPS: e.g., they may compromise a server to run a botnet server, but their goal is not to disrupt the physical system. On the other hand, attackers specifically targeting the disruption of the operation of a CPS can vary from basic attackers with a curiosity for CPS systems (like an attacker who changes the chemical dosing parameters of a water system [42]), to disgruntled employees with detailed knowledge of the system they are attacking [43]. Groups of attackers can launch more sophisticated attacks, like hacktivists attempting to cause damage for political purposes, to attackers backed by nation-states [44, 38].

A unique property of CPS is that the integrity of these systems can be compromised even without a computer-based exploit. By targeting the way sensors capture real-world data, an attacker can inject a false sensor reading by manipulating the physical environment around the sensor. These attacks are known as **transduction attacks**. For example, attackers can use speakers to affect the

gyroscope of a drone [45] and other sound waves can affect accelerometers in wearable devices to make them report incorrect movement values [46]. Attackers can also inject inaudible voice commands to digital assistants [47], lasers can affect the stability of drones using cameras for hovering stability [48] and other radio waves can trick pacemakers into disabling pacing shocks [49]. Classical security mechanisms such as software security, memory protection, authentication or cryptography are not enough to protect CPS, as transduction attacks represent a new class of attacks that are not being effectively handled by classical software security [50]. A related attack to transduction attacks are physical-layer attacks on wireless systems like selective wireless jamming [51] and GPS spoofing [52].

Having described some of the academic research into attacks against control systems, we now summarise some high-profile real-world attacks on CPS by malicious parties in order to motivate the growing importance of this problem, as well as the next sections on security protections.

1.3.1 High-Profile Attacks on CPS

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

While not an attack, the Therac-25 software error is one of the best-known classical examples of how software bugs 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 [53]. Similar accidents have happened more recently such as a power plant shutdown caused by a computer rebooting after a patch [54]. The concern here is what if these problems were not accidental but malicious?

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 which inadvertently infected the Davis-Besse nuclear power plant [55], affecting the ability of the engineers to monitor the state of the system. Another non-targeted attack is the case of a controller who used to be sent spam at a water filtering plant [56].

In this section, we focus on *Targeted attacks*. These are attacks where the adversaries know that they are targeting a CPS and, therefore, *they tailor their attack strategy with the aim of creating a desired physical effect*.

The first publicly reported attack on a SCADA system was the attack on the Maroochy Shire Council's sewage control system[1] in Queensland, Australia [43], 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 to be a pumping station. During a three-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, jeopardising public health, and costing more than $200,000 in clean-up and monitoring costs.

In the two decades since the Maroochy Shire attack, there have been many other confirmed attacks on CPS; however, no other attack has demonstrated the new sophisticated threats that CPS are facing such as the Stuxnet worm which targeted the nuclear enrichment program in Natanz, Iran [44]. Stuxnet intercepts requests to read, write and locate blocks on a Programmable Logic Controller (PLC). By intercepting these requests, Stuxnet is able to modify the data sent to, and returned from, the PLC without the knowledge of the PLC operator. The most popular Stuxnet attack variant consisted of sending incorrect rotation speeds to the motors powering the centrifuges enriching the uranium, causing the centrifuges to break down so that they needed to be replaced.

[1] There are prior reported attacks to control systems [57] but there is no public information corroborating these incidents.

Two other high-profile confirmed attacks on CPS were the December 2015 and 2016 attacks against the Ukrainian power grid. These attacks caused power outages and clearly illustrate the evolution of attack vectors. While the attacks in 2015 required a human to be remotely operating the human-machine interfaces in the power companies, the attacks in 2016 leveraged the Industroyer malware [58] to automate their attack.

The most recent example in the malware creation arms race, which is targeting control systems is the TRITON malware, which targeted safety systems in industrial control systems in the Middle-East. An attempt to inject TRITON into a controller memory by the attacker caused at least one industrial process to shut down [59].

Stuxnet, Industroyer, and TRITON demonstrate a clear arms race in state-sponsored attacks to create purpose-built malware to disrupt or destroy CPS. 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 will be waged, as we will discuss in the last section of this chapter.

2 Cross-Cutting Security

This section looks at cross-cutting security efforts to prevent, detect, and mitigate attacks, and the next section will look at specific CPS domains such as the power grid or intelligent transportation systems.

2.1 Preventing Attacks

To prevent attacks, CPS designers and developers have to follow the same best-security practices as for classical IT systems; i.e., they need to follow a secure development lifecycle to minimise software vulnerabilities, implement access control mechanisms, and provide strong cryptographic protections along with a secure key management system. Several standards organisations have developed guidelines on how to apply best-security practices for CPS; for example, the U.S. National Institute of Standards and Technology (NIST) has a Guide to Industrial Control System (ICS) Security [60], a guideline to smart grid security [61] and a guideline for IoT security and privacy [62]; several industry-specific organisations have basic security standards for their systems such as the North American Electric Reliability Corporation (NERC) critical infrastructure protection standards for the power grid [63] or the International Society of Automation (ISA) security standards for process control systems [64].

Most standards are recommendations or guidelines on how to apply traditional security best practices in specific CPS domains, although, there are new standards that try to create new functionalities to improve the CPS security [65]. One particular new proposed standard by the Internet Engineering Taskforce (IETF) is the Manufacturer Usage Description (MUD) standard [66]. The goal of this standard is to automate the creation of network *white lists*, which are used by network administrators to block any unauthorised connections by the device.

There are, however, multiple challenges in CPS for implementing these security best practices, including the fact that several CPS are composed of legacy systems that need to operate 24/7. They are operated by embedded devices with limited resources, and face new vulnerabilities such as *transduction* attacks.

Securing Legacy Systems: The lifecycle of CPS devices is an order of magnitude larger than regular computing servers, desktops, or mobile systems. Consumers expect their cars to last longer than their laptops, hospitals expect medical equipment to last over a decade, and industrial asset owners expect their control systems to last for at least 25 years [67]; therefore, most CPS 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 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.

