Challenges in Cybersecurity for Industry 4.0

Vitor Jesus and Mark Josephs
School of Computing and Digital Technology
Birmingham City University
City Centre Campus, Millennium Point, Birmingham, UK. B4 7XG.
Email: vitor.jesus@bcu.ac.uk

Abstract
Industry 4.0 is an ongoing transformation that aligns Industry with new computing and business models. Examples of enabling technologies are Cloud Computing, Cyber-Physical Systems, Artificial Intelligence and Big Data. Some technologies are well established in other sectors, such as Financial and IT, but the adaptation effort is nevertheless significant. Among the risks, cybersecurity is at the forefront. This chapter discusses why Industry 4.0 brings unprecedented cybersecurity challenges to Manufacturing and the overall Industrial sector. To overcome them, we make the case for new codes of practice that take a holistic view of the IT and OT world whilst adopting a framework that should be native to Industry 4.0.

Keywords
Cybersecurity, Industry 4.0, Industrial Internet

INTRODUCTION

Industry 4.0 (or "Industrie 4.0" as the German initiative is called) is now on the agenda of all industrial sectors as the Fourth Industrial Revolution. Similar initiatives, although with important differences, exist elsewhere with the Industrial Internet (from the United States) being at the forefront. Given that there are more similarities than differences, we shall collectively refer to these initiatives as Industry 4.0 (I4.0). In our opinion, I4.0 is more likely to be an evolution than a revolution but one that, nevertheless, will transform industry and manufacturing. A 2014 report from PricewaterhouseCoopers envisioned €140 billion annual spending by European industry until 2020 with more than 80% of companies seeing their value chain digitised and an increase of productivity of 18% (PricewaterhouseCoopers, 2014).

The notion of digitisation is central to I4.0. In opposition to Information Technologies[1] (IT), that essentially handle information, materials cannot be digitised. However, the operations environment concerning People, Processes and Products (commonly called the 3P) can indeed be digitised with the corresponding improvements in productivity (Thames & Schaefer 2016). Furthermore, it enables new business models where different parties, not necessarily connected, collaborate to create new products, sometimes called Social Products (Rüßmann et al 2015), in an agile way. Such digitisation has two main axes: vertically, it should cover the business units of the same organisation, from the plant to the business

[1] In this chapter, we collectively call IT any field that is not Industrial while fully appreciating that other fields, such as Telecommunications or Medical devices, do not perfectly fall under Information Technologies.

intelligence; horizontally, it should cover the whole supply chain, from customers to suppliers to partners or agencies.

I4.0 is, in the first place, a convergence of traditional manufacturing techniques with current trends in information technologies. It goes beyond that, however, as it also sets a new paradigm in terms of business collaboration and the use of technology with two overarching goals, namely, zero-defects and turnaround efficiency from design to finished product.

The opportunity to rethink Industry comes at a time when a number of key technologies has matured sufficiently – such as Cloud Computing and Mobile Technologies – technologies that are ready to be embedded in a sector that is traditionally conservative and/or has long upgrade cycles. Past the effort involved in the transformation, cybersecurity is raised as a top concern of business leaders (Bughin et al 2015), given the exploding complexity of the technologies involved, which creates risks and an attack surface that did not exist before. In a simplistic way, what before could be protected with walls and physical security, now requires a matching level of sophistication and management.

The remainder of this chapter is organised as follows. In the next section, we review the key technologies involved in I4.0, and then go on to identify the old and new cybersecurity risks. In the last section, we propose directions for mitigation of the identified risks.

INDUSTRY 4.0 ENABLERS

We start by reviewing the key elements of Industry 4.0 to guide the later discussion on cybersecurity. We split the key enablers of Industry 4.0 into four categories: Cyber-Physical Systems (CPS); Cloud-assisted Manufacturing; Mobile Technologies and Augmented Reality; and Big Data, Artificial Intelligence and Analytics.

