Industry 4.0 Manufacturing Systems

Subjects: Engineering, Industrial

Contributor: Jaco Prinsloo

Manufacturing systems are generally “physical” systems in a physical world. The internet is a cyber-world. The internet has allowed for global connectedness. At the same time, infused with this connectedness, is a “dark web.” The dark web constitutes malware, viruses, “ransomware-as-a-service,” and other divisive instruments. Industry 4.0 brings together in the form of “cyber-physical” systems a new range of opportunities for additive manufacturing. While the opportunity of connectedness maps, at the same time, the challenges of the “dark web” also maps into this world of manufacturing. On a growing basis, measures to improve cybersecurity continue to develop. These measures include the lever of machine and deep learning. In this entry, the authors use engineering control systems and other relevant theories, including augmented artificial intelligence, as a way of making more secure cyber-physical systems and thereby making practical the considerations for Industry 4.0.

Industry 4.0 WEF Cybersecurity Dark Web

The migration from conventional industrial manufacturing to manufacturing in Industry 4.0 contains a complete paradigm shift in the way that process control flow and the associated security measures are approached. To understand why this is indeed such a big paradigm shift, it is necessary first to look at how process control flow and the associated security measures are implemented in the conventional/traditional sense, i.e., before Industry 4.0. Thereafter, we briefly consider the increasing trend of bridging two similar technological platforms that are designed for entirely different applications, along with a unique style of collaboration that is becoming the new norm within industries. Finally, a broad definition for the term “Industry 4.0” can be formulated and brought into context with the observed technological trends of today. Once the concept of Industry 4.0 is introduced, the associated risks involved within this paradigm shift can be identified and explored, particularly in terms of informational and cybersecurity.

1. Traditional Approach to Manufacturing Process Security

The typical manufacturing plant infrastructure consists of two main technological platforms, namely operational technology (OT) and information technology (IT) [1]. OT refers to the combination of hardware and software used to monitor plant processes by means of, e.g., sensors and feedback data-streams from plant machinery, in order to control these processes by components such as pumps, valves and actuators. Typical examples of equipment that forms part of OT are supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLC), measuring equipment and human-machine interfaces. Combinations of these platforms are used to ensure that plant operations run as intended by design, and to prevent hazardous conditions through processes that operate outside the process limitations and safety margins. Figure 1 illustrates the basic concept of the interconnectivity of OT in the typical manufacturing plant:

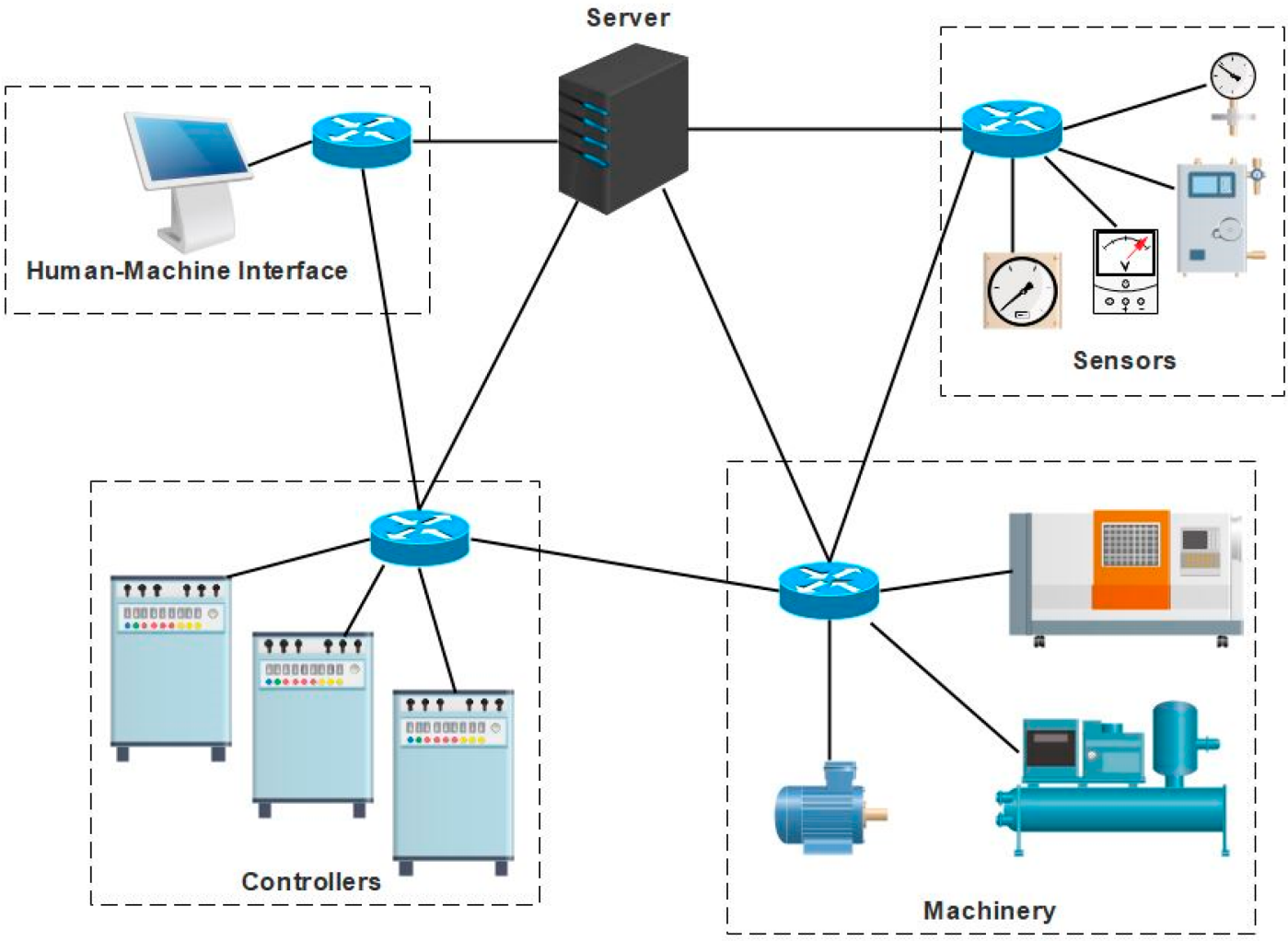

Figure 1. A typical operational technology (OT) industrial systems network architecture.

It can be seen from Figure 1 that OT platforms are typically connected to a central authority that monitors and controls the manufacturing processes. This can be in the form of multiple PLCs and SCADA systems that receive data from sensors and make adjustments to the manufacturing process by means of controlling valves, pumps and actuators, based on the data received from the sensors. Furthermore, many processes rely upon human interaction, ranging from changing equipment settings to manually changing the states of systems through mechanical switches. These actions are to be performed by plant technicians and engineers who are skilled and knowledgeable in the manufacturing processes, and have exclusive access to the associated hardware and software platforms. This immediately points out one of the key vulnerabilities in OT systems security, since the state of the OT systems security is highly dependent on the trustworthiness of the plant technicians and engineers. A significant amount of trust is put into these plant personnel to perform the right manipulations to the OT systems and to perform their activities without any malicious motives at all times.

The significance of plant technicians' and engineers' trustworthiness can be appreciated by considering the Maroochy Shire sewage spill incident that occurred in Queensland, Australia in the year 2000 [2]. This incident was allegedly the result of the behavior of a disgruntled contractor whose malicious actions allegedly resulted in

the spillage of nearly 1 megaliter of raw sewage into a nearby river. The spill stretched out up to nearly 12 km away from its source. An investigation into the incident revealed that a number of SCADA systems that controlled over 140 sewage pumping stations had been hacked and controlled by means of inducing faults in the SCADA systems through compromised control messages. Communication between the central control center and the pumping stations was facilitated by means of a private two-way radio communication system that operated through a number of repeater stations, as illustrated in Figure 2 below. Because of a lack of proper access control and cyber-security measures of the sewage plant's control systems, it was possible for the ex-employee to easily obtain access to the control systems' network of the plant, particularly given the fact that he had in-depth knowledge of the architecture of the network.