As a result, to prevent attacks on CPS, we have to deal with (1) designing systems where security can be continuously updated and (2) retrofitting security solutions for existing legacy systems. Updating the security of devices is challenging in several CPS use-cases as devices tend to be certified and any changes in software or operational practices must be followed by an extensive safety revision or re-certification. On the other hand, several standards attempt to add security to legacy systems, for example, the IEEE P1711 standard is designed for providing security in previously unsecured legacy serial links [68]. Several other efforts have attempted to bring security practices to previously insecure industrial protocols.

Some communications between 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** [69]. 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 unencrypted 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,which then removes the security protections and sends the original packet to the final destination.

A similar concept has been proposed for wireless devices such as 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** [70, 71] can be used near the vulnerable devices. The wireless shield will jam any communication attempt to the vulnerable devices except those from devices authorised by the owner of the shield. There are, however, some limitations to this type of wireless shield based on the challenges of selective jamming [51].

Retrofitting Security in Legacy Communications: There are attempts to extend legacy protocols while keeping legacy compatible [72, 73]. In these cases, cryptographic signatures are introduced as separate (legacy compliant) sensor streams or tags/addresses. This approach allows supporting devices to obtain and verify signatures, while legacy devices will just ignore the signatures. It also avoids issues with restricted message lengths (e.g., in the case of CAN), which would otherwise force short/insecure signature lengths.

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. For symmetric crypto, NIST has plans for standardising a portfolio of lightweight cryptographic algorithms [74] and the current CAESAR competition for an authenticated-encryption standard is evaluating the performance of their submissions in resource-constrained devices [75]. 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 [76].

High Assurance Systems: The design of secure operating systems with formal proofs of security dates back to the *Orange Book* [77]. Because the increasing complexity of the code in monolithic kernels makes it hard to prove 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 again. One example of such a system is the seL4 microkernel, which is notable because of several security properties which have been machine-checked with formal proofs of security [78]. DARPA's HACMS program [79] used this microkernel to build a quadcopter with strong safety and security guarantees [79]. While seL4 is open-source, private industries are also building microkernel-based operat-

ing systems for embedded platforms, for example, the security firm Kaspersky recently announced a secure micro-kernel operating system (Kaspersky OS) targeting IoT devices, industrial systems, and cars, but because the OS is not open source, the security claims have not been independently verified.

Preventing Transduction Attacks: Some of the solutions for preventing transduction attacks 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 securing amplifiers that prevent signal clipping [46, 50].

2.2 Detecting Attacks

Detecting attacks can be done by observing the internal state of a CPS device, or by monitoring the information exchanged between devices to spot anomalous activities.

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 exploit mitigations themselves. Remote attestation relies on verifying the current internal state (e.g., RAM or flash) of an untrusted device by a trusted verifier. There are two classical variants of remote attestation: software-based attestation and hardware-assisted attestation. Software-based attestation does not rely on any special security hardware in the device, but it has weak security guarantees. In contrast, hardware-based attestation provides stronger security, but requires a dedicated secure hardware component in the device, which in turn increases their cost. The challenge for embedded low-end CPS devices is that some of the hardware-based technologies supporting attestation available for desktops and mobile devices, including TPM, TrustZone, and SGX cannot be supported in constrained low-cost devices. Another key difference is that remote attestation for CPS devices might not be done via the Internet but within wireless range, so the question is what is the minimal set of hardware requirements needed to support memory attestation in embedded systems? Hybrid approaches attempt to find a middle ground for embedded systems by reducing the secure hardware requirements while overcoming the security limitations of pure software-based approaches [80, 81, 82, 83].

Exploit detection in embedded CPS devices also requires unique solutions, including guaranteeing control flow integrity [84] and detecting whenever malware is being attempted to be loaded into CPS devices [85].

The second category of solutions for detecting attacks relies on monitoring CPS network communications. By comparison to classical IT systems, CPS exhibit comparatively simpler network behaviour: servers rarely change, there is a fixed network topology, a stable user population, regular communication patterns and a limited 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 [86].

Network Specification: 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 [87]. If there is no specification of the network behaviour, this behaviour can be learned. Because most of the communications in CPS networks are between machines (with infrequent human intervention), they happen automatically and periodically, and given their regularity, these communication patterns can be captured by finite state models such as Deterministic Finite Automata [88, 89] or via Discrete-Time Markov Chains [90, 91].

Physics-Based Attack Detection: A 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 the network patterns of a specific network protocol, another line of work studies how monitoring sensor and control values can be used to detect attacks; this approach is usually called *physics-based* attack detection [92]. When fingerprinting the physical

behaviour of a CPS, sometimes the physics of the process are not enough, and we need to take into consideration the device's physics as well [93].

There are two main classes of anomalies: **historical anomalies** and **physical-law anomalies**. A historical anomaly denotes a physical configuration we have not seen before. A typical example is to place limits on the observed behaviour of a variable [94]. For example, if during the learning phase, the 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 these variables can also capture their historical correlations; for example, they can capture the fact that when the water level of a tank is high, the water level of a second tank in the process is always low [95]. A similar approach is to use data consistency checks, where the sensor's trustworthiness can be verified through its consistency with other related or correlated sensors [96].

A complementary approach to historical observations, is to create models of the physical evolution of the system. This approach is inspired by the field of fault diagnosis, which has long been using physical models to detect faulty devices [97, 98] (the main difference is that fault diagnosis does not usually consider strategic adversaries, and if used for security purposes, they might force the operator to perform erroneous countermeasures [99]). For example, if 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 of a power grid (electromagnetics) 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 the sensors is consistent with the expected behaviour of the system. For example, if we open an intake valve, we expect the water level in the tank to rise, otherwise we may have a problem with the control, the 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) [100], although 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 detect this previously unseen state [101].

Active Detection: In addition to passively monitoring a network, an intrusion detection system can actively query devices to detect anomalies in how devices respond to these requests [102]. Active detection for physics-based attack detection systems (also known as **physical attestation** [103, 104, 95]) uses a control signal to alter the physical world and, in response, it expects to see the changes 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 [105], vary the physical plant and actuator gains of industrial systems to detect zero-dynamics attacks [35], use a change in a camera's field of vision to detect hacked surveillance cameras [106], or use a watermarking signal in a control algorithm [107].