Cyber-Physical Systems

CPS are any systems that provide an interface between the computing infrastructure and the physical reality. A simple split is sensors and actuators that are enabled with networking interfaces in order to report measurements and/or actuate on the physical environment (Igor 2016). Internet-of-Things is a close concept, although the CPS mostly relate to the physical devices and IoT typically combine devices and a cloud counterpart. Consider a scenario of an automotive wheel made of a light alloy containing magnesium or aluminium with each unit needing to have a unique identifier. A simple example of a CPS is an actuator that marks the wheel with a Quick Response (QR) code and a set of sensors that later track the same code in order for each manufactured unit to have a globally unique identity (Cheng et al 2016).

CPS may also take the form of embedded devices that have computing capabilities and run a complex embedded Operating System, such as Linux or QNX. Depending on the application, such devices may process data before sending to a centralised point (that can be in the Cloud). An alternative is to send the data to other nearby intermediary devices that will pre-process and aggregate data from multiple devices before sending to a central architecture to either control an industrial process or for analysis – a so-called Fog Computing architecture (Peralta et al 2017).

Considering that the backbone of Industry 4.0 is the digitisation of the manufacturing process, CPS play a central role as they are expected to be pervasive both vertically, from data at the plant floor to business analytics, and horizontally by communicating reliable data to multiple stakeholders. A key element associated with CPS is, naturally, industrial robots. By achieving increasingly greater autonomy, the human element can be removed from adverse environments with corresponding efficiency and flexibility gains. When fully integrated in the Smart Factory, robots are on the critical path of end-to-end digitisation.

Cloud-assisted Manufacturing

Cloud Computing is a fairly recent, yet mature, paradigm for computing that relies on using shared and remote resources, often in an imprecise physical location or distributed across multiple ones. In terms of business, this model has several advantages when considering the Total Cost of Ownership of a server infrastructure which, beyond economies of scale, has important manageability properties since the physical infrastructure is often outsourced. Cloud computing intensively uses virtualisation techniques that allow a multi-tenancy model: multiple users have access to the same physical server while applications and services run as if using dedicated hardware. A common provider of a (public) Cloud is Amazon with its Amazon Web Services: using simple interfaces, servers and services can be deployed extremely quickly – minutes in contrast with the months it might take to buy and provision an actual server infrastructure before applications and services can be installed.

A common way of defining a cloud paradigm is to say that its adoption converts resources and processes into programmatic software interfaces. An industrial use case would be customer fulfilment that is as simple as placing an order and uploading CAD files on a web site, then waiting for the package to be delivered. The cloud service sets in motion all the required manufacturing processes, internally manages scheduling and availability of resources and hands-over the product to other parties for further handling and delivery. Such on-demand self-service is a possible delivery model and is particularly applicable when considering Additive Manufacturing (AM). Although not commonly used in today's die cast industry, where mostly alternative methods depending on the product are used, AM is commonly considered one of the enablers of Industry 4.0. In AM, manufacturing is often envisioned as evolving to a model where any part with any geometry can be uploaded to be (3D-) printed with high efficiency in raw materials waste.

Cloud-assisted Manufacturing takes advantage of this computing model to enable new business models. Not only does it have the potential of virtualising, via software interfaces, physical processes, but it has also the ability of combining and matching suppliers, providers, tools and space in order to create value (Mabkhot et al 2018) from the composition of virtualised services. In fact, one can imagine a full virtualised factory in this way, where multiple specialised suppliers are composed using an online tool that more or less autonomously organises and defines the workflow, from the design files to physical delivery. Another example is a customer creating different customised products. Such horizontal integration of multiple parties dynamically cooperating along a chain of value is also seen as a key driver towards Smart Factories (Strange 2017).

Mobile Technologies and Augmented Reality

Mobility and Augmented Reality are, in this scope, tightly connected. We gather here those requirements that enable different stakeholders, from a business owner to an operator, to have access anywhere and anytime to required and detailed information, in a human-friendly way, or even be able to control a process remotely. Whereas mobile technologies in conjunction

with a Cloud infrastructure, enable an anywhere-anytime-anyone paradigm, Augmented Reality creates new usability patterns. For example, a CAD model can be virtually manipulated in real-time as if it is a physical object and, given availability of information, can even be visually matched with a part during its manufacture.

