J. E. Rubio, R. Roman, and J. Lopez, "Analysis of cybersecurity threats in Industry 4.0: the case of intrusion detection", *The 12th International Conference on Critical Information Infrastructures Security* vol. Lecture Notes in Computer Science, vol 10707, pp. 119-130, 2018.
NICS Lab. Publications: `https://www.nics.uma.es/publications`

Analysis of cybersecurity threats in Industry 4.0: the case of intrusion detection

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

Abstract

Nowadays, industrial control systems are experiencing a new revolution with the interconnection of the operational equipment with the Internet, and the introduction of cutting-edge technologies such as Cloud Computing or Big data within the organization. These and other technologies are paving the way to the Industry 4.0. However, the advent of these technologies, and the innovative services that are enabled by them, will also bring novel threats whose impact needs to be understood. As a result, this paper provides an analysis of the evolution of these cybersecurity issues and the requirements that must be satisfied by intrusion detection defense mechanisms in this context.
Keywords: industry, control systems, internet, iot, cloud, big data, critical infrastructure, intrusion detection, ids

1 Introduction

Traditionally, industrial facilities and critical infrastructures have been governed by SCADA (Supervisory Control and Data Acquisition) systems, which provide real-time data and remote management of the devices that are deployed over the production cycle, like Programmable Logic Controllers (PLCs) or field devices. However, these systems are now experiencing a growing interconnection with other services to share information and uptake new business processes. This is a consequence of the standardization of the software and hardware used in control systems, mainly caused by the adoption of Ethernet or TCP/IP and wireless technologies like IEEE 802.c or Bluetooth in this context.

Yet it seems this is only the beginning of the evolution of industrial ecosystems. Following with this tendency, the so-called fourth Industrial Revolution, or Industry 4.0 [1], is being heralded by the integration of communication technologies as novel as the Internet of Things or Cloud/Fog Computing to the current control and automation systems. Other concepts, such as the creation of

virtual representations of entities (virtualization) and the acquisition and analysis of operational information (big data), are also under consideration. This evolution will facilitate the deployment of innovative industrial services such as "digital twins", "cloud-based manufacturing", and "digital workers", amongst others.

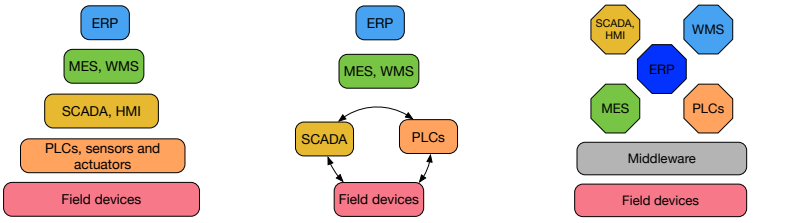
While the integration of IT and OT (operational technology) environments has several major benefits, it has also facilitated the emergence of several IT attack vectors in industrial ecosystems [2]. It is then to be expected that the number and impact of these cyber-security threats will also increase in future industrial environments. However, due to the lack of analyses on this subject, it is essential to study and understand the cyber-security threats caused by the previously mentioned enabling technologies and innovative services, plus their influence on the creation of specific intrusion detection systems.

For this purpose, in this work we will carry out a study of this nature, applying the following methodology: in Section 2 we will review the main enabling technologies included under the concept of Industry 4.0, identifying the local security threats against those areas and their most representative attack vectors in Section 3. Having understood the issues associated to the enabling technologies, Section 4 will focus on the security threats associated to the most innovative Industry 4.0 services. Finally, Section 5 will make use of the previous results to provide an overview of the additional requirements that must be fulfilled by intrusion detection systems in the context of the industry of the future. Note that, due to the lack of available space, only the most relevant references have been included.

2 Industry 4.0 technologies

The Industry 4.0 refers to the digitization of all components within the industry. This concept is not mature due to a lack of agreement on the set of technologies considered and the different interests of the actors involved (e.g., researchers, standardization committees, governments). However, it can be defined from a technical perspective as the combination of productive processes with leading technologies of information and communications. This allows all the elements that conform the productive processes (suppliers, plant, distributors, even the product itself) to be digitally connected, providing a highly integrated value chain [1].

