Journal of Manufacturing Systems 47 (2018) 93–106

Contents lists available at ScienceDirect

Journal of Manufacturing Systems

journal homepage: www.elsevier.com/locate/jmansys

Security of smart manufacturing systems

Nilufer Tuptuk*, Stephen Hailes

Department of Computer Science, University College London, London, United Kingdom

ARTICLE INFO

Keywords:
Smart manufacturing
Sustainable manufacturing
Design for manufacturing
Internet of Things
Information security
Cyber-physical systems

ABSTRACT

A revolution in manufacturing systems is underway: substantial recent investment has been directed towards the development of smart manufacturing systems that are able to respond in real time to changes in customer demands, as well as the conditions in the supply chain and in the factory itself. Smart manufacturing is a key component of the broader thrust towards Industry 4.0, and relies on the creation of a bridge between digital and physical environments through Internet of Things (IoT) technologies, coupled with enhancements to those digital environments through greater use of cloud systems, data analytics and machine learning. Whilst these individual technologies have been in development for some time, their integration with industrial systems leads to new challenges as well as potential benefits. In this paper, we explore the challenges faced by those wishing to secure smart manufacturing systems. Lessons from history suggest that where an attempt has been made to retrofit security on systems for which the primary driver was the development of functionality, there are inevitable and costly breaches. Indeed, today's manufacturing systems have started to experience this over the past few years; however, the integration of complex smart manufacturing technologies massively increases the scope for attack from adversaries aiming at industrial espionage and sabotage. The potential outcome of these attacks ranges from economic damage and lost production, through injury and loss of life, to catastrophic nation-wide effects. In this paper, we discuss the security of existing industrial and manufacturing systems, existing vulnerabilities, potential future cyber-attacks, the weaknesses of existing measures, the levels of awareness and preparedness for future security challenges, and why security must play a key role underpinning the development of future smart manufacturing systems.

1. Introduction

Levels of investment in smart manufacturing have been rising rapidly – more than half of manufacturers have invested at least $100 million in the activity. Industry is starting to see rewards from this: according to Capgemini [1] smart manufacturing has helped factories achieve productivity gains of 17–20% whilst simultaneously achieving quality gains of 15–20%. It is no surprise then that many manufacturers – with numbers reaching as high as 67% for industrial manufacturing – have smart factory initiatives and, if Capgemini's estimates are to be believed, the result will be a gain to the global economy of $500 billion to $1.5 trillion over the next five years.

Much of this projected growth is predicated on the use of Internet of Things (IoT) technologies, coupled with cloud computing, data analytics, machine learning and AI. In this, it is IoT that provides the bridge between the digital domain, including new analytical methods, and the physical domain of the plant and within the supply chain. This aligns well with the Industry 4.0 vision of transforming the supply chains into a smart network of connected intelligent and autonomous objects that communicate and interact with each other in real time [2]. As a result, since its inception in 2013, Industry 4.0 has recognised central role to be played by IoT as a key enabler for advanced smart manufacturing. Germany is not alone in this ambition, there are a number of other EU-level initiatives [3] and China's Made in China 2025 initiative [4] to digitalise and automate their manufacturing to preserve their competitiveness in highly globalised and competitive markets. The most significant risk in this rush towards flexibility, quality and productivity is that security is seen as being of secondary concern rather than an essential component of the process of development and deployment. The increase in cyber-based attacks on industrial and manufacturing systems shows that even existing systems are vulnerable, those vulnerabilities are poorly understood and, as a result, organisations are not prepared for the security threats that exist. Since smart manufacturing capabilities are predicated on levels of technical sophistication, integration and automation far beyond those conventional manufacturing processes, there will be new vulnerabilities and the lack of clarity on security is doubly concerning.

In the past, security in manufacturing systems was achieved through

* Corresponding author.
E-mail addresses: nilufer.tuptuk.13@ucl.ac.uk (N. Tuptuk), s.hailes@cs.ucl.ac.uk (S. Hailes).

https://doi.org/10.1016/j.jmsy.2018.04.007
Received 6 November 2017; Received in revised form 21 February 2018; Accepted 11 April 2018
Available online 15 May 2018

isolation based on the control of physical access. Recently, for reasons of cost and convenience, Ethernet and the IP protocol stack are becoming a core part of plant and factory networks, with the consequence that connecting such networks to wider corporate systems is becoming easier and more common. Similarly, to extend network infrastructure to remote areas, increase sensing capacity, handle mobility and reduce installation costs, there is an increase in the deployment of wireless networks. Both approaches have the potential to leave networks vulnerable and the scale of this vulnerability is under-appreciated in the industry: according to data collected from Project SHINE, between April 2012 and January 2014, an excess of 500,000 Internet-accessible manufacturing devices in control system environments were found [5]. The custom-designed search engine for searching Internet-connected things, SHODAN, was used to search for devices such as Programmable Logic Controller (PLC) systems, Remote Terminal Unit (RTU) systems, Supervisory Control and Data Acquisition (SCADA) servers, Human Machine Interface (HMI) servers, Distributed Control Systems (DCS) sensors and Intelligent Electronic Devices (IEDs) that are used to monitor and control systems. As the increase in the number of cyber-attacks illustrates, adapting Internet-connected devices without considering security is making the manufacturing industry one of the top industries targetted and amongst the most vulnerable [6].

The remainder of the paper is structured as follows: in Section 2 we discuss current and smart manufacturing systems and introduce some of the reported attacks on these systems. In Section 3, we discuss why security should be a key characteristics in smart manufacturing systems and examine some of the incidents against manufacturing systems and technologies. In Section 4, we explain the fundamental differences between the IT and manufacturing system security, and discuss the vulnerabilities, types of attacks and adversaries. In Section 5, we discuss the existing active and passive countermeasures, we report on some of the standards and guidelines, cryptographic techniques, and intrusion detection systems. In Section 6 we discuss future research directions, and in the final section, we provide an overview and conclude with some recommendations.

2. Current manufacturing systems

The research and development efforts from academia and industry on networked control systems, robotics, industrial wireless sensor networks, and smart manufacturing [7], together with innovation efforts for manufacturing SMEs [8] are all directed towards the creation of smart factories delivering cost-effective, efficient (machine, labour, energy and material), sustainable and safe manufacturing systems.

The Computer-Integrated Manufacturing (CIM) model illustrated in Fig. 1 shows the hierarchical architecture of computer systems and communication connections that are found in manufacturing automation systems. This is a highly integrated model that has been used and

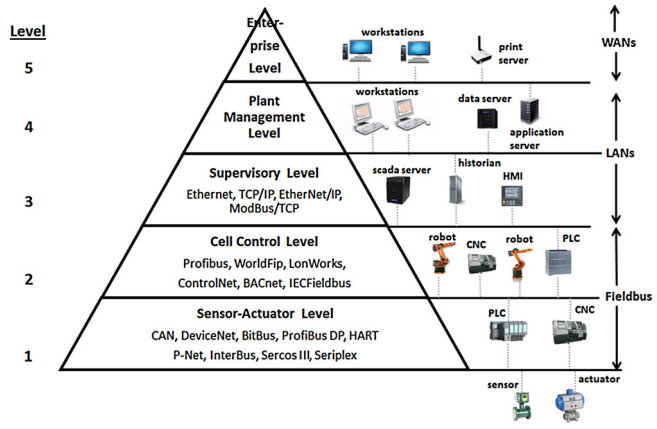

Fig. 1. Computer-integrated manufacturing (CIM) model.

incorporated into many other models and standards in the manufacturing industry. The model is divided into five layers in which general purpose network protocols are used at higher layers, and special protocols are utilised at lower layers to deliver increasingly tight latencies and more specialised requirements. As illustrated in Fig. 1, on the top level the Enterprise/Corporate Level, the decisions related to the operational management which define the work flows to produce the end product are made. At the Plant Management Level, these decisions are managed locally on the plant management network. On the Supervisory Level, various manufacturing cells are managed, each performing a different manufacturing process. At the Cell Control Level, different actions of the process are performed. At the bottom level, Sensor-actuator level, controllers, sensors and actuators are integrated to perform the physical process. This model is vulnerable to security attacks because it is insecure by design. Communication protocols used to support this infrastructure such as Modbus, Distributed Network Protocol (DNP3), PROFIBUS, Building Automation and Control Networking (BACnet), Industrial Ethernet are widely used on the supervisory and control level to connect devices, buses or networks. These communication protocols were not designed with security in mind, and lack mechanisms to provide authentication, integrity, freshness of the data, non-repudiation, confidentiality and measures to detect faults and abnormal behaviour.

The concept of CIM differs from the Industry 4.0 vision, as it is rather rigidly structured. At the lower layers (3-1), master/slave architectures are widely used, in which communication is typically initiated by the master. Industry 4.0 and other similar initiatives for cyber-physical systems propose a more decentralised architecture in which elements of the CIM model are autonomous. Autonomous elements are aware of their environment and can communicate with other elements to control what is required. This results in a decentralised autonomous model in which products and machines will become active participants in the IoT, behaving as autonomous agents throughout the production line. As the product moves through the production line, it will communicate with each machine, and tell it the process that it requires at that point, enabling flexible control between products and machines. Within this vision, decentralised decision making is key, acquiring data and processing it on the spot in real-time. Self-governance, self-awareness, self-organisation, self-maintenance and self-repair are some of the attributes used to describe the capabilities of the components and systems of future factories and plants.

Such an open environment is prone to a wide range of both passive and active security attacks ranging from conventional eavesdropping and denial of service (DoS) attacks to man-in-the-middle attacks that subtly alter the quality or consistency of the end product. Compared to attacks on conventional networks, the consequences of attacks on elements of manufacturing systems can be catastrophic as they have the ability to cause physical damage to production, people and the physical environment. The only way to address this problem is to embed consideration of security (and the ongoing management of security) from the design stage, a lesson that was learned the hard way in conventional networked systems [9]. The openness of the architecture, the flexibility in reconfiguring it, and the use of data analytics in effecting internal change lead to complex dynamic behaviours that are hard to reason about. Most particularly, it is not currently possible robustly to articulate the expected behaviour in detail and so it is hard to reason about the source of problems or the particular set of dynamic interactions that led to problems. This means that the range of possible attacks are larger in the Industry 4.0 model than for CIM, but the chances of detection are lower and the approach to mitigation is unclear.

3. Smart manufacturing systems

As is the case with many emerging technologies, there is no single universally accepted definition of smart manufacturing. In the main it is defined rather loosely, often in terms of its objectives or the

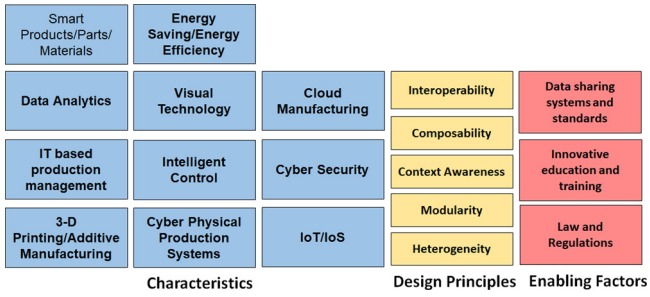

Fig. 2. Characteristics, design principles and enabling technology defining smart manufacturing [10].

contributing technologies. In Fig. 2 we re-present an ontology drawn from the recent review found in [10], which explains smart manufacturing in terms of eleven technology characteristics, five defining principles and three enabling technologies that are used to define smart manufacturing.