Big Data and Artificial Intelligence

Techniques to analyse large volumes of data, both offline and in real-time, are now available that allow unprecedented efficiency, both in terms of obtaining the current status of a process or workflow and in terms of identifying hidden trends and value. Whereas Big Data is the set of technologies that enable the analysis of very large volumes of information, Artificial Intelligence (AI), in its primary form as Machine Learning, consists of giving inference capabilities to computer systems. The vision is that information is collected at many different points and lifecycles, with collection points ranging from CPS to business workflows (logistics, finance, scheduling, etc.) and sent to be analysed. The data mining can be used at any point in the business: from real-time data to assist the industrial processes to business analytics to inform strategic and operational decisions.

THE CYBERSECURITY CHALLENGE

Industry 4.0 dramatically changes the threat landscape in comparison to traditional manufacturing. For one thing, its inherent technological basis dramatically increases the attack surface, exposing a business or process to the possibility of being compromised in many different ways. Furthermore, the human element is now a key source of risks: considering the dense network of actors in the chain of value of I4.0, from users to suppliers, third-parties and inter-domain interfaces now pose a management problem that was much smaller (often negligible) before. We now discuss how Industry 4.0 impacts cybersecurity practices.

Operational Technologies versus Information Technologies

A simple starting model in cybersecurity is the CIA triangle: Confidentiality, Integrity and Availability. Different sectors have different priorities. Whereas a financial business will be mostly concerned with Confidentiality and Integrity, an electricity supplier will focus its security practices on Availability. Manufacturers would typically focus on either Availability, in the case of high-volume but low added-value products, or Integrity, in the opposite case. By Integrity, one means a high-quality, repeatable and accurate production. Industry 4.0 requires all three elements at the same level of attention.

When compared with Information Technologies, securing Operational Technologies (OT) has inherently different requirements – Table 1 briefly makes a comparison. For diverse reasons, OT requires a cybersecurity approach that is distinct from IT and the first author has first-hand experience in seeing cybersecurity programmes designed with IT in mind systematically fail or quickly be found to be inadequate. One reason is to do with the difference of cultures between the two domains. Whereas IT uses widespread and conventional technologies, that get updated and upgraded in very short cycles, OT projects can take years to develop and can have a field longevity of decades. Furthermore, industrial projects always have, regardless of the sector, a safety-critical element. It is often said that, if an IT system fails, the business gets phone calls from angry users, but if a furnace explodes it can take human lives. OT is nevertheless converging with IT, both in terms of adapting mature and advanced IT technologies to OT projects and also because IT is increasingly seeing requirements that once were only for OT – for example, with operations running on a 24x7x365 basis. Another reason is that OT equipment and software is usually different from what is found in IT,

coming from different, specialised vendors whose software development processes often do not have the maturity, or the same resources, as those of well-known vendors. The result is that devices are often more limited in terms of features and support is not as agile, which impacts on the cybersecurity world when it comes to vulnerability management and updates.

It is also worth pointing out that cybersecurity for OT has only recently started to be taken seriously throughout the sector. It can be argued that the Stuxnet case (Lachow 2011) in Iran, 2010, was a turning point for industrial cybersecurity. Since then, the world has seen multiple high-profile incidents, while numerous small ones remain to be analysed. Cybersecurity for OT was, until then, often considered a lesser concern. In fact, cybersecurity for OT relied – and still often does – in physical isolation of the plant from the rest of the business, the so-called "air gap". This apparently seems to reduce the problem to one of physical security which has been repeatedly proven to not provide the expected assurances (Cisco Blogs 2018). For example, industrial networks often have wireless access points in order to facilitate remote maintenance, but attackers can exploit them too.