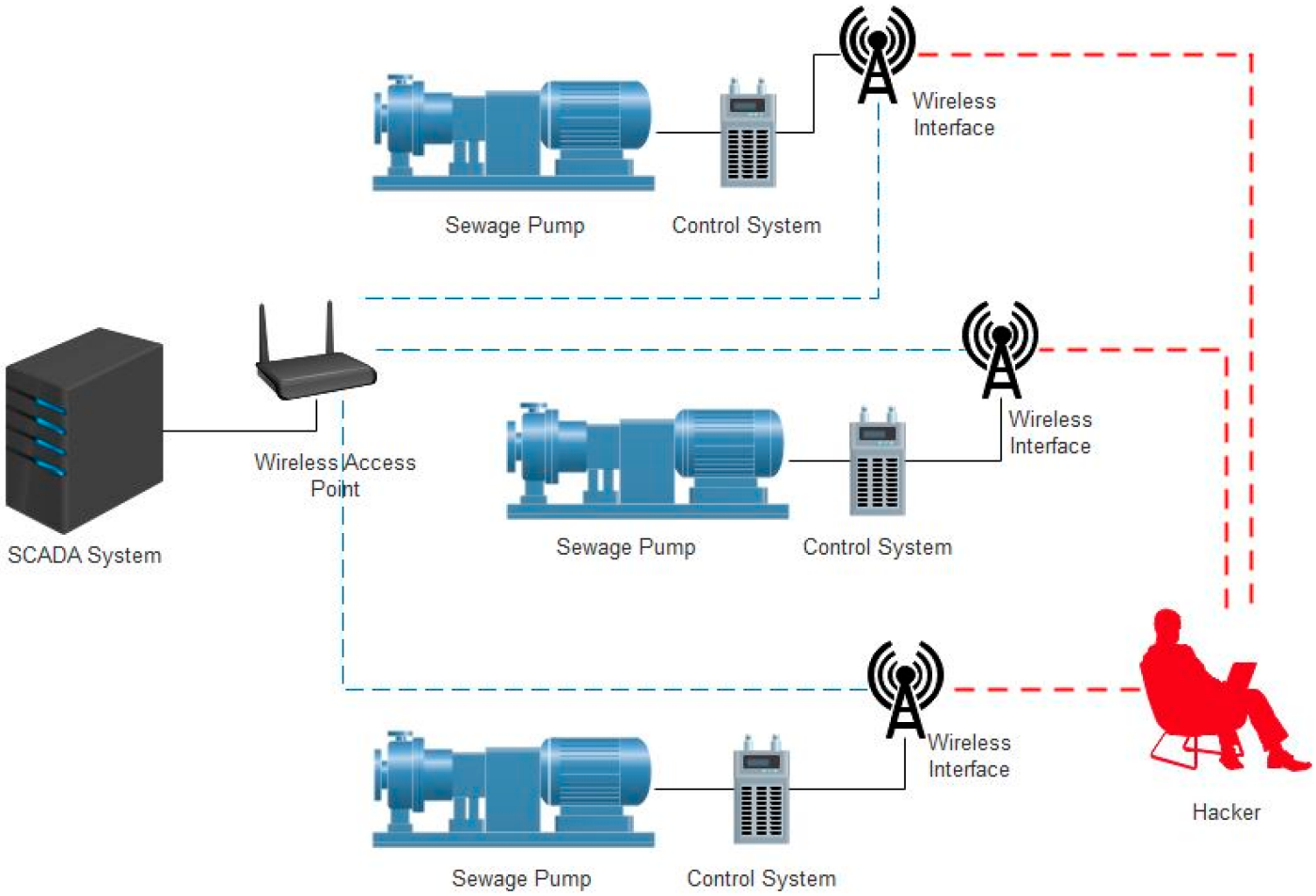

Figure 2. Illustration of the OT network at the Maroochy Shire sewage plant. SCADA: supervisory control and data acquisition

The Maroochy Shire sewage spill is a classic example of a security breach within a SCADA system. Historical data of industrial control system (ICS) incidents indicate that such incidents already started occurring as early as 1982 [1]. However, after the introduction of SCADA systems that communicate via transmission control protocol/Internet protocol (TCP/IP) in the early 2000s, the number of ICS incidents increased dramatically. Although numerous well-established security measures for TCP/IP communications are available today, such security measures were still in

their infancy (if existent at all) when TCP/IP-compatible SCADA systems were introduced. However, these security measures are mostly applicable to IT systems networks, and are generally not compatible with OT systems networks—a topic that is discussed in more detail in Section 2.2. Such a lack of well-established security measures is more than enough of a vulnerability in process control security to allow any person with sufficient knowledge of the process control architecture to gain unauthorized access to the control network and to induce changes in the process control settings that are driven with malicious intent. This fact highlights another important security vulnerability of traditional OT systems, namely that control networks have little or no security that can protect the networks from unauthorized access.