2.3 Mitigating Attacks

Much of the effort made to mitigate faults in CPS has focused on safety and reliability (the protection of systems against random and/or independent faults). Attack mitigation is an extension of safety and reliability protections when the faults in the systems are created by a strategic adversary.

There are two main types of mitigating technologies: i) proactive and ii) reactive. Proactive mitigation consists of 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; they reconfigure the control actions online in order to minimise the impact of the attack. We first describe proactive approaches.

Conservative Control: One of the earliest ideas for mitigating the impact of attacks was to operate a system with enough safety margins so that if an attack ever occurred, it would be harder for the

attacker to reach an unsafe region [32]. This usually comes at the cost of suboptimal operations under attack-free conditions. One intuitive idea for this type of control algorithm is to use Model Predictive Control (MPC) to design a control strategy while predicting that an attack will happen starting at the next time step [32].

Security Indices: Another early idea on attack mitigation consisted of identifying the most vulnerable points of a system and improving its robustness by either increasing or diversifying the number of sensors or controllers, or by allocating a limited security budget to protect a critical subset of the system's components [108] so that the system can maintain reliable operations by relying on this subset of trusted components, even if other devices are compromised. Vaidya et al. [109] also used a measure of network vulnerability based on controllability and observability Gramians. This mitigation strategy is obtained by using convex optimisation to minimise the vulnerability measure and, as a result, we can find the optimal location for a secure set of sensors. Similarly, Vukovic et al. [110] defined a measure that quantifies the importance of individual systems and the cost of attacking individual measurements. The goal was to mitigate integrity attacks by modifying the routing and data authentication.

Resilient Estimation: Estimation algorithms attempt to obtain the system's state from sensor values, and resilient estimation algorithms attempt to obtain this state, even if a subset of sensors is compromised [111, 112]. The idea is to use redundancy and resilient algorithms such as error-correcting codes to estimate a value accurately, even when a subset of sensor values is compromised. The objective of the system operator is to find the optimal estimator that minimises the estimation error while knowing an upper bound on the number of sensors that are under attack (i.e., the operator knows or assumes l).

Inertial Resets: Another idea for mitigating attacks is to reset and diversify the system as frequently as possible so that attackers are unable to gain constant control of the system [113, 114]. The basic idea is that if a system is compromised by malware, a full software reset will make the system boot again in a trusted state, thus eliminating the attacker's presence. While the system is rebooting, the CPS operates by the inertia provided by the last control action and if the reboot is fast enough, the system can be controlled with no major performance impacts. This solution 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.

Constraining Actuation: A similar principle of operating conservatively is to physically constrain the actuators of a CPS so that if an 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 [115].

Reactive defences rely on reconfiguring the control system to react against faults in sensors or actuators in the control loop (also known as fault-tolerance control [116]). When sensors or controllers are under attack, new actions are generated in order to maintain the safety of the system.

Virtual Sensors: When we use *physical-law 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, which can then be provided to the control algorithm [117, 101]. The physical models are not perfect, and while they might mitigate the impact of an attack, it is, therefore, important to evaluate the safety of the system whenever virtual sensors are being used as a response to a false alarm [117].

Game Theory: Game theory is often useful to capture the strategic nature of adversaries when they take over control inputs to the CPS. In these 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 sequential (e.g., a Stackelberg game) [118, 119, 120] which would correspond to a reactive defense; however, the defence can also be proactive by

considering simultaneous games (zero-sum or minimax) [121, 122, 123, 124].

Safe Controls: 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 into unsafe states [125]. 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 [34]. The proposed approach depends on a controller of controllers (C^2), which mediates all the 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 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 overheads).

2.4 Testbed Development

In order to design, test, and deploy some of these security solutions, researchers need a CPS environment representative of real-world systems. Designing CPS testbeds is another of their distinguishing factors compared to other security problems in IT where researchers can reuse commodity servers or devices to test their soltuions. Testbeds and simulated high-fidelity virtual environments can also be used to create CPS Honeypots [126].

The challenge of designing CPS testbeds is that–as we will describe in the next section–CPS systems are very diverse, and most testbeds will have only limited applicability to generalise their results. Some testbeds attempt to provide a general framework to model a variety of CPS through software [127], others use a combination of real CPS devices coupled with simulations (sometimes called Hardware in the Loop testbeds) [128] while others represent fully-realised real-world processes [129, 130, 131, 132].

3 CPS Domains

Having described CPS attacks and defences in general CPS terms, in this section we show their uniqueness in security problems and solutions to different domain-specific CPS.

3.1 Industrial Control Systems

While some of these infrastructures have used sensing and control for almost a century—the steam engine governor was introduced in 1788, and the first programmable controller (the Modicon 0844) was released in 1969—it is only in the last decade that new technological advances, combined with drastic reductions in the costs of deploying (1) wireless sensors (wirelessHART, ISA-100), (2) embedded computers, and (3) communication networks have enabled the ubiquitous use of networking and embedded devices in diverse CPS sectors.

Industrial control systems represent a wide variety of networked information technology (IT) systems connected to the physical world. Depending on the application, these control systems are also called Process Control Systems (PCS), Supervisory Control and Data Acquisition (SCADA) systems (under industrial control or under the control of the critical infrastructures), or Distributed Control Systems (DCS).

Control systems are usually composed of a set of networked agents, consisting of sensors, actuators and control processing units such as programmable logic controllers (PLCs) and communication devices. For example, the oil and gas industry use integrated control systems to manage refining operations at plant sites, to remotely monitor the pressure and flow of gas pipelines, and to control

the flow and pathways of gas transmission. Water utilities can remotely monitor well levels and control the well 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.

Earlier in the document we discussed one of the most active areas for protecting industrial system: anomaly detection [86, 117, 88, 89, 90, 91, 94, 100]. In addition to attack detection, preventing industrial control systems from reaching unsafe states is also an active area of research [34, 133, 134]. A concise survey of *research* in ICS security is presented by Krotofil and Gollmann [135].

