Analysis of Intrusion Detection Systems in Industrial Ecosystems

Juan Enrique Rubio, Cristina Alcaraz, Rodrigo Roman and Javier Lopez
Lenguajes y Ciencias de la Computación, University of Málaga, Spain

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

Abstract: For an effective protection of all the elements of an industrial ecosystem against threats, it is necessary to understand the true scope of existing mechanisms capable of detecting potential anomalies and intrusions. It is the aim of this article to review the threats that affect existing and novel elements of this ecosystem; and to analyze the state, evolution and applicability of both academic and industrial intrusion detection mechanisms in this field.

1 INTRODUCTION

Control of industrial environments through systems such as SCADA (Supervisory Control and Data Acquisition) is now present in most critical infrastructures (e.g. power grids, nuclear plants or transport systems). These control systems allow remote and real-time access to devices that govern the production cycle, whether they are controllers such as PLC (Field Programmable Logic Controllers), or RTU (Remote Terminal Units). Traditionally, SCADA systems and industrial networks had to be isolated from other environments. However, at present, we are dealing with the interconnection of SCADA systems for the storage of data or the outsourcing of services, as well as a standardization of the software and hardware used in control systems. Consequently, there has been a substantial increase in security risks (Xu et al., 2014) based on new specific threats operating under different threat modes (Cazorla et al., 2016).

A solution to mitigate these effects is the provision of awareness-based approaches (e.g. situational-awareness (Alcaraz and Lopez, 2013)), which help to provide the necessary tools to favor the detection and response to attacks and/or anomalies (Xu et al., 2014). Many of these anomalies arise from conflicts or security breaches due to interoperability issues, probably caused by multiple communication and control protocols (Alcaraz and Zeadally, 2013). For example, in the literature it is possible to find protocols working in Ethernet and TCP/IP, such as Ethernet/IP, Ethernet POWERLINK, from fieldbus protocols (eg HART, wirelessHART, etherCAP, IO-Link) CANopen, PROFINET, Modbus / TCP or HART / IP. In addition to these, there are others designed for the management and control of all industrial equipment, such as the CIP, OPC UA, and MTConnect protocols, without forgetting existing, open source alternatives such as Woopsa or REST-PCA. This complexity is further compounded by new communication infrastructures (e.g. IoT or cloud computing) along with their specific digitization services for managing multiple types of data, as well as the integration of new resources and services within the so-called Industry 4.0 (Khan and Turowski, 2016). As a result, a system can become complex and critical, besieged by multiple threats.

For these reasons, this paper explores the existing techniques and mechanisms that try to detect specific threat vectors within an industrial context, without losing sight of the future industrial paradigm that has started to be applied gradually. This is organized as follows: Section 2 highlights the threats to which the control is exposed today. Taking into account this landscape, Section 3 addresses the search, by the industry and academia, for defense techniques suitable for intrusion detection systems in these critical environments, as explained 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

2.1 Traditional Threats in IS and ICS

The threat model that can be applied to the elements of traditional industrial control elements (PLCs, in-

Rubio, J., Alcaraz, C., Roman, R. and Lopez, J.
Analysis of Intrusion Detection Systems in Industrial Ecosystems.
DOI: 10.5220/0006426301160128
In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT*, pages 116-128
ISBN: 978-989-758-259-2

dustrial communication protocols, IT elements) is highly diverse (Federal Office for information Security, 2016)(ICS-CERT, 2016). For the purposes of our analysis, the attack vectors that affect these elements can be classified following the taxonomy given by the IETF standard-7416 (Tsao et al., 2015), in which the threats are grouped according to the attack goals against the minimum security services (Alcaraz and Lopez, 2010) such as availability, integrity, confidentiality and authentication.

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 (Moser et al., 2007) 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 be 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.

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. 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 misconfigurations or unsuitable access control, both at the logical (use of simple passwords) and physical (access to equipment) level.

