Current Cyber-Defense Trends in Industrial Control Systems

Juan E. Rubio, Cristina Alcaraz, Rodrigo Roman, Javier Lopez
Department of Computer Science, University of Malaga,
Campus de Teatinos s/n, 29071, Malaga, Spain
{rubio,alcaraz,roman,jlm}@lcc.uma.es

Abstract

Advanced Persistent Threats (APTs) have become a serious hazard for any critical infrastructure, as a single solution to protect all industrial assets from these complex attacks does not exist. It is then essential to understand what are the defense mechanisms that can be used as a first line of defense. For this purpose, this article will firstly study the spectrum of attack vectors that APTs can use against existing and novel elements of an industrial ecosystem. Afterwards, this article will provide an analysis of the evolution and applicability of Intrusion Detection Systems (IDS) that have been proposed in both the industry and academia.

Keywords: SCADA, Industrial Control, Intrusion Detection, APT, Industry 4.0

1 Introduction

Critical Infrastructures like nuclear plants of power grids have their production cycle managed by industrial control systems, such as SCADA (Supervisory Control and Data Acquisition) systems. These industrial networks comprise a wide range of devices such as sensors, PLCs (Programmable Logic Controllers), or RTUs (Remote Terminal Units), that ultimately gather real-time data about the production chain and accordingly issue control commands to regulate the entire process remotely.

Traditionally, SCADA systems and industrial networks have been working in an isolated way during decades, since all the aforementioned devices used to run proprietary communication protocols in a closed environment. However, they are nowadays being interconnected to external networks (e.g., Internet) for the outsourcing of services and the storage of data. Amongst the reasons of this tendency are the decrease in costs and the standardization of hardware and software used in industrial control systems (ICS). Namely, industrial communication protocols working with Ethernet and TCP/IP, such as Ethernet/IP, Ethernet POWERLINK, CANopen, PROFINET, Modbus/TCP or HART/IP; and also fieldbus protocols (e.g., HART, wirelessHART, etherCAP, IO-Link). Additionally, there are other protocols designed for the management and control of all industrial equipment, such as the CIP or OPC UA. As a result of this evolution, the complexity of communication infrastructures in ICS is dramatically increasing. However, this is just the beginning: new paradigms like IoT (Internet of Things) or Cloud computing are also being integrated into current industrial environments, giving shape to the so-called Industry 4.0 [1]. Under this concept, all industrial entities are able to collaborate with each other so as to take real-time decisions in a distributed way, enabling the deployment of innovative industrial services of all kinds.

Consequently, this modernization of the industry with the introduction of IT technologies is coupled with a substantial increase in security risks [2] based on new specific threats, operating under different threat modes [3] that have not been addressed before. As a result, an industrial system becomes complex and critical, besieged by multiple attack vectors that can be ultimately leveraged to perpetrate an Advanced Persistent Threat (APT) [4, 5]. This represents a sophisticated attack perpetrated by an expert adversary, and is characterized for its ability to go undetected within the victim network for a certain period of time. Due to the complexity of these attacks – which involve several steps – and the high amount of successful APT campaigns perpetrated by malicious actors [6], it is crucial to understand what is the true scope and detection capabilities of the first line of defense; that is, existing Intrusion Detection Systems (IDS).

This article is an extended version of the conference paper [7]. It explores the existing techniques and mechanisms that try to detect specific threat vectors within an industrial context, making emphasis on the special case of APTs but without losing sight of the future industrial paradigms. The remainder of this article is organized as follows: Section 2 highlights the threats to which control systems are exposed today. Taking into account this landscape, Section 3 addresses the search for defense techniques against APTs, specially intrusion detection systems. Solutions from both the industry and academia are presented in Sections 4 and 5, respectively. Finally, Section 6 discusses the application of these mechanisms in practice, and the conclusions drawn are presented in Section 7.

2 Cybersecurity threats

After several years of being subject to a multitude of threats [8], today's industry is still at risk. According to the annual reports of ICS-CERT [9], IBM® X-Force® Research [10], and Sikich [11], the number of threats has tended to rise annually in the manufacturing industry, either because of unforeseen occurrences or through planned actions. Irrespective of the causes, the consequences affect the normal performance of control and industrial process, thereby affecting the expected production rate and the final distribution to end-users. This situation is unfortunately aggravated when interconnecting traditional technologies and information systems to production environments. For the purposes of our analysis, both types of attack vectors that affect the industrial environment (i.e., the ones inherited from the traditional industrial systems and those arisen with the interconnection of IT technologies) can be classified following the taxonomy given by the IETF standard-7416 [12], in which the threats are grouped according to the attack goals against the minimum security services [13] such as availability, integrity, confidentiality and authentication.

2.1 Traditional Threats in IS and ICS

Availability threats: apart from the typical subtraction of devices (e.g. PLC and RTU) or communication infrastructures, it is essential to highlight the threats related to (distributed) denial of services ((D)DoS) attacks, the techniques of which mainly focus on the routing (e.g. relay attacks, selective forwarding, grey hole, black hole or botnets).

Integrity threats: includes from the typical sabotage of the industrial equipment to the injection of malware [14] to slow down the operational performance, obtain sensitive information, modify the operation of the devices, etc. These threats are also related to the alteration of the industrial communication protocols and/or the real traffic values produced by field devices, controllers or corporate network equipment. Impersonation of nodes and spoofing are also applicable to an industrial context, due in part to the susceptibility to Man-in-the-Middle attacks and the existing weaknesses of the industrial communication protocols. We also have to consider that the vast majority of such protocols are still legacy protocols, in the sense that they were originally designed to transfer control information without considering various cybersecurity requirements such as authentication between peers, integrity of messages, or the confidentiality of the communication channels.

Confidentiality threats: within this category the illicit disclose techniques through passive traffic analysis (regarding topologies and routes) and theft of sensitive data (related to industrial process, customers, administration) or configurations should be highlighted. An example of information theft is that achieved by injecting code in the operational applications (often webs through cross-site scripting (XSS) or SQL Injection) so as to obtain or corrupt the control measurements/actions, the company and/or end-users privacy, or the security credentials.

Authentication/authorization threats: the authentication in this point includes those attackers that generally try to escalate privileges by taking advantage of a design flaw or vulnerability in the software in order to gain unauthorized access to protected resources. For example, according to the IBM® X-Force® research report [10], 45% of all attacks registered in 2015 focused on unauthorized accesses, followed by malicious code (29%) and sustained probe/scan (16%) attacks. In order to carry out these attacks, attackers need to apply specific social engineering techniques (e.g. phishing attacks, chain of spam letters) to collect strategic information from the system. Apart from this, the easy mobility of in-plant operators and their interactions through the use of hand-held interfaces (smart-phones, tablets, laptops) also lead to numerous security problems, probably caused by mis-configurations or unsuitable access control, both at the logical (use of simple passwords) and physical (access to equipment) level.

2.2 Present and future landscape of threats in IS and ICS

Besides addressing the aforementioned security issues, it is necessary to envision a set of future security threats that might appear, especially pertinent when integrating new trending technologies such as IoT or Cloud computing infrastructures. As explained earlier, these technologies are already being applied to ICS and herald the so-called fourth Industrial Revolution, or Industry 4.0 [1].

2.2.1 Industrial Internet of Things threats

IoT interconnects sensors and all kinds of devices with Internet networks, to gather information about physical measures, location, images, etc. The Industrial IoT (IIoT) specifically pursues a vertical integration among all the components that belong to the industrial architecture, ranging from machines to operators or the product itself. With respect to security, the situation is further complicated when we take into consideration the scarce autonomy and computational resources that these devices have. Continuing with the IETF standard 7416 [12], we can distinguish the following range of threats:

Availability threats: comprises the disruption of communication and processing resources: firstly, against the routing protocol [15], influencing its mode of operation (creating loops, modifying routes, generating errors, modifying message delays, etc.) through different attacks, which can be directly committed at the physical level through jamming or interferences. Secondly, against the equipment itself, including the exhaustion of resources (processing, memory or battery) exploitation of vulnerabilities in the software (as well as reverse engineering) that govern control devices such as PLCs, in addition to running malicious code or malware: viruses, Trojans, etc. [16]. Thirdly, we have to stress the data traffic disruption, undermining the functionality of the routers in the network, causing a lack of availability of certain services. It is caused by vectors such as selective forwarding, wormhole or sinkhole attacks.

Integrity threats: it means the manipulation of routing information to influence the traffic and fragment the network, like a Sybil attack [17]. This becomes the gateway to other attacks such as black hole or denial of service, causing the routes to pass through the more congested nodes. The form of attack includes falsification of information (the node advertises anomalous routes), routing information replay, physical compromise of the device or attacks on the DNS protocol [18]. Node identity misappropriation can also be taken into account, opening the door to other attacks that result in the modification of data of all types.