To better understand the innovations that Industry 4.0 introduces in the existing infrastructure, we must pay attention to its architectural changes. The ISA-95 standard defines five levels of operations in the industrial automation, in the form of a pyramid: this way, the productive process itself is located in the base (level 0), whereas those devices that interact with it (i.e., PLCs) are set in level 1. On top of these (level 2) we find the devices that control the production process (i.e., SCADAs, HMIs), and those that control the workflow (i.e., MES systems), represented at level 3. Lastly, the highest level contains the infrastructure of logistics, inventory, ERP or planning.



(a) ISA-95 model (b) Basic Industry 4.0 (c) Full Industry 4.0 model

Figure 1: ISA-95 pyramid and evolution towards Industry 4.0

In traditional industrial environments, the information processing infrastructure follows the pyramidal structure reflected by this standard. One of the objectives of researchers in the field of Industry 4.0 is to analyze how to change this pyramid to a model that provides a more dynamic and reconfigurable decentralized infrastructure [3], as depicted in Figure 1. By creating well defined services and interfaces, in which each element of the ecosystem has a specific functionality and purpose, it would be possible to redefine the structure of an industrial environment through various configurations, enhancing new services and optimizing existing ones [4]. The following is a summary of the most common conceptual features that this new model would enable:

- **Interoperability.** The application of the technologies that belong to the Industry 4.0 would ensure an interoperability between each of the elements of the productive processes.
- **Virtualization.** Within industry 4.0, it would be possible to create a virtual copy of each of its elements.
- **Decentralization.** Each of the elements of Industry 4.0 might be able to intelligently make decisions for itself, in conjunction with other elements, or globally.
- **Capabilities in real time.** The ecosystem would allow the acquisition and analysis of data in real time.
- **Service orientation.** The elements of Industry 4.0 would be able to abstract their functionality into a service-oriented architecture, and would also be able to consume services offered by other assets. In addition, these services would be indexed and easily accessible by authorized entities.
- **Modularity.** An Industry 4.0 environment would not function in a monolithic way, but would allow adaptation to new requirements by integrating new modules and extending or replacing existing modules.

- **Interactivity.** Industry 4.0 operators at all levels would be able to interact with various physical and logical elements in a simple and effective way.

These principles can be accomplished by a set of enabling technologies that can be summarized into four areas: Industrial Internet of Things, Cloud and Fog computing, Big Data and Virtualization.

Firstly, the goal of the **Internet of Things** (IoT) paradigm is to massively interconnect the objects that surround us – the "things" – using standardized interfaces, allowing them to produce and consume services. Applied to the industrial context, the so-called Industrial Internet of Things (IIoT) vertically integrates all the components within the architecture, ranging from control systems to machines or even the product itself. Moreover, due to their interconnection capabilities, all entities could interact with each other at an horizontal level, enabling decentralized interactions such as monitorization (between operators and machinery) and decision making (between the machines themselves). There are other concepts that are related to the IoT, such as Cyber-Physical systems (CPS), that can also be applied to this context. Note that CPS focus on feedback between systems (i.e., looping) in a more local environment, while IIoT assumes a greater global connectivity.

Cloud computing can be considered as another of the pillars of Industry 4.0 for a variety of reasons. On the one hand, it carries on the analytic procedures with the data provided by the industrial process, retrieved by IIoT devices. On the other hand, it provides support for the delegation of production processes and control to the cloud – enabling new productive processes (e.g. product customization) and innovative services such as "Cloud-based manufacturing" [5]. However, there are various situations, such as management of swarms of robots, where the cloud might not the most suitable solution due to its inherent features (high latency and jitter, lack of local contextual information). For this very purpose, it can be possible to apply emerging paradigms such as *Fog Computing* [6], which focus on the deployment of cloud-like services at the edge of the network.