The mixture of characteristics includes aspects of technology (visual technology, data analytics, intelligent control, IoT, CPS/CPPS, and cybersecurity), aspects of process (3D printing, cloud manufacturing, IT-based production management), aspects of input, reusability and traceability (Smart products/parts/materials), and aspects of sustainability (Energy efficiency). This clearly is not an exhaustive list of any of the above – for example, energy use is common, but rarely the only consumable one wishes to use efficiently.

From a security viewpoint, a number of interesting things emerge from this categorisation:

- IT-based production management links planning systems within the IT domain to the CPPS that are extend onto the shop floor. As a consequence, the security of the full smart manufacturing process depends on the joint and several security properties of the IT domain, the CPPS domain, and the communications link that must exist between them.
- Subverting the process of data analytics and intelligent (adaptive and/or learned) control by poisoning the data on which analysis or learning is undertaken could have significant effects on the physical integrity of the plant or the quality of its output. Since the data provided is typically high dimensional, and small changes might have significant effects on learning methods that are often more fragile than might be commonly understood, such problems are extremely hard to detect. The problem is exacerbated by the fact that we are only just beginning to explore learning systems in which a human-understandable narrative about what was learned emerges from the learning process.
- Cybersecurity is regarded as a characteristic rather than a design principle. This misconception has led to the production of insecure systems throughout the Internet. Security is not a product that can be bought and added to a system: instead, it is a process that starts at or before the design stage and must pervade all aspects of the system produced. Moreover, it is a continuing process: the emergence of new threats may necessitate a fundamental review of the security of the entire plant, which can only be understood from the perspective of system design. Naturally, the flexibility to add or remove modular subsystems further complicates matters.

The enabling factors in Fig. 2 are given as standardisation, education and law/regulation. These enabling factors are every bit as critical to security as they are to other aspects of smart manufacturing. Since manufacturing has been computerised for many years one might expect that progress would have been made in developing standards, education and law that are tailored to the needs of manufacturing industry. However, this is far from the case: if security is even considered, there is frequently an implicit assumption that all computer systems are like IT systems; there is widespread ignorance of likely threats and adversaries; and, whilst there are standards for all aspects of manufacturing, many ignore security on the presumption that there is no need credible threat. If one adds in the richness of smart manufacturing, the threats one might expect to face are not yet even well identified, let alone researched.

The remainder of this paper is dedicated to exploring these issues in more detail, starting with an examination of some of the incidents that have been reported in respect of attacks on manufacturing systems.

3.1. Reported incidents against manufacturing systems

In view of the fact that the deployed base of smart manufacturing systems is considerably smaller than that of conventional manufacturing systems, it is perhaps unsurprising that there are few reported attacks against them. This is not an indication of the lack of vulnerabilities in such systems, but argues more strongly towards their relative novelty and complexity. This, in turn, suggests that, with the possible exception of governmental information warfare programmes, the hacking community have yet to acquire the specific knowledge that would allow them to launch successful attacks. To rely on this remaining the case would be foolhardy in exactly the same way that relying on the discouraging effect of the challenges in attacking conventional manufacturing systems has proved to be. To that end, an awareness of the attacks that have been reported against conventional systems is an important precursor to understanding the potential for attacks against smart manufacturing systems.

The reported attacks targeting industrial and manufacturing systems demonstrate that the threats are real, and that the consequences of these attacks can be severe. One of the most recent attack against manufacturing systems was the attack on Ukraine's power grid in December 2015 [11]. Combining a number of tactics, including using malware and denial of service, attackers managed to bring the electricity distribution infrastructure into an undesirable state, causing power outages. These outages resulted in several blackouts, causing 225,000 customers to lose power across Ukraine.

At the end of 2014, attackers gained access to a steel factory in Germany. According to the report [12] written by the German Federal Office for Information Security (Bundesamt für Sicherheit in derInformationstechnik), the attackers leveraged spearphishing and social engineering techniques to gain access to control network through the corporate network. As a result, the attackers managed to cause unspecified, but massive, physical damage to the system by manipulating individual control components, thereby bringing the blast furnace under their control. The skill sets required to carry out this attack were not only in the field of information security, but extended to the industrial control systems and production processes [12].

Another key incident in 2014 was Havex/Dragonfly, in which a Remote Access Trojan (RAT) was used to compromise industrial control systems including SCADA, PLC and DCS used within the energy sector [13] across the globe. The aim of the RAT was industrial espionage. Security companies observed targetted spearphishing attempts with PDF attachments against mainly US and UK companies from the energy sector from early 2013 [14]. A Watering-hole attack was used to install the RAT on the machines operating industrial control systems. Legitimate energy vendor websites were compromised and redirected to download malware from attackers' servers.

In 2011, a sophisticated instance of a RAT known as Duqu infected control systems in Europe, Asia and North Africa. Duqu's payload modules contained remote access capabilities that were used to connect to a command and control (C&C) server (a computer that issues commands and receives reports from the infected machines) and download additional executables including those used to perform network enumeration, record keystrokes and collect system information. The intention of the RAT was to gather intelligence that could be used to carry out future attacks on industrial control system facilities and other

industries. The intelligence collected was encrypted and packed into an empty JPG image file received from the C&C server. Duqu had a number of variants, and made use of C&C servers located in various places including India, Belgium and Vietnam. By default, Duqu was configured to run for 3 days, and then remove itself from the system automatically. However, adopting a peer-to-peer C&C model, it had the capability to receive additional commands to extend the length of the attack.

Stuxnet [15], first reported in 2010, is believed to be the first worm that was designed with the sole aim of causing physical damage. There is very little irrefutable information about its heritage but it is thought to have been created by or on behalf of a government due to the technical expertise and resources needed perform such an attack. Analysis carried out by Symantec [15] showed most of the infected machines (approximately 60%) were from Iran. This led the security experts to suspect the attack was specifically targeting Iran's uranium enrichment facility at the Natanz enrichment plant. Researchers estimated Stuxnet may have destroyed about 1000 (10%) of the centrifuges installed at the time of the attack [15]. The malware was designed to attack two models of Siemens PLC (Siemens S7-125 and S7-417) which were controlled by Siemens' Step 7 software. It exploited four zero-day vulnerabilities, propagated itself via removable media and USB drives that would later be connected to the control systems, and used advanced techniques to mask itself under legal programs to avoid detection. The worm used legitimate certificates, using private keys stolen from two separate companies to sign the device drivers on the Windows operating system [15].

In 2005 a worm called Zotob disabled 13 of Daimler Chrysler's car manufacturing plants [16] across the US, causing them to be offline from 5 to 50 min (a substantial amount of production time), stopping the activities of 50,000 assembly line workers. The worm exploited a buffer overflow vulnerability on a TCP Port found in Windows 2000 systems and some earlier versions of Microsoft Windows to open a backdoor. According to the reports [17], while executing the worm the operating systems became unstable, resulting in an unplanned cycle of shut down and rebooting. It is believed that the worm and the new variants of it affected more than 100 companies including the construction and mining equipment company Caterpillar.

The analysis of security incidents is beset by under-reporting. This has been examined more thoroughly in the case of Internet-related systems, and usually occurs either because an incident was not identified as the result of a security breach or because the reputational damage was considered to be too significant to publicly report a security failure. The Internet community have moved forwards somewhat, and there are annual reviews of cybersecurity incidents that better reflect the lived experience of business. Unfortunately there is still rather little reporting of incidents relating to manufacturing and the most prominent examples are those that caused significant damage or that appreciably failed to remove the evidence of their existence.

3.2. Reported incidents against smart manufacturing systems technologies

As discussed above, it is not unexpected that the numbers of attacks against smart factories has been low. However, there have been some significant attacks launched against some of the enabling technologies for smart manufacturing, most notably IoT.

Typical IoT nodes combine a relatively low-powered processor with wireless networking capabilities and so can be attacked directly by individuals within their radio range. This undermines the traditional model of security in which there is a defined perimeter and devices (e.g. firewalls and intrusion detection systems) that are responsible for securing that border. Instead, each device must be at least partially responsible for its own security, a task that is made more difficult by the reduced processing capabilities of a typical IoT node. Naturally, this is not helped when manufacturers fail to appreciate the large-scale implications of failing to secure individual devices appropriately and the high-profile IoT botnet Mirai [18], which caused the largest ever seen distributed denial of service attack, is a salutary example of this failure. The operation of Mirai botnet is illustrated in Fig. 3. Mirai identifies vulnerable IoT devices by scanning those that can be reached using the Internet. Once these devices are identified, a brute force attack with a simple dictionary attack (composed of factory default usernames and passwords such as admin/admin) [19] is carried out (1). The bots report the identified IP addresses of the vulnerable devices to report servers (2), which then distribute the vulnerable devices to load servers (Mirai had three) (3). A load server loads malware specific to the victim's operating system (4). Once the device runs the malware it becomes a bot (5), and receives new commands from the command and control server (C&C server) (6). Mirai also had capabilities to eradicate other malware processes by closing all processes that use SSH, telnet and HTTP ports, and searches for and then kills other botnet processes that might be running on the device. The C&C server communicates with report server to keep an eye on the infected devices (7). Bots carry out distributed denial of services attacks (DDoS) on targets (8), and they continue to scan and infect new victims, and receive new instructions from the C&C server (9).

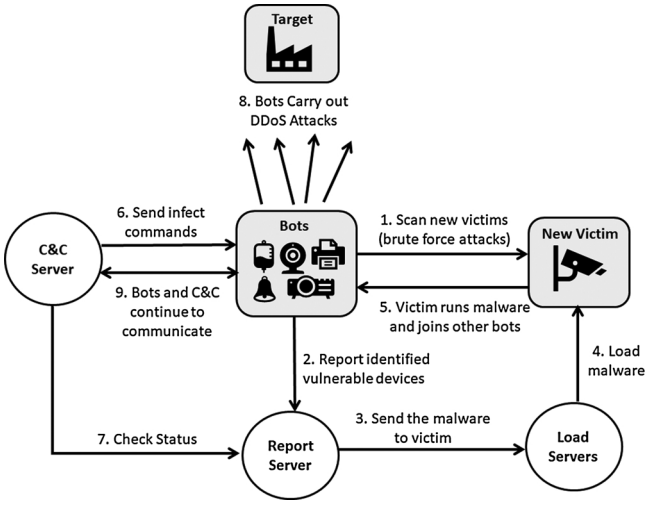

Fig. 3. Mirai botnet operations.

The Mirai botnet and its variants [20,21] show how attacks could leverage the lack of security in IoT devices and conduct successful attacks that could cause production downtime and equipment failure, or reputational damage as the source of the attack on other systems.

4. Smart manufacturing systems security fundamentals

4.1. Difference between manufacturing systems and IT systems

A common misconception in manufacturing is that the challenges of computer security are similar irrespective of which computers are being secured. Whilst it is certainly the case that lessons learned from the Internet world are often applicable to other networked systems, the characteristics of manufacturing systems makes their security requirements distinct from the IT systems that are used at the corporate level. Table 1 presents a comparison between the system, operational, and security aspects of the two domains. The components used within the smart manufacturing systems domain are heterogeneous, with a high number of legacy systems and devices, that can have a lifetime up to 20 years. Tasks, managed by a small number of users (operators and engineers), have real-time constraints that need to be imposed to ensure the continuity of the process. These systems have complex interactions with physical processes, and failures can manifest in physical events. Regular patching and upgrades are a *sine qua non* of IT systems security, and most companies patch at least monthly and sometimes on an *ad hoc*

Table 1
Comparison between manufacturing systems and IT systems.

