applied sciences

MDPI

Review

A Review of Industry 4.0 Manufacturing Process Security Risks

Jaco Prinsloo [1,*], Saurabh Sinha [1] and Basie von Solms [2]

[1] Faculty of Engineering and the Built Environment, University of Johannesburg, Auckland Park, Johannesburg 2006, South Africa; ssinha@uj.ac.za

[2] Centre for Cyber Security, Faculty of Science, University of Johannesburg, Auckland Park, Johannesburg 2006, South Africa; basievs@uj.ac.za

* Correspondence: wave.jaco@gmail.com; Tel.: +27-72-736-0829

Received: 28 October 2019; Accepted: 18 November 2019; Published: 26 November 2019

Abstract: The advent of three-dimensional (3D) printing has found a unique and prominent role in Industry 4.0 and is rapidly gaining popularity in the manufacturing industry. 3D printing offers many advantages over conventional manufacturing methods, making it an attractive alternative that is more cost-effective and efficient than conventional manufacturing methods. With the Internet of Things (IoT) at the heart of this new movement, control over manufacturing methods now enters the cyber domain, offering endless possibilities in manufacturing automation and optimization. However, as disruptive and innovative as this may seem, there is grave concern about the cyber-security risks involved. These security aspects are often overlooked, particularly by promising new start-ups and parties that are not too familiar with the risks involved in not having proper cyber-security measures in place. This paper explores some of the cyber-security risks involved in the bridge between industrial manufacturing and Industry 4.0, as well as the associated countermeasures already deployed or currently under development. These aspects are then contextualized in terms of Industry 4.0 in order to serve as a basis for and assist with future development in this field.

Keywords: industry 4.0; additive manufacturing; industrial manufacturing; fourth industrial revolution; Internet of Things (IoT); Industrial Internet of Things (IIoT); cyber-physical systems; manufacturing network security

1. Introduction

Since the dawn of the first industrial revolution in the eighteenth century, there has been continual development in all areas of the manufacturing industry. The first industrial revolution stemmed from the first innovations in industrial machinery (such as the steam engine) that enabled large-scale manufacturing and mechanization. The second industrial revolution followed. With the invention of electricity that could be utilized to develop new infrastructure that could further expand upon industrial capacity, the second industrial revolution occurred during the late nineteenth century to the early twentieth. The third industrial revolution was caused by the invention of computers in the 1950s. The introduction of computers in the industrial context led to many new possibilities in terms of process automation and optimization [1,2]. Although these past revolutions had enormous ramifications in the industrial sector, we have now arrived at what is arguably the most prominent and disruptive phase of the manufacturing industry that has ever taken place. Industry 4.0, denoting this new phase as the "fourth industrial revolution", has already become a buzzword in industrial manufacturing circles. This new phase in the manufacturing industry is rapidly expanding, with the introduction of new and innovative technologies designed to provide more cost-effective, robust and efficient solutions to manufacturing paradigms [1].

One of the most prominent of these new technologies is 3D printing. As an additive manufacturing process, 3D printing has made it possible for manufacturers to produce complex products at a fraction of the manufacturing cost that conventional manufacturing methods would entail. At the same time, 3D printing offers a production efficiency that is orders of magnitude higher than conventional manufacturing processes [1,3].

Another driving force of Industry 4.0 is the Internet of Things (IoT) movement, which involves interconnecting various digital and electronic devices and platforms through communications networks, particularly through the Internet. This method of interconnecting various technological platforms presents the ability to interface with manufacturing equipment located anywhere in the world, from anywhere in the world. As a result, product designers are able to send product designs for manufacturing to an ever-growing list of possible manufacturing houses, causing a transformation of the manufacturing industry where a more flexible yet optimized production environment is presented. In a study conducted between April 2012 and January 2014, titled Project SHINE (short for "SHodan INtelligence Extraction"), the number of manufacturing devices deployed in control systems environments connected to the Internet (either intentionally or unintentionally) were already in excess of 500,000. At a reported average rate of 2000 to 8000 new devices detected on a daily basis, one can only imagine the sheer magnitude of Internet-connected devices that are present in these environments today [3,4]. In fact, according to a press release by Gartner, the number of IoT devices in use around the world is estimated to reach in excess of 20.4 billion devices in 2020 [5]. As a result of this growing trend, some industries and government bodies have already started acting towards exploring, researching and developing new strategies and technologies to address the needs of such a trend. For example, a resolution on developing an integrated industrial digitalization strategy for the European Union (EU) was already adopted by the European Parliament in June 2017 [6].

As disruptive and innovative as 3D printing in Industry 4.0 is, there is paramount concern about the cyber-security aspects involved. Industries around the world are all too familiar with the risks involved if proper digital security measures are not in place. For example, industrial espionage and industrial sabotage are very real concerns for industries where sensitive and proprietary data could be exposed or even destroyed. Another example is the deliberate disruption of manufacturing processes by malicious hackers to cause damage to manufacturing entities [2]. Despite the fact that 3D printing is rapidly being adopted as a prominent manufacturing process, many of the security measures required to provide a secure interconnection platform are still in the development phase. Lack of proper security measures in this industry could pose a number of potentially devastating risks. For example, aviation parts that do not conform to the required specifications, or medical implants that contain manufacturing defects, could have serious consequences when such components fail mechanically. Furthermore, in the advancement of materials for 3D printing, including "programmable materials," there is a further risk that commercialization could precede the required due diligence. This aspect, referred to as 4D printing, is however beyond the scope of this article [1,7].

It is therefore of critical importance that proper cyber-security measures are developed and implemented in order to provide efficient and cost-effective additive manufacturing platforms that are digitally safe and secure from cyber-attacks. Since the topic of cyber-security aspects in Industry 4.0 is a relatively new field, many of the proposed countermeasures are still in their infancy. As a result of the lack of digital security knowledge among some designers and engineers involved in the development and maintenance of equipment in industrial control systems environments, the implementation of digital security measures in these environments is often viewed as a secondary priority [3]. The constant race for higher yields and productivity on the production line also contributes prominently to the notion of viewing security in such environments as a non-critical component. In the quest for this production efficiency, the usage of an artificially intelligent algorithm is also included, and there are therefore further ethical, legal and technological challenges embedded in the manufacturing process.

Arguably, this is one of the greatest risks that the industrial manufacturing environment faces in the foreseeable future. However, significant progress has already been made by some of the leading players in the field of digital security, aimed specifically at the industrial environments through innovative approaches to problems that are unique to this field.

2. A Complete Paradigm Shift

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 cyber-security.

2.1. 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) [8]. 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:

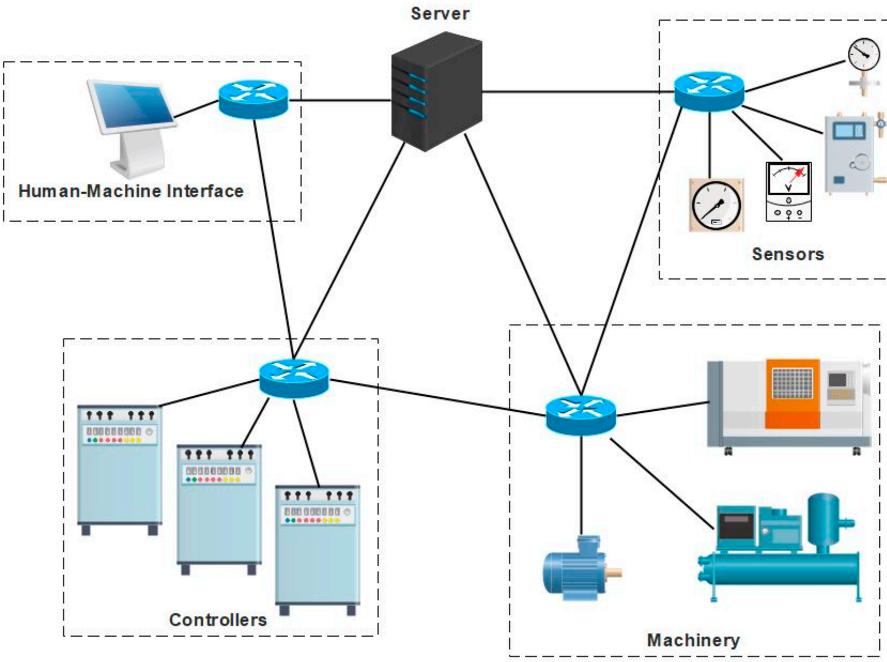

Figure 1. A typical operational technology (OT) industrial systems network architecture.

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.