Third, Industry 4.0 will facilitate the evolution of industrial decision making processes, mainly due to the multiple sources of information that will be available to both operators and systems alike. In order to distill all this information and extract both business and operational intelligence, it is necessary to conduct advanced data analytics procedures. This area includes both the analysis of information at a more local level (e.g., the independent optimization of the operation of a machine based on its interactions with other elements of the production line) and the concept of **Big Data** - the processing of all information provided by entities of the industrial ecosystem, looking for added value services such as monitoring the operation of the ecosystem entities, process optimization, and the identification of anomalies.

Lastly, we can highlight a group of technologies whose target is to change the way of designing and interacting with the production chain, that we will refer to as **Virtualization**. One of these consists in the creation of virtual rep-

resentations (e.g. 3D abstractions [7]) of all machines and components involved in the production process. This is facilitated by the previously mentioned enabling technologies, and it will allow the creation of novel services based on the concept of "digital twins", where it will be possible to conduct simulations to prevent failures and optimize the production line. Aside from this paradigm, the introduction of modern Human-Machine Interfaces (HMI) can also be included in this category, that make use of augmented and virtual reality devices that ultimately make the operations easier and more flexible for the workers. In addition, the use of advanced robots (autonomous, mobile, modular, multifunctional, etc.) also contribute to improve the performance of certain tasks within the production chain.

3 Landscape of cyber-security threats of Industry 4.0 enabling technologies

There are various researchers that have identified the most impactful threats that affect current industrial infrastructure ecosystems. Examples include social engineering, malware infection, compromising Internet-connected components, and insider threats [8]. Still, while these threats are also applicable to Industry 4.0 environments, it is necessary to understand the threats that might arise due to the integration of the enabling technologies introduced in section 2. For this very purpose, this section will provide a taxonomy of such threats. The taxonomy described here has been created according to the IETF standard 7416 [9], that proposes an analysis of security issues whose classification is based on their effect on the main security services: availability, integrity, confidentiality and authentication. Nevertheless, it is important to note that many of the threats affect several of these services. An overall summary of the main threats of each technology, which have been extracted from the current literature, is presented in Table 1.

Industrial Internet of Things. In terms of security, IIoT's main concerns are the privacy protection, authentication and control of access to heterogeneous resources, information management, etc. which are aggravated due to the scarcity of computational resources and autonomy that they present. This causes that most attacks are perpetrated against their *availability*, this is, the exhaustion of the node resources (processing, memory or battery) by overloading them with traffic and repetitive requests (cf. [10]). Nodes can also be physically or remotely compromised by exploiting vulnerabilities or running malware that can put the data *confidentiality* and *integrity* under risk: on the one hand, by exposing sensitive information (e.g., node internal status), as well as intellectual property or personal information retrieved by wearable devices. On the other hand, by manipulating information of all kinds: firstly, the routing information (i.e., neighbor states, available links), which allows the attacker to influence other nodes within the production chain. Secondly, the sensing data itself, that

can be potentially falsified when appropriate encryption mechanisms are not applied. In this sense, the node identity misappropriation is also considerable (e.g., with Man-in-the-Middle attacks), which opens the door to other types of attacks. This is the main *authentication* issue, that appears as a consequence of ineffective access control mechanisms to IoT devices.

Cloud/Fog Computing. As it gains interest among the organizations to externalize multiple services (at remote – Cloud – or close – Fog – locations) along the product life cycle, it is crucial to ensure the security and privacy protection of data from internal or external attackers [11]. Again, the most common attack goes against its *availability*, by means of a Denial of service (DoS) attacks against the cloud services. Another example is a service theft attack, where the attacker use the cloud services at the expense of other clients, exploiting vulnerabilities of the underlying hypervisor. Data *integrity* is threatened in presence of malware (e.g., replacing legitimate virtual machines with malicious ones in order to read and manipulate information), and *confidentiality* problems arise when putting trust in the service provider, who has total access to the stored data. Also concerning confidentiality, side-channel attacks must be also mentioned, where malicious virtual machines analyze certain shared features such as the amount of shared memory used. As for *authentication* problems, the major issue appears through social engineering or phishing, where attackers host websites in the cloud that imitate the appearance of legitimate services. It is important to remark the difficulty for the cloud provider to detect such behavior in its servers, since they are also required to not be able to access the data hosted by its clients, for privacy reasons. However, it is necessary to apply robust control access policies, agreed by both client and provider.