3.2 Power Grids

In the approximately 140 years since their inception, electrical grids have extended transmission lines to five billion people around the world, bringing light, refrigeration and many other basic services to people across the globe. This accomplishment was recognised by the U.S. National Academy of Engineering, which selected the power grid as the greatest engineering achievement of the 20th century. While the current power grid architecture has served well for many years, there is a growing need to modernise the world's power grids to address new requirements and to take advantage of new technologies. The rationale for modernising power grid includes (1) Efficiency, (2) Reliability and (3) Consumer choice.

To achieve these objectives, the main initiatives associated with the smart grid are the Advanced Metering Infrastructure (AMI), Demand Response (DR), Transmission and Distribution Automation, Distributed Energy Resources (DER) and the integration of Plug-in Hybrid Electric Vehicles (PHEVs).

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 [136]. 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 types of devices they own [137]).

One of the most popular lines of work in the power systems community is the study of false-data injection attacks against state estimation in the power grid. In the power grid, operators need to estimate the phase angles x_k from the measured power flow y_k in the transmission grid. These bad data detection algorithms were meant to detect random sensor faults, not strategic attacks, and as Liu et al. [138] 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 [139]). There has been a significant amount of follow-up research focusing on false data injection for state estimation in the power grid, including the problem of identifying which are the best k sensors to protect in order to minimize the impact of attacks [140], as well as attackers trying to minimise the error introduced into the estimate, and defenders with a new detection algorithm that attempts to detect false data injection attacks [141].

3.3 Transportation Systems and Autonomous Vehicles

New vehicular applications leverage ubiquitous sensing and actuation capabilities [142], mobile and embedded computing with smart phones [143], participatory sensing [144], and wireless communication networks [145] to improve transportation operations. These new operations include *Traffic flow control* with ramp metering at freeway on-ramps and signal timing plans at signalled intersections to reduce congestion; *Demand management*, which focuses on reducing excess demand during peak hours; *Incident management*, which targets resources to alleviate incident hot spots; and *Traveller information*, which is used to reduce traveler buffer time, i.e., the extra time travellers 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 as location data are highly sensitive because they can reveal a variety

of personal habits [146, 147]. To address these emerging privacy concerns from sensor data, many techniques have been proposed, including differential privacy [148].

Although privacy is an important concern for these systems, it is, unfortunately, not the only one. Widespread vulnerabilities such as those from traffic sensors [149, 150, 151] can be readily exploited to cause traffic problems such as congestion [152, 153, 154, 155]. Air traffic systems have similar problems, a new technology complementing (or potentially replacing) RADAR systems is the Automatic Dependent Surveillance-Broadcast (ADS-B) protocol [156]. ADS-B consists in 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 [157]. Similar problems occur with the Automatic Identification System (AIS), which is used to track and monitor ships [158].

In addition to traffic management problems, the security of individual vehicles is also important, and researchers have been able to find a variety of vulnerabilities in modern automobiles [159], and potential avionic threats through the airplanes' entertainment networks [157]. Sea vehicles also have security problems. Naval warships, for example can remotely monitor equipment with a hardwired LAN using systems such as the Integrated Condition Assessment System (ICAS) [160]. ICAS are generally installed with connections to external PLCs, which are used in a vessel's control room to direct the movement of the control equipment that performs the actual manipulation of the physical devices on the ship such as propulsion and steering (e.g., controlling the rudder) [160, 161]. Navy ships have, therefore, similar security problems (and solutions) to those in the ICS domain.

The increased autonomy of ground, air and sea vehicles will also lead to new security challenges in robotic vehicles. The popularity 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 [162], including falsifying GPS information, or manipulating their control commands.

Autonomous vehicles have multiple sensors that help them to assess their physical environments such as 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 commercial systems, it is not a sustainable practice, as autonomous vehicles become more pervasive; for example, accelerometers and gyroscopes, as well as camera sensors, can be easily attacked to report false data [45, 46, 48].

Autonomous vehicles have a variety of sensors at their disposal to interact with the physical environment ranging from cameras to GPS and Inertial Measurement Units (IMU). An IMU is a standard component in AVs and includes *accelerometers*, *gyroscopes*, and *magnetometers*. Accelerometers measure the acceleration of a vehicle, gyroscopes measure the angular velocity of a vehicle, and magnetometers act as a compass for the vehicle. In addition to IMUs, AVs typically use other sensors such as GPS receivers for location information, RADARs, LiDARs or ultrasonic sensors to detect nearby obstacles, and cameras. Unfortunately, all of these sensors are vulnerable to transduction attacks, including IMU [45, 46], RADAR [163], LiDAR [164, 165], ultrasonic [163], and camera [166, 164, 163] sensor measurements. In addition, GPS signals can be spoofed [167, 52, 28]. GPS spoofing attacks have happened in real-world systems; for example, several instances of GPS spoofing attacks affecting the navigation of more than 24 vessels in the Black Sea have been reported [168].

Attacking individual autonomous vehicles can have large-scale consequences. For example, vehicular platoons are a set of vehicles that travel together, and an attack on one vehicle can cause malicious traffic dynamics, including resonant frequencies [169].

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 becomes more sophisticated, the threats are increasing [170]. Manufacturing defects can be introduced by compromised design files [171], and attacks can target the structural integrity (scale, indent, or vertex) or material integrity (strength, roughness, or colour) of the manufactured products [172]. Physical tests such as non-destructive tests and visual inspection, weight measure, dimension measure, 3D laser scanning, interferometry, X-ray, CT and destructive mechanical tests such as employing the tensile and yield properties of a material can help in detecting attacks.

The security of manufacturing robots has also been studied before, and researchers have found several vulnerabilities in modern systems [173, 174]. One of the most popular open-source software middleware to facilitate the development and operation of a variety of robot systems is the Robot Operating System (ROS). ROS is deployed in several commercial systems, but the original version of this software did not consider security; to enable the authentication of all devices and information exchange between robotic systems in untrusted environments a new extension of ROS called Secure ROS (SROS) is being developed [175].

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. Modern implantable medical devices 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 to security and privacy threats.