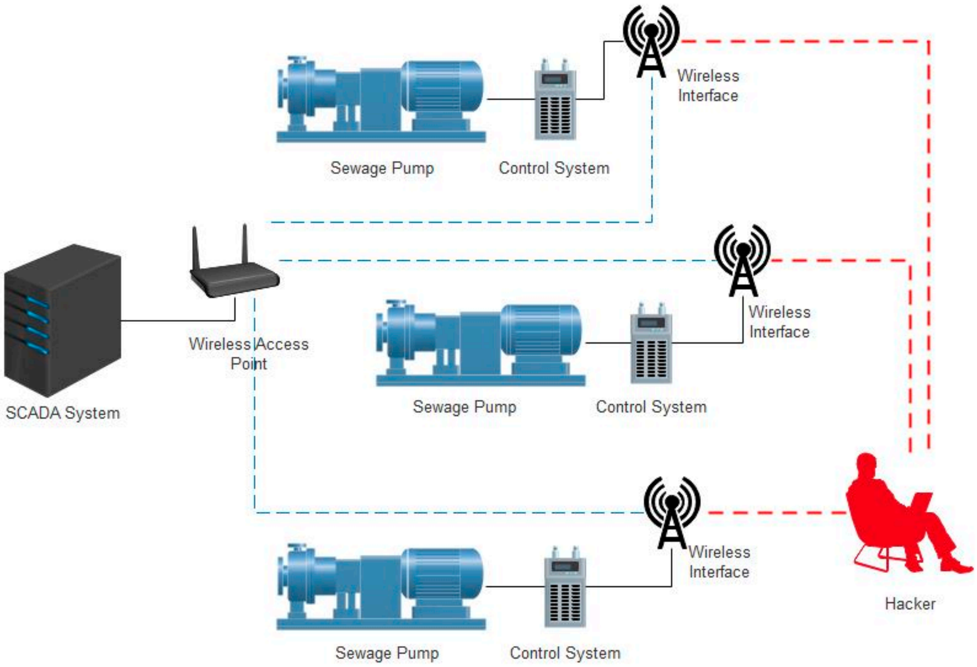

Figure 2. Illustration of the OT network at the Maroochy Shire sewage plant. SCADA: supervisory control and data acquisition

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 [8]. 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 [8].

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) [8,9]. 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.

2.2. 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 [8]. 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 [10]. 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 hyper-text transport protocol (HTTP) [8,9]. 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 [8,9].

2.3. 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 [8,9]. 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.

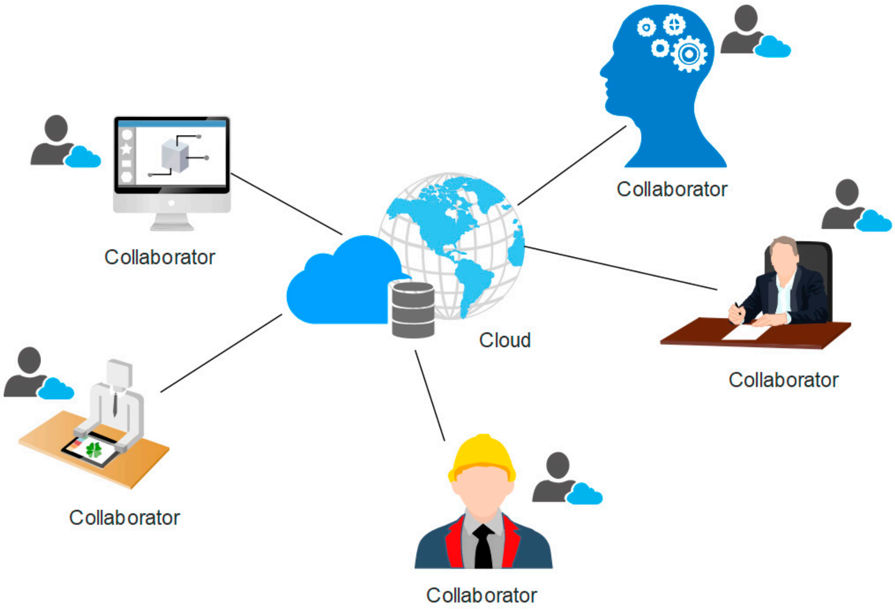

Figure 3. Global collaboration on a project.

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 [11].

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 [12]. 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 [13], 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 [14]. 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.

2.4. Definining 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 [15,16]. 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 [15,17,18], 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 [8,9].

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 [9].

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 [19,20].

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" [17,21]. 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 [15].

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" [22,23] 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.

3. Identifying the Problem

In this section some of the risks associated with the cyber-security aspects of the current industrial manufacturing industry will be put into perspective. These risks are unique in the sense that although the OT platforms typically utilized in the industry are widely familiar, they pose certain cyber-security risks that are of a different nature from those encountered in an IT environment. Consequently, these risks have not been considered as such until now. First, a few case studies of historic cyber-physical attacks are briefly introduced in order to put into perspective the true nature of such attacks on industrial control systems networks. While a comprehensive study into the details of how these attacks work is beyond the scope of this article, some key aspects in terms of the associated security vulnerabilities can still be identified in order to formulate more clearly defined cyber-physical security problem statements. Putting these security aspects into perspective, they can be contextualized to identify and formulate solutions to the problems.

3.1. Case Studies of Cyber-Physical Attacks

Since the number of smart manufacturing devices that are deployed in the industry is significantly smaller than the number of conventional manufacturing devices, the number of reported and documented attacks against these systems is relatively low. The same applies to a comparison of the typical sizes of OT network systems vs. IT network systems, where the number of deployed IT network systems is orders of magnitude higher than the number of deployed OT network systems. However, there are a few well-known documented cases of cyber-physical attacks, of which some will now be briefly introduced.

3.1.1. The Zotob Worm

In August 2005, 13 Daimler Chrysler car manufacturing plants (among over 170 other major corporations) were attacked by a worm called Zotob. The worm caused a temporary (5 to 50 min) shutdown of the entire production line in each of these plants, affecting more than 50,000 production personnel, and resulting in financial damage in the order of thousands of US dollars, apart from the financial damage caused by the loss of the man-hours of more than 50,000 personnel [24].

The Zotob worm came into effect shortly after Microsoft announced a security vulnerability in the Windows 2000 operating system. Within a matter of days from the announcement of the vulnerability, the code for the Zotob worm had already been developed and distributed within the computer networks of several institutions before IT security personnel could apply the required security patch. In particular, the Zotob worm exploited the Microsoft Windows Plug and Play Buffer Overrun Vulnerability on TCP port 445, which opened a back door to the operating system (OS) that enabled the hacker to perform malicious actions with full user rights and privileges [25,26]. The vulnerability also made it possible for the hackers to install malicious software on the operating system. From there on, the worm cold replicate and progress further into the computer network, and thus affect any systems connected to the manufacturing network. This is exactly what happened in the attack on the Daimler Chrysler manufacturing plants.

The Zotob worm successfully illustrated how fast the black hat hacking community can respond to the announcement of a security vulnerability before any preventative action can be taken by cyber-security personnel in a particular industry.

3.1.2. Stuxnet

The Stuxnet worm, developed in 2010, had the reputation of being one of the most threatening and complex computer worms ever created at the time of its inception. Written primarily to target industrial control systems, the worm would propagate through a computer network and multiply itself without detection with the aim to reprogram PLCs and other similar industrial control system devices. Malicious instructions compiled by the hacker could then be executed on the infected systems, while the changes to the equipment programming were hidden to avoid detection by personnel operating or maintaining the equipment. Stuxnet is considered by Symantec as one of the most complex security threats ever analyzed, and dealing with it required extensive efforts from a large number of security analysts [27].

Making use of a vast number of components to maximize the possible attack vectors, including among others, multiple zero-day exploits, antivirus evasion techniques, process injection and peer-to-peer updates, the Stuxnet worm succeeded in infecting thousands of computers around the world, in order to maximize the chances of eventually entering “air-gapped” control systems networks. This was made possible in particular by its ability to hide itself on removable drives. Making use of a vulnerability in the way shortcuts and .lnk files are processed on a computer (identified by Microsoft as MS10-046) [27,28], the worm could replicate and propagate further within the computer and to external devices by itself. Since many industrial control systems were not designed with security in mind, the fact that no integrity checks were performed on messages received by these systems played a key role in the ability of the worm to infect systems without detection [8]. Once it had manifested itself on infected machines, the worm would regularly send encrypted updates to the Stuxnet command and control (C&C) servers with identification information of the infected systems, such as IP addresses, operating systems and computer names.

The first variant of the Stuxnet worm was encountered in June 2009. This variant did not make use of any signed driver files, but in January 2010 the Stuxnet worm was found to make use of a driver that was digitally signed with a compromised certificate by the Realtek Semiconductor Corporation. In March 2010 the Stuxnet worm was found to exploit the vulnerability that was only identified as MS10-046 by Microsoft in August 2010.

By the time Symantec issued a comprehensive analysis of Stuxnet, an estimated 100,000 hosts had been infected in over 25 countries, with infection rates of up to 6000 hosts per day [27].

3.1.3. Duqu and Flamer—Followers of Stuxnet

With Stuxnet paving the way for the development of extremely complex and powerful cyber-attacks, two new threats that are very similar to Stuxnet made their entry less than a year after the Stuxnet worm went viral. Although very similar to the Stuxnet codebase, the Duqu threat was developed primarily to steal information from industrial manufacturing entities, so as to facilitate the development of more specific and focused attacks on other third parties. Consisting mainly of a driver file, a dynamic link library (DLL) and configuration file that were installed by an executable file through a Microsoft Word document that contained a zero-day kernel exploit, the threat would search for detailed design information (among other proprietary information) and make use of HTTP and HTTPS to upload and download information between the infected devices and its C&C servers. One variant of the threat had a particularly novel way of hiding the DLL containing the primary functions of the threat. This DLL was hidden as encrypted data contained in a JPEG file which featured an image taken by the Hubble Space Telescope. Another novel feature of the Duqu threat in general was that it would remove itself from the infected device after approximately 30 days, thus minimizing the possibility of its detection [29].