Table 1 – Requirements of OT versus IT

	Information Technologies (IT)	**Operational Technologies (OT)**
Different Industries	Enterprise, Datacentres, Financial, Services	Energy, Oil&Gas, Manufacturing, Automotive, Transportation, Smart Cities, Smart Buildings
Different Goals	Information-centric: data confidentiality, business support, can usually be stopped if necessary; fast development and obsolescence lifecycles (5y)	Process-centric: 24x7x365 availability, critical infrastructure, real-time interactions, cannot usually be stopped (societal/environmental); long project lifecycles (up to 25 years)
Different Technologies & Vendors	Servers, Enterprise networks, Applications, Web, End-user, laptops and mobile devices	PLCs, Remote telemetry, HMIs, historians, industrial or real-time protocols, raw materials, critical real-time control, telemetry centric, field devices, mixed technologies (OS, embedded, proprietary, legacy)
Different Practices	ISO 27001; OWASP; CISSP; EU/GDPR; SOC; FedRAMP; CSA	ISA99/IEC62443; GIAC GICSP; Industry specific; Operations Reliability

Increased Surface Attack of Industry 4.0

Industry 4.0 removes the split between IT and OT while dramatically increasing the surface attack of compared to traditional manufacturing. We identify four main reasons: the inherent complexity of I4.0, assimilation of IT risks, transition and change management, and, finally, Third-Party management.

Scale and Complexity

Industry 4.0 is a system-of-systems which raises unparalleled complexity and scale when compared to traditional manufacturing, given the expected dense interconnectivity between processes, products and people. To contrast, whereas before the industrial processes could simply be protected inside a physically secure space, now the myriad of devices and systems can be converted to a point of compromise, which can be remote and from which the whole business becomes vulnerable. Such complexity and scale needs to be properly managed

across the lifecycle of a security programme which has both a technical and business dimension. Furthermore, considering all risks, a single successful attack is now able to cause significant damage (in the order of the investment effort in Industry 4.0) if cybersecurity is not designed in from the outset.

A striking source of complexity and scale is the ubiquity of networked CPS that now become an attack vector. For example, a CPS in a I4.0 setting should to be reconfigurable which raises its software complexity and increases the risk of vulnerabilities – in fact, it could conflict with safety requirements. A key risk is a CPS running compromised software which is only fairly addressed by using trusted hardware (cryptographic functions directly implemented on electronics) (Waidner & Kasper 2016) and which is harder to develop software for. Table 2 lists some of the high-level threats to which CPS are exposed. A successful attack rarely uses a single vector; instead, they are usually a combination of actions and steps that may take months to carry out until a goal is reached. A common technique is lateral movements: a device is compromised only to serve as a foothold and, from there, other devices or systems are compromised in accordance with a strategic plan.

Table 2 – some cybersecurity attacks associated with CPS

Attack type	**Description**
Physical	Changing the hardware or software by physically modifying it.
Impersonation	A malicious device hiding between legitimate devices.
Man-in-the-middle	Intercepting and/or modifying in-flight communications
DoS	Denial of Service: compromise availability of services, machines or communications
Malware	Malicious software installed and undetected

Assimilation of IT risks and requirements

Off the plant floor, the I4.0 factory will bring in all the risks that IT currently has which will add to the typical risks of OT. The Cloud component is an example – see Table 3 for typical attacks. On the one hand, exposing software interfaces to the public Internet will attract remote attacks and will facilitate reconnaissance, a key stage in any attack where discovery of vulnerabilities is made. On the other hand, mobile users will have access to important assets and will have to use trusted devices and, above all, have enough training in order to be aware of the risks and cybersecurity best-practices. The current trend of Bring-Your-Own-Device (BYOD) will require special measures as a trade-off between efficiency, personal freedom and cybersecurity is likely to exist.

Table 3 – some cybersecurity attacks associated with Cloud Computing

Attack type	**Description**
Data Breaches	Stealing valuable data
Account mismanagement	Compromised credentials or keeping legitimate owners out of service
Insecure interfaces	The software interfaces used in interacting with the cloud are vulnerable
DoS	Denial of Service: compromise availability of services, machines or communications
Compliance violation	Storing or using data in a fashion not compliant with regulations
Compromised shared hardware	The servers on which the applications and services run are compromised.