One of the general causes of these types of security vulnerabilities of traditional OT systems is a direct result of the technological platforms around which they are designed. For example, although many of the “intelligent” OT systems make use of embedded microcontroller platforms, these platforms generally do not possess the computational capacity required to implement proper security measures. Furthermore, these embedded platforms typically use standard (and somewhat primitive) peripherals such as RS-232, inter-integrated circuit or serial peripheral interface to communicate with each other. Although some of the protocols used between OT systems are typically proprietary, the simple nature of the communication peripherals makes them relatively easy to intercept [1].

Besides OT platforms in general, many manufacturing plants also contain a network of IT equipment that typically includes devices such as computers, printers, servers and routers. This type of equipment usually possesses a much higher computing capacity, so that advanced security measures can be implemented, such as antivirus software and firewalls.

Information and data security in IT systems is characterized by three key aspects: confidentiality, integrity and availability (CIA) [1,3]. These are known as the three CIA pillars of information and data security. Information of a confidential nature should be protected from parties that are unauthorized to view it. This may be, for example, in the form of documentation that contains sensitive information that could cause harm to a company should it be leaked into the wrong hands. The integrity of information is a very important aspect that concerns the validity of the data. Should information be maliciously manipulated without detection, it could be difficult to determine whether or not the information is actually legitimate. When information loses its integrity, it can hide important detail that, if not interpreted as it should be, could have detrimental consequences in a production environment. An example of such a case would be data containing the safety parameters of an industrial plant’s processes that are manipulated, in order to represent a false indication of the actual states of the processes to which control systems could erroneously react. Of course, no data would be useful without being available to the parties that need the data. Therefore, data should always be available to the intended parties without landing in the hands of unauthorized individuals. It can thus be intuitively deduced that an effective IT security system requires a fine balance between these three key aspects (confidentiality, integrity and availability), which can very easily be in conflict with one another if not properly implemented.

2. Convergence of IT and OT

The introduction of low-cost devices that have Internet connectivity capability brought about a rapid evolution of a new type of low-cost technology that offers endless application possibilities while presenting the ability to be controlled over the Internet. This new movement of interconnecting devices over the Internet is known as the Internet of Things (IoT). Typical examples of such IoT devices are office printers and home appliances that have Wi-Fi capability, and smart watches that connect to the Internet to log data of people's daily movements and activities.

As IoT technology became a well-established field, the scope of applications started expanding into the industrial sector. With an increasing number of industrial devices that started to use the IP for communication, these devices started to enter the IT network domain. This made it possible for OT equipment to be connected to an IT network router or switch and be controlled over the Internet. The new approach of connecting OT equipment to the Internet gave rise to an extension of the IoT called the Industrial Internet of Things (IIoT).

In the previous section the three CIA pillars of information and data security have been introduced. Introducing OT equipment to the IT domain means extending these IT security aspects to the OT domain as well. However, it is immediately apparent that the platforms upon which these three security aspects have to be implemented are very different from one another. IT equipment is typically in the form of high-performance computers and servers that have a huge amount of computing capability compared to more low-level OT embedded devices. Consequently, the security measures implemented on IT equipment are not easily transferable to OT equipment in general, if at all in some cases [1]. This results in OT systems that are connected to the Internet without proper security measures in place, leaving these systems open to hacking and being maliciously controlled.

Several attempts have been made in the past to merge IT security measures with OT systems, but the results showed that this can often lead to an OT system malfunction, with devastating consequences. Such an example is the incident when the United States' National Aeronautics and Space Administration (NASA) explored the introduction of IT security measures to the OT systems in their critical and supporting infrastructure [4]. One of NASA's large-scale engineering temperature chambers, that uses an OT system to monitor and regulate the temperature inside the chamber malfunctioned when the computer connected to it required a reboot after a security patch was installed. After the computer rebooted, the temperature chamber's control system stopped working, causing the temperature to rise steadily until it caused a fire inside the chamber that completely destroyed spacecraft hardware that was undergoing tests. In addition to the control system malfunction, the alarm mechanism of the temperature chamber also malfunctioned, resulting in the fire only being detected hours later by one of the employees.