The first attack by the Duqu threat was recorded in early April 2011, with additional variants encountered in October 2011. By the time that a comprehensive analysis of the Duqu threat was published by Symantec in November 2011, more than eight countries had fallen victim to the 15 variants of the threat [29].

Similar to the Duqu threat, the Flamer threat also has deep roots in the Stuxnet codebase, and has been in existence since 2010. Symantec considered the Flamer threat the most complex malware that had ever been written at the time of its detection and analysis, and it is anticipated that it will retain this reputation for many years to come. Its size is in excess of 20 megabytes, and the software architectural design is on a par with professionally developed software. The purpose of the Flamer threat was similar to that of the Duqu threat, i.e., industrial espionage, but on a much larger scale [30].

3.1.4. BlackEnergy3 and the Ukraine Power Grid

The cyber-attack on the Ukrainian power grid in December 2015 was the first documented case of a power grid being targeted by means of a cyber-physical attack. Presumably developed by the Russian cyber espionage team Sandworm, the BlackEnergy3 worm acted as a Trojan horse that contained distributed denial of service (DDoS) capabilities. The worm made its first appearance in 2007 (known as BlackEnergy), and underwent upgrades with more advanced features in 2010 (known as BlackEnergy2). Finally, in the spring of 2015, after the BlackEnergy3 version of the worm was released, attacks on power distribution companies by means of malicious e-mails commenced. When the attackers gained entry into the control systems network of the Prykarpattyaoblenergo power distribution center in December 2015, they disabled the entire plant by commanding all the circuit breakers to open, leaving more than 200,000 people without electricity. This incident was particularly catastrophic, since the people left without electricity could not operate heating systems in the middle of the winter. Although the electricity supply was cut off for only approximately six hours, plant technicians still struggled to restore the electricity supply fully to all of the affected regions [30].

In the case of the Ukrainian power grid cyber-attack, the malicious entity was spread by means of malware through classic cyber-attack distribution techniques, such as infected e-mails and compromised networks. DDoS attacks prevented proper functioning and recovery of the infected industrial systems, while the worm prevented plant technicians from gaining access to the control system by logging them out of their user accounts and changing their passwords [3,31].

3.2. *Types of Cyber-Physical Attacks*

The case studies presented in the previous section outline only a few of the types of cyber-physical attacks that are known today. While not an exhaustive list of historical cyber-physical attacks by any means, it presents a comprehensive overview of the typical types of cyber-physical attacks that could be performed. The most common types of cyber-physical attacks that occurred can be summarized as follows:

3.2.1. Zero-Day Attacks

The term "zero-day attack" refers to a cyber-physical attack that exploits a security vulnerability that has not yet been disclosed publicly [32]. Since such a vulnerability has not been disclosed publicly, there is a high probability that knowledge thereof is only possessed by a selected few individuals who have somehow managed to find such a vulnerability. Although this could mean that the chances of an immediate serious threat are not as high, the probability is equally high that cyber security entities are also not aware of the vulnerability. This means that until such a vulnerability is publicly disclosed (unless it is disclosed privately through confidential channels), there is little to no chance of developing a security patch that would eliminate it. Historic cases indicate that users of commercially popular software, such as Adobe Reader, WinRAR [14] and Microsoft Word, are particularly vulnerable to zero-day attacks without even having the slightest notion that they can easily fall victim to a threat. Consequently, by the time it is disclosed, it could already be too late to rectify any malicious activity executed through such an attack [3,8,32].

The implications of such an attack on an industrial scale could be disastrous to such an industry, particularly if it involves a production line being compromised and the malicious software resisting any attempt to install a security patch that would disable it.

3.2.2. Eavesdropping Attacks

Attackers can obtain confidential and sensitive information by eavesdropping on communication channels that are known to be used by individuals or institutions to communicate such information. Eavesdropping can take a number of forms, such as tapping into telephone lines, phishing and monitoring network traffic. Should any information that contains sensitive content relating to how a certain system or production process operates be shared on an insecure communication channel, it could be of great value to an attacker to eavesdrop on such communications in order to plan an attack in advance.

3.2.3. Denial of Service Attacks

Arguably one of the most common types of attacks, denial of service (DoS) attacks, are specifically aimed at crippling systems by denying access to any form of computational resources, effectively bringing the process that the system is in control of to a halt. For example, a server that controls industrial processes can be prevented from communicating with lower-level industrial control systems by denying these systems access to the server network [3]. There have even been cases where DoS attacks have been used as a decoy by cyber attackers to cover their tracks after an attack of another form has been carried out [33].

Another form of DoS attacks, namely distributed denial of service (DDoS) attacks, makes use of multiple infected systems to distribute cyber-attacks on a larger scale. This is one particular concern regarding the security of next generation industrial control systems. Since many next generation industrial sensors and items of control systems equipment have the capability to connect directly to computer networks and the Internet, a DDoS attack in such an environment could have catastrophic consequences for production lines, where such equipment is critical for efficient and safe operations.

3.2.4. False Data Injection Attacks

In systems where few or no authentication mechanisms are present, false data injection attacks can be used to inject malicious code and commands into control systems networks [3]. Lack of authentication mechanisms means that there is no way the targeted equipment can verify the authenticity of any of the commands it receives. Therefore, it is a vulnerability that cyber attackers with malicious intent can exploit relatively easily. Such attacks can range from commanding industrial control systems to performing actions that are outside of safe operating margins, to completely reconfiguring the control systems' equipment to perform totally differently from how it had originally been designed to function (the Stuxnet worm is an example of such an attack).

If attackers can gain undetected access to an industrial control systems network with weak security, entire production lines can be compromised by commanding manufacturing equipment to assemble manufactured products incorrectly, which will compromise the proper functionality of the product.

3.2.5. Replay Attacks

Even though authentication mechanisms can to a great extent prevent malicious commands from being executed by equipment that is targeted through cyber-attacks, an authenticated data packet can be retransmitted, but with modified data or instructions. Since the data packet appears to have a legitimate origin, it is still possible that such a packet can be altered so that it is transmitted to and processed by electronic equipment with no suspicion of malicious intent.

Replay attacks can be avoided by incorporating a tracking mechanism, such as the use of a sequence number, to detect packets that have already been processed but have been retransmitted with possibly malicious commands and data. These packets could pass authenticity verification and execute the attack for which they were formulated.3.2.6. Side-Channel Attacks

Side-channel attacks entail the collection of data due to information leakage by industrial equipment. For example, fluctuations in power usage due to processing data can leak out and provide attackers with valuable information on the inner workings of the system. More sophisticated attacks can be carried out by means of an in-depth monitoring of industrial manufacturing equipment, such as monitoring the positional characteristics of a robotic arm during production in order to formulate a near-precise reproduction of the manufacturing instructions sent to the robotic arms.

With smartphones constantly evolving into highly advanced and increasingly complex devices, the possibilities of extending the platforms on which side-channel attacks are performed using smartphones are on the increase. Studies [34,35] are already in progress investigating the effect of smartphone-based side-channel attacks on 3D printers using the phone's built-in sensors. The focus of these studies has primarily been on acoustic and magnetic side-channel attacks [36,37].

The aforementioned attacks are by no means an exhaustive and complete list. Numerous different techniques exist that cyber attackers can use to attack cyber-physical systems. It can also be deduced that many of the known attacks found in the IT network domain can be equally threatening to devices in the OT network domain.

3.3. *Lifecycle of an Attack*

Most cyber-physical attacks are driven by a clear motive to target a specific organization or industry. Attackers often collect the greatest amount of data they can by various means (such as eavesdropping attacks, for example) in order to plan an attack ahead of time to maximize its impact. The motives for the attacks are primarily data harvesting and sabotage. Data harvesting concerns the collection of sensitive data from system networks that could provide important information to attackers that can be used to facilitate an attack. Sabotage is aimed at disrupting the functionality of a system and possibly damaging it [3,8]. These two motives are usually used in combination to ensure an effective attack.

Besides the fact that there are a number of different possible attacks that can be carried out, they have a lot in common in terms of their execution and lifecycle. Figure 4 illustrates the lifecycle of a typical cyber-attack.

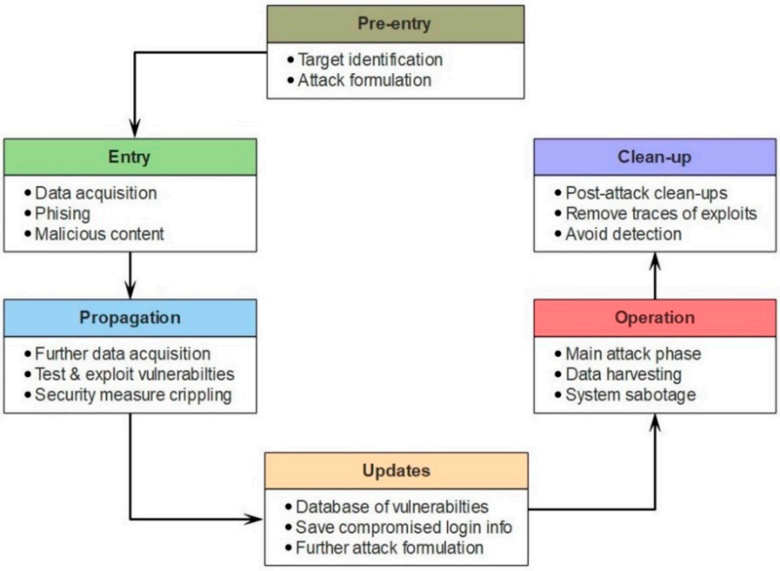

Figure 4. Lifecycle of a typical cyber-physical attack.