Category	Attributes	Manufacturing systems	IT systems
Systems	Components	Heterogeneous	Homogenous
	Lifetime	Long (< 20 years)	Short (< 5 years)
	Network protocols	Real-time proprietary protocols and some open protocols	Open protocols
	Network	Serial, Ethernet	Ethernet
	Users	Low	High
Operation	Real-time	Time-critical	Best-effort
	Availability	Critical	Outages, rebooting tolerable
	Resources	Limited	Enough resources for security
	Patching and upgrading	Not frequent	Frequent
Security	Order of priorities	Safety, availability, integrity, confidentiality	Confidentiality, integrity, availability
	Awareness	Inadequate	Good
	Experts	Low	High
	Prevention	Physical protection	Defence in depth
	Forensics	Limited	Available
Impact	Losses	Catastrophic (monetary, deaths and injuries, damage to physical equipment and environment)	Recoverable (monetary)
	Incident recovery and contingency planning	Rare	Common

basis, as the importance of a threat becomes apparent. Patching and upgrading are becoming more common in industrial control operations; however, these need to be planned carefully because halting systems for a patch or an upgrade may involve a whole production line in significant downtime, with costs to match. Indeed, many manufacturing systems owners may not patch immediately, and may decide not to patch to avoid the risk associated with some of these challenges. To be able to patch, vendors need release patches, and the time between vulnerability disclosure and patch release may not be sufficiently short to prevent attacks. Another challenge associated with patching ICS is that it often requires people with expert skills to carry out the patching process.

This is one instance in which IT systems are typically constructed to maintain an adequate level of service given the inevitability of delays and downtime driven by the need to manage security subsystems. The traditional approach to manufacturing systems design emphasises the primacy of operational performance, but this optimisation is done without considering the need to maintain system security as an integrated part of that process. It is assumed that it can be added at a later date. It is no surprise, then, that the industry currently relies heavily on a large number of legacy systems that have little security (e.g. default passwords, no access control and undocumented backdoors), and relies on vendors to provide security services. By definition, these should be holistic, but they often extend no further than basic encryption. Through experience and necessity, the IT industry has built better security awareness, skills and people than the industrial and manufacturing sector. Moreover, the security priorities of the both sectors are fundamentally different. In IT systems, the security is often defined in terms of three key principles: confidentiality, integrity and availability (also known as the CIA-Triad). Confidentiality focuses on ensuring assets are not disclosed those entities who are not authorised to view it; integrity relates to protecting assets from unauthorised modifications; and availability is defined in terms of making the assets accessible to authorised entities at all permitted times. The CIA-triad helps to determine the security risk management priorities. The greatest concern for industrial and manufacturing systems is generally the availability and integrity (which one comes first depends on the system), as lack of data and false data could damage the process or production. The confidentiality goal is not unimportant; however, budgetary constraints might mean availability and integrity goals will have a higher priority. Similarly, for corporate networks, the importance of the data itself means that more is invested in confidentiality and integrity. The safety aspects of systems in the computing world has been discussed under dependability (Fig. 4). Safety and reliability have been important

Fig. 4. Dependability and security attributes [22].

design parameters for industrial and manufacturing systems for decades; however the focus of this is on prevention and diagnostic capabilities to prevent conditions arising (hazards and failures) that could cause harm to humans and the environment, damage to or loss of process, equipment or any other assets. With the increase of cybercrime, the tools and methodologies to carry digital forensics and handle digital evidence have emerged and gained importance as a research field within the IT infrastructures; however, forensics for manufacturing systems infrastructures is still in its infancy.

Looking forwards, one might expect that lessons learned from securing IoT, cloud computing and data analytics deployments outside of manufacturing might be applicable to smart manufacturing systems, and most of them will be. However, for the same reasons that the lessons learned from IT systems are not the only knowledge needed to secure manufacturing systems, the lessons learned from isolated deployments of the component parts of smart manufacturing systems are unlikely to encompass the knowledge needed to secure the integrated whole of smart manufacturing systems. This is particularly true for IoT since, at present, the most sophisticated uses of IoT technologies lie precisely within smart manufacturing rather than in more general deployments. That said, the MIRAI botnet and the various spinoffs from it, discussed in Section 3.2, illustrate the damage that can be done when IoT security is neglected.

4.2. Vulnerabilities

To understand the likely avenues of attack, one needs to understand the vulnerabilities of systems. Again, little has been done to explore this for smart manufacturing systems, but there has been work for manufacturing systems as a whole that is pertinent to the broader understanding of risk. Fig. 5 shows the number of vulnerabilities reported and logged in ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) from 2010 to 2015 [23]. This is not a comprehensive

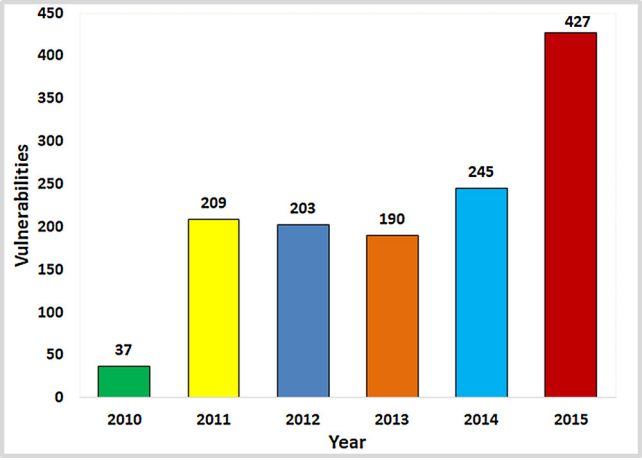

Fig. 5. Reported manufacturing vulnerabilities [23].

analysis, but it illustrates the significant increase that has happened since 2010. Others have also reported similar growth in the number of industrial control system vulnerabilities in technologies that are widely used in manufacturing systems in 2015 [6,24]. In this section, we describe how vulnerabilities are introduced to the systems.

Manufacturing systems have typically either been designed without security in mind, or with the explicit presumption that the system is isolated and so not subject to (outsider) attack. Secure software development practices focusing on the prevention of software vulnerabilities, including the specification of security requirements, and the implementation of the security properties, including testing, code review, and patch management have not been widely considered when building these systems. Attempts to retro-fit security to existing systems in the light of attacks has a poor track record: in view of the fact that the system is operational, it is hard to ensure that the new security systems are as fully tested as the original design, and as a result they are often overly conservative in places whilst failing fully to protect the system and introducing new bugs and vulnerabilities. Thus consideration of security is vital at each phase of the system's life cycle [25].

Adopting *commercial off-the-shelf (COTS)* products, such as open protocols and workstations running well known operating systems such as Microsoft Windows or Linux, has reduced the installation costs and provided greater interconnectivity. However, these also inherit the vulnerabilities of these products and provide greater opportunity to attack these systems. Industrial Control Systems make use of a wide variety of *insecure communication protocols* such as Modbus, PROFINET, DNP3 and EtherCAT. Although Modbus and DNP3 began as serial protocols, they were both extended to work with TCP/IP and Ethernet, and they are widely used to connect devices on different field buses or networks. These systems do not have the security mechanisms to support authentication (for example, anyone can masquerade as a master and send commands to slave devices), integrity of packets, anti-repudiation or anti-replay [26].

Vulnerabilities are often introduced to manufacturing systems through *poor security policies and practices*. Even today, commonly accepted and 'obvious' good practice such as disabling unnecessary connections and changing default connection settings and passwords are rather less common in the industry than one might reasonably anticipate given the history of attacks. It should not be surprising then that, given the novelty of IoT systems and given the uncertainties introduced into those systems by the dynamic changes that arise from opaque learned behaviours, there is no commonly agreed view of what the vulnerabilities of smart manufacturing systems might be. Without such an understanding and without the action that follows from it, part of which can admittedly only come from experience, the inevitable conclusion is that such systems are vulnerable in ways we have yet to discover.

4.3. Attack types

Given the lack of understanding of the precise vulnerabilities of smart manufacturing systems, we can only consider how similar systems have been attacked in the past. In this section, we consider the general classes of attack that have been seen in networked systems in the past. Ideally, this would include substantial detail about attacks on manufacturing systems; however, the number of manufacturing systems attacks made public and confirmed are relatively low [27]. The relatively small number of reported attacks is likely down to some combination of four factors: (i) attacks are hard: they require specialist knowledge of manufacturing systems that is not widely present in the community of potential attackers; (ii) attackers shun manufacturing systems for their own social reasons: given a similar amount of effort, it may be possible to generate an IT systems attack that has global reach and so generate greater kudos for the attacker; (iii) people are simply unaware that they are under attack because the effects of those attacks are subtle or because there is a failure to associate the symptoms with the possibility of an attack; (iv) attacks are simply not reported, because to do so would damage business credibility. It would be extraordinarily foolish to rely on the first two reasons above remaining the case. The communication network protocols used for industrial automation were not designed with security in mind, and rather little analysis has been done of their security properties in comparison to similar Internet protocols. That which has been done suggests that their security properties vary significantly, leaving both known and (presumably) unknown vulnerabilities.

To design security it is essential to understand from where the potential threats arise. Attacks can be launched over all network links: through enterprise connections, connections through other networks at the control network layer, and/or connections at the field device level. Some of the common attacks are:

- **Denial of service (DoS) attack:** This attack aims to deny the availability of some assets such as a network, a system device, or any other computational resources such as memory, process or file system to legitimate users. Distributed Denial of Service Attacks (DDoS) employ multiple compromised systems, which are infected with malware to attack a target. In the past one year, several high profile IoT botnets, such as the Mirai botnet [18], was responsible for some of the largest DDoS attacks seen to date. These botnets compromised hundreds of thousands of IoT devices, demonstrating the invulnerability. New Mirai-like botnets are emerging, such as the Brickerbot [28] and the Repaer [29] botnets, demonstrating the danger of set up and forget approach to IoT devices.
- **Eavesdropping attack:** By monitoring the network, an adversary can gain sensitive information about the behaviour of the network (passive reconnaissance) to perpetrate further attacks. Network traffic analysis, even of encrypted packets, can reveal information (e.g. who is talking to whom and when) and compromise privacy.
- **Man-in-the-middle attack:** In this attack, the adversary sits between communicating devices and relays communication between them. For example, it could sabotage the key exchange protocol (many industrial control systems do this in the clear without any encryption) between a control system and an actuator device.
- **False data injection attack:** A false injection attack is a deception attack, in which the adversary injects false information into the network; for example, by sending malicious commands on a field bus.
- **Time delay attack:** An attacker injects extra time delays into measurements and control values of the systems which can disturb stability of the system and cause equipment to crash [30,31].
- **Data tampering attack:** Data tampering attacks cause unauthorised alteration of data, which could be in storage or in transit. For

example, the data held in data historians' and engineers' workstations could be altered, or the network data packets could be changed causing, significant damage to the operation of the plant.