The exploitation of many of these threats may also arise in some of the states of an advanced persistent threat as discussed in (Singh et al., 2016; Chen et al., 2014): (i) *recognition* (R) and *communication* (C) through social engineering or compromising a third party such as a provider; (ii) *tracking* (T) of zero-day vulnerabilities and *execution* (E) of remote actions by previously launching malware and installing backdoors; and (iv) *propagation* (P) and *information filtration* (F). Stuxnet was the first APT recognized by the industry in 2010 (Langner, 2011), but later others appeared such as DuQu, Dragon Night, Flame, Aurora, Shamoon or the Mask (Blumbergs, 2014).

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.

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 (Tsao et al., 2015), we can distinguish the following range of threats:

Availability Threats. Comprises the disruption of communication and processing resources: firstly, against the routing protocol (Wallgren et al., 2013), 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. (Sadeghi et al., 2015).

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 (Zhang et al., 2014). 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 (Lévy-Bencheton et al., 2015). 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 (Zhao and Ge, 2013), 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 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 (Wu et al., 2015). 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 (Sen, 2013)(Sun et al., 2014):

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 analyz-

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	✓		

ing 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.

A complete overview of the present and future threats faced by an Industrial System is summarized in Table 1. 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

Intrusion Detection Systems (IDS) are a first defense solution to the wide range of cybersecurity threats described in section 2. The objective is to 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 (Patcha and Park, 2007).

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 (Bhuyan et al., 2014), each with a different level of adaptation depending on the scenario of the application to be protected (Gyanchandani et al., 2012):

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** (Sekar et al., 2002). 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.

4 INDUSTRIAL IDS PRODUCTS

At present, there are several types of IDS systems available on the market. They correspond to the strategies described in section 3: from more traditional signature detection systems to more novel anomaly detection systems and "honeypot" systems. 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 IDS services and appliances. In addition, a short summary of the main solutions available in the market as of Q1 2017 is provided in the next sections.

4.1 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 (CISCO Systems, 2017). Such attack signatures include not only generic attacks on elements of the industrial network (e.g. denial of service in 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 (Cyberbit, 2017). 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.

4.2 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 (AlertEnterprise, 2017). 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.

Another example of in-depth analysis solutions is Wurldtech's OPShield (WurldTech (GE), 2017) 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.

Table 2: Leading companies in the market.

Detection Strategies	Leading Companies
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 Analytics, HeSec, ICS2, Indegy, Leidos* *Nation-E, Nozomi, PFP Cybersecurity, RadiFlow, SCADAfence, SecureNok, Sentryo, SIGA, ThetaRay*

4.3 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 (Attivo Networks, 2017), 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.

4.4 Anomaly-based Solutions

As of Q1 2017, 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. 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 (Control-See, 2017), retrieve system information directly from the industrial process management layers. Other products, such as the Smart Agent services by HeSec (HeSec, 2017), 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 (SIGA, 2017); or even systems embedded within the field devices themselves, such as those offered by MSi (Mission Secure, 2017), 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 (Control-See, 2017), 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 (CyberX, 2017), 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 (Halo Analytics, 2017), 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 (DarkTrace, 2017) 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 (Leidos, 2016), which offer a proactive and real-time platform for internal threat detection. This platform not only monitors system activity indicators, but also the behavior of human employees.

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 (ICS2, 2017), that can acquire such behavior offline by loading and processing a file. The aim of this is to reduce the time required for the deployment and commissioning of these products.

Table 3: Evolution according to detection coverage.

Coverage	2013	2014	2015	2016
Field devices	2	-	3	15
Control networks – PLCs	4	8	9	5
Control networks	1	3	3	9
Complete system	-	1	-	5

Table 4: Evolution according to protocol analyzed

Protocol	2013	2014	2015	2016
Fieldbus protocols	2	1	2	3
Communication protocols	2	3	10	14
Control & management protocols	1	-	1	1

Table 5: Evolution according to detection mechanism.