During the pre-entry phase the attacker identifies a target and acquires any prerequisite knowledge to plan and formulate an attack. The tools and skills required to perform the attack are also identified and acquired during this phase. After the necessary tools, skills and knowledge have been acquired, the entry phase begins by collecting information that will be of use to the attacker to plan the attack. This typically involves basic cyber-attacks such as phishing by means of malicious e-mails, social media platforms and infiltrating the supply chain, where for example, software updates from trusted entities are compromised with malware to harvest information that can be valuable to the attacker. As the harvesting of data continues to delve deeper into the targeted network, network systems with poor security measures are exploited to gain further access deeper into the network by obtaining higher access privileges inside the targeted network. The use of C&C servers are very common during this phase of the attack to harvest more data and to infect the network further with more malware (such as in the case of the Stuxnet, Duqu and Flamer threats) by means of malicious updates.

When enough information has been harvested and the security of the targeted system has been sufficiently crippled, the main aim of the attack can be reached by carrying out the attack in the operation phase. This is where the true motive of the attack comes into play. Depending on the motive of the attack (harvesting data or sabotage), this phase can last anything from a few minutes to months and even longer if the attack remains undetected. Finally, when the attack has been carried out, the attackers might cover their tracks by clean-up processes in order to minimize the possibility of being detected or traced.

The success of an attack depends largely on the state of the targeted network's security measures. Since OT systems networks are mostly designed without proper consideration for security, the chances of successful attacks on these networks are vastly higher than those attacks that target IT systems networks.

3.4. The Problem in the Context of Industry 4.0

Since one of the key characteristics of Industry 4.0 is the use of next generation smart manufacturing equipment, sensors and processes, the attack vectors known to cyber attackers need to be considered in the context of the Industry 4.0 environment. Sensors used in the Industry 4.0 environment incorporate some of the latest technological advancements, and typically have the ability to function as small sub-systems in the broader context of the manufacturing information architecture. For example, instead of just providing a simple analog measurement output that is directly fed into the corresponding monitoring and control system, these sensors can instead transmit their data to such higher-level systems via a standard peripheral. The use of peripherals for communication between sensors and higher-level systems also makes it possible to re-configure sensor sub-systems directly from within the manufacturing information architecture. It is thus apparent that the malicious re-configuration of these sensors will be a key concern, requiring appropriate security measures to prevent such an event. Unfortunately, many of these next generation systems are designed with security viewed as a secondary priority. As has been discussed broadly in Section 2, there are inevitable compatibility issues if new industrial manufacturing equipment is not designed with security as an integral part of the design. There are also many more possible attack vectors in the industrial manufacturing environment that can be exploited (and combined) to cause massive damage to these industries. Each of these attack vectors can be directed at specific security vulnerabilities in the broader scope of the manufacturing information architecture, with each being unique in its nature and corresponding security challenges.

Industrial manufacturing equipment without proper security measures is not the only concern in this context. There are other platforms and infrastructure that can also be compromised before the effects of the threat extend into the industrial network domain. For example, computers that are used to design computer-aided design (CAD) models can be infected with malware specifically designed to target and compromise these CAD models. This is a particularly prominent threat, given the increasing adoption of cloud-based design, as discussed in Section 2.3.

It is thus apparent that there are a number of unique security problems that Industry 4.0 faces, each with different facets that require specific attention to its underlying mechanisms in order to be effectively addressed. These types of security problems are briefly explored in the following subsections.

3.4.1. The Manufacturing Information Architecture

In previous sections the issue of intercepting manufacturing information between IT and OT platforms has been briefly introduced. In this section, we will zoom out on the problem statement in order to consider the flow of information between platforms in the digital manufacturing ecosystem as a whole.

The case studies considered in Section 3.1 (which certainly do not represent an exhaustive selection) briefly introduced the nature of some cyber-physical attacks that have taken place in the past. Since these attacks have been aimed specifically at cyber-physical systems, and have been successful in their malicious intent, this paints a clear picture of what the scale of impact could be if similar attacks are performed on future smart manufacturing industries. It is also evident that the convergence between IT and OT platforms is a decisive factor in these types of attacks. Attackers can operate remotely from any location in the world via the Internet and subsequent digital networks, infiltrating vulnerable IT systems to carry out an attack on the underlying OT systems.

Any malicious interception of information within the digital manufacturing ecosystem will mostly be aimed at obtaining and altering critical information on the product's manufacturing process. Apart from manufacturing process security, this also raises the issue of the protection of intellectual property [38]. Such critical information will be information that, if altered, could affect the product's functionality or structural integrity. Examples of such critical information include the bill of materials (BOM), the product design files and the manufacturing equipment control parameters. Each of these critical information items presents a unique attack vector that could be utilized for malicious intent.

Consider as an example the 3D printing of a particular product within an industrial manufacturing environment. The filament specified in the product's BOM could be replaced with a filament that has a lower tensile strength, which would undoubtedly cause the end product to fail structurally if exposed to mechanical stress levels that cannot be withstood by the wrong filament. The effect of alterations to the CAD model design and manufacturing files has already been discussed in the previous section. Control parameters of the manufacturing equipment are also important in the product manufacturing process. For example, the temperature of the 3D printer's heat bed on which the product is printed is dependent on the type of filament used for the print. If the incorrect temperature setting is used with a specific filament, it could cause the foundation of the printed product to warp, and lead to an end product that is not dimensionally accurate compared to its design. Another example of such control parameters is the speed at which the 3D printer prints the product. If it is set higher than a specified standard (or according to the machine's specifications) it could cause the layer of filament to be too thin according to the design parameters. The printing speed could also be intermittently adjusted throughout the print, resulting in inconsistent layer thickness throughout the end product. Similarly, the speed of the head containing the spindle of a milling machine could be maliciously configured to a speed exceeding that specified by safe operating parameters, leading to damage to milling bits, causing unplanned downtime for maintenance.

Along with the case studies considered in Section 3.1, the Maroochy Shire sewage spill considered in Section 2.1 is yet another typical example of how a cyber-physical system can be compromised, and to what extent it can have an impact beyond the environment of the cyber-physical system itself.

As can be deduced from the examples presented in the previous paragraph, there are numerous possible scenarios of malicious interception that could each be detrimental to the final manufactured product. It would be impractical to formulate a unique security countermeasure for each of these scenarios. Instead, the problem needs to be addressed in the scope of the bigger picture. By analyzing each of these scenarios, certain common attack vectors can be identified that, if accounted for, could avoid the occurrence of many subsequent scenarios. Most of these attack vectors have one key aspect in common—the communications network between hardware and software platforms (especially IT and OT platforms). Furthermore, the use of cloud-based design increases the number of available attack vectors. If a hacker can obtain access to the communications network, an interception of data can be performed, and malicious data can even be injected into the communications network to disrupt the manufacturing process. Figure 5 illustrates the general context of the manufacturing information architecture and where the associated attack vectors are introduced.

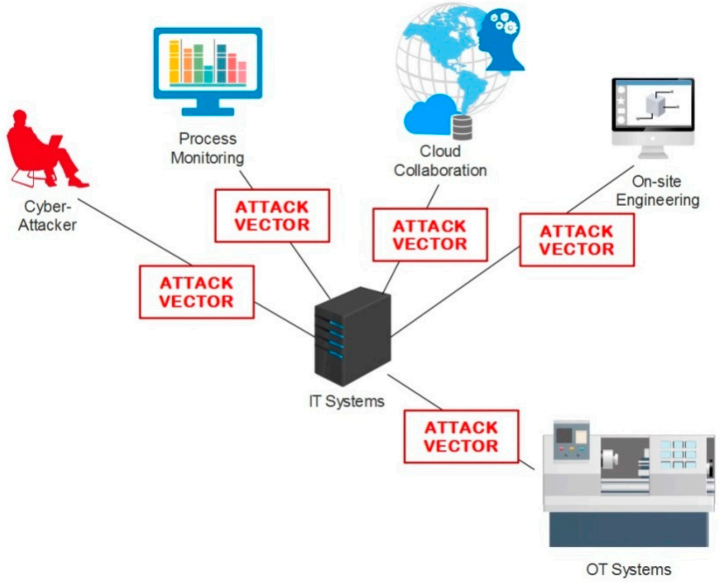

Figure 5. Attack vectors in a typical industrial systems architecture.

Therefore, an efficient and effective security solution for the communications network would form a very important and key integral part of the entire manufacturing ecosystem. It is thus a vital starting point for next generation manufacturing industries to introduce proper security measures in order to ensure a cyber-secure (and consequently, to a great extent, physically secure) manufacturing ecosystem.