- **Replay attack:** In a replay attack, legitimate packets can be retransmitted by an adversary. This can happen in several ways: an authentic but compromised node could send the data, e.g. an adversary who managed to intercept an authentication message.
- **Spoofing attack:** Spoofing attacks are where an attacker's node impersonates a system entity. A lack of adequate authentication control mechanisms means that entities can masquerade as one another by falsifying their identity to gain illegitimate access.
- **Side channel attacks:** Side channel attacks are carried out using a variety of techniques that analyse information leakage from hardware and software such as analysing power consumption, light emissions, optical signal, traffic flow (e.g. to gain knowledge about the network topology), timings (e.g. time it takes for an operation), electromagnetic, acoustic and thermal emission from hardware components and faults that occur in the system.
- **Covert-channel attacks:** This is an attack that makes use of a compromised device, and legitimate communication channels to leak sensitive information out of a secure environment, bypassing security measures [32].
- **Zero day-attacks:** These are attacks that exploit unknown vulnerabilities (those that are not disclosed publicly) to exfiltrate data or sabotage the system. The average duration of zero-day attacks is 312 days; however, for some it has taken 30 months to discover the attack, fix the code and distribute a software patch [33]. Once these vulnerabilities are disclosed, the number of attacks exploiting them may increase in an attempt to find unpatched systems. There is a growing market for zero-day attacks, with buyers paying over 100,000 USD for certain exploits [34].
- **Physical attack:** By gaining physical access to manufacturing systems equipment, attackers can manipulate the devices that are accessible, for example de-calibrating sensors to modify input signals; changing the location of a device (e.g. a sensor), causing the received input to contain errors; introducing a rogue device into the network to masquerade as a legitimate device; and attacking physical properties of the devices (e.g. through glitch attacks involving modification of the clock or the power supply to the chip to manipulate the operation of the system).
- **Attacks against machine learning and data analytics:** Machine learning techniques are widely used in security from biometrics to network security monitoring. For smart manufacturing systems, data analysis lies at the heart of the benefits that this smart approach is likely to bring. As a result, if machine learning process can be subverted either directly or through the poisoning of the data on which it relies, consequences will follow. Given the opacity of the learning process it is not always clear, either to the attacked or even the attacker, what the consequences might be or how to identify such an attack. Examples of attack on machine learning include spam filtering [35], malware classifiers [36–38] and biometric recognition systems [39]. Machine learning can be subjected to attacks during training and inference phases. Potential attacks during training include manipulating the training sample to control the model's accuracy; attacking the availability of the sample data to reduce the confidence of the model [40], and confidentiality attacks that reveal information about the training model. Oracle attacks can be carried out during inference to extract confidential information about the model and exploratory attacks can be carried to cause malicious behaviour identified as legitimate [41].

4.3.1. Malware

The most common route to carrying out attacks on manufacturing systems is by installing *malware* with the intentional or unwitting help of insiders. Malware can threaten the availability, integrity and confidentiality of manufacturing systems. As the number of attacks against manufacturing systems has increased, there has also been an increase in the amount of complex malware with advanced evasion capabilities targeting manufacturing systems. Malware is often installed on these systems via *removable media* such as infected USB drives; *spearphishing* attacks (tricking the user into downloading malware from a malicious server, opening an email, or installing an application that contains malware); and *watering-hole attacks* (a compromised legitimate site visited by operators and engineers used, to install malware). In the past attackers made use of a collection of malware tools called *rootkits* to obtain unauthorised access to systems, thereby providing the attacker with sufficient privilege to access confidential data, hide their presence and have the ability to install other malicious software [42]. Rootkits adopt a stealth strategy, hiding themselves within objects (e.g. processes, files and network connections), while carrying out malicious activities on the infected system [43]. These activities include logging user keystrokes, disabling security software, and installing backdoors for other malicious activities [44]. Rootkits are, by and large, installed along with other malicious programs such as *backdoors* or *trojans* [45]. Stuxnet [15] is believed to be the first rootkit targeting a plant. Readily available attack toolkits, known as *exploit kits* have been around for some time, containing prepackaged software tools, that can be used by attackers with unsophisticated skills to carry out an entire attack. The kits are used to identify and exploit vulnerabilities in software, download malware automatically onto users' computers without their consent, known as the *drive-by download* method, and manage attacks. Symantec claims these kits are responsible for two thirds of web attack activity and on average, contain about 10 exploits, mainly browser vulnerabilities [46]. When new exploits are found, they are incorporated into old kits, and published as new releases. The BlackHole exploit kit was first spotted in 2010, and increased in popularity until 2013 with new versions and a sound rental strategy (e.g. rentals were available from $50 a day to an annual license fee of $1500, and support for the duration of the rental). To best of our knowledge, there are no exploit kits that come with pre-packaged multiple exploits that will try to exploit known vulnerabilities in manufacturing systems. However, as attackers become more interested in manufacturing systems similar tools are likely to emerge.

4.4. Adversary model

The motivation for, and sources, of attacks against these systems encompass a wide number of adversaries, including nation states, foreign intelligence services, rival organisations, terrorist groups, organised crime, hacker hobbyist, hacktivists and insiders (current and former employees). There is little reason to suggest that the pool of attackers will differ significantly for smart manufacturing systems, and the population of attackers at any moment in time is likely to evolve from those with significant resources and/or knowledge (nation states, insiders) to hobbyists and script-kiddies, in the same way as has been seen for other forms of system. Attacks on computer systems, particularly those for which source code can be obtained, gradually become public goods and, whilst there are often patches available by the time that hobbyists obtain them, the very many unpatched systems remain vulnerable.

In this section, we illustrate some of the attacks carried out by these classes of attackers.

- **Nation-state** and state-sponsored actors are highly sophisticated adversaries that are significant threats to manufacturing systems. The capabilities of these attackers mean that espionage, sabotage and destruction attacks that could cause physical damage are all plausible. It is not surprising that most countries are developing cyber security capabilities and the ability to target other nations. Recently, the German Chancellor said they were dealing with cyber attacks that could influence the coming German election [47]. The USA claimed spies from China, Russia and other countries tried to

penetrate their electricity grid. State sponsored attacks can be very sophisticated and their potential to cause damage is high as they have the ability to draw on sources of finance, resources and people with advanced skills, and may be able to influence vendors to modify software or hardware systems/devices and install malware or backdoors with which they can carry out these attacks. While attribution of cyber attacks is technically very difficult, it is an area that is also not receiving enough attention from the academic research community at the present; the existing work in this area is probably carried out by state agencies and so remains hidden. When the cyberattack on Ukraine's energy grid took place in December 2015, Ukraine's intelligence services were quick to blame the Russian state-backed hackers [48]; however, there was little concrete evidence to attribute this to the Russians.

- **Terrorist Groups** motivated by ideology may want to attack the operation of manufacturing systems to threat national security, cause causalities, damage the economy and create fear. These attacks have the potential to be very sophisticated as these groups often have the necessary means to finance them. So far we are not aware of any instances of manufacturing systems attacks that have been classified as terrorist attacks. However, as crime is moving online, it is only natural for these groups to try to carry out and coordinate their attacks remotely.
- **Rival organisations** or companies may carry out attacks to damage reputation or for industrial espionage to steal intellectual property.
- **Cybercriminal** attacks by individual criminals or organised networks of criminal entities are usually motivated by financial gain. Criminals are currently very active in the online world. By analogy, attacks on control systems may be carried out for monetary gain, including intellectual property theft and threatening asset owners for ransom. Ransomware is emerging as one of the most dangerous cyberthreats organisations are facing today, with 17% of the manufacturing sector infected [49]. Increasingly, new types of ransomware are emerging in the cybercrime underground. Groups are buying these as services, since they can be used by those with no technical skills. The WannaCry ransomware [50] attacked relatively soft targets around the world, including hospitals. It encrypted users' data and demanded a ransom in bitcoins, to release access to the data. Whilst there is some debate about how targetted WannaCry was, the scale of the impact will undoubtedly have awakened the interest of cybercriminals. Going forwards, systems that have critical characteristics will be most attractive to criminals.
- **Hacker Hobbyists** are typically motivated by curiosity, the thrill of doing something not permitted, or the desire for recognition and status. These attacks are generally unsophisticated, often exploiting vulnerabilities that are public, but can still cause substantial damage. Over the past few years, independent security researchers have reported most manufacturing systems vulnerabilities to ICS-CERT (the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team) [23] around the world. As in the Internet world, as the market for manufacturing systems attacks increases in size, there may be hacker hobbyist with advanced skills that are motivated to find manufacturing systems vulnerabilities, and either exploit them or sell them to third parties.
- **Hacktivists** are patriotic hackers that are often driven by a political ideal; hactivism a form of online activism [51]. The motivations for their actions may be anything from defence of free speech to an anti-nuclear stance. Over the past years, two powerful hacking collectives, Anonymous and Lulzsec, carried out a large number of attacks on the Internet. These attacks include support for election protests in Iran; protesting against the Australian Government's Internet filtering legislation and web censorship regulations; compromising web sites and emails of oil and gas companies to protest against rising oil prices; and bringing attention to WikiLeaks and other political causes. Security services with responsibility for critical national infrastructure have also been targetted by hacking communities; for example, a hacker collective called the Syrian Electronic Army (SEA) has targetted the national infrastructure of Israel [52].
- **Insiders** are current and former employees, business partners, contractors, service providers, vendors, visitors, and anyone else that has access to the organisation's assets. The most common insider attacks are unauthorised access to, and use of, corporate information; unintentional exposure of private or sensitive data; viruses, worms or other malware; and theft of intellectual property. However, threatening insider behaviour occurs in many contexts and appears in various forms, and, often only becomes public if legal action is taken against the attacker. In many cases this does not occur due to concerns about negative publicity, being unable to identify the individual/s committing the act, and lack of evidence [53]. A well known insider attack happened in 2000 in which, an ex-employee of Hunter Watertech, the water treatment control system supplier to Maroochy Shire Council of South East Queensland, too control of sewage equipment by masquerading as an authorised controller [54]. He was able to stop the normal operation of the pumps, and the communication (including alarms) between the pumps and central computers. The attack caused 800,000 l of sewage to be pumped into the environment, including onto local parks and into rivers and hotels. The motives behind insider attacks include financial gain, espionage, emotional backlash, ideology, fear/coercion and excitement [55]. Not all apparent attacks from insiders are malicious: insiders may cause unintentional exposure of sensitive data or systems by error or misuse. Furthermore, rules are often broken due to deadline pressures, lack of awareness or ineffective policies.

4.5. Lifecycle of a targetted attack

The targetted attacks discussed in Section 3.1, launched to date against industrial and manufacturing systems, such as Stuxnet [15], a steel factory [12] in Germany and Ukraine's electricity grid [48] have had clear objectives, and they have usually been specifically tailored to target particular organisations. There are two primary motivations behind these targetted attacks aimed at control systems: (1) exfiltration: harvesting sensitive information from the system and (2) sabotage: disrupting the operation of a system. The attacks discussed in Section 4.3 can be used for sabotage (e.g. DoS, replay, spoofing, data tampering) and exfiltration attacks (e.g. man-in-the middle, covert channels, keyloggers). As discussed earlier, these attacks are carried out by installing malware, exploiting zero-day vulnerabilities, and with the help of insiders. The current skill set and investment required means that many of these attacks are attributed with nation-state hackers.