Two recent surveys describe the security problems as well as the solutions proposed in this field [176, 177]. One novel security mechanism proposed in medical devices is the use of 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 or not this extra wearable device is present or not. One of the biggest challenges is the problem of security and safety and how to satisfy both. In general, for security we do not want unauthorised devices to be able to reprogram medical devices, although, if the user of the device has a medical emergency and is unconscious when first-responders arrive, they should have the ability to access the device to treat the patient.

3.6 Building Automation and Smart Cities

Building Automation Systems (BAS) are designed to control a building's Heating, Ventilation, and Air Conditioning (HVAC), lighting, air humidity, building security, fire monitoring, CCTV, elevators, power supply, and room access authentication [178]. Many of these systems are unprotected and connected to the Internet, opening the door to various security problems. For example, in 2013, two security researchers accessed the BAS of a Google office in Sydney and gained access to some panels with buttons marked as active overrides, alarms, schedules and a building management key. In addition, they accessed the blueprints of the floor and roof plans as well as a clear view of the water pipes and their temperature [179]. While the researchers reported the vulnerabilities to Google and did not exploit their access, there is a real-world instance of malicious attackers demanding ransomware from a hotel so they could let their guests enter their rooms [180].

City infrastructures are also becoming modernized, from intelligent transportation systems, to smart infrastructure and management of power, water, and gas. One of the problems is that a city-wide deployment of a monolithic architecture can result in a single vulnerability affecting the whole city. An example of this type of threat was discovered with a type of ZigBee enabled city public lighting system where an attacker could exploit wirelessly a vulnerability in one light, and then because all of these system are connected wirelessly, an infected system could create a chain reaction and spread wirelessly hop by hop to the entire city, allowing the attacker to turn all the city lights on or off [181].

3.7 The 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 Wi-Fi consumer drones and remote-controlled Wi-Fi devices.

Consumer IoT devices are particularly vulnerable, and while some researchers can dismiss the threat, it is important to understand that attacks can have significant real-world consequences. For example, a growing consumer technology is the use of Internet connected toys for children, as they can help children remain engaged in many subjects and improve their problem-solving skills, but new advances and devices can also bring new challenges and problems. Children's brains are still developing until the age of 25, and, therefore, they are easily molded to develop ideas and norms based on their early experiences. For example, if children are tracked with the help of IoT devices, they will grow up normalising this type of surveillance.

There are several examples of IoT attacks, such as the use of vulnerable IoT devices to orchestrate massive distributed denial-of-service (DDoS) attacks (e.g., the Mirai botnet) [182], attackers who compromised a fish tank to penetrate the internal network of a casino [183], and an attacker who remotely deactivated hundreds of vehicles in Austin, TX, leaving their owners without transportation [184]. Two recent surveys explored the security challenges as well as security solutions for IoT devices [185, 186].

4 Policy and Political Aspects of CPS Security

We conclude this chapter with some of the most pressing non-technical problems for securing CPS; the lack of incentives in the free market to deliver security for these systems. We also discuss the evolution of CPS security and their role in future cyberconflicts.

4.1 Incentives and Regulation

While investing in security protection is a challenge for most industries, there is a difference between industries operating conventional IT systems and industries that work with CPS. Companies that use traditional IT (e.g., have a web-presence or handle any financial transaction) are constantly targeted by financially-motivated criminal groups. For IT companies attacks are common, so they constantly upgrade and improve the security of their systems to minimise losses. In addition, the public also tends to know about security breaches in these companies because of data protection laws enacted in several countries that require companies to disclose their breaches. This public disclosure is another factor that IT companies need to take into consideration when investing in cyber-security mechanisms.

On the other hand, as we discussed earlier in this chapter, *most* industries in the CPS domain have rarely experienced attacks sabotaging their physical process, in part because CPS attacks are hard to monetise by criminals. In addition to being rare, attacks on CPS are not openly reported, and this lack of data used by actuarial science leads to low-quality risk estimates; as the U.S. Department of Energy (DoE) stated in their Energy Delivery Systems Cyber Security Roadmap [187], '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 CPS firms, 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 CPS has resulted in several calls for government

intervention [188, 189, 190].

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 U.S. but after the August 2003 blackout, regulations that were once optional are now mandatory [191]. However, CPS industries have pushed back against regulation, arguing that regulations (e.g., mandating compliance with specific security standards) will stifle innovation, as more regulation tends to create a culture of *compliance* instead of a culture of *security*.

In the U.S. because of the inaction of the federal government, some states are starting to take regulation into their own hands; for example, the recently proposed California Senate Bill SB-327 will make California the first state in the U.S. with an IoT cyber-security law, where, 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.

Another alternative to imposing broad regulation, is to use the influence of a governments procurement process, by mandating a minimum set of cyber-security requirements 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.

An alternative to asking industries to follow specific standards is for governments to nurture a cyber-insurance market for CPS protection. Instead of asking companies to follow specific standards, governments could require firms to have cyber-insurance for their operations [192, 193, 194, 195]. There is a popular view that under certain conditions, the insurance industry can incentivise investments in protection [196]. The idea is that the premiums charged by insurance companies would reflect the cyber-security position of CPS companies; if a company follows good cyber-security practices, the insurance premiums would be low, otherwise, they would be very expensive (and this would in principle incentivise companies to invest more in cyber-security protections).

Private organisations are also proposing new alternatives to educate consumers about the security practices of IoT products, for example, the nonprofit organisation Consumer Reports announced in 2017 that as part of the general rating evaluation provided for IoT devices, it will also include a security score for these devices [197].

It is unclear if government incentives to improve security in CPS will require an event similar to the August 2003 blackout, 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*' [198].

4.2 Cyber-Conflict

Computer networks enable the way we interact with others to be extended, and any conflict in the *real world* will have its representation in cyberspace; including (cyber-)crime, activism, bullying, espionage, and war. The role of computer networks in warfare has been a topic of academic discussion since 1998 [199], and CPS are making a fundamental difference on how wars are waged, from robotic units and unmanned vehicles supporting soldiers in the field, to discussions of cyberwar.

War is an act of force (physical harm or intimidation) for political purposes. Most nations now consider cyberspace as the 5th official theatre of conflict (in addition to land, air, sea, and space). For example, the U.S. established Cyber Command to conduct full spectrum *operations* (offensive capabilities) in 2009, and several other countries also announced similar efforts around the same time, including South Korea, North Korea, Great Britain, and China.