Mechanism	2013	2014	2015	2016
Signature-based detection	-	3	-	4
Data mining mechanisms	2	2	4	5
Statistical anomaly detection	-	-	4	5
Knowledge based detection	1	1	2	1
Machine learning based detection	3	3	2	8
Specification-based detection	1	3	2	8
Other mechanisms	-	-	3	5

5 ACADEMIC RESEARCH

Due to the importance of protecting industrial control infrastructures before, during and after an attack, the academia has also been paying 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 2016. 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. Due to space constraints, this section will only provide citations to those articles that are explicitly mentioned.

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 paid 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 (Krotofil and Gollmann, 2013). As such, these elements can be modeled through various set of rules. It should also be mentioned that signature-based detection and statistical techniques are becoming increasingly important – and successfully applied – in 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, several authors are using parameters that have not previously been taken into account in this context, such as network telemetry. Through indirect or direct analysis (e.g. via ICMP messages) of the telemetry, it is possible to detect fake control devices (Ponomarev and Atkison, 2016), and even discover covert manipulations of the controller device code (Lontorfos et al., 2015). 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 (Stone et al., 2015).

There are also other researchers that incorporate concepts such as the physical simulation of the monitored system (McParland et al., 2014). 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, mainly by analyzing the configuration and system description files (Caselli et al., 2016).

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. (Cheminod et al., 2016), 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 (Mitre, 2017). 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 (Lin, 1974), this is, the continuity of the industrial process and the connectivity between nodes in presence of attacks (Rahimian and Aghdam, 2013). 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 (Vern Paxson et al., 2017) tool to perform their analyses. This 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 have increased exponentially. The reason is simple: these mechanisms can detect attacks against the field devices at the very moment they occur. Direct monitoring is usually done by extracting the data directly from the sensors and actuators, either through the machine's own interfaces (Junejo and Goh, 2016), or through a "capillary network" that monitors the operation of the machinery through several types of external sensors (Jardine et al., 2016). On the other hand, there are also mechanisms that integrate a hypervisor within the control devices themselves (e.g. PLCs (Garcia et al., 2016)). This hypervisor is then responsible for reviewing the behavior of all control programs executed within the device.

Moreover, in 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. These architectures represent an evolution of the industrial correlation systems defined in section 4.2 in various ways. For example, certain architectures allow field devices to be fully monitored alongside all other elements of the control system (Jardine et al., 2016), while other architectures improve the detection of anomalies whose impact is distributed to all elements of the system (Ghaeini and Tippenhauer, 2016).

5.3 Analysis: Protocols Analyzed

Currently there are a large number of scientific articles that have developed specific detection mechanisms for communications protocols such as Modbus/TCP (Goldenberg and Wool, 2013). 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. It is extremely important to analyze and protect these specific protocols in the near future: not only they are considered as one of the cornerstones of Industry 4.0 (H. et al., 2013), but there are already various commercial products that currently use these protocols in production environments (Siemens, 2017).

Finally, it should be mentioned that the vast majority of detection mechanisms that analyze the integrity of fieldbus protocols are focused on the analysis of wireless industrial IoT protocols such as WirelessHART (Bayou et al., 2016). 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.

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. 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.

There are still certain aspects that require of more research and validation. 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 (Liu et al., 2009). 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.

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 (Joshi et al., 2017). 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 (Khan and Turowski, 2016). However, such integration will bring new challenges that need to be understood and overcome when developing threat protection and detection mechanisms. One of these aspects, already mentioned in section 5.3, is the detection of those anomalies that will affect control & management protocols such as OPC-UA. Another aspect to consider is the integration of physical and virtual processes within the industry, giving birth to novel services such as the "digital twins". This opens up both new opportunities (detection of anomalies through analysis of simulations) and challenges (control of virtualized environments).

Another aspect to consider is the assumption that, 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. Finally, 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.

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. Even so, it is necessary to move forward in various aspects in order to completely cover the full spectrum of potential threats, such as the integration of mechanisms oriented to protect IIoT and cloud infrastructures, the deployment of novel research mechanisms in real scenarios, the analysis of certain command & control protocols, and various challenges related to the industry of the future.