Big Data. As the industry processes huge amounts of information about their business, usually through cloud computing resources, it becomes critical to securely store and manage this bulk of data by means of preventive, detective and administrative mechanisms. Such data is characterized by its volume (huge amount), velocity (speed of generation) and variety (multiple formats), and is usually processed in a parallel way by a distributed network of nodes in charge of running MapReduce operations [12]. It is hence difficult to know where the computation takes place and equally tricky to ensure the security of all components (e.g., databases, computing power, etc.), so small weaknesses can put the *availability* of the entire system or its data at risk [13]. As for *confidentiality* and *integrity*, data can be exposed or modified if encryption or integrity measures are not respectively applied, which is frequent in this context to improve efficiency. Data input validation is thereby essential to protect the information during its transmission from several sources (e.g., the corporative network, field devices, the web, etc.). In addition, Big Data also has privacy implications when data is analysed massively, which can draw accurate conclusions about the infrastructure or behaviour patterns of workers within the organization. *Authentication* problems also arise with the unauthorized access to sensitive data (by both

Table 1: Main Cyber-security threats of Industry 4.0 enabling technologies

	IIoT	**Cloud/Fog**	**Big Data**	**Virtualization**
Availability	Exhaustion of resources (traffic, requests)	Network flooding, service theft	Multiple points of failure	Multiple points of failure
Confidentiality	Exposure of sensitive information	Data accesss by the provider, side-channel attacks	Lack of cryptography, privacy issues when massively analyzing data	Simulations information leakage
Integrity	Data or routing information manipulation	Malicious VMs	Untrusted mappers, lack of integrity measures	Disparity between physical and virtual parameters
Authentication	Identity misappropriation	Phishing	Lack of fine-grain access controls to nodes and tables	Lack of AAA services to access data from heterogeneous devices

insiders or external attackers) spread over multiple nodes. Therefore, it is crucial to introduce security services such as granular access controls, real time monitoring of devices, exhaustive logging procedures, and others.

Virtualization. For the creation and integration of the virtualization technologies in the industry of the future, it is necessary to create standards for the secure information exchange between the physical assets and their virtual representations in order to achieve interoperability among all the interfaces [14]. Again, in terms of *availability*, the multiplicity of devices (each one with its own vulnerabilities) and technologies in this context complicates the assurance of fault-tolerance and the realization of multi-platform user interfaces (e.g., augmented/virtual reality glasses, smartphones). Regarding the *integrity*, the representation of the cyber-physical world also implies the synchronization of coherent data among virtual and real endpoints (e.g., control commands and 3D coordinates) to avoid producing incorrect predictions or dysfunctions in those resources. This information used in simulations could also be leaked due to various reasons (e.g. unsecure execution environments, workers lacking the necessary training), posing a threat to *confidentiality*. In addition, privacy must be taken into account, as the location of operators should be tracked in order to propagate information efficiently. Moreover, *authentication* issues exist with the dissemination of information over multiple platforms and the virtualization of services, blurring the barriers of data protection and easing its access by unauthorized entities, which is aggravated with the use of smartphones and similar devices that are easily breakable. It is thereby necessary to establish trust management procedures when sharing critical information, as well as strict control over the data produced by collaborating partners.

4 Cyber-security threats in Industry 4.0 innovative services

In the previous section we have introduced the security threats that affect the main enabling technologies of Industry 4.0. Yet it is also vital to review what are the threats that could affect the most innovative services of this novel industrial ecosystem. The reason is simple: while these services inherit the threats of their enabling technologies, there are also various novel threats that arise due to their particular features. For this analysis, whose results have been obtained through an expert review of the available Industry 4.0 state of the art, we will continue following the IETF standard 7416 [9]. We also provide an overall summary of the main threats of each service in Table 2.