The NASA example of what could happen when OT systems fail owing to incompatible IT security measures illustrates the devastating consequences this could have for any industry where such security measures are applied. This highlights what is arguably the greatest challenge that is presented by converging IT and OT—how to implement proper security measures that are 100% compatible with both IT and OT systems, without the disruption of any underlying processes. A deeper look into the nature of this challenge reveals that one of the underlying differences between IT and OT systems is the way in which the systems communicate with one another.

IT devices generally act as either servers or clients, with a one-way control authority between servers and clients that makes use of protocols such as the hypertext transport protocol (HTTP) [1,3]. Conversely, OT devices commonly act as both servers and clients, depending on various parameters within the larger-scale system of which they form a part. For example, HTTP works well with networks using a one-way control authority between devices, but is not designed for the unique nature of the control authority of which OT system networks make use. Although it is possible to implement HTTP in OT system networks, it involves adapting its use to work in applications for which it is not specifically designed, which presents its own unique set of challenges. Several new protocols have been designed to address this particular issue. One example is the new International Organization for Standardization (ISO) protocol named message queuing telemetry transport that makes use of a publish-subscribe mechanism, specifically designed to address the network communications issue between IT and OT systems. Other such protocols are the extensible messaging and presence protocol, advanced messaging queuing protocol and data distribution service [1,3].

3. Cloud-Based Design

The advent of the Internet has had a huge impact on how engineering teams collaborate. The traditional “in-house” design approach is rapidly being replaced by a new approach where engineers and technical personnel collaborate from all walks of life all around the world. In an era where optimization and efficiency are keywords for all types of businesses, especially for engineering design and manufacturing entities, it is increasingly becoming the norm for businesses to outsource certain tasks. Global collaboration between technical teams leads to more innovative solutions to technical problems. Because of the distances that sometimes separate these technical teams, it is often impractical for such teams to regularly meet and share information in person at a particular location. Therefore, new and innovative ways need to be used to share information effectively and to collaborate.

Many businesses are migrating to newer business models that make use of global mass collaboration. In other words, certain tasks that require the skills of a specialist in a particular field are rather outsourced to such specialists, instead of hiring an in-house specialist. Online sharing platforms such as GitHub and DropBox offer the ability to easily share information associated with certain tasks [1,3]. In fact, it is becoming the norm for engineers and developers to use such platforms to host and share entire projects with team members from around the world over the Internet. Such a methodology to engineering design offers a number of advantages. For example, a project can be worked on around the clock by design teams that are located in different time zones across the world. A 24-h period in a project’s timeframe can essentially undergo three 8-h working days’ worth of design effort, essentially tripling the output per time unit available to the project. Figure 3 below illustrates this concept.