Based on the past targetted attacks such as Stuxnet, discussed in Section 3.1, the basic steps of the targetted attacks are illustrated in Fig. 6. Pre-Entry activities consist of the ground work to design and implement the attack. This involves identifying targets and goals (objectives); acquiring the necessary knowledge, skills, resources and tools to develop and implement the attack; identifying the routes to infect the system; and testing the attack (e.g. in a mirrored environment). Methods used for initial infection include the exploitation of insiders; the use of social engineering tactics (e.g. phishing or spear phishing with aggressive tactics); and hacking the supply chain (e.g. watering hole attacks in which malware is placed with the original software updates from a compromised trusted vendor website). The propagation phase involves infecting other systems and devices to escalate privileges to gain access to necessary resources (sensitive data or systems of interest). Propagation is typically achieved by exploiting other vulnerabilities. Sometimes, an attack might need simply to maintain a listening presence until further instructions are received from the controller. While in the system, attacks may send data and receive updates via peer-to-peer communication or a C&C server. The operation phase consists of carrying out the necessary steps to achieve the

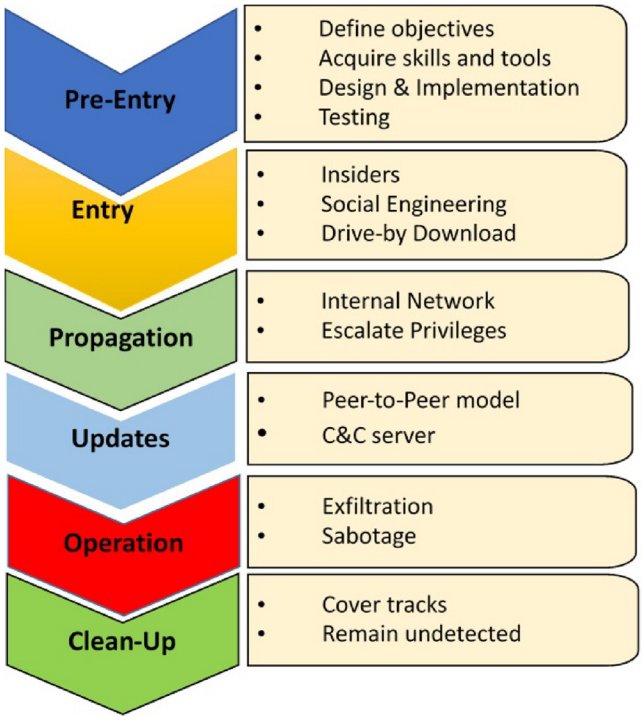

Fig. 6. Lifecycle of the targetted attack.

objectives of the attack (i.e. disrupt the operation of the system, harvest data). Finally, throughout the lifecycle of the attack, the attackers may carry out clean-up operations to evade detection and extend their presence within the network.

In most cases, manufacturing industry has no mechanisms to prevent, detect, and recover from targetted attacks, and, when things go wrong, manual approaches are used to bring the system back to a normal operating state. The response is invariably reactive and, given the novelty of Internet-facing manufacturing systems to the attacker communities, the potential variety of attacks is extensive and unknown. The only way we can begin to understand our exposure to the risk of attack is to develop research programmes in which systems and ideas are actively attacked in advance of deployment. Failing to do this simply means that the attackers have an easier task: the exploits they use might attack systemic failings in deployed systems that could have been detected earlier, and the time available to respond to an attack is shorter than that available to patch a vulnerability.

5. Security solutions for manufacturing systems

Existing security solutions for manufacturing systems can be divided into two main categories: static and active defence. The static defence method focusses on following regulations, typically derived from industrial standards and guidelines. Dynamic defence methods are cryptographic countermeasures, intrusion detection and prevention systems, training and incident management. In the following sections, we discuss some of the most relevant of these security solutions.

5.1. Regulations, standards and guidelines

Traditionally, most of the demands for security came from regulatory bodies that regulate critical national infrastructure such as water, gas, oil and electricity. Over the years, a huge amount of effort by governmental bodies, professional societies and industry has been dedicated to standardisation. Although standards are not regulations, regulators may dictate compliance with a standard such that it becomes part of the regulation. The benefits of regulation and how well it fosters security is open to debate: when security is regulated, companies start to look for ways to escape regulation. For example, the experience drawn from the North American Electric Reliability Corporation showed that companies removed black-start capabilities to avoid paying for compliance [65,66]. The consequences of heavy regulations may lead to organisations to create new vulnerabilities in bypassing demanding regulatory approaches.

There are number of special guidelines to guide the security of industrial systems The National Institute of Standards and Technology (NIST) special publication *NIST SP 800-82*, Guide to Industrial Control Systems (ICS) [67], guides the industrial control sector on how to achieve security of SCADA systems, Distributed Control Systems (DCS), and other control systems; the Department of Homeland Security (DHS) provides several documents aimed at increasing the security of industrial control systems including the *Catalog of Control Systems Security: Recommendations for Standards Developers* [68] and the *Control Systems Cyber Security: Defense in Depth Strategies* document [69]. The Centre for the Protection of National Infrastructure (CPNI) in the UK provides a set of good practice guidelines on *Cyber Security Assessments of Industrial Control Systems* [70] and *Securing the move to IP-based SCADA/PLC networks* [71].

Table 2 illustrates some cross-level standards standards available to develop, implement and maintain the security of manufacturing systems. Much as for guidelines, there are many international and national standardisation efforts, most of which are aimed at industrial automation and control systems. Although these standards do have great importance for manufacturing, there are currently no standards for cybersecurity specific to manufacturing, let alone smart manufacturing. Moreover, what organisations should do with all of this information, and how to select and integrate the most suitable standards into their own organisations, is not obvious. Addressing this problem requires not only expert skills but the ongoing resources required to evaluate and monitor the effectiveness of a selected approach. This requires significant investment and a clear perception of the likely value to be obtained. Unfortunately, the evaluation and monitoring process is also problematic: there are no success metrics with which to analyse supposedly secure systems and determine how well they work. Indeed, a significant risk is that these standards and guidelines can provide a false sense of security.

5.2. Cryptographic techniques

Industrial and manufacturing environments consist of hundreds or even thousands of devices. These devices use software and networking protocols to communicate with other devices and human operators. Cryptographic countermeasures are widely used in corporate networks to achieve confidentiality and integrity of the data. Use of symmetric encryption algorithms, public key infrastructure (PKI), hybrid encryption schemes, cryptographic hash functions, digital signatures, key agreement and distribution protocols are widely used to ensure only authorised entities. Use of encryption, identity and context-based access control are not widely used in automation and manufacturing industry. Existing key management techniques are often manual, and require the operator to carry out the necessary actions such as renewing or revoking a key manually. The difficulties for designing appropriate key management systems for these environments are discussed in [72]. A number of studies including [73–76], proposed key management systems for industrial environments but these do not meet the diverse deployment challenges and performance requirements of plant and factory settings. In these, the key management system needs to be scalable; must work well with limited computational power; must undertake key exchange while not interfering with the the real-time availability of the process; must provide interoperability among systems and devices; and must provide automated key revocation when under attack.

Table 2
Standards available for managing the security of manufacturing systems.

Standard	Domain	Scope
ISA/IEC 62443	Industrial Automation and Control Systems (IACS)	Builds on the ISA99 (on industrial automation and control Systems security) [56], and the current status of the work consists of set of sub-standards, grouped into four categories: *general*, *policies and procedures*, *system*, and *components* [57]. It provides detailed guidance on management, operation and product development of IACS components
ISO/IEC 27019-2013	Energy utility industry	Provides information security management guidelines for process control systems specific to energy sector [58]. Provides guidance based on the ISO/IEC 27000 series of international standards to the process control and automation domain. A new standard ISO/IEC 27019 [59] is currently under development which is primarily based on the 2013 version, ISO/IEC 27001 and 27002 (the information security standards), ISA/IEC 62443, and IEC 62645 (provides security guidance for computer-based systems used within the nuclear power plants)
ISO/IEC 27033-1:2015	IT network security	Provides guidance on the network security (management, operation and use of information system networks, and their interconnection), and aimed at anyone operating or using a network [60].
ISO/IEC 29180:2012	Sensor networks	Provides security framework for telecommunications and information exchange between systems for ubiquitous sensor networks [61].
IEC 61508	Electronics in industry	Provides functional safety standard applicable to all kinds of industry with systems comprised of electrical and/or electronic elements [62].
IEC 61784	Industrial communication networks	Provides a set of specific standards for communication device and profile standard for fieldbuses involved in communications in factory manufacturing and process control. The series includes functional safety and security [63].
ISO/IEC 27000-series	All domains – information security management	Consists of more than a dozen of standards to help organisations keep information assets secure. The standards provides guidelines and practices to keep their critical assets (e.g. financial information, intellectual property, employee details) secure and manage risks [64]. They are aimed at helping organisations implement, maintain, and improve their information security management.

5.3. Intrusion detection systems for production or process systems

Security is a dynamic process that requires a range of measures to cope with the attacks that are continuously evolving. Regardless of the degree of preparation, vulnerabilities will remain, and attackers will try to find them by attacking the system. To counter this, it is necessary to observe the dynamic behaviour and seek to determine whether it is abnormal. In this section, we explain some of the proposed intrusion detection system (IDS) approaches that have been built by academia and industry, specifically to undertake this endeavour for industrial control systems. IDS are classified by source of data (audit source) and detection technique (the data needed for analysis). The former is often classified as *network-based* or *host-based*, and the latter *knowledge-based*, *behaviour-based*.

Host-based IDS are based on gathering data on a single host, and therefore make use of data maintained by that host to determine unauthorised behaviour. *Network-based intrusion detection* collects evidence from the whole or segment of the network. In smart manufacturing systems, in which IoT nodes may be attacked individually by utilising their wireless connections, at least part of the intrusion detection infrastructure will have to run on each (resource poor) host. This is a challenge because intrusion detection systems are typically relatively compute intensive, and we are at an early stage in the development of such techniques. See, for example, [97,98].

Knowledge-based (also known as signature or pattern-based detection) is based on collecting knowledge about previous attacks and vulnerabilities, and looking for patterns to identify intrusions. *Behaviour-based* (also known anomaly-based) intrusion detection systems look for anomalies with respected to the 'normal' or 'expected' behaviour. Normal behaviour is often determined by learning normal system behaviour under conditions in which there is believed to be no attack, using techniques such as machine learning. An approach to behaviour based intrusion detection is a *specification-based* technique, which relies on modelling the system operation to derive deviations from the norm. The performance of intrusion detection systems are often rated by a Receiver Operating Characteristics (ROC) curve, which illustrates the detection probability versus false alarm probability. Table 3 illustrates some of the studies in this area. As illustrated in the table, most effort in this area has been placed on behaviour-based network intrusion systems since knowledge-based IDS require detailed knowledge of previous exploits to define characteristics of the attack. As a result they are unable to detect new intrusions or those exploiting previously unknown vulnerabilities (e.g. zero-day attacks).

IDS research for manufacturing systems and IoT systems is still immature, and the studies are poorly implemented due to limited testbed availability and a paucity of data from real incidents. A common complaint about research in this area is that credible empirical evidence is often not provided when IDS systems are evaluated. These shortcomings make it difficult to make any reliable inference about how well academic IDSs will perform in real smart manufacturing environments, the more so because such environments are adaptive by design and so past history is not necessarily a good guide to current behaviour, even in the absence of attack.