Confidentiality threats: includes the exposure of information of multiple kinds: firstly, the one related the state of the nodes and their resources (available memory, battery, etc.). One way is the so-called side channel attacks [19], where the electromagnetic emanations of devices leak information about the execution of certain operations. Secondly, it also includes the exposure of routing information and the topology, which constitutes rich information for the attackers as it enables them to identify vulnerable equipment. Since this information resides locally in the devices, attacks against the confidentiality of this information will be directed at the device, either physically compromising it or via remote access. Lastly, it is also possible to have the exposure of private data, usually collected by wearable devices belonging to operators within the organization, which can reveal information about their performance at work or their location. One attack vector could be the use of social engineering or phishing.

Authentication threats: we can highlight the impersonation and introduction of dummy / fake nodes, capable of executing code or injecting illegitimate traffic to potentially control large areas of the network or perform eavesdropping. An attack vector consists of the forwarding of digital certificates used in authentication protocols or physical or network address spoofing. Escalation of privileges can also be faced as a consequence of a non-existent or poor access control, when the attacker can take advantage

Table 1: Overview of threats that affect industrial systems

	Threats	Traditional	IIoT	Cloud Comp.	APT-states	Impact on		
						Control in-plant	Corp. Net.	End users
Availability	Subtraction of devices	✓	✓		E	✓		
	DDoS attacks	✓	✓	✓	C, E, P	✓	✓	
	Attacks on-path	✓	✓		C, E, T, F, P	✓	✓	
	Exhaustion of node resources	✓	✓		C, E	✓	✓	
	Service theft			✓	C, E	✓	✓	
Integrity	Incorrect configuration	✓	✓	✓	C, E	✓	✓	
	Reverse engineering and/or malware injection	✓	✓	✓	R, C, P, E, T, F	✓	✓	
	False data injection	✓	✓		C, E, P	✓		
	Spoofing	✓	✓		C, E	✓	✓	✓
	Manipulation of routing information	✓	✓		C, E, P	✓		
Confidentiality	Sensitive information theft	✓	✓	✓	C, E, F	✓	✓	✓
	Nodes status exposure (side-channel attacks)		✓	✓	R, C, E, F	✓		
	Passive traffic analysis	✓	✓		R, C, E, T, F, P	✓	✓	
	Infrastructure information exposure (shared memory systems attacks)			✓	C, E, T, F, P	✓	✓	✓
AAA	Privilege escalation	✓	✓	✓	C, E, P	✓	✓	✓
	Social engineering	✓		✓	R, C, E	✓	✓	✓
	Deficient control access	✓	✓	✓	C, E	✓	✓	✓
	Impersonation of nodes (fake/dummy nodes)	✓	✓		C, E	✓		

of design flaws or vulnerabilities in IoT devices to access protected resources without authorization.

2.2.2 Cloud Computing threats

In recent years cloud computing has changed the way in which information technology (IT) is managed, through an environment that provides on-demand resources over the Internet with a low cost of investment and easy deployment. For our work, cloud computing acquires dual importance. On the one hand, many organizations use the cloud to provide IoT services, acquiring sensor data and sending commands to actuators. On the other hand, it is also necessary to take into account the delegation of certain analysis and production processes to the cloud, in what is known as cloud-based manufacturing [20]. The ultimate goal of this model is to enable customers to design, configure and manufacture a product through a shared network of suppliers throughout its life cycle, enhancing the efficiency and reducing costs. In summary, these factors make it necessary to analyse the full range of threats that cloud computing faces [21][22]:

Availability threats: This category includes the so-called service theft attack, which takes advantage of the vulnerabilities and inaccuracies that exist in the scheduler component of some hypervisors, where the service is charged considering the time spent running virtual machines – instead of based on the CPU time in use. This can be exploited by attackers in order to use services at the expense of other clients, making sure that the processes of interest are not executed at each tick of the scheduler. We also contemplate denial of service attacks: the attacker causes the service to become inaccessible for its legitimate users. This is the most serious type of attack on cloud computing, because of the ease with which it can be carried out and the difficulties in preventing them.

Integrity threats: the most important one comes with a malware injection attack, where the attacker replicates the service instance that is provided to a client (a virtual machine, for example) and replaces it with a manipulated one that is hosted again in the cloud. This means that requests sent by the legitimate user are processed in the malicious service, and the attacker can access the exchanged data. To do this, the most common way is to appropriate access privileges or introduce malware into multiple format files, jeopardizing the confidentiality and privacy of the data.

Confidentiality threats: firstly, side-channel attacks with virtual machines must be stressed, in which the attacker, from his virtual machine, attacks others that are running on the same physical hardware. This allows them to access their resources by studying the electromagnetic emanations, the processor cache, etc. This information can be useful in choosing the most attractive targets to attack. This category also includes attacks on shared memory systems: they work as a gateway to other types of attacks such as malware or side-channel attacks, and consist in analyzing the shared memory (cache or main memory) used by virtual and physical machines to obtain technical information about the infrastructure, such as the processes that are running, the number of users, or even the memory dump of virtual machines.

Authentication threats: the attacker tries to obtain information from the clients of different applications or trusted companies by posing as themselves. This is done through malicious services with the same appearance as those are normally offered through a link sent by email. Thus, the attacker can obtain sensitive information from his/her victims by entering their data, such as passwords or bank cards. This way, the attacker can illicitly host services in the cloud and access accounts of certain services.

Altogether, many of these attack vectors (from both traditional and future threats in industrial systems) are implemented in advanced persistent threats (APTs). This is a class of sophisticated attack perpetrated against a particular organization, where attackers have significant experience and resources. Such attackers infiltrate victim networks by taking advantage of a multitude of vulnerabilities (often unknown, i.e. zero-day), and go unnoticed for a prolonged period of time [4, 5]. Stuxnet was the first APT recognized by the industry in 2010 [23], but later many others have appeared, such as Duqu, DragonFly, BlackEnergy, and ExPetr [24, 6].

As discussed in [3], the exploitation of many of these threats also occur during the stages of an advanced persistent threat:

1. Recognition (R) of the victim network, so as to search for exploitable vulnerabilities to penetrate its defenses.

2. Communication (C): the attacker sends exploits to the victim, either directly (e.g., using spear phishing emails) or indirectly (e.g., compromising a third party such as a provider). By doing this, the first intrusion within the network is performed.

3. Tracking (T) of zero-day vulnerabilities that allow the attacker to execute (E) remote actions by previously launching malware or installing backdoors (e.g., to install a command and control).

4. Propagation (P) of the attack to other areas of the network (also called lateral movements), infiltrating new devices, modifying their operations and collecting sensitive information.

5. Information filtration (F): lastly, the information obtained is sent back to the domain of the attacker.

A complete overview of the present and future threats faced by an Industrial System is summarized in Table 1, where all of them are linked with the APT stages introduced before. We can observe that most of these threats can be potentially leveraged for the first intrusion and the subsequent execution of exploits. However, the initial information gathering about points of entry and vulnerabilities is mainly performed by analyzing metadata emanated from servers to sensors, and also by social engineering. As for the final exfiltration of information, it normally requires that the attacker has taken over the device to send data such that it resembles normal network traffic, making any detection attempts challenging.

Even though most of these are in general inherited by IoT and cloud technologies, they also pose new hazards to be addressed. Firstly, because the technical constraints that the new devices and communication protocols feature create new vulnerabilities and attack vectors. Secondly, due to the impact they cause in the assets within the organization, which comprise control and corporative resources as well as end-users (e.g., clients or operators). Altogether, this makes it necessary to find new defense solutions and tailor the current detection mechanisms, as discussed in the following.

3 Defense techniques

Due to the variety of attack vectors that an APT exposes, multiple security solutions must be combined at different levels. In this sense, Intrusion Detection Systems (IDS) pose the first line of defense, as they detect unauthorized access to the network or one of its systems, monitoring its resources and the traffic generated in search of behaviors that violate the security policy established in the production process.

There are many methods for performing intrusion detection. One possibility is the ***signature-based*** **IDS**, which tries to find specific patterns in the frames transmitted by the network. However it is precisely for that reason that it is impossible for them to detect new types of attacks whose pattern is unknown [25].

Another possibility is the ***anomaly-based*** **IDS**, which compare the current state of the system and its generated data with the normal behavior of the system, to identify deviations present when an intrusion occurs. However, in the context of control systems, restrictions such as the heterogeneity of the data collected in an industrial environment, the noise present in the measurements, and the nature of the anomalies (attacks vs. faults) must be taken into consideration.