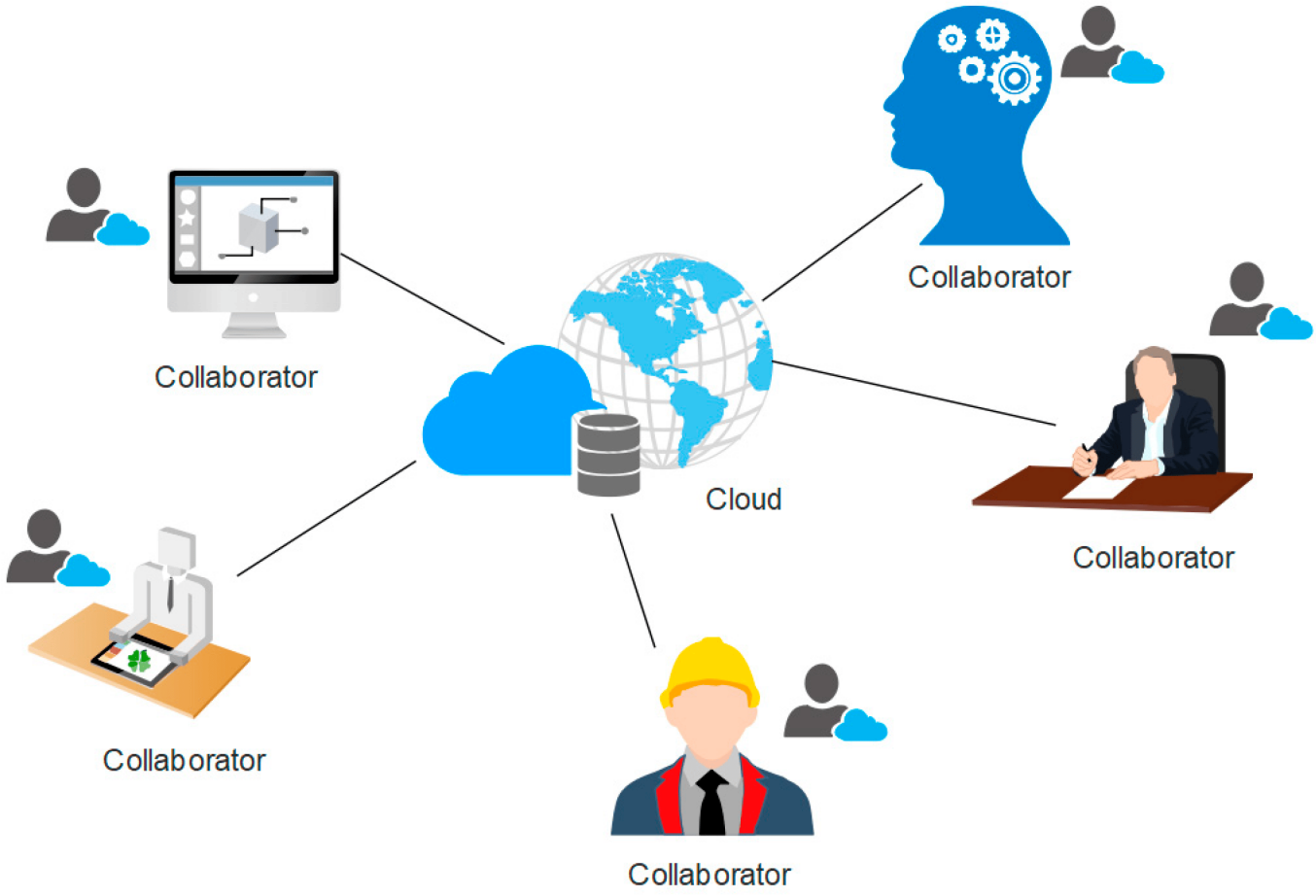

Figure 3. Global collaboration on a project.

Although the concept of global collaboration between engineering teams offers distinct advantages over traditional engineering design approaches, a few key issues are also faced that very quickly apply brakes to the momentum of such a paradigm shift. One of the key issues in this regard is the protection of intellectual property. The moment that confidential design information leaves the proverbial borders of a business, additional measures need to be implemented to ensure the security and confidentiality of such information. The repercussions of inadequate security measures leading to a leak of confidential information cannot be overstressed.

Should an unsuspecting business fall prey to a seasoned hacker that exploits security weaknesses in an online collaboration platform that is not properly designed around sound security measures, the consequences could be life-threatening. For example, the design of life support medical equipment can be altered in such a way that it would not function correctly or even fail when in use. In fact, outsourcing manufacturing tasks to third parties exposes businesses to similar threats that are well-known in the integrated circuit manufacturing industry. A particular example of such threats is where logic gates are designed that do not entirely conform to specification, owing to obfuscation and lack of complete design details that could contain critically important design information [5].

Another example is the design of an aircraft propeller blade in which weaknesses can be maliciously introduced into the structural design, leading to possible catastrophic failure during flight, and thus endangering the lives of all the passengers on board the aircraft. This has particularly been a growing concern since 3D printed fuel nozzles newly developed by General Electric (GE) Aviation for use in jet engines received a US Federal Aviation Administration (FAA) certification. In fact, the next-generation Leading Edge Aviation Propulsion (LEAP) jet engine developed by CFM International, which contains 19 of these 3D printed fuel nozzles, has already undergone several flight tests. Such 3D printed fuel nozzles are also being developed by GE Aviation for the huge new GE9X jet engine [6]. The fact that companies such as GE Aviation are already making use of 3D printing to manufacture aircraft parts is concrete testimony to the sheer disruptive possibilities that 3D printing can offer, but also stresses the urgency of developing the required cyber-security measures in the industrial manufacturing sector.