ACKNOWLEDGEMENTS

This work has been funded by the Spanish Ministry of Economy, Industry and Competitiveness through the SADCIP (RTC-2016-4847-8) and PERSIST (TIN2013-41739-R) projects. The work of the first author han been partially financed by the Spanish Ministry of Education under the FPU program (FPU15/03213).

REFERENCES

Alcaraz, C. and Lopez, J. (2010). 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.

Alcaraz, C. and Lopez, J. (2013). Wide-area situational awareness for critical infrastructure protection. *IEEE Computer*, 46(4):30–37.

Alcaraz, C. and Zeadally, S. (2013). Critical control system protection in the 21st century: Threats and solutions. *IEEE Computer*, 46(10):74 – 83.

AlertEnterprise (2017). Sentry CyberSCADA. http://www.alertenterprise.com/products-EnterpriseSentryCybersecuritySCADA.php. [Online; Accessed March 2017].

Attivo Networks (2017). BOTsink. https://attivonetworks.com/product/attivo-botsink/. [Online; Accessed March 2017].

Bayou, L., Cuppens-Boulahia, N., Espès, D., and Cuppen, F. (2016). 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.

Bhuyan, M. H., Bhattacharyya, D. K., and Kalita, J. K. (2014). Network anomaly detection: methods, systems and tools. *Ieee communications surveys & tutorials*, 16(1):303–336.

Blumbergs, B. (2014). Technical analysis of advanced threat tactics targeting critical information infrastructure. Technical report.

Caselli, M., Zambon, E., Amann, J., Sommer, R., and Kargl, F. (2016). Specification mining for intrusion detection in networked control systems. In *25th USENIX Security Symposium*, pages 791–806. USENIX Association.

Cazorla, L., Alcaraz, C., and Lopez, J. (2016). Cyber stealth attacks in critical information infrastructures. *IEEE Systems Journal*, pages 1–15.

Cheminod, M., Durante, L., Seno, L., and Valenzano, A. (2016). Detection of attacks based on known vulnerabilities in industrial networked systems. *Journal of Information Security and Applications*. In Press.

Chen, P., Desmet, L., and Huygens, C. (2014). A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security*, pages 63–72. Springer.

CISCO Systems (2017). CISCO: Protecting ICS with Industrial Signatures. http://www.cisco.com/c/en/us/about/security-center/protecting-industrial-control-systems-networks-ips.html. [Online; Accessed March 2017].

Control-See (2017). UCME-OPC. http://www.controlsee.com/u-c-me-opc/. [Online; Accessed March 2017].

Cyberbit (2017). SCADAShield. https://www.cyberbit.net/solutions/ics-scada-security-continuity/. [Online; Accessed March 2017].

CyberX (2017). XSense. https://cyberx-labs.com/en/xsense/. [Online; Accessed March 2017].

DarkTrace (2017). Enterprise Immune System. https://www.darktrace.com/technology/#enterprise-immune-system. [Online; Accessed March 2017].

Federal Office for information Security (2016). Industrial Control System Security: Top 10 Threats and Countermeasures 2016. https://www.allianz-fuer-cybersicherheit.de. [Online; Accessed March 2017].

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

Ghaeini, H. R. and Tippenhauer, N. O. (2016). 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. ACM.

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

Gyanchandani, M., Rana, J., and Yadav, R. (2012). Taxonomy of anomaly based intrusion detection system: a review. *International Journal of Scientific and Research Publications*, 2(12):1–13.

H., K., J., H., A., H., and Wahlster, W. (2013). Recommendations for implementing the strategic initiative industrie 4.0: Securing the future of german manufacturing industry. final report of the industrie 4.0 working group.

Halo Analytics (2017). Halo Vision. https://www.halo-analytics.com/. [Online; Accessed March 2017].