For this reason, numerous detection techniques have been based on areas such as statistics or artificial intelligence [26], each with a different level of adaptation depending on the scenario of the application to be protected [27]:

Data mining-based detection: based on the analysis of an enormous amount of information in search of characteristics that enable distinguishing if the data is anomalous. In this category we find: *Classification techniques*: creation of a mathematical model that classifies data instances into two classes: "normal" or "anomalous". This model is trained with already classified example data. *Clustering-based techniques*: like the previous category, they seek to classify instances of data but in different groups or clusters, according to their similarity. This is mathematically represented by the distance in the space between the points associated with that information. *Association rule learning-based techniques*: they process the data set to identify relationships between variables, in order to predict the occurrence of anomalies based on the presence of certain data.

Statistical anomaly detection: in this approach, inference tests are applied to verify whether a piece of data conforms or not to a given statistical model, in order to confirm the existence of intrusions: *Parametric and nonparametric-based methods*: while the former are those that assume the presence of a probability distribution that fits the input data to estimate the associated parameters (which does not have to conform to reality), the second tries to look for the underlying distribution. In general, both are accurate and noise-tolerant models of missing data, which allow us to find confidence intervals to probabilistically determine when an anomaly occurs. *Time series analysis*: they predict the behavior of the system by representing the information it generates in the form of a series of points measured at regular intervals of time. Although they are able to detect slight disturbances in the short term, they are less accurate in predicting drastic changes. *Markov chains*: they consist of mathematical representations to predict the future behavior of the system according to its current state. For this purpose, state machines are used with a probability associated with transitions. Its accuracy increases when using complex multi-dimensional models. *Information based techniques*: they involve the observation of the information generated (for example, the capture of the traffic) and its intrinsic characteristics in search of irregularities associated with threats-packages for denial of service, messages to cause attacks by buffer overflow, etc. They are generally efficient systems tolerant to changes and redundancy in the information. *Spectral theory-based techniques*: these techniques use approximations of the data to other dimensional sub-spaces where the differences between the normal and the anomalous values are evidenced. They are usually complex and are used to detect stealth attacks, those which are specially designed to circumvent detection techniques.

Knowledge-based detection: in this case, the knowledge about specific attacks or vulnerabilities is acquired progressively, ensuring a low rate of false positives, thereby resulting in a system that is resistant to long-term threats. However, the security depends on how often the knowledge base is updated, and the granularity with which information about new threats is specified. Examples of these techniques include state *transition-based* techniques, *Petri nets* or *expert systems*.

Machine learning-based detection: this type of technique bases the detection on the creation of a mathematical model that learns and improves its accuracy over time, as it acquires information about the system to be protected. In this category we find techniques of artificial intelligence whose foundations are also closely linked to statistics and data mining: *Artificial neural networks*: they are inspired by the human brain and are able to detect anomalies when dealing with a large data set with interdependencies. It allows the data to be classified as normal or anomalous with great precision and speed, although they need a long time to create the model, which prevents them from being applied in real time systems. *Bayesian networks*: events are represented in a probabilistic way through directed acyclic graphs where the nodes represent states and the edges define the conditional dependencies between them. The purpose is to calculate the probability of an intrusion from the data collected. *Support vector machines*: this is a technique that classifies the data according to a hyperplane that separates both classes (habitual and anomalous information). Since it works with a linear combination of points in space (given by the input data), its complexity is not high and its quality of precision is acceptable. However, it does not behave accurately in presence of similar data, for which there is no hyperplane that divides them correctly. *Fuzzy logic*: rule-based structures are used to define a reasoning with inaccurately expressed information, like humans do in everyday language (being able to differentiate when a person is “tall” or “short” or something is “slightly cold”). Therefore it models the behavior of complex systems without excessive accuracy (leading to speed and flexibility), but obviously it means the accuracy of the anomaly detection is not high either. *Genetic algorithms*: they simulate the phenomenon of natural selection to solve a complex problem for which there is no clear solution. In the first phase, a set of individuals of a population is randomly generated (representing the possible solutions to that problem). From there, numerous iterations are carried out where successive operations of selection, replacement, mutation and crossing are applied to ultimately find an optimal solution. Although it is moderately applicable to the detection of anomalies, it has been shown that it is unable to detect unknown attacks.

On the other hand, there are also ***specification-based*** **IDS** [28]. The principle behind them is similar to systems based on anomalies, in the sense that the current state of the system is compared to an existing model. However, in this case the specifications are defined by experts, which reduces the number of false positives to the extent that they are defined in detail. State diagrams, finite automata, formal methods, etc. are often used. They are often combined with *signature-based* and *anomaly-based* IDS.

One alternative to IDS solutions are precisely Intrusion Prevention Systems (IPS). These systems have the ability to (i) detect an anomaly within the system and (ii) mitigate the effect of the threat. Cubix’s TippingPoint [29] is a clear example of IPS capable of detecting traffic anomalies in VoIP infrastructures, routers and switches. Similarly, Extreme networks IPS also ensures business continuity by monitoring the behavior and state of the operating systems such as Windows [30]; and Corero Network Security offers in-line intrusion detection and automated response by combining behavior-based and signature-based analysis [31].

However, the inclusion of these systems within complex infrastructures of critical nature is not always feasible. The automation of response actions implies that we need to trust in the reliability and accuracy of such actions; yet, depending on the situation, it is very probable that the actions may not be so suitable for a critical context [32].

In addition, the false positive rates in the detection processes can also significantly impact on the final response – and indirectly affect the performance of the critical control systems [33]. These characteristics are widely reflected in the state of the art, where there are multiple approaches and researches in the field and for general contexts [34, 35], but not enough for critical contexts.

As specified in [36, 37], it is essential to provide customizable IPSs for critical environments, or at least for those remote areas where no human operator with reactive capacity is available – either remotely or on-site. This work will evidently involve more research in the area, since it is essential to find the sequences of parameters and actions that best suit a situation, searching the way to offer proactive measures that help respond to incidents or threats before major disruptions may arise [36]. This protection property was also referenced by the National Institute of Standards and Technology (NIST) in [38].

Even though IDS (and IPS) represent a valid solution to address the first stages of an APT, it becomes essential for security staff to introduce additional techniques and procedures to guarantee a minimum impact on the infrastructure [5]. Some of them can be summarized as follows:

- Advanced detection of malware: for instance, the execution of processes and files from suspicious provenance in sandbox mode, or the on-line analysis of malware, in a non-intrusive way.

- Data loss prevention: as the last line of defense, this software protects against the breach of data by controlling the access and use of sensitive information.

- Whitelisting: since the intruder intends to connect to a external server to set up a command and control service and ultimately filtrate some data, a countermeasure to prevent it consists in the use of access control policies for the inbound and outbound connections (e.g., specifying the exclusive set of URLs that each device can access).

- Trusted Computing: a secure environment is created by means of hardware modules that guarantee the integrity and reliability of the software that is installed and used within the industrial system.

- Intelligence-Driven Defense: based on the knowledge provided by experts and victims of APTs, a intelligence feedback loop is created to identify patterns of intrusions and understand the adversaries' techniques, in order to accurately design and implement proper countermeasures.

- Security Awareness Training: training and consciousness about the best security practices becomes especially important to protect against APTs, since most intrusions are performed with the use of social engineering techniques.

In order to give a more detailed vision of actual technologies that make use of these and other mechanisms, a review of the state of the art of defense solutions in both the industry and academia is given in the following.

4 Industrial IDS Products

Defense Strategies	**Leading Companies**
Zone-based	*Advenica, ARGUS, BAE Systems, Bayshore, Checkpoint, Deep Secure, Distrix, Fortinet, Fox-IT, Icon Labs, Intel, Moxa, Nexor, Paloalto Networks, Phoenix Contact, Positive Technologies, Seclab, Sophos, Tofino Security, Towersec, Waterfall Security*
Configuration-based	*Verve, PAS, Nextnine, DL2C, AlgoSec, Sigmaflow, Dragos Security, Amenaza Tech. LTD, Positive Technologies*
Signature-based	*Cisco, Cyberark, Cyberbit, Digital Bond, ECI, FireEye*
Context-based	*AlertEnterprise, WurldTech (GE)*
Honeypot-based	*Attivo Networks*
Anomaly-based	*Control-See, CritiFence, CyberX, Darktrace, HALO Digital, ICS2, Indegy, Leidos Nation-E, Nozomi, PFP Cybersecurity, RadiFlow, SCADAfence, SecureNok, Sentryo, SIGA, ThetaRay*

Table 2: Leading companies in the market

At present, there are various commercial solutions whose goal is to provide protection mechanisms that can deter the attacks caused by APT actors. Such protection mechanisms not only include the detection mechanisms described in section 3, but also other solutions such as enhancing user awareness, separating the industrial network into various protected zones, and analyzing the configuration of the system. Most of these solutions are passive (i.e. do not affect the operation of the system), transparent (i.e. almost invisible to the existing control systems), and easy to deploy.