3.4.2. Industrial Networks and Security Measure Scalability

As the demand for higher production yield, larger capacity and increased productivity is constantly on the rise, the issue of scalability becomes a key point of consideration. Expanding a manufacturing industry's capacity will typically involve the addition of manufacturing equipment, and subsequently an enlargement of the manufacturing information architecture. While this seems to be a rather simple concept in principle, the reality is that such an expansion requires the extensive planning of the utilization of floor space, placement of equipment and the layout of the underlying information network that interconnects the manufacturing equipment. The security of the underlying information network is critically important to the longevity and efficiency of the industry in question. Section 3.1 briefly explored the potential of cyber-physical attacks to cause massive damage to industries, requiring extensive effort and cost to rectify.

Since the consideration of proper digital security measures are typically viewed as a secondary priority [3], these industries face the risk of expansion without security against any form of cyber-physical attack. The digital platform on which the manufacturing information architecture is built is also a prominent contributor to the complexity in this context. For example, if the expansion of a manufacturing industry requires that equipment be placed in a different building from the one where the existing equipment is currently located, the network interconnection of this equipment must be carefully considered.

Widespread separation of buildings is just one of many examples of factors that will significantly determine the nature of the network expansion. Factors determining the nature of the network expansion will typically include large-scale interconnectivity, high throughput, low latency, and of course, trustworthy security.

The addition of devices within an existing network presents a number of complexities and problems to IT personnel. In many cases, particularly in networks with hierarchical structures, the existing network cannot be extended by simply adding more network connections to a network server using the same implementation as the current network (such as adding more Ethernet connections to a network switch). Adding new devices involves the configuration of network building blocks, such as switches, firewalls and routers. This can lead to downtimes in multiple parts of the network that will ultimately affect the productivity and throughput of the underlying industrial equipment. Since many industries are also constantly in operation, and processes cannot merely be shut down temporarily, scheduled downtimes are difficult to implement. With IT personnel striving to minimize service disruption, network expansion becomes an intricate task to conduct effectively and efficiently.

During network expansion, where large data centers form part of the network, the required data processing capability and network capacity increase rapidly. The implemented networking equipment can only provide a limited amount of network capacity that will ultimately be reached with a constantly growing network. Once this capacity threshold has been reached, the industry in question is faced with the difficult decision of adding new equipment to expand the network capacity, or to redesign the entire network to accommodate the needs of the expanded network. Vendor dependence also plays a prominent role, where vendors' development and production cycles could make it difficult to deliver equipment featuring new capabilities when there is a particular need to be addressed.

The same level of dedication that goes into getting the right expertise to solve the network expansion problem should be applied to obtaining the right expertise to assess the possible security measures that can be implemented, as well as the compatibility and effectiveness of these security measures.

These factors directly translate into costs (both in terms of finances and time) that run the risk of wrongfully influencing the decision-making process. Furthermore, as the networking solution becomes more complex (and perhaps even novel), so do the associated security measures. This trend suggests that there is a fundamental issue with current networking technology in general that needs to be addressed urgently. If all of these factors are not carefully and thoroughly considered and implemented, doors to future cyber-physical attacks will be left open, which will undoubtedly be a ticking time bomb for all industries that rely on inter-connected equipment.

3.4.3. System Security and Safety

Apart from industrial system security measures being viewed as a secondary priority, the same argument could apply for industrial system safety. Particularly with regards to the high degree of system automation required to achieve higher levels of productivity and efficiency, there is an inherit risk that system safety is not equally considered in the design of such industrial systems. For example, in an industrial manufacturing plant, highly automated systems could pose a safety hazard to plant personnel if some form of safety measure is not factored into the design of the system.

Riel et al. [39,40] refer to the concept of secure systems that are not always safety-critical, although safety-critical systems must always be secure. If system safety is to be a high priority in the design of highly automated and integrated systems, then this concept further highlights the importance of implementing strong security measures in cyber-physical systems. If such security measures are not in place, this opens the door to cyber-attacks that could not only be detrimental to the efficiency and productivity of an industrial manufacturing environment, but also to the safety of the plant personnel.

3.4.4. CAD Model Security Gaps

Many industrially manufactured products have their roots in a CAD model that has been designed by an engineer or draftsman according to the required specifications. The CAD model is therefore the first step in a series of processes known as the "digital thread" [8,41], as illustrated in Figure 6 below.

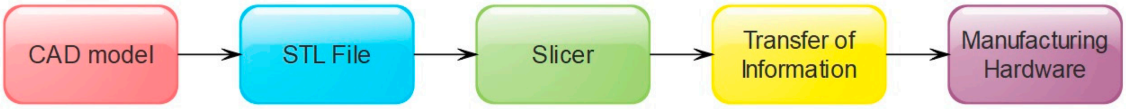

Figure 6. Digital thread for the manufacturing of a three dimensional (3D) modeled product. STL: stereolithography

Once CAD 3D modeling of a product has been completed, the 3D model is converted to a file that contains all of the details of the model's design in a format that can be interpreted by the applicable manufacturing hardware. This particular file is in a format known as the stereolithography (STL) file format, which contains approximations of all the surfaces of the CAD model by means of triangles. In the case of an additive manufacturing process such as 3D printing, the product is manufactured in layers that are tightly packed on top of one another. The conversion from the STL file format to the layered format of the CAD model is known as "slicing", and is performed by a utility called a "slicer". The slicing process involves generating sets of 2D slices that are essentially sets of intersecting points between the 3D model and the slicing plane. This 3D model is then manufactured one layer at a time. This process can be represented mathematically [42] as

$$S = \{S_i \big| \, i \in [1, N]\}$$

where S represents the set of N2D slices. Furthermore, each slice can be mathematically described as

$$S_i = \left\{p_{i,j} \big| \, j \in [1, \ |S_i|]\right\}$$

where $|S_i|$ represents the number of intersecting points $p_{i,j}$ in slice i at the jth point, represented by a coordinate pair $\left(x_{i,j}, y_{i,j}\right)$.

Once the STL file has been processed by the slicer, it can be sent to the manufacturing hardware's interface so that it can be interpreted and converted into machine code that controls the manufacturing hardware. Finally, the machine code that is executed is translated into commands to the actual components of the manufacturing hardware that produces the final product.

In Section 2.2, the fact that many OT devices and platforms do not have adequate security measures in place, was discussed. With this in mind, it can be deduced that there are several possible attack vectors in the digital thread illustrated by Figure 6. For example, it is possible to alter the design of the final product by compromising the CAD model through malicious changes to the intended CAD model design. The STL and slicer output files can be intercepted, and several changes can be induced that could compromise the structural integrity of the final product. Such changes can be subtle enough to remain undetected to perhaps even the informed eye. Furthermore, the control interface of the additive manufacturing hardware can be hacked, and machine instructions can be altered to command the equipment to operate outside certain limitations and parameters, or execute unauthorized commands during operation (recall the Maroochy Shire sewage spill example from Section 2.1).

It is also apparent that the three CIA pillars (confidentiality, integrity and availability) are at risk of being compromised at various points throughout the digital thread. Consider, for example, the design of a proprietary product through CAD modeling. The design engineer or draftsman is authorized to have access to the product's CAD model. Since any information on the product is of a sensitive nature, access to this information needs to be controlled, especially when the product's design is distributed to the manufacturer. It should be securely stored on the computing platform on which it has been designed, and access to the design information should be restricted to only authorized parties.

Unless such security measures are being followed in the distribution and supply chain of a proprietary product's CAD files, these files can be acquired by unauthorized parties, thus violating the confidentiality of the CAD model. It will then be possible for an unauthorized party to reproduce the product and put it on the market, compromising the business of the original producer of the product.

The translated CAD model information, such as the STL file and the slicer output, are especially prone to malicious attacks. Although various CAD programs could make use of their own proprietary CAD model file formats, the translated CAD model information is typically in a standard and non-proprietary format that can be interpreted by the digital interface of manufacturing platforms. It is therefore possible to intercept this information, either during the distribution phase, or in-line to the digital interface of the manufacturing hardware, and introduce malicious changes that could affect the structural integrity or the proper functioning of the end product. This would result in compromising the integrity of the CAD model, since adherence to the product's design specifications can no longer be guaranteed.

During all the phases from a product's design to its manufacturing, the relevant parties need to have access to this information. For example, two teams of engineers need to have access to a product's CAD model during the design phase to ensure that the product will fit within a certain space as part of a larger system designed by one engineering team, while the other engineering team ensures that any required changes to the product's CAD model remain within the limitations of the product's design. When the product needs to be manufactured, the translated CAD model information needs to be sent to a manufacturer. It is thus apparent that the availability of the product's information is a crucially important aspect throughout a product's design and manufacturing cycles. This influences the level and type of security measures that can be utilized to secure the product's design information, since an optimal balancing point between confidentiality, integrity and availability (CIA) is required to have a practical yet efficient security solution in terms of these three CIA pillars. Since the manufacturing equipment concerned can be classified under OT-type systems, it can be expected that the traditional IT security measures would possibly be insufficient or even incompatible to provide an effective security solution in this context, as has been discussed in Section 2.2.

3.4.5. The Human Element

Although the security of industrial manufacturing systems relies heavily on properly implemented security measures, there is always the human element that could pose an inherent threat. The Maroochy Shire sewage spill incident [2] is a classic example of how the human element can threaten the security of an entire industrial systems network. Such incidents could be the result of either negligence or ignorance by technical personnel during maintenance or production, in which case it is possible that proper security and technical policies and procedures were not being complied with. Conversely, activities of personnel driven by malicious motives are an equally dangerous threat to the industrial systems network. A person who has a motive to attack a system from the inside will typically have advanced insider knowledge and comprehension of how the system works, enabling such a person to perform a very effective and catastrophic attack. Therefore, the human element as a potential cyber security threat should never be overlooked.