Novel infrastructures. The gradual transition to more decentralized architectures shown in section 2 is bringing a more heterogeneous and complex environment, where any element could (theoretically) interact and cooperate with any other element. Besides the potential dangers of unresponsive components, from the point of view of *availability* this transition means that not only a malicious insider could target any element, but also that a DoS attack could be launched from any element of the infrastructure. In terms of *integrity*, we need to consider that an adversary can alter the overall global behaviour (e.g. process workflows) by tampering with local decision makers. This is related to the *confidentiality* issues, where malicious attacks against local entities might expose high-level behaviour. Finally, regarding *authentication* threats, as the barriers between the different subsystems are blurred, it is necessary to deploy adequate security policies that can limit the damage caused by unauthorized accesses. However, the expected complexity of such policies will surely result on misconfigured systems, which can be exploited by adversaries.

Retrofitting. It is possible to bring the benefits of the Industry 4.0 to legacy systems by deploying and connecting new technologies to older subsystems [15]. Still, these deployments also bring additional security issues that need to be considered. The existence of a parallel subsystem (e.g. a monitoring system) might bring certain *availability* and *integrity* issues: not only the components that serve as the bridge between the old and the new can become a single point of failure, but also the new technologies could be used to launch attacks against the legacy elements. *Confidentiality* threats also exist, as the new technologies usually act as a "sensing layer" that can expose information about the status and behaviour of the monitored industrial processes. As for the impact of *authentication* threats, it mostly depends on the granularity of the integration of the novel subsystems: black-box interfaces limit the amount of information that can be retrieved from internal subcomponents.

Industrial data space. One of the goals the Industry 4.0 is to create common spaces for the secure exchange of information between industrial partners [16]. The creation of such cooperative spaces could bring additional threats from the point of view of *availability* and *integrity*: the existence of DoS attacks that interrupt the information flow at critical times, or tainted components generating bogus data, will probably affect other elements – opening the door to potential cascade effects. *Confidentiality* is also especially important in this context: it is essential to assure that the information exchanged by partners does not facilitate the extraction of competitive intelligence. Still, misconfigurations and other internal attacks might open the door to more serious information leaks. *Authentication* threats are also aggravated in this cooperative space, as unauthorized accesses can have a wider impact in the extraction of valuable information.

Cloud manufacturing. One of the tenets of this paradigm is the creation of cloud-based industrial applications that take advantage of distributed manufacturing resources [17]. This distribution of resources creates certain threats that have been already described in the context of the novel digital architectures: from DoS attacks that can be launched from anywhere to anywhere (*Availability*), to the manipulation of the distributed components (*Integrity*). The main difference here is the nature of these threats, such as malicious VMs targetting the hypervisors, DoS against the cloud/fog servers or the network connection, etc. *Confidentiality* threats also become more critical, as the cloud infrastructure not only contains sensitive data, but also sensitive business processes as well. Finally, the complexity in the management of these kind of cloud-based infrastructures also opens more opportunities for *authentication* attacks.

Agents. There are already various proof-of-concepts related to the integration of agents in manufacturing, such as workflow planners to self-organising assembly systems [18]. But there are dangers associated to the deployment of agents in an industrial environment, too. A malicious agent can behave like a piece of malware, affecting the *availability* of other industrial elements. Besides the *integrity* of the agents themselves, we also have to consider how other manipulated elements can exert a (in)direct influence over the behaviour of the agents. By tampering with the environment that surrounds the agent, or even the agent itself, it is possible to launch several *confidentiality* attacks that aim to extract the information flow that goes to the agent, and the information created by the agent itself. Finally, without a proper *authentication* infrastructure, malicious/manipulated agents will tamper with the overall workflow.

Other enhanced interactions. As aforementioned, Industry 4.0 enabling technologies such as virtualization allow the creation of novel services such as "digital twins" (virtual representations of subsystems) and "digital workers" (interaction with advanced HMI). Yet there are certain threats related to the actual usage of such technologies and services that need to be highlighted here.