Table 2 provides an enumeration of the leading companies in the market that provide such protection mechanisms. In addition, a short summary of the main solutions available in the market as of Q2 2018 is provided in the next sections.

4.1 Zone separation

These products focus on facilitating the separation of the industrial network into different security zones, using traditional security solutions such as firewalls. The main challenge here is the structure of industrial networks: due to their complexity, it is necessary to consider the deployment of various zones, such as the enterprise systems (e.g. ERP), the enterprise middleware (e.g. MOM, ESB), the industrial control systems and the field device networks, and the different demilitarized zones.

Beyond the integration of traditional firewall solutions that focus on IT networks and protocols, there are various companies that provide specific solutions designed for industrial networks. One example is the FortiGate platform developed by FortiNet [39], which has the capacity to analyze multiple industrial protocols (eg Bacnet, DLMS, DNP3, EtherCAT, ICCP, IEC-60870.5.104, Modbus/TCP, OPC, Profinet) and industrial devices (eg ABB, Rockwell, Schneider Electric, Siemens, or Yokogawa). It is also important to note that, due to the manufacturing of extremely complex interconnected systems such as smart cars, there are now specific firewalls that are designed to protect these products beyond the assembly line, such as the Harman Shield solution by Harman [40].

On the other hand, there are several commercial products focused on controlling and filtering the information exchanged between zones. Various platforms, such as

Advenica ZoneGuard [41], provide a bridge between IT and OT networks that implement various information exchange policies. Other solutions, such as Data Loss Prevention [42] and Nexor Border Gateway [43], also allow the definition of policies for certain network interactions, such as outbound connections and inbound email messages, respectively.

Besides, certain products implement the "data diode" communication approach, which physically enforces a one-way flow of data. Some solutions, like Fox Data-Diode [44], focus on the integration of these diodes between IT and OT zones. Other solutions, like SecuriCDS Data Diode [41], also implement additional defense mechanisms (e.g. dual power supplies) that avoid the creation of covert data channels. Finally, there are some approaches, like Waterfall FLIP [45], that actually implement reversible diodes, which can be activated by personnel on-site in case of emergencies.

4.2 Secure configuration

There are various products in the market whose goal is to provide a holistic view of the configuration of the overall system. For example, platforms like the ICS Shield platform developed by Nextnine [46] focus on providing a centralized operations center for the management of various security aspects of the system. They include the automatic discovery and classification of the system assets, the retrieval of hardware/software state information and the management of changes in this state, the management of passwords, the secure transfer of data, the management of software updates and backups, the creation and application of security policies, and the preparation of security reports, amongst others.

Other platforms focus on the analysis of the system configuration, so as to manage and verify existing security policies. For example, the AlgoSec Security Management Solution [47] not only proactively assess existing network security policies related to firewalls and cloud access, but also is able to intelligently design policy changes and implement them whenever necessary. Continuing with the subject of verification, certain tools, such as NERC Compliance by Sigmaflow [48], provide automated compliance monitoring of existing security and reliability industrial standards. These tools not only analyze the documentation of the company in search of discrepancies with existing standards, but also validate certain compliance data in real time, such as security controls, local accounts, and logical access rights.

Finally, there are platforms whose goal is to analyze the configuration and the elements of the system in search of vulnerabilities. Some vulnerability assessment systems, such as MaxPatrol, are specifically designed for industrial settings. Due to their design, these tools can efficiently analyze the system without interrupting its regular use, and are able to monitor even ERP systems such as SAP [49]. On the other hand, there are some tools, such as SecurITree, that focus on the theoretical analysis of attack models and attack trees [50]. These tools can create reports that predict the most likely behaviour of attackers, and can help to identify risks that are otherwise undetected.

4.3 Detection: Signature-based solutions

These products consist mainly of devices that passively connect to the control network, accessing the information flow. One of the pioneers in this field is Cisco Systems, which has a large database of attack signatures on industrial environments [51]. Such attack signatures include not only generic attacks on elements of the industrial network (e.g. denial of service in human-machine interfaces (HMIs), buffer overflows in PLCs), but also specific vulnerabilities in industrial protocols (e.g. CIP Or Modbus). This database is easily upgradeable, and can be integrated into all Cisco intrusion detection systems.

There are also other products on the market that, beyond the detection of attack signatures, provide several value-added services. An example of this is the monitoring system of Cyberbit [52]. This system monitors the traffic of the network in order to map existing devices, giving the operator a real-time view of the elements of a system. In addition, it is possible to take advantage of information acquired from the device to identify elements that have known vulnerabilities.

4.4 Detection: Context-based solutions

One drawback of most products based on the detection of attack signatures and patterns is the lack of correlation between the detected events, which could provide valuable information regarding the actual scope of the attack behind those events. Another drawback is the absence of an in-depth analysis based on the context of the system: the parameters of a command can be valid in a given context, but harmful in another. As a consequence, there are several products that perform correlation and/or in-depth analysis tasks which take into account the general context of the system.

One example of these correlation systems is the Sentry Cyber SCADA software from AlertEnterprise [53]. It combines and correlates events and alerts from various domains (physical, IT and OT networks) and sources, with the aim of providing a complete security monitoring tool for industrial systems. To achieve this objective, this tool allows integration with other security tools, such as vulnerability scanners, SIEM (Security Information and Event Management) systems, IDS/IPS systems or security configuration tools.

Finally, an example of in-depth analysis solutions is Wurldtech's OPShield [54] system. OPShield performs an in-depth analysis of the network traffic, including the syntactic and grammatical structure of the protocols. Through these analyses, OPShield can inspect the commands and parameters sent to the different components of the industrial system, and even block those commands if the administrator has authorized OPShield to do so. Note that the blocking or not of these commands is determined based on the context in which they have been sent. Thus, it is possible to protect the system against seemingly valid and/or legitimate commands that are potentially dangerous for the correct operation of the system if they are sent outside the context for which they were defined.

4.5 Detection: Honeypot-based solutions

Existing solutions based on honeypot systems usually create a distributed system, through which they collect and analyze information related to the threat or attack. Thanks to the analysis and correlation of the collected information, this type of IDS / IPS systems can be able to identify the type of attack launched, the (malicious) activities carried out on the system, as well as the existence of infected devices.

Within the current marketplace, one of the major existing honeypot-based detection platforms is ThreatMatrix from Attica Networks, which is able to detect real-time intrusions in public and private networks, ICS/SCADA systems, and even IoT environments. Its flagship product is called BOTsink [55], and is able to detect advanced persistent threats (APTs) effectively, without being detected by the attackers. The client also can customize the software images that simulate SCADA devices. Such customization allows the integration of both the software and the protocols that are used in the production environment. As a result, fake SCADA devices can be made almost indistinguishable from real SCADA devices.

4.6 Detection: Anomaly-based solutions

As of Q2 2018, there are a wide range of products that make use of deep packet inspection and/or machine learning technologies to detect unusual behaviors or hidden attacks, of which there is no already identified pattern. Such products are usually deployed as rack servers, although many companies also provide virtualized solutions. Regarding the deployment location of these commercial products, most of them operate on the operational network, accessing the information flow through the SPAN ports of existing network devices. Other deployment strategies exist, though. Some products, such as UCME-OPC from Control-See [56], retrieve system information directly from the industrial process management layers. Other products make use of agents that are distributed throughout all the elements – devices and networks – of the industrial system. Finally, there are products in charge of monitoring the interactions with field devices, such as those offered by SIGA [57]; or even systems embedded within the field devices themselves, such as those offered by MSi [58], which are responsible for examining and validating the behavior of field devices.

As for the specific techniques of anomaly modeling and detection, each commercial product makes use of one or several of them. Some products, such as UCME-OPC from Control-See [56], create a model of the system based on certain conditions/rules. Whenever those rules are not fulfilled by the system parameters and values, a warning will be launched. Other products, such as XSense from CyberX [59], base their operation on the classification of system states: if a monitored system transitions to a previously unknown state, such state is classified as normal or malicious depending on multiple signals and indicators. There are also products, such as HALO Vision from HALO Analytics [60], which make use of statistical analysis.