5.4. Security skills training and human factors

One of the challenges of building secure systems in smart manufacturing is the shortage of skilled security personnel. This shortage applies to the entire manufacturing hierarchy from the corporate level to right down to the field/factory level – not just users, but engineers and security managers that are building, managing or using these services. This will become more critical with the move towards IoT systems. Developing security policies that are feasible and usable is not a trivial task, even in well-understood systems; doing this efficiently for adaptive systems, in which security policy may affect both performance and the freedom to adapt, is currently too complex to countenance in practical deployments. If security policies and procedures become a burden to users, history suggests that they will be unwilling to comply with these policies and procedures [99,100] and may misuse the system deliberately. Indeed, despite the increase in personnel awareness training, a large number of incidents are related to the misuse of systems by the personnel [101]. The standards and the guidelines mentioned in Section 5.1 give some directions on staff awareness and training, and emphasise that security is as much a human issue as it is a technical one. However, most of this advice is based on studies on corporate networks and, despite the awareness and training programmes, users continue to become victims of social engineering methods: they regularly fall for phishing attacks [6], for example there is a lack of empirical studies looking at the human factors in security management at the plant level and on factory floors; the importance of this will grow with the increase in attacks.

Table 3
Proposed intrusion detection systems for process systems.

Application	Detection principle	Audit source	Attack type	Data source
SCADA systems [77]	Behaviour specification	Network	Modbus TCP attacks	Operational (communication headers, requests and responses)
SCADA systems [78]	Behaviour	Network	DoS attacks	Operational (server input and output flows)
SCADA systems [79]	Knowledge	Host	Unauthorized access and modification	Operational (authentication commands, events)
Wireless process control systems [80]	Knowledge	Network	Attack against the wireless network	No dataset
SCADA systems [81]	Behaviour	Network	Common vulnerabilities and exposures (CVE) security vulnerabilities	Operational (HTPP and TCP traffic captured from the perimeter and process control networks)
SCADA systems [82]	Behaviour	Network	Critical state detections (zero-day attacks)	Operational (Modbus over TCP traffic)
SCADA systems [83]	Behaviour	Network	Modbus TCP attacks	Operational (network traces)
Embedded control systems [84]	Behaviour	Host	Malware (kernel hijacking)	Operational (operating system kernel)
SCADA systems [85]	Behaviour	Network	Denial of service, unauthorized access, probing	Public (KDD Cup 1999 Data)
SCADA systems [86]	Behaviour	Network	Profinet IO attacks	Operational (Profinet IO frames)
Wireless industrial sensor networks [87]	Behaviour	Network	Packet jamming, impersonation, flooding modification, eavesdropping	Operational (communication traffic, e.g. monitoring neighbor node's traffic)
Power transmission system [88]	Behaviour	Network	Fault replay, command injection, zero-day	Simulation (synchrophasor measurement data and audit logs)
Smart grid [89]	Behaviour	Host	Denial of service, unauthorized access, probing	Public (NSL-KDD dataset
Fluid flow system [90]	Behaviour	Knowledge	Deviations from expected packet stream	Operational (Ethernet network traffic)
SCADA systems [91]	Behaviour	Network	DoS and integrity attacks	simulation testbed (sensor, controller and actuator signals)
SCADA systems [92]	Behaviour specification	Network	Sequence attacks (exploiting valid events)	Operational (data traces from water treatment and purification facility)
Electric substation automation [93]	Knowledge	Network	Password crack attacks, DoS attacks and forged address resolution protocol attacks	Simulation (address resolution protocoL traffic)
SCADA systems [94]	Behaviour specification	Network	Modbus/TCP attacks	Operational (Modbus/TCP request messages)
SCADA systems [95]	Behaviour	Network	Passive and tampering attacks	Simulation testbed
SCADA systems (water treatment system) [96]	Behaviour	Network	SCADA-specific attacks, network attacks, shut-down attack	Operational (testbed using EtherNet/IP and CIP protocol)

5.5. Post incident management

Despite all the security countermeasures, successful attacks will always happen. Once an incident takes place, the ability to respond safely to the incident, to bring the system to a safe state and to resume operations as quickly as possible is crucial. In smart manufacturing systems, the consequences of the attack may extend beyond harm to an industrial process: people may be hurt and the environment or the plant damaged. When an attack takes place, response and recovery should ideally be immediate to mitigate potential losses including production, equipment and reputation. Naturally, this requires that resources to do this should be in place before the attack occurs and that there are appropriate policies and guidelines in place to allow the responsible individuals to operate rapidly and effectively. Regulations such as the North American Electric Reliability Corporation critical infrastructure protection (NERC CIP) [102] and Chemical Facility Anti-Terrorism Standards (CFATS) policy [103] require organisations to have incident management reporting and a response plan.

In practice, little is known about the security incident response and recovery capabilities of manufacturing systems operators, and still less for smart manufacturing operations. Thus, it is difficult to determine how well the organisations are prepared and responding to security incidents. One of the few studies carried out in this area [104] shows common incident management measures such as documentation, awareness and training, and response, are limited and poorly established within the industry. They also report that, despite the standards and guidelines, there are fundamental differences among operators on what constitutes a security incident.

There is already a vast amount of data available from ICS that could be used to identify not just the source of the attack and the motivations of the attackers but also to provide in-depth knowledge of what went wrong. That said, current data collection practices could be adapted to provide more focussed information that is useful in incident management and forensic analysis [105]; the more complex and adaptive the systems, the more data is required to understand how the system failed. Once data are collected about an incident, it is necessary to analyse the collected information and to document the findings. These are also not common practices for ICS operators [104], and the complexities of undertaking this for smart manufacturing systems have yet to be understood, let alone explored.

The threats facing manufacturing systems are critical and incidents, whether they are malicious or accidental, will take place at least occasionally. However, it would not be an understatement to say that the existing approach of manufacturing systems organisations to incident management is unsystematic and manual; incidents will be managed when they are noticed using whatever means happens to be available.

6. Future research directions

Throughout this paper we have argued that the issue of security in smart manufacturing is receiving too little attention relative to the issue of functionality. The risk in this is that we will deploy systems too early: they may be functional, but they could be highly vulnerable to attackers. Large scale deployments of vulnerable smart manufacturing systems on which the economic health of a country becomes dependent, let alone the emergence of smart critical national infrastructure on which the physical health of a country becomes dependent, should be a matter of national concern, rather than simply business decisions made by individual companies. We are missing fundamental research that would allow us to probe and evaluate the security of smart manufacturing systems. In our view, this includes:

Simulators and testbeds: A substantial impediment to the development of academic research in the field of security for smart manufacturing lies in the practical challenges of conducting that research. There are many more academics who would be interested in the security challenges of smart manufacturing than there are academics with access to testbeds or real plant on which to conduct experiments. As a consequence, much of the research that is relevant is instead conducted either in toy scenarios or on simulated systems. The Tennessee-Eastman chemical process, a real-world industrial chemical manufacturing

process, with available Matlab/Simulink code is one of the go-to simulator for security work in the field, and NIST have produced a cybersecurity performance testbed based on this model [106]. There has been a number of testbeds that have been proposed for industrial control systems research [107], however, most of these testbeds fail to accurately represent the real system under study. We are not aware of any testbeds for smart manufacturing that get close to representing reality. For example, it is not, at present, possible to understand the implications of information leakage using techniques such as that found in [32]. Until the tools that permit widespread experimentation are available, the pool of researchers in the area of security of smart manufacturing systems will necessarily be very small.

Attack generation and intrusion detection: Much existing security work is undertaken on the basis of traces of real attacks, or hand-crafted attacks of varying degrees of subtlety. For smart manufacturing systems there are no traces on which to test new intrusion detection systems; moreover, given the complexity of interactions within such a system, it is not clear that small numbers of traces are ever likely to allow the creation of intrusion detection systems that are sufficiently generic to protect against the panoply of threats. An alternative approach that we are currently researching is to use machine learning approaches to the generation of attacks, in order then to improve intrusion detection systems. When coupled with realistic simulations, this approach promises to allow the creation of intrusion detection systems that can both leverage information about real attacks and that constantly improve as the result of constant exercise by intelligent adversaries.

Forensics: In order to secure prosecutions, and in order to understand more fully the nature of previously unseen attacks, new approaches to forensics are needed. The extremely high dimensional information on which learning strategies are designed to operate, and the opaque nature of that learning, may make it hard to explain the form of a subtle attack that exploits the smart nature of smart manufacturing systems. Research is needed in this space, both to discourage potential attackers and to allow the sharing of information in a form that conveys the nature of the attack without revealing undue detail about the commercially sensitive nature of the underlying manufacturing processes. Again, credible simulators and testbeds will aid this process since the full ground truth can be revealed alongside the synoptic information.

Security policy specification and enforcement: Planning for security involves understanding the nature of threats, identifying vulnerabilities, quantifying the value to be lost if those vulnerabilities are exploited, and investing in security appropriately. The process of managing security is typically determined by a policy that captures both this high level strategic process and the restrictions that must be put in place to reduce the likelihood of breaches of security related to particular vulnerabilities, and the responses to actual breaches, both in real time and after the event. Much of this process is generic and as applicable to smart manufacturing as it is to the IT world; however, the detailed specification of what actions are allowed (or required) or not, under what circumstances, and by what agents is something that must be determined dynamically. In systems with behaviour as complex as those found in smart manufacturing, it is far from clear how such constraints should be expressed or policed, and under what circumstances they should be adapted. Moreover, there is no automated system that can currently articulate how the set of such constraints will (or may) alter system performance. Considerable work has been undertaken in this field in the IT world, but there is no settled consensus as to what form of system combines sufficient expressibility with enough ease of understanding that a human can with confidence predict the likely real-time effects of their constraints.

7. Conclusions

The common assumption in securing smart manufacturing systems – that the system at hand is isolated and access can only be achieved by those physically present inside a protected perimeter – is no longer true. The move to COTS technologies reduces the protection currently afforded by the implicit requirement for specialised knowledge in attacking manufacturing systems: there is a wealth of prior knowledge for attackers to draw upon. Finally, the move towards subsystems that create value through a mix of autonomous, adaptive, intelligent behaviour and real-time interactions increases complexity to the point where it becomes hard to reason about the expected behaviour of systems let alone their reaction to attack. This raises the potential to create undesirable emergent behaviours through small, hard-to-find, perturbations.

The potential consequences of security attacks on smart manufacturing systems cannot be overstated: injuries, death, and damage to physical infrastructure, equipment and environment is likely to occur simply because the actuators in manufacturing systems are intimately connected to such things. Industrial and manufacturing organisations need to consider these concerns and commit to making security a fundamental activity, bearing in mind the truism that security is a process not a product. While IT security is moving towards two factor authentication, prevention, detection and response models, manufacturing systems rely on limited security mechanisms such as shared short default passwords, rarely encrypted data, firewalls between various layers of the network infrastructure and the adoption of demilitarised zone architectures. Not only it is relatively easy to gain access, there is little to stop the attackers from modifying process parameters once they have access to critical systems or data.

At present, we are protected only by the difficulties inherent in the process of launching an attack on a specialised system, and the lack of recognition this is likely to bring within hacker communities as compared to the IT-based alternatives. Since those difficulties could evaporate much faster than our ability to counter attacks in smart, highly heterogeneous long-term-deployed systems with a variety of legacy components, it is time to establish ways of migrating best practice from the IT sphere to manufacturing systems, as well as to discover and neutralise specific avenues of attack against mart manufacturing in a proactive manner. Attackers are imaginative: the current defences are neither fit for purpose at present nor easily adaptable or extensible for the future. The complexity of the systems, a move towards increased autonomy, the shortage of manufacturing systems security experts, and the heavy reliance on vendors all impact the effective security of manufacturing systems. To develop effective security solutions, the research and industry communities need to work together and focus on efficient, robust, reliable, low-cost security solutions that can cope with the deployment and runtime requirements of the current and future manufacturing systems. Any system that fails to consider the human factors inherent in deployment and security management is ever likely to fail, just as they have failed in IT systems. It is essential that the adoption of IoT technology embeds security from the start, integrated with functionality, not as a secondary dimension that can be brought in later and retrofitted: this has never worked effectively, and it is unlikely to start working now. Finally, the systems managing the manufacturing of future will run and be maintained by future generations, and it is also crucial to start the process of educating the educators of the next generation of security experts and manufacturing control engineers.