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 laws of war apply to cyberspace: (1) The Tallinn Manual and (2) the Koh Speech [200].

The Tallinn Manual is a non-binding study, by NATO's cooperative cyber-defence centre of excellence, of how the laws of war apply to cyber-conflicts, and the Koh Speech was a speech given by Harold Koh, a U.S. State Department legal advisor, which explained how the U.S. interprets international law in cyberspace. Both of these sources agree that a key reason for authorising the use of force (*jus ad bellum*) as a response to a cyber-operation, is when the physical effects of a cyber-attack compare with kinetic effects of other armed conflicts, for example, when a computer attack triggers a nuclear plant meltdown, opens a dam upriver or disables an 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 cases where 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 on the financial or electoral infrastructure of a nation may not be enough to be considered an act of war.

Once a war has started, 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 nonmilitary objectives. Military objectives can include war-fighting, war-supporting, and war-sustaining efforts. The problem with attacking critical infrastructures is that some of the infrastructures supporting these efforts are in dual-use by the military and the civilian population. For example, 95% of military communications in the U.S. use civilian networks at some stage, and the power grid supports military as well as civilian infrastructures.

Another factor to consider when designing CPS attacks is that the law of war in general prohibits uncontrollable or unpredictable attacks, in particular those that deny civilian populations indispensable objects, such as food or water. While physical weapons have a limited geographical area of impact, cyberweapons can replicate and escape their intended target and infect civilian infrastructures.

In short, any future conflict in the physical world will have enabling technologies in the cyber-world, and computer attacks will play an integral role in ongoing and future armed 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 the consequences. It is the 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.

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 cover the multidisciplinary nature of CPS security, such as transduction attacks. In addition, as the technologies behind CPS security mature, some of them will become industry-accepted best-practices and will transition to industry, while others might be forgotten. In 2018, one of the areas with the greatest momentum was the industry for network security monitoring in cyber-physical networks. Several start-up companies in the U.S., Europe, and Israel offer services for profiling and characterising industrial networks, to help operators with their asset inventory and to better understand what assets and traffic are allowed and what should be blocked. On the other hand, there are other areas that are just starting to be analyded such as the work on attack mitigation, which places too many performance constraints for operating CPS when there are no attacks. We are only at the starting point in CPS security research, and the decades to come will bring new challenges as we continue to understand the interplay between cyber and physical components in CPS, the behaviour of physical processes under attack and more effective security protections.

CROSS-REFERENCE OF TOPICS VS REFERENCE MATERIAL

	das2012handbook [201]	*Other*
1.1 Characteristics of CPS	c1	[1]
1.2 Security and Privacy Concerns		[8]
2.1 Preventing Attacks	c6,c9	[62]
2.2 Detecting Attacks	c18	[92]
2.3 Mitigating Attacks		[202]
3.1 Industrial Control Systems		[60]
3.2 Power Grids	c25	[191, 63]
3.3 Transportation Systems and Autonomous Vehicles	c26, c29	[203, 162]
3.4 Robotics and Advanced Manufacturing		[204]
3.5 Medical Devices	c27	[176]
3.6 Building Automation and Smart Cities		[205]
3.7 The Internet of Things		[62]
4.1 Incentives and Regulation		[198]
4.2 Cyber-Conflict		[206, 200]

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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*, pp. 1–4.

[6] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*. IEEE, 2008, pp. 495–500.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] N. Wells, "Busybox: A swiss army knife for Linux," *Linux Journal*, vol. 2000, no. 78es, p. 10, 2000.

[12] F. Fainelli, "The OpenWrt embedded development framework," in *Proceedings of the Free and Open Source Software Developers European Meeting*, 2008.

[13] 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.

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

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

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

[17] 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.

[18] 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.

[19] C. Sun, "No IoT without IPv6," *Computer World*, 2016.

[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] I. Series, "Business blackout," 2015.

[27] A. Greenberg, "Hackers remotely kill a jeep on the highway?with me in it," *Wired*, vol. 7, p. 21, 2015.

[28] 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.

[29] 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.

[30] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard law review*, pp. 193–220, 1890.

[31] 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.

[32] 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.

[33] 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.

[34] S. McLaughlin, "Cps: Stateful policy enforcement for control system device usage," in *Proceedings of the 29th Annual Computer Security Applications Conference*, ser. ACSAC '13. New York, NY, USA: ACM, 2013, pp. 109–118.

[35] 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.

[36] 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.

[37] 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.

[38] 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/

[39] 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.

[40] M. Rocchetto and N. O. Tippenhauer, "On attacker models and profiles for cyber-physical systems," in *European Symposium on Research in Computer Security*. Springer, 2016, pp. 427–449.

[41] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[42] "Data breach digest. scenarios from the field." Verizon, Tech. Rep., 2017.

[43] 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.

[44] K. Zetter, *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Broadway books, 2014.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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 *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, 2013, pp. 145–159.

[50] K. Fu and W. Xu, "Risks of trusting the physics of sensors," *Communications of the ACM*,

vol. 61, no. 2, pp. 20–23, 2018.

[51] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, 2013, pp. 160–173.

[52] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 75–86.

[53] N. G. Leveson and C. S. Turner, "An investigation of the therac-25 accidents," *IEEE computer*, vol. 26, no. 7, pp. 18–41, 1993.

[54] B. Krebs, *Cyber Incident Blamed for Nuclear Power Plant Shutdown*. http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html: Washington Post, June 2008.

[55] R. J. Turk, "Cyber incidents involving control systems," Idao National Laboratory, Tech. Rep. INL/EXT-05-00671, October 2005.

[56] R. Esposito, "Hackers penetrate water system computers," http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html, October 2006.

[57] T. Reed, *At the Abyss: An Insider's History of the Cold War*. Presidio Press, March 2004.

[58] A. Cherepanov, "Win32/industroyer, a new threat for industrial control systems," *White Paper. ESET*, 2017.