Other products consider industrial control systems from a holistic point of view, and include the behavior of various actors, including human operators, into their own detection systems. For example, Darktrace's Enterprise Immune System [61] makes use of a variety of mathematical engines, including Bayesian estimates, to generate behavioral models of people, devices, and even the business as a whole. There are also other products, such as Wisdom ITI from Leidos [62], which offer a pro-active and real-time platform for internal threat detection. This platform not only monitors system activity indicators, but also the behavior of human employees. Another example of this is the Privilege Account Security Solution by CyberArk [63], which monitors user activity to detect not only anomalous activity caused by abuse of existing privileges, but also potential symptoms of compromised credentials.

Finally, it is necessary to point out that the majority of these products start with no knowledge about the environment or industrial system that they aim to protect. As such, they need to be trained, acquiring the knowledge they need mostly by monitoring the network traffic. Even so, there are some products, like the suites marketed by ICS2 [64] or the products developed by ThetaRay [65], that can acquire such behavior offline. For example, by loading and processing training files, or by retrieving information provided by the manufacturer about the expected behaviour of the different system components. The aim of this is to reduce the time required for the deployment and commissioning of these products.

5 Academic Research

Coverage	**2013**	**2014**	**2015**	**2016**	**2017**	**2018.Q1**
Field devices	2	-	3	15	9	2
Control networks – PLCs	4	8	9	5	9	3
Control networks	1	3	3	9	17	4
Complete system	-	1	-	5	2	2

Table 3: Evolution according to detection coverage

Protocol	**2013**	**2014**	**2015**	**2016**	**2017**	**2018.Q1**
Fieldbus protocols	2	1	2	3	2	1
Communication protocols	2	3	10	14	8	2
Control & management protocols	1	-	1	1	1	-

Table 4: Evolution according to protocol analyzed

Mechanism	**2013**	**2014**	**2015**	**2016**	**2017**	**2018.Q1**
Signature-based detection	-	3	-	4	5	2
Data mining mechanisms	2	2	4	5	6	2
Statistical anomaly detection	-	-	4	5	3	1
Knowledge based detection	1	1	2	1	-	2
Machine learning based detection	3	3	2	8	9	3
Specification-based detection	1	3	2	8	10	1
Other mechanisms	-	-	3	5	5	1

Table 5: Evolution according to detection mechanism

As it is crucial to protect industrial control infrastructures against all kind of attacks, including advanced persistent threats, the academia has paid special attention to the development of intrusion detection systems for this particular context. In these systems, all the defense mechanisms described in section 3 have been integrated to some extent, trying to cover all the elements of an industrial control network: field devices, the interactions between the control network and field controllers such as PLCs, the control network itself, and even the complete system in a holistic way.

Tables 3, 4 and 5 provide a classification by categories (according to detection coverage, protocol analyzed, and detection mechanism, respectively) of the number of articles published in the field between years 2013 and 2018 (first quarter). Within this classification, we have included the most relevant articles that appeared in international journals and/or conferences. This relevance has been measured by factors such as the relevance of the corresponding journal or conference, and the number of references per article.

5.1 Analysis: Detection Mechanisms

In recent years, all detection mechanisms described in section 3 have been taken into account. We can observe in table 5 that research in the field has been growing over time. We can also observe that the academia has been paying special attention to machine learning and specification-based mechanisms. One possible reason is that the elements of the control networks can behave in a more or less predictable way [66]. As such, these elements can be modeled through various set of rules. Still, the importance of signature-based detection and statistical techniques is still high, as they are being successfully applied in the analysis of the interactions between the corporate network and the control network.

Still, there are certain detection strategies, which will be highlighted here, that are still being studied only within the academia. For example, in the last years, several authors have started analyzing parameters such as industrial telemetry and response time. Mainly due to the behaviour of control networks, these parameters are providing novel and exciting insights over the behaviour of such control systems. For example, through indirect or direct analysis (e.g. via ICMP messages) of these parameters, it is possible to detect variations in the traffic patterns that are indicative of ongoing attacks [67], detect fake control devices [68], discover covert manipulations of the controller device code [69], and even deduce the CPU load of PLCs [70]. There are also researchers who have considered other less traditional parameters within the context of anomaly and intrusion detection, such as the radio-frequency emissions emitted by the control devices [71], or even their power consumption [72].

There are also other researchers that incorporate concepts such as the physical simulation of the monitored system [73]. This simulation allows not only to predict the malicious intent of a command, but also to predict an imminent system failure. In addition, within the context of specification-based research, there are a large number of papers that seek to generate the system behavior rules in an automatic or semi-automatic way. Various works, such as [74] [75], retrieve this information by analyzing the configuration and system description files. Other works, such as [76], extract the system states by analyzing the bursts of traffic that are exchanged between the control network and the PLCs.

Besides, there are also other strategies whose goal is to identify and analyze the most critical elements of a control network. An example of this is the system developed by Cheminod et al. [77], which can identify the sequence of vulnerabilities that could affect an existing system by (i) analyzing the elements of that system and (ii) analyzing vulnerability databases such as CVE [78]. Other research lines provide a support to the aforementioned IDS/IPS technologies from a theoretical perspective, adopting a reactive policy by means of recovery mechanisms when topological changes are detected. Their target is to ensure the structural controllability of the network and achieve resilience [79], this is, the continuity of the industrial process and the connectivity between nodes in presence of attacks [80]. For such goal, graph theory concepts are leveraged. Finally, it should be mentioned that the vast majority of new signature-based detection systems use, in addition to the SNORT tool, the BRO [81] tool and the SURICATA [82] tool to perform their analyses. These new tools are used because they provide additional benefits. For example, the BRO tool provides a modular and extensible framework that allows the generation and analysis of events through a Turing-complete language.

5.2 Analysis: Detection Coverage

Regarding the evolution of the coverage of detection systems developed in the academia, it is worth commenting that in 2016 the mechanisms in charge of protecting the field devices increased exponentially, and is still a very active area of research as of 2018 Q1. The reason is simple: these mechanisms can detect attacks against the field devices at the very moment they occur, making them a very useful last line of defense against APTs that aim to manipulate the field devices. Direct monitoring is usually done by extracting the data directly from the sensors and actuators, either through the machine's own interfaces [83] [84], or through a "capillary network" that monitors the operation of the machinery through several types of external sensors [85]. On the other hand, there are also mechanisms that integrate a hypervisor within the control devices themselves (e.g. PLCs [86]). This hypervisor is then responsible for reviewing the behavior of all control programs executed within the device, either through a set of rules [87] or by modeling the different states of the program and checking for potential deviations [88].

Moreover, starting from 2016, various researchers have designed novel theoretical architectures whose objective is to protect all the elements of an industrial production system in a holistic way. This is achieved by deploying various detection components, both hardware and software, which obtain information and process it at a local level. This information will then be sent to a central system, which can more efficiently detect threats that affect several elements of the system in a covert way [89]. Although there are various industrial solutions that already apply this approach, certain elements of these academic architectures represent an evolution of the industrial correlation systems defined in section 4.4 in various ways. For example, some architectures allow field devices to be fully monitored alongside all other elements of the control system [85], while other architectures improve the detection of anomalies whose impact is distributed to all elements of the system [90]. There are also architectures, such as [91], that divide the overall system states into several logical partitions, in order to facilitate the work of anomaly detection systems. Finally, some architectures deploy host agents that are specifically designed to look for APT malware infections [92].

5.3 Analysis: Protocols analyzed

Currently there are various scientific articles that have developed specific detection mechanisms for communications protocols such as Modbus/TCP [93], Ethernet/IP [82] and S7comm [94]. These works focus mostly on two strategies: i) defining and detecting attack signatures, and ii) analyzing the behavior of these communication protocols with the detection mechanisms described in section 3. However, there are very few works that have studied the security of control & management protocols such as OPC UA. These protocols are considered as one of the cornerstones of Industry 4.0 [95], and there are already various commercial products that currently use these protocols in production environments [96]. Yet the amount of research that has been done in this area has been extremely limited, and only a few works exist [97]. It is extremely important to analyze and protect these specific protocols in the near future.

Another important aspect related to the communication protocols is that many detection mechanisms that analyze the integrity of fieldbus protocols are focused on the analysis of wireless industrial IoT protocols such as WirelessHART [98]. This is mainly because an attacker can more easily manipulate a wireless network if he has the necessary information: he can not only inject information from anywhere within the range of the network, but he can also deploy a malicious element in a covert way. Finally, it is important to note that there have been multiple developments in the area of anomaly detection systems for certain industry-specific protocols, such as CAN bus (vehicular systems) and IEC 61850 (electrical substations).