Acknowledgements

This work was conducted under EPSRC Grant No: EP/G037264/1 as part of University College London's Security Science Doctoral Training Centre.

References

[1] Smart factories: how can manufacturers realize the potential of digital industrial revolution. 2017.
[2] Trade G. Invest, Industrie 4.0 smart manufacturing for the future. 2014http://

spectrum.ieee.org/telecom/internet/the-internet-of-fewer-things.
[3] Parliment E. Industry 4.0. 2016http://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf.
[4] Research H. China's 13th Five-Year Plan: made in China 2025 and Industrie 4.0 cooperative opportunities. 2016http://economists-pick-research.hktdc.com/business-news/article/Research-Articles/China-s-13th-Five-Year-Plan-Made-in-China-2025-and-Industrie-4-0-Cooperative-Opportunities/rp/en/1/1X32LK39/1X0A6AZ7.htm.
[5] Radvanovsky B, Brodsky J. Project SHINE (SHodan INtelligence Extraction), Findings Report. 2015.
[6] Internet Security Threat Report: Volume 21. 2016.
[7] Parliment E. Smart manufacturing. 2016https://ec.europa.eu/digital-single-market/smart-manufacturing.
[8] Commission E. The I4MS initiative (ICT Innovation for Manufacturing SMEs). 2017http://i4ms.eu/i4ms/i4ms_in_a_nutshell.php.
[9] Flechais I, Sasse MA, Hailes SMV. Bringing Security Home: a process for developing secure and usable systems. Proceedings of the 2003 workshop on New Security Paradigms, NSPW '03. 2003. p. 49–57. ISBN 1-58113-880-6.
[10] Mittal S, Khan MA, Romero D, Wuest T. Smart manufacturing: characteristics, technologies and enabling factors. Proc Inst Mech Eng Part B J Eng Manuf 2017;0(0). http://dx.doi.org/10.1177/0954405417736547.
[11] Tuptuk N, Hailes S. The cyberattack on Ukraine's power grid is a warning of what's to come. 2016https://theconversation.com/the-cyberattack-on-ukraines-power-grid-is-a-warning-of-whats-to-come-52832.
[12] Die Lage der IT-Sicherheit in Deutschland 2014. 2014.
[13] Havex Hunts for ICS/SCADA systems. 2014https://www.f-secure.com/weblog/archives/00002718.html.
[14] Dragonfly: cyber espinoage attacks against energy suppliers. 2014.
[15] W32.Stuxnet Dossier (Version 1.4), Tech. Rep. 2011.
[16] Roberts PF. Zotob, PnP Worms Slam 13 DaimlerChrysler Plants. 2005http://www.eweek.com/c/a/Security/Zotob-PnP-Worms-Slam-13-DaimlerChrysler-Plants.
[17] W32.Zotob.E. 2007http://www.symantec.com/security_response/writeup.jsp?docid=2005-081615-4443-99.
[18] Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, et al. Understanding the Mirai Botnet. 26th USENIX Security Symposium (USENIX Security 17). Vancouver, BC: USENIX Association; 2017. p. 1093–110. ISBN 978-1-931971-40-9, https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.
[19] Breaking Down Mirai: an IoT DDoS Botnet analysis. 2016https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.
[20] Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other Botnets. Computer 2017;50(7):80–4. http://dx.doi.org/10.1109/MC.2017.201. ISSN 0018-9162.
[21] Beek C. Satori Botnet turns IoT devices into Zombies by borrowing code from Mirai. 2018https://securingtomorrow.mcafee.com/business/satori-botnet-turns-iot-devices-zombies-borrowing-code-mirai.
[22] Avizienis A, Laprie J-C, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. IEEE Trans Dependable Secur Comput 2004;1(1):11–33. http://dx.doi.org/10.1109/TDSC.2004.2. ISSN 1545-5971.
[23] NCCIC/ICS-CERT FY Annual Vulnerability Coordination Report, Tech. Rep., Department of Homeland Security, National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team. 2015.
[24] Smarter Security for Manufacturing in the Industry 4.0 Era, Tech. Rep. 2017.
[25] Viega J, McGraw G. Building secure software: how to avoid security problems the right way. Addison Wesley; 2006. ISBN 978-0321425232.
[26] Fovino I, Carcano A, De Lacheze Murel T, Trombetta A, Masera M. Modbus/DNP3 state-based intrusion detection system. 2010 24th IEEE international conference on advanced information networking and applications (AINA) 2010:729–36.
[27] HACKMAGEDDON: information security timelines and statistics. 2016http://www.hackmageddon.com/.
[28] Burton G. BrickerBot: Mirai-like Malware threatens to brick insecure IoT devices. 2017https://www:theinquirer:net/inquirer/news/3008037/brickerbot-mirai-like-malware-threatens-to-brick-insecure-iot-devices.
[29] Page C. A new IoT Botnet storm is coming. 2017https://research.checkpoint.com/new-iot-botnet-storm-coming/.
[30] Korkmaz E, Davis M, Dolgikh A, Skormin V. Detection and mitigation of time delay injection attacks on industrial control systems with PLCs. In: Rak J, Bay J, Kotenko I, Popyack L, Skormin V, Szczypiorski K, editors. Computer network security. Cham: Springer International Publishing; 2017. p. 62–74. ISBN 978-3-319-65127-9.
[31] Wang JK, Peng C. Analysis of time delay attacks against power grid stability. Proceedings of the 2nd workshop on cyber-physical security and resilience in smart grids, CPSR-SG'17. New York, NY, USA: ACM.; 2017. p. 67–72. http://dx.doi.org/10.1145/3055386.3055392. ISBN 978-1-4503-4978-9.
[32] Tuptuk N, Hailes S. Covert channel attacks in pervasive computing. 2015 IEEE international conference on pervasive computing and communications (PerCom) 2015:236–42. http://dx.doi.org/10.1109/PERCOM.2015.7146534.
[33] Bilge L, Dumitras T. Before we knew it: an empirical study of zero-day attacks in the real world. Proceedings of the 2012 ACM conference on computer and communications security, CCS '12. New York, NY, USA: ACM; 2012. p. 833–44. http://dx.doi.org/10.1145/2382196.2382284. ISBN 978-1-4503-1651-4.
[34] Kuehn A, Mueller M. Shifts in the cybersecurity paradigm: zero-day exploits, discourse, and emerging institutions. Proceedings of the 2014 workshop on new security paradigms workshop, NSPW '14. New York, NY, USA: ACM; 2014. p. 63–8. http://dx.doi.org/10.1145/2683467.2683473. ISBN 978-1-4503-3062-6.
[35] Barreno M, Nelson B, Joseph AD, Tygar JD. The security of machine learning. Mach Learn 2010;81(2):121–48. http://dx.doi.org/10.1007/s10994-010-5188-5. ISSN 0885-6125.
[36] Grosse K, Papernot N, Manoharan P, Backes M, McDaniel PD. Adversarial perturbations against deep neural networks for Malware classification. 2016. CoRR abs/1606.04435, http://arxiv.org/abs/1606.04435.
[37] Biggio B, Fumera G, Roli F. Security evaluation of pattern classifiers under attack. IEEE Trans Knowl Data Eng 2014;26(4):984–96. http://dx.doi.org/10.1109/TKDE.2013.57. ISSN 1041-4347.
[38] Laskov P, Lippmann R. Machine learning in adversarial environments. Mach Learn 2010;81(2):115–9. http://dx.doi.org/10.1007/s10994-010-5207-6. ISSN 1573-0565.
[39] Biggio B, Fumera G, Russu P, Didaci L, Roli F. Adversarial biometric recognition: a review on biometric system security from the adversarial machine-learning perspective. IEEE Signal Process Mag 2015;32(5):31–41. http://dx.doi.org/10.1109/MSP.2015.2426728. ISSN 1053-5888.
[40] Papernot N, McDaniel P, Sinha A, Wellman M. Towards the science of security and privacy in machine learning. 2016. ArXiv e-prints.
[41] Papernot N, McDaniel PD, Goodfellow IJ, Jha S, Celik ZB, Swami A. Practical Black-Box Attacks against Deep Learning Systems using Adversarial Examples. 2016. CoRR abs/1602.02697, http://arxiv.org/abs/1602.02697.
[42] Joy J, John A, Joy J. Advances in parallel distributed computing. Nagamalai D, Renault E, Dhanuskodi M, editors. Communications in computer and information science, vol. 203. Springer Berlin Heidelberg; 2011. p. 366–74.
[43] Josse S. Rootkit detection from outside the Matrix. J Comput Virol 2007;3(2):113–23. ISSN 1772-9890.
[44] Bianchi A, Shoshitaishvili Y, Kruegel C, Vigna G. Blacksheep: detecting compromised hosts in homogeneous crowds. Proceedings of the 2012 ACM conference on computer and communications security, CCS '12. New York, NY, USA: ACM; 2012. p. 341–52. ISBN 978-1-4503-1651-4.
[45] Golovanov S. TDSS loader now got legs. 2011http://securelist:com/blog/events/30844/tdss-loader-now-got-legs/.
[46] Internet Security Threat Report: 2011 Trends Volume 17, Tech. Rep. 2010.
[47] Guardian Russian cyber-attacks could influence German election, says Merkel. 2016https://www:theguardian:com/world/2016/nov/08/russian-cyber-attacks-could-influence-german-election-says-merkel.
[48] Zetter K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. 2016https://www:wired:com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
[49] An Special Report: Ransomware and Businesses 2016, Tech. Rep. 2016.
[50] Alex H, Samuel G. What is WannaCry ransomware and why is it attacking global computers? 2017https://www:theguardian:com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20.
[51] M. Joyce (Ed.), Idebate Press, 2010.
[52] Hackers Shut Down a Tunnel Road in Israel. 2013http://cryptome:org/2013/05/sea-haifa-hack:htm.
[53] 2014 US State of Cybercrime Survey. CSO Magazine; 2014.
[54] Jill JS, Miller M. Lessons learned from the Maroochy Water Breach. Goetz E, Shenoi S, editors. Critical infrastructure protection, vol. 253. US: Springer; 2008. p. 73–82.
[55] Keeney M, Kowalski E, Cappelli D, Moore A, Shimeall T, Rogers S. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, Tech. Rep. 2005.
[56] ISA99: Developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS). 2017http://isa99.isa.org/ISA9920Wiki/Home.aspx/.
[57] ISA99: Developing the Vital ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security. 2001http://isa99.isa.org/.
[58] ISO/IEC TR 27019:2013: Information technology – security techniques – information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. 2013https://www.iso.org/standard/43759.html.
[59] ISO/IEC 27019 Information technology – security techniques – information security controls for the energy utility industry. 2017https://www.iso.org/standard/68091.html.
[60] ISO/IEC 27033-1:2015 Preview Information technology-Security techniques – Network security – Part 1: Overview and concepts. 2015https://www.iso.org/standard/63461.html.
[61] ISO/IEC 29180: 2012 Information technology – Telecommunications and information exchange between systems – Security framework forubiquitous sensor networks. 2012https://www.iso.org/standard/45259.html.
[62] Functional safety and IEC 61508. 2010http://www.iec.ch/functionalsafety/.
[63] IEC 61784-1:2014: Industrial communication networks – Profiles – Part 1: Fieldbus profiles. 2014https://webstore.iec.ch/publication/5878.
[64] ISO/IEC 27000 family – Information security management systems. 2014https://webstore.iec.ch/publication/5878.
[65] Anderson R, Fuloria S. Security economics and critical national infrastructure. In: Moore T, Pym D, Ioannidis C, editors. Economics of information security and privacy. Springer US; 2010. p. 55–66.
[66] Is NERC CIP compliance a game? 2008http://www:controlglobal:com/blogs/unfettered/electric-power-2008-is-nerc-cip-compliance-a-game.
[67] Stouffer K, Lightman S, Pillitteri V, Abrams M, Hahn A. Guide to Industrial Control Systems (ICS) Security, Tech. Rep. AGaithersburg, MD, USA: National Institute of Standards and Technology; 2014.
[68] Catalog of Control Systems Security: Recommendations for Standards Developers. 2011.