HeSec (2017). HeSec Smart Agents. http://he-sec.com/products/. [Online; Accessed March 2017].

ICS-CERT (2016). Overview of Cyber Vulnerabilities. http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities. [Online; Accessed March 2017].

ICS2 (2017). ICS2 On-Guard. http://ics2.com/product-solution/. [Online; Accessed March 2017].

Jardine, W., Frey, S., Green, B., and Rashid, A. (2016). 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. ACM.

Joshi, R., Didier, P., Jimenez, J., and Carey, T. (2017). The Industrial Internet of Things Volume G5: Connectivity Framework. Industrial Internet Consortium Report.

Junejo, K. N. and Goh, J. (2016). 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. ACM.

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

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

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

Leidos (2016). Insider Threat Detection Platform - Wisdom ITI. https://cyber.leidos.com/products/insider-threat-detection. [Online; Accessed March 2017].

Lévy-Bencheton, C., Marinos, L., Mattioli, R., King, T., Dietzel, C., Jan, S., et al. (2015). Threat landscape and good practice guide for internet infrastructure. *Report, European Union Agency for Network and Information Security (ENISA)*.

Lin, C.-T. (1974). Structural controllability. *IEEE Transactions on Automatic Control*, 19(3):201–208.

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

Lontorfos, G., Fairbanks, K. D., Watkins, L., and Robinson, W. H. (2015). 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.

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

Mission Secure (2017). MSi Secure Sentinel Platform. http://www.missionsecure.com/solutions/. [Online; Accessed March 2017].

Mitre (2017). Common Vulnerabilities and Exposures. https://cve.mitre.org/. [Online; Accessed March 2017].

Moser, A., Kruegel, C., and Kirda, E. (2007). Exploring multiple execution paths for malware analysis. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pages 231–245. IEEE.

Patcha, A. and Park, J.-M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer networks*, 51(12):3448–3470.

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

Rahimian, M. A. and Aghdam, A. G. (2013). Structural controllability of multi-agent networks: Robustness against simultaneous failures. *Automatica*, 49(11):3149–3157.

Sadeghi, A.-R., Wachsmann, C., and Waidner, M. (2015). 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. ACM.

Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H., and Zhou, S. (2002). 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.

Sen, J. (2013). Security and privacy issues in cloud computing. *Architectures and Protocols for Secure Information Technology Infrastructures*, pages 1–45.

Siemens (2017). SIMATIC OPC UA. http://www.industry.siemens.com/topics/global/en/tia-portal/software/details/pages/opc-ua.aspx. [Online; Accessed March 2017].

SIGA (2017). SIGA Guard. http://www.sigasec.com. [Online; Accessed March 2017].

Singh, S., Sharma, P. K., Moon, S. Y., Moon, D., and Park, J. H. (2016). A comprehensive study on apt attacks and countermeasures for future networks and communications: challenges and solutions. *The Journal of Supercomputing*, pages 1–32.

Stone, S. J., Temple, M. A., and Baldwin, R. O. (2015). 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.

Sun, Y., Zhang, J., Xiong, Y., and Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*.

Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and Richardson, M. (2015). A security threat analysis for the routing protocol for low-power and lossy networks (rpls). Technical report.

Vern Paxson et al. (2017). The Bro Network Security Monitor. https://www.bro.org/. [Online; Accessed March 2017].

Wallgren, L., Raza, S., and Voigt, T. (2013). Routing attacks and countermeasures in the rpl-based internet of things. *International Journal of Distributed Sensor Networks*.

Wu, D., Rosen, D. W., Wang, L., and Schaefer, D. (2015). Cloud-based design and manufacturing: A new paradigm in digital manufacturing and design innovation. *Computer-Aided Design*, 59:1–14.

WurldTech (GE) (2017). OPShield. https://www.wurldtech.com/products/opshield. [Online; Accessed March 2017].

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

Zhang, K., Liang, X., Lu, R., and Shen, X. (2014). Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, 1(5):372–383.

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