6 Discussions

6.1 Intrusion detection and existing threats

In an industrial control ecosystem, and due to the diversity of devices and protocols, there is no single ‘silver bullet’ that can address all potential threats described in section 2. Yet it might be possible to combine various solutions to provide an adequate level of protection against all kinds of attacks, including APTs. The state of the art described in previous sections has shown that it is possible to detect threats against the availability of the system by detecting malicious network traffic and by mapping the behavior and location of existing devices. There are other detection mechanisms that are specialized in the detection of integrity threats: either directly, by detecting the presence of malicious entities, or indirectly, by uncovering the attacks and side effects caused by such entities. Finally, various techniques, such as in-depth traffic analysis, anomaly-based detection, and user monitoring can help in the detection of malicious insiders that bypassed the AAA infrastructure.

However, although we have already developed the basic necessary tools to detect and deter APTs, there are still some issues that need of further exploration. First, very few research works have made use of the existing research on APT behaviour [6, 99] to validate their detection mechanisms. Another issue is related to the hardening of the industrial infrastructure, with the goal of reducing the attack surface. Some works have considered this approach [100], yet more research is needed. Last but not least, it is extremely important to facilitate the integration of holistic defense solutions in existing critical infrastructures, not only in terms of cost but also in terms of usability (e.g. availability of tools to facilitate the traceability of potential APT intrusions) and user training [101].

Besides, there are still certain aspects that require of more research and validation in the area of intrusion detection and intrusion prevention for industrial ecosystems. For example, any attack that aims to passively extract information from the system (i.e. data exfiltration) can create anomalous traffic that might be flagged by anomaly detection systems [102]. However, most industrial-oriented detection systems have been more focused on detecting other kind of anomalous traffic, such as DoS attacks and malware patterns. Another open issue is the identification of misconfigured services and other proactive defense mechanisms, whose designs are limited due to the critical nature of the monitored system. As mentioned in sections 4.2 and 3, there are some works in in these areas, but more research is needed.

Moreover, other aspects related to the integration of technologies such as IIoT and cloud computing must be carefully considered. Regarding IIoT threats, while there are various detection systems that are specialized in analyzing IIoT protocols such as WirelessHART, it is still necessary to expand this coverage to other potential IIoT protocols such as CoAP, MQTT and oneM2M [103]. Besides, as IIoT attacks can be extremely localized (i.e. attacks using the wireless channel), it is essential to assure that all elements and evidence are properly monitored; making use, if possible, of lightweight accountability mechanisms based on granular information in which it is required to identify what, who and how these events were launched.

As for the threats that cloud computing faces, if the industrial system makes use of an external cloud computing infrastructure, it is mandatory to integrate various attestation and accountability mechanisms in order to check that all outsourced processes are being correctly managed. Even if the cloud infrastructure is local, it is still necessary to monitor the cloud infrastructure itself in order to detect if the cloud resources are being misused or not. On the other hand, these resources can also be used by constrained devices and systems as a means of executing time-consuming complex detection algorithms.

6.2 Intrusion detection and the industry of the future

Within the context of the so-called Industry 4.0, the integration of cutting-edge technologies within industrial environments is being planned. This will generate new scenarios and services such as flexible production lines or predictive maintenance systems [1]. However, such integration will bring new challenges that need to be understood and overcome when developing threat protection and detection mechanisms. The nature of these challenges is in fact related to the specific features of Industry 4.0 environments [104]. Both are summarized as follows:

- **Novel infrastructures.** In the near future, most Industry 4.0 elements will be interoperable with each other. As a result, those elements will become semi-autonomous, able to make collaborative decisions that could improve various businesses and industrial processes (e.g. automatic production line planning). This will make necessary the development of new detection mechanisms, focused on analyzing both the behavior of these semi-autonomous systems and their interactions. Yet these interoperability mechanisms and principles can also be used to improve the integration of all devices with existing correlation systems and other holistic detection architectures.

- **Retrofitting.** By integrating Industry 4.0 services and components with existing industrial infrastructures (e.g. extending the sensing capabilities of existing machinery through the use of "capillary networks"), it is possible to bring certain benefits of the Industry 4.0 to legacy systems. However, the existence of these parallel subsystems will increase the attack surface, as these new layers can be attacked – or even be used as a platform to launch attacks.

- **Industrial data space.** The various organizations that will make up the industry of the future will be part of a common space, in which producers, suppliers and users will be able to share information. This implies the need to create safe collaborative spaces in which to share safety information regarding anomalies that may affect other members of the ecosystem. Yet this also implies that such collaborative spaces can (and probably will) be used by internal and external adversaries to launch attacks against all members.

- **Cloud-based manufacturing.** As mentioned in section 2.2.2, the cloud is becoming an integral part of the industrial ecosystem. In the industry 4.0, this integration will go one step further, as cloud-based manufacturing will bring dynamic deployment and configuration of industrial components on the cloud. However, since the physical limits between the IT and OT networks will dissolve, this integration will bring various novel security issues beyond the existing cloud security challenges.

- **Agents.** Within the vision of the Industry 4.0, it will be possible to deploy agent-based systems: from workflow planners to self-organising assembly systems [105]. The existence of these agents in this ecosystem is a doubled-edged sword. One the one hand, malicious agents can travel anywhere in the network and manipulate any of its components, opening the door to novel APT attacks. On the other hand, agents can also be used for good, analyzing the behaviour of existing systems and providing support for the management of system failures.

- **Other enhanced interactions.** The integration of physical and virtual processes within the industry will give birth to novel services such as the "digital twins" (virtual representations of subsystems) and "digital workers" (interactions with advanced human-machine interfaces). This opens up both new opportunities (detection of anomalies through analysis of simulations) and challenges (control of virtualized environments, targeted attacks against workers).

7 Conclusions

There have been significant progress in the development of intrusion detection techniques for industrial ecosystems in the last years. Not only there are commercially available products that integrate advanced solutions such as honeypot systems and information correlation systems, but also there are novel detection mechanisms and architectures developed in the academia. There are still various areas that need of further research, such as the applicability and integration of proactive defense mechanisms, the integration of defense mechanisms into IIoT and cloud computing deployments, and the advent of the Industry 4.0. Moreover, regarding APTs, it is imperative to i) incorporate the knowledge of existing APTs and APT stages into the validation of defense mechanisms, and ii) facilitate the integrability and usability of these defense mechanisms, so they can be easily included in more critical infrastructures.

Acknowledgements

This work has been funded by the Spanish Ministry of Economy, Industry and Competitiveness through the SADCIP (RTC-2016-4847-8) and SMOG (TIN2016-79095-C2-1-R) projects. The work of the first author had been partially financed by the Spanish Ministry of Education under the FPU program (FPU15/03213).

References

[1] A. Khan and K. Turowski. A survey of current challenges in manufacturing industry and preparation for industry 4.0. In *First International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'16)*, pages 15–26. Springer International Publishing, 2016.

[2] L. D. Xu, W. He, and S. Li. Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4):2233–2243, Nov 2014.

[3] Lorena Cazorla, Cristina Alcaraz, and Javier Lopez. Cyber stealth attacks in critical information infrastructures. *IEEE Systems Journal*, pages 1–15, March 2016.

[4] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, Daesung Moon, and Jong Hyuk Park. A comprehensive study on apt attacks and countermeasures for future networks and communications: challenges and solutions. *The Journal of Supercomputing*, pages 1–32, 2016.

[5] Ping Chen, Lieven Desmet, and Christophe Huygens. A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security*, pages 63–72. Springer, 2014.

[6] Antoine Lemay, Joan Calvet, François Menet, and José M. Fernandez. Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, 72:26–59, 2018.

[7] Juan E. Rubio, Cristina Alcaraz, Rodrigo Roman, and Javier Lopez. Analysis of intrusion detection systems in industrial ecosystems. In *14th International Conference on Security and Cryptography (SECRYPT 2017)*, 2017.

[8] Symantec. Protecting critical systems while promoting operational efficiency. Technical report, 2012. [Online; Accessed May 2018].

[9] ICS-CERT. Overview of Cyber Vulnerabilities. http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities, 2016. [Online; Accessed May 2018].

[10] IBM® X-Force® Research. 2016 Cyber Security Intelligence Index: A survey of the cyber security landscape for financial services. http://www.ciosummits.com/2016_Cyber_Security_Intelligence_Index_for_Fnl_Svcs.pdf, 2016. [Online; Accessed May 2018].

[11] Sikich. 2016 Manufacturing Report, Taking your business to the next level and ensuring a successful future. https://www.leadingedgealliance.com/thought_leadership/sikich_manufacturing_report_2016r.pdf, 2016. [Online; Accessed May 2018].

[12] T Tsao, R Alexander, M Dohler, V Daza, A Lozano, and M Richardson. A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). Technical report, 2015.

[13] Cristina Alcaraz and Javier Lopez. A security analysis for wireless sensor mesh networks in highly critical systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 40(4):419–428, July 2010.