[59] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, and C. Glyer, "Attackers deploy new ICS Attack Framework" TRITON" and cause operational disruption to critical infrastructure," *Threat Research Blog*, 2017.

[60] 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.

[61] U. NIST, "Guidelines for smart grid cyber security (vol. 1 to 3)," *NIST IR-7628, Aug*, 2010.

[62] K. Boeckl, M. Fagan, W. Fisher, N. Lefkovitz, K. Megas, E. Nadeau, B. Piccarreta, D. Gabel O'Rourke, and K. Scarfone, "Considerations for managing internet of things (iot) cybersecurity and privacy risks," National Institute of Standards and Technology, Tech. Rep., 2018.

[63] NERC-CIP, *Critical Infrastructure Protection*. http://www.nerc.com/cip.html: North American Electric Reliability Corporation, 2008.

[64] E. Byres, P. Eng, and I. Fellow, "Using ansi/isa-99 standards to improve control system security," *White paper, Tofino Security*, 2012.

[65] R. Ross, M. McEvilley, and J. Oren, "Nist special publication 800-160: Systems security engineering considerations for a multidisciplinary approach in the engineering of trustworthy secure systems," *Gaithersburg: National Institute of Standards and Technology*, 2016.

[66] E. Lear, R. Droms, and D. Romascanu, "Manufacturer usage description specification (work in progress)," Internet-Draft draft-ietf-opsawg-mud-18. IETF Secretariat. http://www. ietf. org/internet-drafts/draft-ietf-opsawg-mud-18. txt, Tech. Rep., 2018.

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

[68] S. Hurd, R. Smith, and G. Leischner, "Tutorial: Security in electric utility control systems," in *61st Annual Conference for Protective Relay Engineers*, April 2008, pp. 304–309.

[69] 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.

[70] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4. ACM, 2011, pp. 2–13.

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

[72] 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.

[73] S. Nürnberger and C. Rossow, "–vatican–vetted, authenticated can bus," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2016, pp. 106–124.

[74] 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.

[75] 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.

[76] 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.

[77] D. C. Latham, "Department of defense trusted computer system evaluation criteria," *Department of Defense*, 1986.

[78] G. Klein, K. Elphinstone, G. Heiser, J. Andronick, D. Cock, P. Derrin, D. Elkaduwe, K. Engelhardt, R. Kolanski, M. Norrish *et al.*, "sel4: Formal verification of an os kernel," in *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles*. ACM, 2009, pp. 207–220.

[79] 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.

[80] K. Eldefrawy, G. Tsudik, A. Francillon, and D. Perito, "Smart: Secure and minimal architecture for (establishing dynamic) root of trust." in *NDSS*, vol. 12, 2012, pp. 1–15.

[81] 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.

[82] 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.

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

[84] A. Abbasi, T. Holz, E. Zambon, and S. Etalle, "Ecfi: Asynchronous control flow integrity for programmable logic controllers," in *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACM, 2017, pp. 437–448.

[85] 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.

[86] 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.

[87] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *2011 17th IEEE Pacific Rim International Symposium on Dependable Computing*. IEEE, 2011, pp. 184–193.

[88] 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.

[89] C. Markman, A. Wool, and A. A. Cardenas, "Temporal phase shifts in scada networks," *arXiv preprint arXiv:1808.05068*, 2018.

[90] 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.

[91] 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.

[92] 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.

[93] 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.

[94] 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.

[95] 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.

[96] M. Krotofil, J. Larsen, and D. Gollmann, "The process matters: Ensuring data veracity in cyber-physical systems," in *Proceedings of the ACM Symposium on Information, Computer and Communications Security (AsiaCCS)*. ACM, 2015, pp. 133–144.

[97] R. J. Patton, P. M. Frank, and R. N. Clarke, *Fault diagnosis in dynamic systems: theory and application*. Prentice-Hall, Inc., 1989.

[98] S. X. Ding, *Model-based fault diagnosis techniques: design schemes, algorithms, and tools*. Springer Science & Business Media, 2008.

[99] G. Bernieri, E. E. Miciolino, F. Pascucci, and R. Setola, "Monitoring system reaction in cyber-physical testbed under cyber-attacks," *Computers & Electrical Engineering*, vol. 59, pp. 86–98, 2017.

[100] 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 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 1092–1105.

[101] 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.

[102] 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.

[103] 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.

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

[105] R. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the 1st Workshop on Secure Control Systems*, 2010.

[106] 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.

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

[108] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in

power networks," in *Proceedings of the Workshop on Secure Control Systems*, 2010.

[109] 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.

[110] 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.

[111] 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.

[112] 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.

[113] 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.

[114] 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.

[115] 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.

[116] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and fault-tolerant control*. Springer-Verlag, September 26 2003.

[117] 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 6th ACM symposium on information, computer and communications security*. ACM, 2011, pp. 355–366.

[118] 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.

[119] 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 Computing*, vol. 9, no. 4, pp. 482–493, July 2012.

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

[121] 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.

[122] 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.

[123] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *To appear in Proceedings of INFOCOM*, 2015.

[124] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 46–65, 2015.

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

[126] S. Litchfield, D. Formby, J. Rogers, S. Meliopoulos, and R. Beyah, "Rethinking the honeypot for cyber-physical systems," *IEEE Internet Computing*, vol. 20, no. 5, pp. 9–17, 2016.

[127] X. Koutsoukos, G. Karsai, A. Laszka, H. Neema, B. Potteiger, P. Volgyesi, Y. Vorobeychik, and

J. Sztipanovits, "Sure: A modeling and simulation integration platform for evaluation of secure and resilient cyber–physical systems," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 93–112, 2018.

[128] B. Potteiger, W. Emfinger, H. Neema, X. Koutosukos, C. Tang, and K. Stouffer, "Evaluating the effects of cyber-attacks on cyber physical systems using a hardware-in-the-loop simulation testbed," in *Resilience Week (RWS), 2017*. IEEE, 2017, pp. 177–183.

[129] B. Green, A. T. Le, 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," 2017.

[130] A. P. Mathur and N. O. Tippenhauer, "Swat: A water treatment testbed for research and training on ics security," in *Cyber-physical Systems for Smart Water Networks (CySWater), 2016 International Workshop on*. IEEE, 2016, pp. 31–36.