4. Solutions

Having identified some of the security problems that the manufacturing industry faces, particularly in terms of Industry 4.0, solutions to these problems can now be formulated in order to produce countermeasures against the associated attack vectors. This is the area that will require the most innovation from researchers and security experts in order to develop security measures that are specifically tailored to the security needs of the next generation industrial manufacturing systems network. A lot of progress in this field has been made by researchers around the world thus far, although many of the proposed solutions and attack countermeasures are still in their infancy.

This section will explore some of the proposed solutions and the progress that has been made in research and development on this matter.

4.1. Securing the Manufacturing Information Architecture

4.1.1. Network Security and Information Flow

The digital manufacturing information architecture presents a large number of attack vectors, each unique in its own sense. Since the interception of manufacturing information occurs via the communications network, there are two possibilities for securing the information flow [8]. The first is to secure the entire network by routing all traffic through a single entity that interconnects all the relevant equipment in the manufacturing architecture, such as the case of a typical IT network architecture, for example with firewalls and intrusion detection software. Although this approach sounds plausible, there are a number of problems with it. The first is the fact that the digital manufacturing architecture consists of a combination of IT and OT devices. As discussed in Section 2.2, OT equipment typically does not have the same computing power as IT equipment. Therefore, any form of network management and security solution typically implemented in an IT environment would not be practical in a network with a combination of IT and OT equipment.

Although the computing capability of many embedded platforms utilized in OT equipment has increased significantly since the introduction of the first embedded platform OT equipment, it could still cause a bottleneck that would introduce intermittent delays or disruptions in the manufacturing process. OT equipment, particularly in the IIoT perspective, is generally not designed to have high throughput, since a bandwidth limitation is applicable. Therefore, most OT equipment in use today communicates over simple communication protocols, where relatively little information is transferred between platforms.

In many manufacturing processes where process timing is essential, an unexpected delay in the order of milliseconds could have a significant impact on the manufacturing process outcome [9]. It is therefore clear that any security measure that would introduce such a delay is not a viable solution in this context. Because of the constant evolution of malicious tactics used to compromise security networks, regular updates to the security software are required to ensure that a network remains protected against the latest forms of attack. In a typical IT infrastructure, this would involve a download of the latest security updates, and sometimes even a system reboot. Such a system reboot could result in unplanned down-time of machinery, which could hugely influence a manufacturing process. Such security updates would have to be scheduled well in advance to ensure that the impact on the production line is limited. This once again emphasizes the incompatibility of IT security measures used in an OT environment. A viable security solution would thus be one that considers system availability as the highest priority.

Another crucial aspect that must be considered when proposing a solution to the security problem in OT networks is that of the current infrastructure used by manufacturers. In contrast to the approach to building an IT network with IT equipment that can easily be replaced or upgraded as requirements change, manufacturing entities normally procure OT equipment with the focus on longevity and term robustness. Whereas some IT equipment could be replaced or upgraded within a five-year timeframe, OT equipment typically remains in service for much longer time frames, sometimes in the order of decades. The conclusion can then be drawn that much of the OT equipment currently in use by manufacturers could already be decades old. In such cases there is most probably much more advanced and sophisticated equipment available that would be ideal replacements for this old equipment. However, upgrading OT infrastructure with newer equipment is not as easy as installing a new printer and updating some drivers. Any change to the OT infrastructure would require extensive planning and thorough testing to ensure that the new equipment functions within the applicable control parameters, and that the process flow remains unaffected. The costs associated with upgrading OT equipment, including for transition redundancy, is also a weighted matter on its own.

If OT equipment in a manufacturing plant cannot be easily and regularly upgraded, and traditional IT network security solutions are not viable to OT applications, what viable solution could there then be to the aforementioned problems? The answer lies in a combination of the IT-based security mechanism that is tailored for OT applications, while adhering to the critical requirements of OT networks. A proposed solution to this problem [8] presents the concepts of a comptroller and a manufacturing security enforcement device (MSED) as a combined solution to the problem.

A comptroller would be a device running software that performs security tasks on the fly during information exchanges between IT and OT equipment. Such security tasks could be capturing the output data of one system meant as input data to another system, performing cryptographic processes such as authorization in the form of digital signatures and generating output data that can be sent to the destination equipment in encrypted format. An MSED would then be connected directly in-line and in front of any equipment that makes use of information sent over the network so that any information sent to the equipment can be cryptographically validated and the integrity thereof verified. The MSED will essentially perform decryption in real-time as data are received from the comptroller. Furthermore, it will perform any additional cryptographic authentication required to ensure that the data it receives are indeed authentic and valid. The MSED will thus be the final entity that sends commands to the destination equipment. Figure 7 illustrates the concept of a comptroller and MSED in an OT network.

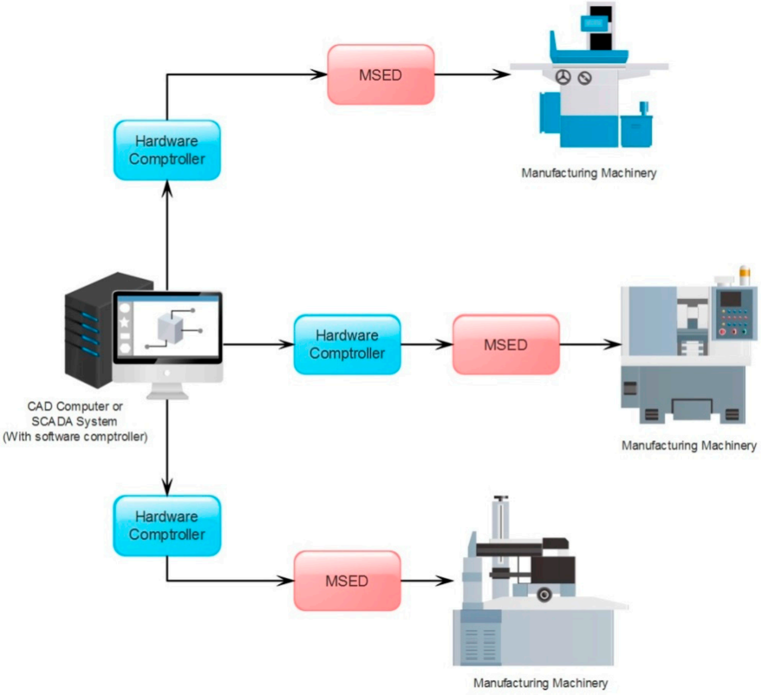

Figure 7. Comptroller within an industrial manufacturing environment. MSED: manufacturing security enforcement device

Any information sent to an MSED for verification will be discarded if its integrity cannot be verified. This would make it nearly impossible for an attacker to inject maliciously altered manufacturing information into the OT network destined for equipment to perform unauthorized actions. Although relatively simple in concept, the comptroller and MSED combination principle could essentially eliminate the problem of the malicious hacking of OT equipment.

4.1.2. Architectural Approach to System Design and Integration

As briefly introduced in Section 3.4.3, system safety is also of considerable concern in highly integrated and automated systems, particularly with respect to the risk of cyber-physical attacks compromising the safety of such equipment. In order to address this issue, the same basic approach for the inclusion of security measures can be applied to an inclusion of safety measures in the design of such systems.

Riel et al. [39,40] discuss an architectural approach to the integration of both security and safety aspects in automated and integrated systems. Although this approach also considers the inclusion of system safety in system design (which should be of equal importance in the broader perspective), it particularly introduces the concept of dividing the signal flow within a cyber-physical system into individual layers. These signals that pass through each layer can then be analyzed to determine the authenticity thereof. For example, when system commands must be executed, each layer can verify that the applicable signals are authentic, by making use of measurements from various interconnected sensors to determine if the combination of measurements is in accord with the signals received from interfacing subsystems.

The architectural approach for the integration of safety and security measures within an integrated system relies on layers of security being implemented in every subsequent subsystem to perform the localized (and unique) analysis of data, instead of relying on a single, all-inclusive security measure. This approach presents a considerable advantage, in that security measures can be enforced on multiple functional layers, providing a multi-layered security framework against cyber-attacks. For example, a cyber-attack could make use of a certain combination of known attack techniques to break an individual layer of security, but is prevented by a subsequent layer of security performing more rigorous analysis of data and signal flow. On the contrary, a single dedicated security measure could present a single point of failure in the system's security if it has been breached [39].

Another added benefit of dividing security measures in multiple layers is that a more robust overall security solution is obtained by providing localized protection against multiple attack vectors over the broader scope of the entire system. Furthermore, it is even possible to provide protection against attacks that are not yet known through rigorous and interleaved signal and data analysis that eventually block an attack due to, e.g., a combination of measurements that are not in accord with a certain combination of system commands.

4.1.3. Cryptographic Techniques

Finding widespread use within various IT networks, cryptographic techniques such as encryption algorithms, digital signatures, cryptographic hashing functions and key agreement protocols, have been very successful in securing these networks from various forms of cyber-attack. However, the industrial manufacturing industry has seen little to no presence of these techniques in manufacturing systems networks. This is mainly due to the fundamental differences between IT and OT systems and the underlying platforms, as discussed in Section 2.2.