[14] Andreas Moser, Christopher Kruegel, and Engin Kirda. Exploring multiple execution paths for malware analysis. In *IEEE Symposium on Security and Privacy (SP'07)*, pages 231–245. IEEE, 2007.

[15] Linus Wallgren, Shahid Raza, and Thiemo Voigt. Routing Attacks and Countermeasures in the RPL-based Internet of Things. *International Journal of Distributed Sensor Networks*, 2013.

[16] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. Security and privacy challenges in industrial internet of things. In *Proceedings of the 52Nd Annual Design Automation Conference*, DAC '15, pages 54:1–54:6, New York, NY, USA, 2015. ACM.

[17] Kuan Zhang, Xiaohui Liang, Rongxing Lu, and Xuemin Shen. Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, 1(5):372–383, 2014.

[18] Cédric Lévy-Bencheton, Louis Marinos, Rossella Mattioli, Thomas King, Christoph Dietzel, Stumpf Jan, et al. Threat landscape and good practice guide for internet infrastructure. *Report, European Union Agency for Network and Information Security (ENISA)*, 2015.

[19] Kai Zhao and Lina Ge. A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on*, pages 663–667. IEEE, 2013.

[20] Dazhong Wu, David W Rosen, Lihui Wang, and Dirk Schaefer. Cloud-based design and manufacturing: A new paradigm in digital manufacturing and design innovation. *Computer-Aided Design*, 59:1–14, 2015.

[21] Jaydip Sen. Security and privacy issues in cloud computing. *Architectures and Protocols for Secure Information Technology Infrastructures*, pages 1–45, 2013.

[22] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu. Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, 2014.

[23] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51, 2011.

[24] Bernhards Blumbergs. Technical analysis of advanced threat tactics targeting critical information infrastructure. Technical report, 2014.

[25] Animesh Patcha and Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer networks*, 51(12):3448–3470, 2007.

[26] Monowar H Bhuyan, Dhruba Kumar Bhattacharyya, and Jugal K Kalita. Network anomaly detection: methods, systems and tools. *IEEE Communications Surveys & Tutorials*, 16(1):303–336, 2014.

[27] Manasi Gyanchandani, JL Rana, and RN Yadav. Taxonomy of anomaly based intrusion detection system: a review. *International Journal of Scientific and Research Publications*, 2(12):1–13, 2012.

[28] R Sekar, Ajay Gupta, James Frullo, Tushar Shanbhag, Abhishek Tiwari, Henglin Yang, and Sheng Zhou. Specification-based anomaly detection: a new approach for detecting network intrusions. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 265–274. ACM, 2002.

[29] Cubix. Tippingpoint intrusion prevention system (ips). `http://cubixindia.com/index.php?option=com_content&view=article&id=12&Itemid=476`, [Online; Accessed May 2018], 2018.

[30] NetSolution Store. Extreme networks intrusion prevention. `http://www.netsolutionstore.com/IPS.asp`, [Online; Accessed May 2018], 2018.

[31] Corero. Corero network security. `https://www.corero.com`, [Online; Accessed May 2018], 2018.

[32] Cristina Alcaraz and Sherali Zeadally. Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection (IJCIP)*, 8:53–66, 01/2015 2015.

[33] Cristina Alcaraz and Javier Lopez. Analysis of requirements for critical control systems. *International Journal of Critical Infrastructure Protection (IJCIP)*, 5:137–145, 2012 2012.

[34] Bilal Maqbool Beigh, Uzair Bashir, and Manzoor Chahcoo. Article: Intrusion detection and prevention system: Issues and challenges. *International Journal of Computer Applications*, 76(17):26–30, August 2013.

[35] Deris Stiawan, Abdul Hanan Abdullah, and Mohd. Yazid Idris. Article: Characterizing network intrusion prevention system. *International Journal of Computer Applications*, 14(1):11–18, January 2011. Full text available.

[36] Cristina Alcaraz, Lorena Cazorla, and Javier Lopez. Cyber-physical systems for wide-area situational awareness. In *Cyber-Physical Systems: Foundations, Principles and Applications*, number Intelligent Data-Centric Systems, chapter 20, pages 305 – 317. Academic Press, Boston, 2017 2017.

[37] Lorena Cazorla, Cristina Alcaraz, and Javier Lopez. Awareness and reaction strategies for critical infrastructure protection. *Computers and Electrical Engineering*, 47:299–317, 2015.

[38] NIST. Guidelines for smart grid cybersecurity - volume 1 - smart grid cybersecurity strategy, architecture, and high-level requirements. NISTIR 7628 Rev 1., 2014.

[39] FortiNet. FortiGate Enterprise Firewall. `https://www.fortinet.com/products/next-generation-firewall.html`, 2018. [Online; Accessed May 2018].

[40] Harman. Harman Shield. `https://services.harman.com/solutions/automotive-cybersecurity`, 2018. [Online; Accessed May 2018].

[41] Advenica. Security Solutions for Critical Infrastructures. `https://advenica.com/`, 2018. [Online; Accessed May 2018].

[42] BAE Systems. Data Loss Prevention. `https://www.baesystems.com/en/product/data-loss-prevention`, 2018. [Online; Accessed May 2018].

[43] Nexor. Nexor Border Gateway. `https://www.nexor.com/nexor-border-gateway/`, 2018. [Online; Accessed May 2018].

[44] Fox IT. Fox Data Diode. `https://www.fox-it.com/datadiode/`, 2018. [Online; Accessed May 2018].

[45] Waterfall Security. FLIP. `https://waterfall-security.com/products/flip`, 2018. [Online; Accessed May 2018].

[46] Nextnine. ICS Shield. `https://nextnine.com/solutions/ics-shield/`, 2018. [Online; Accessed May 2018].

[47] AlgoSec. AlgoSec Security Policy Management Solution. `https://www.algosec.com/`, 2018. [Online; Accessed May 2018].

[48] Sigmaflow. NERC CIP Compliance. `http://www.sigmaflow.com/`, 2018. [Online; Accessed May 2018].

[49] Positive Technologies. MaxPatrol. https://www.ptsecurity.com/ww-en/products/maxpatrol/, 2018. [Online; Accessed May 2018].

[50] Amenaza Technologies LTD. SecurITree. https://www.amenaza.com, 2018. [Online; Accessed May 2018].

[51] CISCO Systems. CISCO: Protecting ICS with Industrial Signatures. https://tools.cisco.com/security/center/, 2018. [Online; Accessed May 2018].

[52] Cyberbit. SCADAShield. https://www.cyberbit.net/solutions/ics-scada-security-continuity/, 2018. [Online; Accessed May 2018].

[53] AlertEnterprise. Sentry CyberSCADA. http://www.alertenterprise.com/products-EnterpriseSentryCybersecuritySCADA.php, 2018. [Online; Accessed May 2018].

[54] WurldTech (GE). OPShield. https://www.ge.com/digital/cyber-security, 2018. [Online; Accessed May 2018].

[55] Attivo Networks. BOTsink. https://attivonetworks.com/product/attivo-botsink/, 2018. [Online; Accessed May 2018].

[56] Control-See. UCME-OPC. http://www.controlsee.com/u-c-me-opc/, 2018. [Online; Accessed May 2018].

[57] SIGA. SIGA Guard. http://www.sigasec.com, 2018. [Online; Accessed May 2018].

[58] Mission Secure. MSi Secure Sentinel Platform. http://www.missionsecure.com/solutions/, 2018. [Online; Accessed May 2018].

[59] CyberX. XSense. https://cyberx-labs.com/en/xsense/, 2018. [Online; Accessed May 2018].

[60] Halo Digital. Halo Vision. https://www.halo-digital.com/, 2018. [Online; Accessed May 2018].

[61] DarkTrace. Enterprise Immune System. https://www.darktrace.com/technology/#enterprise-immune-system, 2018. [Online; Accessed May 2018].

[62] Leidos. Insider Threat Detection Platform - Wisdom ITI. https://cyber.leidos.com/products/insider-threat-detection, 2018. [Online; Accessed May 2018].

[63] CyberArk. Privileged Account Security Solution. https://www.cyberark.com/products/, 2018. [Online; Accessed May 2018].

[64] ICS2. ICS2 On-Guard. http://ics2.com/product-solution/, 2018. [Online; Accessed May 2018].

[65] ThetaRay. ThetaRay Analysis Platform. `https://www.thetaray.com/platform/`, 2018. [Online; Accessed May 2018].

[66] M. Krotofil and D. Gollmann. Industrial control systems security: What is happening? In *11th IEEE International Conference on Industrial Informatics (INDIN'13)*, pages 670–675, July 2013.

[67] Chih-Yuan Lin, Simin Nadjm-Tehrani, and Mikael Asplund. Timing-based Anomaly Detection in SCADA Networks. In *12th International Conference on Critical Information Infrastructures Security (CRITIS'17)*, Oct 2017.