However, in a combined effort by researchers of the Ben-Gurion University of the Negev, the University of South Alabama and the Singapore University of Technology [7], an experiment was performed where the propeller blades for a remote-controlled drone were designed and 3D printed with structural defects at critical points in the propeller blade construction that would reduce the fatigue life of the propeller blades. After less than 2 min of flying time, the defective propeller blade failed catastrophically during mid-flight tests, causing the drone to crash and effectively be destroyed. Regardless of the fact that the propeller blade design was compromised, the research team performed the design compromise by means of a full-cycle simulated cyber-physical attack that made use of security vulnerabilities that had been in the public domain for a number of years already. In particular, the WinRAR ZIP file name spoofing vulnerability played a key role in delivering a malicious file to trigger other exploits utilized in the attack [8]. Needless to say, the research team succeeded in illustrating how a relatively simple cyber-physical attack could lead to catastrophic and potentially deadly consequences. This notion becomes extremely serious when it is viewed in the context of aircraft parts already being manufactured by means of 3D printing.

With design companies increasingly outsourcing manufacturing tasks and sharing information via the cloud, it is therefore clear that proper security measures are urgently required to make use of cloud-based design platforms safely.

4. Defining Industry 4.0 in Context

The previous sections have highlighted a new trend that is being increasingly observed in various industries. The fact that various technological platforms are brought together to function in an entirely new fashion that neither of the platforms were necessarily designed for, is what makes this new trend a paradigm shift and revolutionary.

Industry 4.0 involves the integration of various technologies, particularly IoT technologies, into existing technologies used in the industrial manufacturing and production sectors [9],[10]. The integration of these technologies enables new possibilities in terms of manufacturing capabilities, industry productivity and efficiency. A key focus on the integration of these technologies is the concept of industrial value creation [9],[11],[12], to account for and react to various factors such as market volatility, innovative problem solving, competitor influence and competition. As a result, new trends in problem solving, collaboration and innovation start to emerge, such as

global collaboration via the Internet to perform engineering and design work between teams across the globe [1], [3].

With increased process efficiency and productivity being key drivers in the Industry 4.0 movement, the business models for industries and businesses will also be adapted to reap the maximum possible benefit [3].

The large scale integration of technologies particularly involves the use of many sensors within a manufacturing or production environment. The constant analysis of data from these sensors to monitor the states of the equipment and processes involves the transmission of large amounts of data between systems, also known as “big data”. Big data from these sensors can also be used to perform predictive maintenance of systems, improve system reliability and risk management [13],[14].

Another definition for Industry 4.0 is the “real-time, intelligent, horizontal, and vertical networking of people, machines, objects, and information and communication systems with the aim of dynamically controlling complex systems” [11],[15]. Although this definition can be considered rather broad in scope, it essentially captures the thought of the interaction between humans and machines. Furthermore, with the Internet at the heart of the Industry 4.0 movement, there is essentially a bridging between the virtual world and the real world [9].

Although there is a reference of interaction between humans and machines, there is also concern about the social and ethical impact that Industry 4.0 keeps in store. With industrial environments becoming increasingly automated, there is a very real possibility that jobs in the industrial manufacturing and production sectors will evolve into jobs with a focus more towards roles such as maintenance and production management instead of manual labor. This would mainly be due to machines that could perform hard-labor tasks at a scale that is not possible to be sustained by humans. This forms part of what is referred to as the “Triple Bottom Line” [16],[17] that considers the sustainability of industries and businesses in the context of the associated economic, environmental and social impacts. However, the consideration of these aspects is beyond the scope of this article.

The adoption of new technologies always includes some measure of uncertainty and unknown aspects that are discovered as the adoption thereof progresses. This is particularly true for technologies where the Internet forms a key part of this technological interconnection, essentially exposing the technologies to the outside world, and within anyone’s reach in terms of digital interconnectivity. As such, there are a number of security risks that must be considered to ensure that the integration and ultimate use of these technologies can be done in a secure manner. This article focuses on building a train of thought to identify such risks, and possible solutions to address these risks.

