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

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

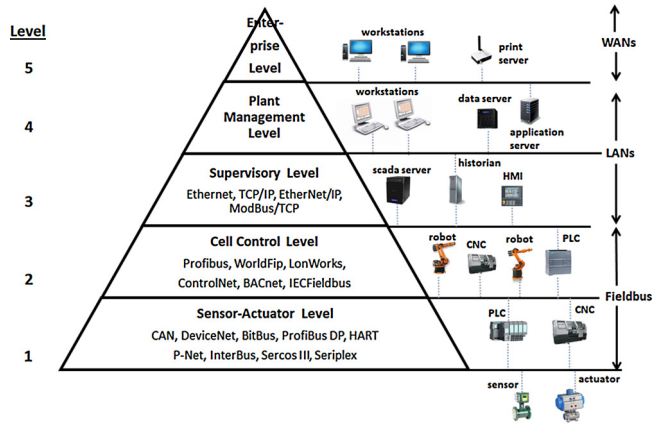

Fig. 1. Computer-integrated manufacturing (CIM) model.

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