[131] M. H. Cintuglu and O. A. Mohammed and K. Akkaya and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 446–464, 2017.

[132] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "Scada cyber security testbed development," *Power Symposium, 2006. NAPS 2006. 38th North American*, pp. 483–488, Sept. 2006.

[133] 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.

[134] 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 ACM workshop on Smart energy grid security*. ACM, 2013, pp. 29–34.

[135] 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.

[136] Government Accountability Office, "Electricity grid modernization. progress being made on cybersecurity guidelines, but key challenges remain to be addressed," January 2011.

[137] 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.

[138] 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.

[139] 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.

[140] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proceedings of IEEE Smart Grid Commnunications Conference (SmartGridComm)*, October 2010.

[141] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proceedings of IEEE Smart Grid Commnunications Conference (SmartGridComm)*, October 2010.

[142] 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.

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

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

[145] 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.

[146] A.-M. Olteanu, K. Huguenin, R. Shokri, M. Humbert, and J.-P. Hubaux, "Quantifying interdependent privacy risks with location data," *IEEE Transactions on Mobile Computing*, 2016.

[147] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *2011 IEEE Symposium on Security and Privacy*. IEEE, 2011, pp. 247–262.

[148] 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.

[149] 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.

[150] "Guess what's 'easily hacked'? yes, that's right: Smart city transport infrastructure," 22 April 2016, http://www.theregister.co.uk/2016/04/22/smart_transport_hackable/.

[151] (2014, October 28) Sensys networks traffic sensor vulnerabilities (update a). https://ics-cert.us-cert.gov/advisories/ICSA-14-247-01A.

[152] (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.

[153] 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.

[154] "Defending against sybil devices in crowdsourced mapping services," in *14th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'16)*, 2016.

[155] (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.

[156] 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.

[157] 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.

[158] M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of ais automated identification system," in *Proceedings of the 30th annual computer security applications conference*. ACM, 2014, pp. 436–445.

[159] 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.

[160] 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.

[161] 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.

[162] 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.

[163] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *DEF CON*, vol. 24, 2016.

[164] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," 2015.

[165] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications," in *International Conference on Cryptographic*

Hardware and Embedded Systems. Springer, 2017, pp. 445–467.

[166] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling uavs with sensor input spoofing attacks." in *WOOT*, 2016.

[167] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Radionavigation Laboratory Conference Proceedings*, 2008.

[168] E. Weise. (2017, Sept. 26) Mysterious gps glitch telling ships they're parked at airport may be anti-drone measure.

[169] 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.

[170] M. Yampolskiy, W. E. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum, and Y. Elovici, "Security of additive manufacturing: Attack taxonomy and survey," *Additive Manufacturing*, 2018.

[171] S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and security challenges in 3d printing," *Jom*, vol. 68, no. 7, pp. 1872–1881, 2016.

[172] 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. 3, pp. 45–54, March 2017.

[173] C. Cerrudo and L. Apa, "Hacking robots before skynet," *Cybersecurity Insight, IOActive Report, Seattle, USA*, 2017.

[174] 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.

[175] R. White, D. Christensen, I. Henrik, D. Quigley *et al.*, "Sros: Securing ros over the wire, in the graph, and through the kernel," *arXiv preprint arXiv:1611.07060*, 2016.

[176] 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.

[177] 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.

[178] X. Wang, M. Mizuno, M. Neilsen, X. Ou, S. R. Rajagopalan, W. G. Boldwin, and B. Phillips, "Secure rtos architecture for building automation," in *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*. ACM, 2015, pp. 79–90.

[179] K. Zetter, "Researchers hack building control system at google australia office," *Wired. com, available at https://www. wired. com/2013/05/googles-control-system-hacked (accessed 9th June, 2017)*, 2013.

[180] D. Bilefsky. (January) Hackers use new tactic at austrian hotel: Locking the doors. The New York Times.

[181] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "Iot goes nuclear: Creating a zigbee chain reaction," in *Security and Privacy (SP), 2017 IEEE Symposium on*. IEEE, 2017, pp. 195–212.

[182] 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.

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

[184] K. Poulsen. (2010, March) Hacker disables more than 100 cars remotely. WIRED.

[185] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communi-*

cations Surveys & Tutorials, vol. 20, no. 4, pp. 3453–3495, 2018.

[186] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "Sok: Security evaluation of home-based iot deployments," in *SoK: Security Evaluation of Home-Based IoT Deployments*. IEEE, p. 0.

[187] E. S. C. S. W. Group, "Roadmap to achieve energy delivery systems cybersecurity," U.S. Department of Energy, Tech. Rep., 2011.

[188] B. Schneier, "The internet of things will upend our industry," *IEEE Security and Privacy*, vol. 15, no. 2, pp. 108–108, 2017.

[189] 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

[190] M. Y. Vardi, "Cyber insecurity and cyber libertarianism," *Communications of the ACM*, vol. 60, no. 5, pp. 5–5, 2017.

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

[192] M. Daniel. (2013) Incentives to support adoption of the cybersecurity framework. https://obamawhitehouse.archives.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

[193] "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.

[194] (2014) Protection of critical infrastructure. European Commission. [Online]. Available: https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

[195] 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," 2016.

[196] 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.

[197] "Consumer reports to begin evaluating products, services for privacy and data security," Consumer Reports, March 2017.

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

[199] 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.

[200] M. Schmitt, "International law in cyberspace: The Koh Speech and the Tallinn manual juxtaposed," 2012.

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

[202] R. Langner, *Robust Control System Networks: How to Achieve Reliable Control After Stuxnet*. Momentum Press, 2011.

[203] 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.

[204] 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.

[205] W. Granzer, F. Praus, and W. Kastner, "Security in building automation systems," *IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS*, vol. 57, no. 11, 2010.

[206] P. W. Singer, *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin, 2009.

ACRONYMS

Similarly, you can define acronyms in the document preamble and then refer to them as follows:

CPS Cyber-Physical System

SCADA Supervisory Control and Data Acquisition System.