[68] S. Ponomarev and T. Atkison. Industrial control system network intrusion detection by telemetry analysis. *IEEE Transactions on Dependable and Secure Computing*, 13(2):252–260, March 2016.

[69] G. Lontorfos, K. D. Fairbanks, L. Watkins, and W. H. Robinson. Remotely inferring device manipulation of industrial control systems via network behavior. In *IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops'15)*, pages 603–610, Oct 2015.

[70] Rahul Nair, Chinmohan Nayak, Lanier Watkins, Kevin D. Fairbanks, Kashif Memon, Pengyuan Wang, and William H. Robinson. *The Resource Usage Viewpoint of Industrial Control System Security: An Inference-Based Intrusion Detection System*, pages 195–223. Springer International Publishing, 2017.

[71] Samuel J. Stone, Michael A. Temple, and Rusty O. Baldwin. Detecting anomalous programmable logic controller behavior using rf-based hilbert transform features and a correlation-based verification process. *International Journal of Critical Infrastructure Protection*, 9:41 – 51, 2015.

[72] Yu-jun Xiao, Wen-yuan Xu, Zhen-hua Jia, Zhuo-ran Ma, and Dong-lian Qi. NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers. *Frontiers of Information Technology & Electronic Engineering*, 18(4):519–534, Apr 2017.

[73] C. McParland, S. Peisert, and A. Scaglione. Monitoring security of networked control systems: It's the physics. *IEEE Security Privacy*, 12(6):32–39, Nov 2014.

[74] Marco Caselli, Emmanuele Zambon, Johanna Amann, Robin Sommer, and Frank Kargl. Specification mining for intrusion detection in networked control systems. In *25th USENIX Security Symposium*, pages 791–806. USENIX Association, 2016.

[75] Herson Esquivel-Vargas, Marco Caselli, and Andreas Peter. Automatic Deployment of Specification-based Intrusion Detection in the BACnet Protocol. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy (CPS'17)*, pages 25–36. ACM, 2017.

[76] Chen Markman, Avishai Wool, and Alvaro A. Cardenas. A New Burst-DFA Model for SCADA Anomaly Detection. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy (CPS'17)*, pages 1–12. ACM, 2017.

[77] Manuel Cheminod, Luca Durante, Lucia Seno, and Adriano Valenzano. Detection of attacks based on known vulnerabilities in industrial networked systems. *Journal of Information Security and Applications*, 34:153–165, 2017.

[78] Mitre. Common Vulnerabilities and Exposures. `https://cve.mitre.org/`, 2018. [Online; Accessed May 2018].

[79] Ching-Tai Lin. Structural controllability. *IEEE Transactions on Automatic Control*, 19(3):201–208, 1974.

[80] Mohammad Amin Rahimian and Amir G Aghdam. Structural controllability of multi-agent networks: Robustness against simultaneous failures. *Automatica*, 49(11):3149–3157, 2013.

[81] Vern Paxson et al. The Bro Network Security Monitor. `https://www.bro.org/`, 2018. [Online; Accessed May 2018].

[82] K. Wong, C. Dillabaugh, N. Seddigh, and B. Nandy. Enhancing Suricata intrusion detection system for cyber security in SCADA networks. In *IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE'17)*, pages 1–5, April 2017.

[83] Khurum Nazir Junejo and Jonathan Goh. Behaviour-based attack detection and classification in cyber physical systems using machine learning. In *Proceedings of the 2Nd ACM International Workshop on Cyber-Physical System Security (CPSS'16)*, pages 34–43, New York, NY, USA, 2016. ACM.

[84] Hamid Reza Ghaeini, Daniele Antonioli, Ferdinand Brasser, Ahmad-Reza Sadeghi, and Nils Ole Tippenhauer. State-aware anomaly detection for industrial control systems. In *Proceedings of Security Track at the ACM Symposium on Applied Computing (SAC'18)*, April 2018.

[85] William Jardine, Sylvain Frey, Benjamin Green, and Awais 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 (CPS-SPC'16)*, pages 23–34, New York, NY, USA, 2016. ACM.

[86] L. Garcia, S. Zonouz, Dong Wei, and L. P. de Aguiar. Detecting PLC control corruption via on-device runtime verification. In *2016 Resilience Week (RWS)*, pages 67–72, Aug 2016.

[87] J. Hong and C. C. Liu. Intelligent electronic devices with collaborative intrusion detection systems. *IEEE Transactions on Smart Grid*, 2017. In Press.

[88] Long Cheng, Ke Tian, and Danfeng (Daphne) Yao. Orpheus: Enforcing Cyber-Physical Execution Semantics to Defend Against Data-Oriented Attacks. In *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC'17)*, pages 315–326, 2017.

[89] F. Adamsky, M. Aubigny, F. Battisti, M. Carli, F. Cimorelli, T. Cruz, A. Di Giorgio, C. Foglietta, A. Galli, A. Giuseppi, F. Liberati, A. Neri, S. Panzieri, F. Pascucci, J. Proenca, P. Pucci, L. Rosa, and R. Soua. Integrated Protection of Industrial Control Systems from Cyber-attacks: the ATENA Approach. *International Journal of Critical Infrastructure Protection*, 2018. In Press.

[90] Hamid Reza Ghaeini and Nils Ole Tippenhauer. Hamids: Hierarchical monitoring intrusion detection system for industrial control systems. In *Proceedings of the 2Nd ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC'16)*, pages 103–111, New York, NY, USA, 2016. ACM.

[91] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu. Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems. *IEEE Transactions on Industrial Electronics*, 65(5):4257–4267, May 2018.

[92] Daesung Moon, Hyungjin Im, Ikkyun Kim, and Jong Hyuk Park. DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks. *The Journal of Supercomputing*, 73(7):2881–2895, Jul 2017.

[93] Niv Goldenberg and Avishai Wool. Accurate modeling of modbus/tcp for intrusion detection in {SCADA} systems. *International Journal of Critical Infrastructure Protection*, 6(2):63 – 75, 2013.

[94] Amit Kleinmann and Avishai Wool. Automatic Construction of Statechart-Based Anomaly Detection Models for Multi-Threaded Industrial Control Systems. *ACM Trans. Intell. Syst. Technol.*, 8(4):55:1–55:21, Feb 2017.

[95] Kagermann Henning. Recommendations for implementing the strategic initiative industrie 4.0, 2013.

[96] Siemens. SIMATIC OPC UA. `http://www.industry.siemens.com/topics/global/en/tia-portal/software/details/pages/opc-ua.aspx`, 2018. [Online; Accessed May 2018].

[97] A. Terai, S. Abe, S. Kojima, Y. Takano, and I. Koshijima. Cyber-attack detection for industrial control system monitoring with support vector machine based on communication profile. In *IEEE European Symposium on Security and Privacy Workshops (EuroS PW'17)*, pages 132–138, April 2017.

[98] L. Bayou, N. Cuppens-Boulahia, D. Espès, and F. Cuppen. Towards a CDS-based Intrusion Detection Deployment Scheme for Securing Industrial Wireless Sensor Networks. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pages 157–166, Aug 2016.

[99] MITRE Corporation. MITRE ATT&CK. `https://attack.mitre.org`, 2018. [Online; Accessed May 2018].

[100] Anhtuan Le, Utz Roedig, and Awais Rashid. Lasarus: Lightweight attack surface reduction for legacy industrial control systems. In Eric Bodden, Mathias Payer, and Elias Athanasopoulos, editors, *Engineering Secure Software and Systems*, pages 36–52. Springer International Publishing, 2017.

[101] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *70th Annual Conference for Protective Relay Engineers (CPRE'17)*, pages 1–8, April 2017.

[102] Yali Liu, C. Corbett, Ken Chiang, R. Archibald, B. Mukherjee, and D. Ghosal. Sidd: A framework for detecting sensitive data exfiltration by an insider attack. In *42nd Hawaii International Conference on System Sciences*, pages 1–10, Jan 2009.

[103] Rajive Joshi, Paul Didier, Jaime Jimenez, and Timothy Carey. The Industrial Internet of Things Volume G5: Connectivity Framework. Industrial Internet Consortium Report, 2017.

[104] J. E. Rubio, R. Roman, and J. Lopez. Analysis of Cybersecurity Threats in Industry 4.0: The Case of Intrusion Detection. In *12th International Conference on Critical Information Infrastructures Security (CRITIS'17)*, Oct 2017.

[105] Shiyong Wang, Jiafu Wan, Daqiang Zhang, Di Li, and Chunhua Zhang. Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination. *Computer Networks*, 101:158–168, 2016.