Table 2: Main Cyber-security threats of Industry 4.0 innovative services

	Dig. Arch.	**Retrofitting**	**Data Space**	**Cloud Manuf.**	**Agents**	**Others**
Availability	Wide attack surface	Single point of failure	Cascade effects	Wide attack surface	Agents as malware	Denial of service
Confidentiality	Global data in local context	Exposure of sensing layer	Information leakage	Business processes leakage	Agent data in local context	Information leakage
Integrity	Behavior manipulation	Cross-cutting attacks	Cascade effects	Manipulation of components	Tampered data / agents	Disrupt decision making processes
Authentication	Complexity and Misconfiguration	Fake legacy / sensing layers	Bigger scope of attacks	Management issues	Attacks from/to agents	Privilege escalation

These enhanced systems can be manipulated by their human operators, effectively increasing the damage caused by an insider: a malicious digital worker could perform several attacks such as launching DoS attacks (*Availability*), interfering with the decision making processes (*Integrity*), extracting confidential information (*Confidentiality*), and executing privilege escalation attacks (*Authentication*). On the other hand, these enhanced systems can become attackers themselves, causing damage in subtle ways. For example, a malicious attacker could manipulate the HMI to force the worker to perform an incorrect action – and pin the blame on him.

5 Intrusion Detection in Industry 4.0

The analyses performed in the previous section have shown that Industry 4.0 threats are inherently more complex than the threats that target traditional industrial environments. Since networks and interactions are no longer compartmentalized, the attack surface increases – not only in terms of vulnerable entities, but also in terms of potential attackers and attack strategies (e.g. behavioral attacks). Besides, as the number of elements and business processes increases, the existence of misconfigured elements does so as well. Moreover, the opportunities for collaboration also increase the amount of information that is available to an adversary in case he controls a section of the system. These threats have considerable influence on how intrusion detection systems (IDS) must be designed, deployed and managed in these kind of contexts. In particular, given the threats described in the previous sections, an IDS should comply with several requirements that are described below.

- **Coverage.** Due to the extended attack surface, the IDS must be able to cover all potential interactions and elements of an Industry 4.0 deployment. In addition, it must be able to be easily upgraded with new detection algorithms.

- **Holism.** The IDS must be able to consider not only the different parts of the system – including users, configurations, interactions, potential points of failure and cascade effects, and the like – but also their interactions as a whole, mainly due to the cooperative nature of their elements and the interactions between all actors.

- **Intelligence.** Beyond traditional protocol analysis and information correlation mechanisms, the IDS should take into consideration the existence of more advanced attacks and incorporate more advanced detection techniques such as behavioral analysis.

- **Symbiosis.** The IDS should closely interact not only with other protection mechanisms, such as prevention systems and forensics, but also with other relevant Industry 4.0 services, such as "digital twins".

Notice that these requirements are also desirable for traditional industrial ecosystems, yet such requirements are very difficult to enforce in those contexts – mainly due to the inherent industrial features and necessary trade-offs (e.g. avoid false alarms that can put the production line in jeopardy, minimize the impact of the IDS components in the operational network, etc [19]). Still, the cooperative, dynamic and complex nature of Industry 4.0 ecosystems require that IDS subsystems must interact more closely with the industrial components, in order to detect attacks before their impact becomes too severe.

Understandably, and also due to the specific features of industrial ecosystems, the actual state of the art on IDS for the current industrial ecosystems (cf. [19]) do not fully cover the previously mentioned requirements, and do not consider the services mentioned in section 4. Besides, there are few or no components that search for anomalies in the behavior of Industry 4.0 essential protocols, such as OPC-UA; and the concepts of symbiosis and exchange of security information in this context are still in its infancy.

As for the creation of IDS mechanisms for the industry of the future, there is no need to start from zero: there are various elements in the state of the art that can be adapted and/or enhanced to fulfill the previously presented requirements. For example, there are various platforms that provide event correlation and knowledge extraction from a holistic perspective, although most of such platforms focus on a more centralized architecture. Precisely, there are also agent-based architectures that validate the behavior of the monitored systems [20].