Man in the middle	Capturing data in transit or tampering with service requests

Revisiting the scenario where a customer uploads to the Cloud a CAD file of a part that needs to be manufactured, the file eventually reaches the plant floor but may be compromised with subtle modifications that could be difficult to detect. A case in die cast or additive manufacturing is adding seemingly imperceptible imperfections, such as indents or voids (Cao et al 2015), which weaken or otherwise lower the quality of the final part. Even worse, new smart file types to be designed (CAD, STL, tooling files) may be prone to embedding executable malware which may be a door to an attacker.

Data quality is also now a requirement. A possible attack on Artificial Intelligence agents is where they are remotely re-trained, using legitimate interactions such as a set of customers feeding inconsistent data, in order to skew their inference processes. Overall, a data quality attack is such that data used is subtly contaminated in order to cause inaccuracies.

Finally, one major challenge is the early state of integrated cybersecurity frameworks for Industry 4.0 (Waidner & Kasper 2016). It should be noted that whereas IT is rich in cybersecurity standards and guidance, some at the regulatory level, OT is not. A sign of this is looking at current I4.0 models such as RAMI or IIRA (Ma et al 2017) and realising, surprisingly, that cybersecurity is something of an afterthought.

Transition Management

It is expected that the transition between traditional and smart factories will take time and several upgrade cycles. This means that traditional and modern devices, systems and processes will coexist. There are two cybersecurity implications. The first is that old vulnerable devices will have less cybersecurity capabilities, or have vulnerabilities that cannot be patched. They will, expectedly also be hard, if not impossible, to retrofit and will integrate in a less ideal way with the I4.0 architecture. This requires mitigations based on perimeter infrastructure such as Intrusion Detection Systems which is challenging on its own for Industry 4.0 (Rubio et al 2017) given the heterogeneity of devices, industries and applications.

Secondly, history has proven that change management creates its own vulnerabilities. There are countless examples of forgotten servers or devices that, in the extreme case, are openly accessible on the Internet. In any project, managing change is always complex, both in terms of resources and realignment with processes; in cybersecurity it can temporarily, yet dramatically, raise risks.

Finally, a note on cybersecurity operations. With scale, threat intelligence and incident monitoring become complex bringing the problem to the levels of large IT infrastructures. Even if engineers have proven skills in complex process monitoring, cybersecurity requires different techniques and technologies which may require significant effort in order to adjust and prepare (Moustafa et al 2018).

Third Party Management and Context

Finally, Industry 4.0 brings a new challenge for Manufacturing that typically did not exist before. Given the dynamic business context composed of many parties, administrative borders become critically important: customers, suppliers and partners are now part of the operations. A comprehensive cybersecurity programme needs to account for the lack of good cybersecurity practices of Third Parties.

It is always challenging, in any industry, to manage the cybersecurity of Third parties since, by definition, a business has only signed agreements at their disposal or, at best, some powers to audit that are always limited. Other than that, a simple sharing of a credential to upload, for example, a design file of a part can compromise the whole business. Old problems, such as auditing the provenance of materials and parts are now scaled up.

Furthermore, Confidentiality and Privacy are now also strong requirements. By opening to the wider business context, Intellectual Property of customers, for example, has to be managed in a structured and consistent way. This further opens the space to Regulations connected to cybersecurity. For example, the recent EU directive Networks and Information Systems (NIS), that is essentially a cybersecurity regulation, mostly applies to critical infrastructure operators but will indirectly affect suppliers and intermediaries.

Finally, considerations must be given to incident response and forensics (Eden et al 2016). In handling an incident, as it may escalate up to involving regulatory authorities, there may be a duty to collect evidence in a legally acceptable way. Whereas components sourced from the IT domain typically have security controls in place, such as audit logs, OT components typically do not. Furthermore, collecting evidence in real-time during production may prove extremely challenging and needs to be avoided at all costs.