The publication can be found here: https://www.mdpi.com/2076-3417/9/23/5105/htm

References

1. Thames, L.; Schaefer, D. Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing; Springer: Cham, Switzerland, 2017.
2. Sayfayn, N.; Madnick, S. Cybersafety Analysis of the Maroochy Shire Sewage Spill; MIT Management Sloan School: Cambridge, UK, 2017.
3. Gilchrist, A. Industry 4.0: The Industrial Internet of Things; Apress Media: Berkeley, CA, USA, 2016.
4. NASA Office of Inspector General. Industrial Control System Security within NASA's Critical and Supporting Infrastructure; NASA: Washington, DC, USA, 2017.
5. Steven Eric Zeltmann; Nikhil Gupta; Nektarios Georgios Tsoutsos; Michail Maniatakos; Jeyavijayan Rajendran; Ramesh Karri; Manufacturing and Security Challenges in 3D Printing. *JOM* **2016**, *68*, 1872-1881, 10.1007/s11837-016-1937-7.
6. Kellner, T. The FAA Cleared the First 3D Printed Part to Fly in a Commercial Jet Engine from GE. Available online: https://www.ge.com/reports/post/116402870270/the-faa-cleared-the-first-3d-printed-part-to-fly-2/ (accessed on 29 May 2019)
7. Belikovetsky, S.; Yampolskiy, M.; Toh, J.; Gatlin, J.; Elovici, Y. dr0wned-Cyber-Physical Attack with Additive Manufacturing. In Proceedings of the WOOT'17 11th USENIX Conference on Offensive Technologies, Austin, TX, USA, 10–12 August 2016
8. WinRAR 4.20 ZIP File Name Spoofing Vulnerability. Available online: https://www.rarlab.com/vuln_zip_spoofing_4.20.html
9. Hendrik S. Birkel; Johannes W. Veile; Julian M. Müller; Evi Hartmann; Kai-Ingo Voigt; Development of a Risk Framework for Industry 4.0 in the Context of Sustainability for Established Manufacturers. *Sustainability* **2019**, *11*, 384, 10.3390/su11020384.
10. Khan, A.; Turowski, K. A Survey of Current Challenges in Manufacturing Industry and Preparation for Industry 4.0. In Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'16), Sochi, Russia, 16–21 May 2016; Springer: Cham, Switzerland, 2017; pp. 15–26
11. Daniel Kiel; Julian M. Müller; Christian Arnold; Kai-Ingo Voigt; Sustainable Industrial Value Creation: Benefits and Challenges of Industry 4.0. *Series on Technology Management* **2019**, *21*, 231-270, 10.1142/9781786347602_0009.
12. Julian Marius Müller; Daniel Kiel; Kai-Ingo Voigt; What Drives the Implementation of Industry 4.0? The Role of Opportunities and Challenges in the Context of Sustainability. *Sustainability* **2018**, *10*, 247, 10.3390/su10010247.
13. Jihong Yan; Yue Meng; Lei Lu; Lin Li; Industrial Big Data in an Industry 4.0 Environment: Challenges, Schemes, and Applications for Predictive Maintenance. *IEEE Access* **2017**, *5*, 23484-

23491, 10.1109/access.2017.2765544.

14. Tupa, J.; Simota, J.; Steiner, F. Aspects of Risk Management Implementation for Industry 4.0. In Proceedings of the 27th International Conference on Flexible Automation and Intelligent Manufacturing, Modena, Italy, 27–30 June 2017
15. Yongxin Liao; Fernando Deschamps; Eduardo De Freitas Rocha Loures; Luiz Felipe Pierin Ramos; Past, present and future of Industry 4.0 - a systematic literature review and research agenda proposal. *International Journal of Production Research* **2017**, *55*, 3609-3629, 10.1080/00207543.2017.1308576.
16. John Elkington; Partnerships fromcannibals with forks: The triple bottom line of 21st-century business. *Environmental Quality Management* **1998**, *8*, 37-51, 10.1002/tqem.3310080106.
17. Wayne Norman; Chris Macdonald; Getting to the Bottom of “Triple Bottom Line”. *Business Ethics Quarterly* **2004**, *14*, 243-262, 10.5840/beq200414211.