Because of the limited processing power of some OT systems, either new cryptographic techniques must be developed, or existing techniques must be adapted to suit the needs and be compatible with the OT systems platforms. First and foremost, the cryptographic techniques must present security that is of sufficient strength to withstand and prevent cyber-attacks, while not inhibiting the core functionality of the platform/system itself. Since some cryptographic techniques require relatively high amounts of processing power, a fine balance must be maintained between the effectiveness of the implemented security measures and the efficiency of the actual process for which the system is designed.

Data that are transmitted between devices within a manufacturing systems network should ideally be encrypted with encryption algorithms that can reduce the effectiveness of cryptanalysis and attacks that are aimed specifically at breaking the encryption used in such communications. It is also crucially important that the initial configuration and setting up of cryptographic measures, such as the configuration and loading of cryptographic keys, be performed by trustworthy entities by means of processes and procedures that are specifically tailored to ensure that the security configuration of such systems is as secure as possible. Should any step in the security configuration of such systems be compromised, particularly in terms of configuring cryptographic parameters, the effectiveness of the entire security framework would immediately be reduced. If an attacker compromises a network system before or during a security configuration is performed, the attacker could gain access to sensitive security parameters that can be used to bypass these measures during an attack on the network. The use of strict access control mechanisms on these network systems that employ authentication and verification techniques, such as digital signatures, digital certificates and user key sets, can reduce the possibility of unauthorized access to the network and underlying systems. For example, security configuration updates and patches can be digitally signed in order to prove the authenticity of the files. A digital signature involves the use of a key pair consisting of a public key and a private key. The private key is used by the owner of the data to create a digital signature over the data. The data, along with the signature, are transmitted to the receiving party, who can verify the signature by means of the corresponding public key. If the signature cannot be verified, then the data are not authentic, and the source of the data is possibly compromised.

Security personnel can also be assigned digital certificates that need to be renewed regularly in order to ensure that the persons gaining access to such safety-critical systems are authorized to do so and are trustworthy [3,8]. Requiring multiple security personnel (instead of only a single person) to be present, and digitally verified to perform any maintenance on the systems, can also reduce the risk of a security breach. The use of secret sharing techniques, such as the Shamir secret sharing scheme [43], can be utilized very effectively in this context.

4.1.4. Security Policies and Procedures

The strongest digital security solution that can be implemented within a systems network can be rendered ineffective or even useless if there is no proper adherence to security policies and procedures. Historical analysis of cyber-attacks has shown that insider knowledge and leaked sensitive information were prominent contributing factors to the successful execution of many such attacks [2,8,33]. Strict adherence to security policies and procedures, in combination with strong and effective digital security measures within the systems network, should reduce the risk of both intentional and unintentional information leaks to a minimum. However, history has time and again demonstrated that an excess of security policies and procedures forced upon individuals in an industry, especially if these policies and procedures are poorly formulated, can result in non-compliance [3]. Care should thus be taken to formulate sensible and efficient security policies and procedures within an industry's security environment. Officially published security guidelines specifically aimed at securing the industrial manufacturing environment, such as NIST SP 800-82 [44] and IEC 62443 [45], can be used to aid in the formulation of these security policies and procedures [3].

The IEC 62443 in particular is a prominent standard that defines the cyber-security lifecycle as four major phases. The first phase concerns the identification and calculation of the associated security risks that the industry faces. Once the relevant risks have been identified, suitable countermeasures can be developed and implemented in the second phase. In the third phase the security measures are maintained and monitored for performance. Any cyber-security-related incidents are also responded to and logged during the third phase. The fourth phase concerns the continuous improvement of the implemented security measures, both in terms of the incidents that could have occurred, as well as keeping up with the latest trends and developments in cyber-security measures.

Industries can obtain different levels of IEC 62443 certification, ensuring adherence to internationally recognized cyber-security standards, which will provide peace of mind to both the industries themselves and their clients/stakeholders [45].

4.2. Efficient and Secure Scaling of Information Networks

As briefly discussed in Section 3.4.2, the requirement of scaling information networks in an industry can be complex, involving large costs. Care must be taken that the network-scaling solutions are the most cost-effective and efficient for the particular application. With the increasing adoption of IoT devices in the manufacturing sector, the predominant nature of the information network inevitably migrates towards wireless technologies. Current technologies that facilitate the wireless interconnection of manufacturing equipment and IoT devices include 2G/3G/4G, Bluetooth, ZigBee, SigFox and WiFi [8,9,46]. However, recent research and current developments in this domain propose and offer unique possibilities that could be implemented as highly effective and scalable solutions to the information network architecture while making provision for the necessary security measures.

4.2.1. 5G and the Internet of Things

One of the latest developments in wireless technologies and soon-to-be successor of the highly successful 4G and "long-term evolution" (LTE) technology is 5G. Although the current 4G LTE technology provides data transmission rates of up to 1 gigabit per second (Gbps), the technology is still relatively susceptible to disruptions due to interferences caused by other wireless signals and physical obstructions such as buildings [46]. The 5G technology will be able to transmit data at a rate of up to 10 Gbps, and will incorporate mechanisms that will provide even more reliable connections. Furthermore, 5G will provide a suitable platform to securely interconnect billions of IoT devices within a flexible networking architecture that is particularly suited for the interconnection of such a high number of devices [6].

However, since it is currently still under development, the standardization process for 5G is only expected to be completed by 2020, with worldwide full 5G capable networks expected to be active by 2025 [47]. The technology is thus still in its infancy, but existing early 5G networks that are already active present very promising features that will have a profound impact on IoT-driven networks. There is therefore no better time than now for developers and researchers to focus on developing new networking strategies and security measures that are fully compliant and compatible with 5G. This will result in networking and security technologies being developed that can immediately be incorporated into 5G networks, while collaboration with developers and vendors can provide the necessary exposure for end-users of these technologies to change the mindset of viewing network security as a secondary priority, thus eliminating a problem at its roots.

4.2.2. Software-Defined Networks and Network Function Virtualization

Section 3.4.2 briefly focused on the complex problem of information network scaling. The concept of a software-defined network (SDN) presents a unique and very promising solution to this complex networking problem. Where network control and data-forwarding functionalities are typically embedded within the same device for a conventional network, the concept of an SDN enables the possibility of decoupling network functionality from actual network infrastructure [6,48,49]. The main aspect of this network decoupling process is the abstraction of the underlying network infrastructure that interconnects network devices. This allows the entire network to be treated as a logical entity. The network intelligence and network control logic are contained in a central, software-defined network controller that forms the heart of the SDN. From within this software-based network controller, a global view of the interconnection of devices on the network is kept and maintained.

An SDN network can be divided into three main entities, namely the management plane, control plane and data plane [49]. This also introduces the concept of network function virtualization (NFV), where networking functions such as firewalls, switching and routing are separated from the rest of the network infrastructure [6,49]. The separation of a network into these three entities makes it possible to optimize the underlying functionalities of each of these entities. The entities make use of dedicated interfaces called the northbound, southbound, eastbound and westbound interfaces [49]. Figure 8 illustrates this network separation into the three main entities, and summarizes the architectural layout of an SDN:

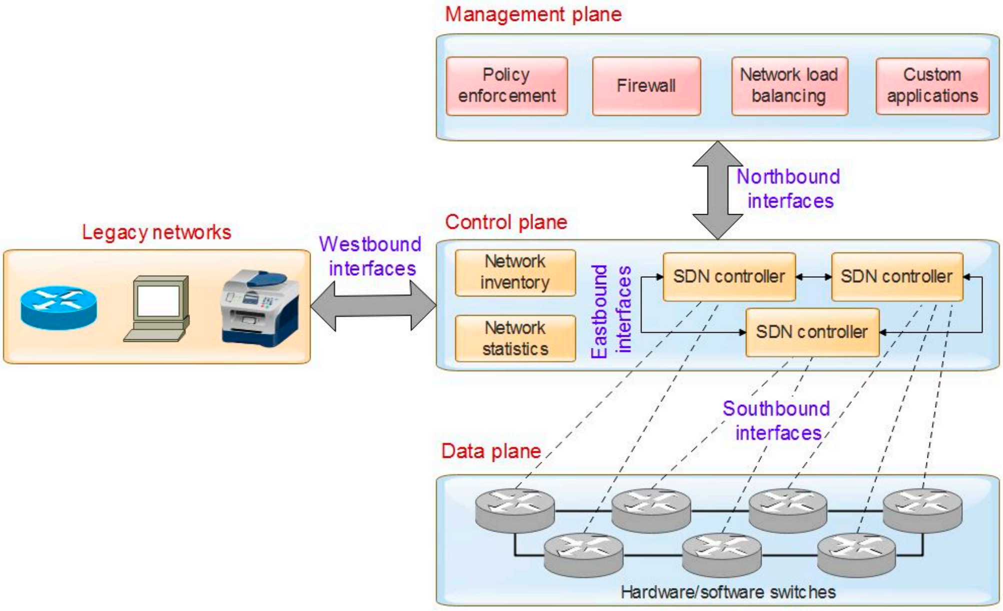

Figure 8. Network entity separation and software-defined network (SDN) architectural layout.