Moreover, there are various preliminary works that could serve as a foundation for the more advanced features required by Industry 4.0 IDS, such as the dynamic deployment of honeypots adapted to the requirements of the system, the automatic identification of critical elements, and the interaction with physical simulation systems in order to detect anomalies [21].

6 Conclusions

In this article we have provided an overview of the threats and requirements that are related to the enabling technologies and innovative services of Industry 4.0. As cyber-attacks against industrial ecosystems are increasing, the integration of novel technologies will create new avenues to exploit. Therefore, it is crucial to take these novel threats into consideration and further study how to apply the highlighted requirements in the design of intrusion detection mechanisms for 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) project. The work of the first author han been partially financed by the Spanish Ministry of Education under the FPU program (FPU15/03213).

References

[1] R Davies. Industry 4.0. digitalisation for productivity and growth. *European Parliamentary Research Service, Briefing*, 2015.

[2] ICS-CERT. Overview of cyber vulnerabilities. `https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities`, June 2017.

[3] Paulo Leitão, José Barbosa, Maria-Eleftheria Ch Papadopoulou, and Iakovos S Venieris. Standardization in cyber-physical systems: The arum case. In *IEEE International Conference on Industrial Technology (ICIT'15)*, pages 2988–2993, 2015.

[4] Armando W Colombo, Stamatis Karnouskos, and Thomas Bangemann. Towards the next generation of industrial cyber-physical systems. In *Industrial cloud-based cyber-physical systems*, pages 1–22. Springer, 2014.

[5] Xun Xu. From cloud computing to cloud manufacturing. *Robotics and computer-integrated manufacturing*, 28(1):75–86, 2012.

[6] M. Chiang and T. Zhang. Fog and iot: An overview of research opportunities. *IEEE Internet of Things Journal*, 3(6):854–864, December 2016.

[7] Aitor Moreno, Gorka Velez, Aitor Ardanza, Iñigo Barandiaran, Álvaro Ruíz de Infante, and Raúl Chopitea. Virtualisation process of a sheet metal punching machine within the industry 4.0 vision. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, pages 1–9, 2016.

[8] Federal Office for information Security. Industrial control system security: Top 10 threats and countermeasures 2016. `https:`

//www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005E.pdf?__blob=publicationFile\&v=3, June 2017.

[9] 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.

[10] 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.

[11] Issa M Khalil, Abdallah Khreishah, and Muhammad Azeem. Cloud computing security: a survey. *Computers*, 3(1):1–35, 2014.

[12] Jeffrey Dean and Sanjay Ghemawat. Mapreduce: simplified data processing on large clusters. *Communications of the ACM*, 51(1):107–113, 2008.

[13] Govind Murari Upadhyay and Harsh Arora. Vulnerabilities of data storage security in big data. *IITM Journal of Management and IT*, 7(1):37–41, 2016.

[14] Malte Brettel, Niklas Friederichsen, Michael Keller, and Marius Rosenberg. How virtualization, decentralization and network building change the manufacturing landscape: An industry 4.0 perspective. *International Journal of Mechanical, Industrial Science and Engineering*, 8(1):37–44, 2014.

[15] T. Stock and G. Seliger. Opportunities of sustainable manufacturing in industry 4.0. *Procedia CIRP*, 40:536–541, 2016.

[16] Industrial Data Space Association. Industrial data space: Reference architecture. `http://www.industrialdataspace.org/en/`, June 2017.

[17] Dazhong Wu, Matthew John Greer, David W. Rosen, and Dirk Schaefer. Cloud manufacturing: Strategic vision and state-of-the-art. *Journal of Manufacturing Systems*, 32(4):564–579, 2013.

[18] 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.

[19] 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'17)*, 2017.

[20] HeSec. HeSec Smart Agents. `http://he-sec.com/products/`, June 2017.

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