[69] Control Systems Cyber Security: Defense in Depth Strategies. 2009.
[70] Cyber Security Assessments of Industrial Control Systems. Good Practice Guide; 2011.
[71] Securing the move to IP-based SCADA/PLC networks. 2011.
[72] Piètre-Cambacédès L, Sitbon P. Cryptographic key management for SCADA systems-issues and perspectives. Proceedings of the 2008 international conference on information security assurance (ISA 2008), ISA '08. Washington, DC, USA: IEEE Computer Society; 2008. p. 156–61. http://dx.doi.org/10.1109/IS.A.2008.77. ISBN 978-0-7695-3126-7.
[73] Choi D, Lee S, Won D, Kim S. Efficient secure group communications for SCADA. IEEE Trans Power Deliv 2010;25(2):714–22. http://dx.doi.org/10.1109/TPWRD.2009.2036181. ISSN 0885-8977.
[74] Choi D, Kim H, Won D, Kim S. Advanced key-management architecture for secure SCADA communications. IEEE Trans Power Deliv 2009;24(3):1154–63. http://dx.doi.org/10.1109/TPWRD.2008.2005683. ISSN 0885-8977.
[75] Pal O, Saiwan S, Jain P, Saquib Z, Patel D. Cryptographic key management for SCADA system: an architectural framework. 2009 International conference on advances in computing, control, and telecommunication technologies 2009:169–74. http://dx.doi.org/10.1109/ACT.2009.51.
[76] Jiang R, Lu R, Lai C, Luo J, Shen X. Robust group key management with revocation and collusion resistance for SCADA in smart grid. 2013 IEEE global communications conference (GLOBECOM) 2013:802–7. http://dx.doi.org/10.1109/GLOCOM.2013.6831171. ISSN 1930-529X.
[77] Cheung S, Dutertre B, Fong M, Lindqvist U, Skinner K, Valdes A. Using model-based intrusion detection for SCADA networks. Proceedings of the SCADA security scientific symposium. 2007.
[78] Yang D, Usynin A, Hines JW. Anomaly-based intrusion detection for SCADA systems. La Grange Park (United States): American Nuclear Society – ANS; 2006.
[79] Oman P, Phillips M. Intrusion detection and event monitoring in SCADA networks. In: Goetz E, Shenoi S, editors. Critical Infrastructure Protection, vol. 253 of IFIP International Federation for Information Processing. Springer US; 2008. p. 161–73. ISBN 978-0-387-75461-1.
[80] Roosta T, Nilsson DK, Lindqvist U, Valdes A. An intrusion detection system for wireless process control systems. 2008 5th IEEE international conference on mobile ad hoc and sensor systems 2008:866–72. http://dx.doi.org/10.1109/MAHS.S.2008.4660125. ISSN 2155-6806.
[81] Düssel P, Gehl C, Laskov P, Bußer J-U, Störmann C, Kästner J. Cyber-critical infrastructure protection using real-time payload-based anomaly detection. Proceedings of the 4th international conference on critical information infrastructures security, CRITIS'09. Berlin, Heidelberg: Springer-Verlag; 2010. p. 85–97. ISBN 3-642-14378-4, 978-3-642-14378-6.
[82] Carcano A, Coletta A, Guglielmi M, Masera M, Fovino IN, Trombetta A. A multidimensional critical state analysis for detecting intrusions in SCADA systems. IEEE Trans Ind Inform 2011;7(2):179–86. http://dx.doi.org/10.1109/TII.2010.2099234. ISSN 1551-3203.
[83] Hadziosmanovic D, Simionato L, Bolzoni D, Zambon E, Etalle S. N-Gram against the Machine: On the Feasibility of the N-Gram Network Analysis for Binary Protocols. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012. p. 354–73.
[84] Reeves J, Ramaswamy A, Locasto M, Bratus S, Smith S. Intrusion detection for resource-constrained embedded control systems in the power grid. Int J Crit Infrastruct Prot 2012;5(2):74–83. http://dx.doi.org/10.1016/j.ijcip.2012.02.002. ISSN 1874-5482.
[85] Tsang C-H, Kwong S. Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. 2005 IEEE international conference on industrial technology 2005:51–6. http://dx.doi.org/10.1109/ICIT.2005.1600609.
[86] Paul A, Schuster F, König H. Towards the protection of industrial control systems: conclusions of a vulnerability analysis of Profinet IO. Proceedings of the 10th international conference on detection of intrusions and Malware, and vulnerability assessment, DIMVA'13. Berlin, Heidelberg: Springer-Verlag; 2013. p. 160–76. ISBN 978-3-642-39234-4.
[87] Shin S, Kwon T, Jo GY, Park Y, Rhy H. An experimental study of hierarchical intrusion detection for wireless industrial sensor networks. IEEE Trans Ind Inform 2010;6(4):744–57. http://dx.doi.org/10.1109/TII.2010.2051556. ISSN 1551-3203.
[88] Pan S, Morris T, Adhikari U. Developing a hybrid intrusion detection system using data mining for power systems. IEEE Trans Smart Grid 2015;6(6):3104–13. http://dx.doi.org/10.1109/TSG.2015.2409775. ISSN 1949-3053.
[89] Zhang Y, Wang L, Sun W, Alam M. Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Trans Smart Grid 2011;2(4):796–808. http://dx.doi.org/10.1109/TSG.2011.2159818. ISSN 1949-3053.
[90] Linda O, Vollmer T, Manic M. Neural network based intrusion detection system for critical infrastructures. Proceedings of the 2009 international joint conference on neural networks, IJCNN'09. Piscataway, NJ, USA: IEEE Press; 2009. p. 102–9. ISBN 978-1-4244-3549-4, http://dl:acm:org/citation:cfm?id=1704175:1704190.
[91] Kiss I, Genge B, Haller P. A clustering-based approach to detect cyber attacks in process control systems. 2015 IEEE 13th international conference on industrial informatics (INDIN) 2015:142–8. http://dx.doi.org/10.1109/INDIN.2015.7281725. ISSN 1935-4576.
[92] Caselli M, Zambon E, Kargl F. Sequence-aware intrusion detection in industrial control systems. Proceedings of the 1st ACM workshop on cyber-physical system security, CPSS '15. New York, NY, USA: ACM; 2015. p. 13–24. http://dx.doi.org/10.1145/2732198.2732200. ISBN 978-1-4503-3448-8.
[93] Premaratne UK, Samarabandu J, Sidhu TS, Beresh R, Tan JC. An intrusion detection system for IEC61850 automated substations. IEEE Trans Power Deliv 2010;25(4):2376–83. http://dx.doi.org/10.1109/TPWRD.2010.2050076. ISSN 0885-8977.
[94] Kim B-K, Kang D-H, Na J-C, Chung T-M. Detecting abnormal behavior in SCADA networks using normal traffic pattern learning. In: Park JJJH, Stojmenovic I, Jeong HY, Yi G, editors. Computer science and its applications: ubiquitous information technologies Berlin, Heidelberg: Springer Berlin Heidelberg; 2015. p. 121–6. http://dx.doi.org/10.1007/978-3-662-45402-2_18. ISBN 978-3-662-45402-2.
[95] Jardine W, Frey S, Green B, Rashid A. SENAMI: selective non-invasive active monitoring for ICS intrusion detection. Proceedings of the 2nd ACM workshop on cyber-physical systems security and privacy, CPS-SPC '16. New York, NY, USA: ACM; 2016. p. 23–34. http://dx.doi.org/10.1145/2994487.2994496. ISBN 978-1-4503-4568-2.
[96] Ghaeini HR, Tippenhauer NO. HAMIDS: hierarchical monitoring intrusion detection system for industrial control systems. Proceedings of the 2nd ACM workshop on cyber-physical systems security and privacy, CPS-SPC '16. New York, NY, USA: ACM; 2016. p. 103–11. http://dx.doi.org/10.1145/2994487.2994492. ISBN 978-1-4503-4568-2.
[97] Mrugala K, Tuptuk N, Hailes S. Evolving attackers against wireless sensor networks using genetic programming. IET Wirel Sens Syst 2017;7(4):113–22. http://dx.doi.org/10.1049/iet-wss.2016.0090.
[98] Mrugala K, Tuptuk N, Hailes S. Evolving attackers against wireless sensor networks. Genetic and Evolutionary Computation Conference, GECCO 2016, Denver, CO, USA 2016. p. 107–8. http://dx.doi.org/10.1145/2908961.2908974.
[99] Beautement A, Sasse MA, Wonham M. The compliance budget: managing security behaviour in organisations. Proceedings of the 2008 workshop on new security paradigms, NSPW '08. New York, NY, USA: ACM; 2008. p. 47–58. http://dx.doi.org/10.1145/1595676.1595684. ISBN 978-1-60558-341-9.
[100] Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur J Inf Syst 2009;18(2):106–25. http://dx.doi.org/10.1057/ejis.2009.6. ISSN 1476-9344.
[101] White Paper: Protecting your organisation from itself, Tech. Rep. 2016.
[102] CIP008-5 Cyber Security – Incident Reporting and Response Planning. 2016http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-008-5.
[103] USC Chapter 1, Subchapter XVI: Chemical Facility Anti-Terrorism Standards. 2014http://uscode.house.gov/view.xhtml?path=/prelim@title6/chapter1/subchapter16&edition=prelim.
[104] Line M, Tondel I, Jaatun M. Information Security Incident Management: Planning for Failure. IT Security Incident Management IT Forensics (IMF), 2014 Eighth International Conference on 2014:47–61. http://dx.doi.org/10.1109/IMF.2014.10.
[105] Spyridopoulos T, Tryfonas T, May J. Incident analysis amp; digital forensics in SCADA and industrial control systems. 8th IET International System Safety Conference incorporating the Cyber Security Conference 2013 2013:1–6. http://dx.doi.org/10.1049/cp.2013.1720.
[106] Candell R, Zimmerman T, Stouffer K. NISTIR 8089: An Industrial Control System Cybersecurity Performance Testbed. 2015http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.
[107] Holm H, Karresand M, Vidström A, Westring E. A Survey of Industrial Control System Testbeds. In: Buchegger S, Dam M, editors. Secure IT Systems. Cham: Springer International Publishing; 2015. p. 11–26. ISBN 978-3-319-26502-5.