PERSPECTIVES

The rise in sophistication of Industry 4.0 can only be matched by raising the sophistication of the cybersecurity approach itself. Whereas IT practices are robust and mature in their essence, they cannot fully cover the Industrial case. As such, a mix of practices and technologies, both new and old, needs to be drawn upon in order to design a comprehensive cybersecurity programme for Industry 4.0. Figure 1 (left) gives a representative lifecycle of a cybersecurity programme, typically designed for IT. It should be contrasted with Figure 1 (right) that shows a typical model for Manufacturing. Beyond protecting the human, always the top priority, cybersecurity has to be supported by a business case and it is in this sense that it is currently evolving, from a management perspective, as a risk discipline, similar to other business domains (Radanliev et al 2018). An alternative would be to decompose the overall problem of the Industry 4.0 factory and progressively identify and break down possible risks which are then mitigated using either processes or technologies informed by standards and community guidance. Ultimately, as Figure 1 (right) shows, it is integrated into the business strategy and governance.

Considering the diversity of elements in Industry 4.0 that form a continuum between different areas (for example, CPS to Cloud to Business IT), we argue that a combination of current cybersecurity approaches may not completely close all the gaps; rather, a specific approach to Industry 4.0 may prove to be necessary with selective implementation of relevant codes of practice where applicable.

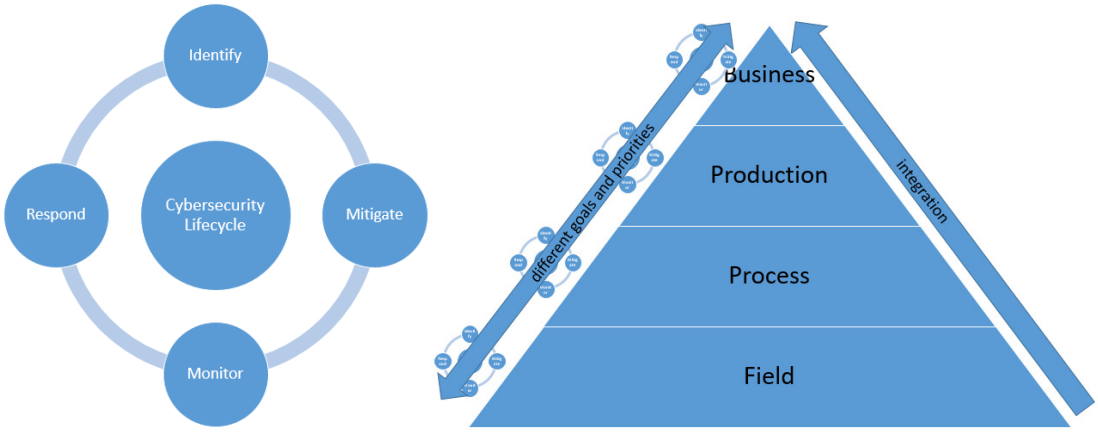

Figure 1 – Cybersecurity governance.

A number of standards exist that can be of help. Table 4 lists some of the prevalent standards and guidance in cybersecurity. IEC/ISA 62443 is particularly fit for Industry 4.0. With current adoption mainly in Oil & Gas, it is a flexible framework for Industrial environments. Others, depending on the particular domain of the Smart Factory, should be used. For example, ISO 27001 should be used to manage a cybersecurity programme based on risk, despite being oriented to Information; and CSA STAR on the cloud subdomain.

Table 4 – Cybersecurity related standards and guidance.

Guidance	Domain	Aim
ISO 27001, SOC 2	IT	IT cybersecurity management
CSA STAR, CIS, ISO 27018	IT, Cloud	Security in the cloud
EU/GDPR	IT	Data Privacy regulation (EU)
NIST	Various	Catalogue of recommendations (US)
OWASP, ISO 27034	IT (Web)	Secure software development
IEC/ISA 62443	Industrial	Industrial and SCADA cybersecurity

Finally, one aspect that can be of help is that Industry 4.0 will accelerate the convergence between IT and OT which may have the benefit of standardising OT technologies in the direction of IT and enable the reuse of mature IT cybersecurity technologies in OT. Examples are next-generation firewalls or Intrusion Detection Systems (Rubio 2017) which are commonly less featured in OT than their counterpart in IT.

CONCLUSIONS AND OUTLOOK

This chapter discussed the challenges that Industry 4.0 face regarding cybersecurity. Because of its transformative character and the complexity of system-of-systems, involving several different technical and business visions, multiple challenges were identified. The paradigm still has to mature and materialise in concrete use-cases as the ones available for analysis are still sparse. Furthermore, cybersecurity frameworks for I4.0 are still lacking which includes models to manage the transition and coexistence of traditional and I4.0 domains. A different framework is therefore needed that, on the one hand, is able to integrate the multiple domains that comprise the new Industrial paradigm (which current standards are able to address) but, on the other hand, has to be native to Industry 4.0 given its own emergent properties.

References

Bughin, J., Chui, M. and Manyika, J. (2015), *An executive's guide to the internet of things*, McKinsey Quarterly, Vol. 4, pp. 92-101, 2015

Cao, B, et al (2015), *Research and Practice on Aluminium Industry 4.0*, 6th Intl Conf on Intelligent Control and Information Processing, Wihan, China, Nov 2015

Cheng, F-T et al (2016), *Industry 4.1 for Wheel Machining Automation*, IEEE Robotics and Automation Letters, vol. 1, no. 1, January 2016

Cisco Blogs (2018), *HAVEX Proves (Again) that the Airgap is a Myth: Time for Real Cybersecurity in ICS Environments*, https://blogs.cisco.com/digital/havex-proves-again-that-the-airgap-is-a-myth-time-for-real-cybersecurity-in-ics-environments, July 3, 2014 (accessed 21 August 2018)

Eden, P, et al (2016), SCADA System Forensic Analysis Within IIoT, Springer Series in Advanced Manufacturing, Cybersecurity for Industry 4.0, 2016

Igor, H, Bohuslava, J, Martin, J (2016), *Proposal of communication standardization of industrial networks in Industry 4.0*, 20th IEEE Intl Conf on Intelligent Engineering Systems, June 2016, Budapest, Hungary

Lachow, I, (2011), *The Stuxnet Enigma: Implications for the Future of Cybersecurity*, Georgetown Journal of International Affairs, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity, 2011, pp. 118-126

Ma, Z, Hudic, A, Shaaban, A, Plosz, S (2017), *Security Viewpoint in a Reference Architecture Model for Cyber-Physical Production Systems*, IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2017

Mabkhot, MM, Al-Ahmari, MA, Salah, B, Alkhalefah, H (2018), *Requirements of the Smart Factory System: A Survey and Perspective*, Machines, MDPI, v6, i23, June 2018

Moustafa, N, et al (2018), A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems, IEEE Access, v6, 2018

Peralta, G, Iglesias-Urkia, M, Barcelo, M, Gomez, R, Moran, A, and Bilbao J (2017), *Fog computing based efficient IoT scheme for the Industry 4.0*, IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM), Donostia-San Sebastian, 2017, pp. 1-6

PricewaterhouseCoopers (2014), *Industry 4.0 – Opportunities and Challenges of the Industrial Internet*, Dec 2014

Radanliev, P, et al (2018), Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-Things in Industry 4.0, Living in the Internet of Things: Cybersecurity of the IoT, London, 2018

Rubio, JE, Roman, R, Lopez J (2017), *Analysis of cybersecurity threats in Industry 4.0: the case of intrusion detection*, CRITIS 2017

Rüßmann, M, Lorenz, M, Gerbert, P, Waldner, M, Justus, J, Engel, P, and Harnisch, M, (2015), *Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries*, The Boston Consulting Group, April 2015

Strange, R, Zucchella, A (2017), *Industry 4.0, global value chains and international business*, Multinational Business Review, Vol. 25, Issue 3

Thames, L, Schaefer, D (2016), *Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges*, Springer Series in Advanced Manufacturing, Cybersecurity for Industry 4.0, 2016

Waidner, M, and Kasper, M (2016), *Security in industrie 4.0 - challenges and solutions for the fourth industrial revolution*, Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, 2016