The management plane contains all the functionalities that manage the network. These management functionalities include tasks such as routing, firewalls and policy enforcement. Another important aspect that falls under the management plane is network load balancing. Since the network functionalities can be controlled in software, it is possible to balance the load on a network evenly within the available network infrastructure, which optimizes the efficiency of the network.

The data plane, also called the forwarding plane, mainly involves the forwarding of packets by interfacing with network switches (either hardware- or software-based) and other physical devices. Within the data plane, tasks such as packet header inspection and packet forwarding to controllers and network ports ensure that data will flow from the relevant data sources to the intended destinations. By matching packet headers to the installed flow tables, packets can be forwarded to the corresponding network devices present in the network. In the case of packets addressed to devices not contained in the flow tables, these packets can either be dropped or forwarded to a separate external network entity.

The control plane maintains a global view of the entire network, while acting as the main decoupling entity between the management and data planes. In the control plane, the data flow between the management and data planes is managed by means of software-controlled flow entries, while providing real-time statistics to the management plane to optimize the load on the network. Auditing and inventory tasks are also performed by the control plane to ensure optimal use of the available network resources. Interfacing with legacy networks is also managed from the control plane.

With network functionality no longer solely dependent on the layout of dedicated network equipment, IT personnel can dynamically (essentially in real-time) alter the network behavior and even add new network services and devices in a much shorter time than would be required on a conventional network.

Furthermore, the software-based nature of the network controller allows the network to be programmatically configured instead of hand-configuring multiple devices on the network. The advantages in terms of downtime and network maintenance that SDNs offer are clearly apparent.

As is the case with many other technologies that are adapted on a broad scale between multiple industries, the issue of standardization is always a key role player in the effectiveness and success of a particular technology. SDNs allow the use of standardized application programming interfaces and protocols to implement and connect to various networking services, such as routing, bandwidth management, access control and policy management, thus simplifying the overall maintenance task of the network while simultaneously optimizing network services. Network automation is another promising feature that SDNs can offer. By dynamically analyzing network traffic and the demand of network services, the network infrastructure and management of network services can be automatically adjusted in real-time in order to make optimal use of all the available network resources. As a consequence, the overall network complexity also reduces, since the functionality of many networking tools (both stand-alone and integrated) that require manual operation are now contained and managed within an automated network management platform. However, standardization of the communications protocol and processes will be a key determining factor in the efficiency of these automated network management platforms.

One example of such a standardized protocol is the OpenFlow protocol developed by the Open Networking Foundation. The OpenFlow protocol was the first standardized communications interface that allowed the direct control and manipulation of network devices and networking services within an SDN [48]. Currently, it is also the most commonly used protocol for SDNs in both the research and commercial sectors [49]. One great advantage that the OpenFlow protocol offers is its ability to be deployed within existing networks, both of a physical and virtual nature. IT personnel can thus progressively introduce OpenFlow-based technologies into existing industrial information networks, and can assess and become familiar with this new technology with minimal impact on the underlying processes. Other technologies such as forwarding and control element separation [50], open virtual switch database [51] and protocol oblivious forwarding [52] are also examples of SDN technologies that are currently being researched and developed.

The concept of the SDN can be extended further to the wireless domain as well. Software-defined wireless networks (SDWNs) utilize the concepts and core principles of SDNs together with wireless technologies to form a truly scalable and efficient network model [49]. SDWNs are ideally suited to IoT and IIoT applications, where multiple devices are wirelessly interconnected to form the various nodes in an industrial information network. The adoption of SDWNs will thus undoubtedly be of tremendous value to manufacturing industries that seek an efficient yet practical networking solution for equipment interconnectivity.

4.3. CAD Model Security

With cloud-based collaborative product development increasingly becoming the norm for many engineering design disciplines, security of proprietary technical information has become an important aspect considered by engineering design entities. In the context of CAD modeling and digital manufacturing, many engineering design entities face the challenge of securing certain aspects of their CAD models, while still making the rest of the CAD model available to other parties.

An innovative approach to the customized encryption of CAD models has been proposed [8], where product designers can divide a CAD model into separate features that can each be separately encrypted to protect proprietary sections of the CAD model. The technique also involves an algorithm for the geometric transformation of these sections in a "protected mode" that still enables the visualization of the features for collaboration purposes. This proposed approach will now be briefly introduced.

The first step of the proposed approach is to separate all the features in the CAD model into three categories: protected features, shared features and public features. Features classified as protected features contain critical parameters and proprietary information of the CAD model that cannot be shared with collaborators.

Thus, the owner of the CAD model has exclusive rights over these features. However, collaboration is still made possible by means of the geometrical transformation algorithm that presents the protected features in such a way that sensitive information and critical parameters are not visible to any collaborators. Shared features of the CAD model are features that are encrypted by the model owner, but can be decrypted by collaborators. Such features may contain confidential information that only collaborators are authorized to access, and should thus not be made available publicly. Features that are classified as public features do not contain any proprietary or confidential information of the CAD model. Such features are not geometrically transformed, since no sensitive parameters are contained in the public features. Similar CAD model encryption approaches are also being researched and developed in [46,53,54].

It has been demonstrated [13] how relatively easily a product can be compromised during its design stages. CAD model security approaches such as the aforementioned approach will play a key role in preventing 3D printed products from being compromised during the design stage.

4.4. Side-Channel Analysis

With the possibility that a cyber-physical attack can avoid detection within the systems network domain, the focus on industrial manufacturing security solutions should be extended to the side-channel domain. This involves the monitoring of the actual manufacturing process from an external perspective where the dynamic aspects of the manufacturing equipment are monitored and verified against an authentic and confirmed baseline. In this approach, it is possible to detect if a manufacturing process has been compromised if any step performed in the manufacturing process does not pass a verification test against the baseline. Production can then immediately be halted to investigate the deviation from the correct manufacturing procedure. This would prevent the complete manufacturing of products with compromised structural integrity, before such products enter the market if they somehow pass quality control during post-production inspections.

The approach of side-channel analysis will require the use of various types of sensors that are finely calibrated in order to provide the most accurate measurements possible to be used for verification. A three-level approach for detecting attacks by means of side-channel analysis is presented in [55]. The first aspect in this approach is to model an attacker in the context of the industrial systems network in order to determine the possible attack vectors that an attacker could exploit. With the possible attack vectors identified, it immediately becomes clear where special attention should be paid to the security and monitoring of the production/manufacturing process. The second aspect involves the modeling of the industrial processes with specific focus on the relationship between control signals and analog emissions (such as machine noise patterns, noise levels and even ambient temperature) by the industrial equipment. Attacks on the manufacturing systems network can then be detected if there is any deviation from the simulated model. Lastly, the relationship between analog emissions and control system parameters is analyzed to provide a measurement metric against which side-channel measurements can be measured.

Expanding on the work presented in [55], further research and development have been performed to formulate these side-channel analysis methods in [56]. According to the authors of [56], attacks that are only detected by means of side-channel analysis could be considered zero-day attacks, since there is a high probability that the attacker exploited a vulnerability unknown to security institutions. Therefore, side-channel analysis will play an important role in the detection and future prevention of cyber-physical attacks, since zero-day vulnerabilities could potentially be detected sooner during the attack lifecycle. However, some fundamental challenges are associated with side-channel analysis techniques. For example, experiments in [56] indicated that accelerometers used in spatial verification are prone to outputting very noisy data, resulting in low digital reconstruction resolution, making it difficult to inspect the real-time (and post-production) digital reconstruction of a manufactured product against a modeled baseline. There are thus some fundamental challenges that still need to be addressed in developing effective side-channel analysis solutions.

4.5. Post-Production Analysis

Structural weak spots introduced into a product during manufacturing by means of a cyber-physical attack could easily escape discovery during the manufacturing process. If proper post-production quality testing is not performed on products leaving the production line, there is a great risk that if a product has been structurally compromised, it can enter the market without ever being suspected of any compromised structural integrity. As has been demonstrated in [13], structural weak points that are maliciously introduced into a product's design can very easily evade detection by even the trained eye. There is thus a need for a unique approach to the post-production analysis of manufactured products.

The use of computed tomography, Raman spectroscopy and other similar material scanning techniques could easily detect any defects in manufactured products before they leave the production line [56]. The authors in [56] suggest a post-production verification technique where a series of markers that are easily detectable during material scanning are embedded into the product as an integral part of the product design. By determining the positions of these embedded markers within the manufactured product, a digital model can be generated based on the exact locations of these embedded markers against which the manufactured product can be verified. The introduction of such embedded markers also opens up the possibility for the detection of counterfeit products.

4.6. Further Research and Development

Although a number of novel and innovative approaches have been proposed to address the great number of possible cyber-physical attacks, a substantial amount of research and development still has to be performed to develop effective and reliable countermeasures against cyber-physical threats. Because of the constant evolution of industrial manufacturing systems, a continuous effort to keep in synchronization with the latest developments on the technological forefront is required by cyber security researchers and developers. This aspect will play a crucial role to ensure that industrial manufacturing systems networks are safe from cyber-physical attacks, since attackers are also constantly endeavoring to find and exploit the latest security vulnerabilities that have possibly not been detected by security institutions first.

5. Conclusions

The next generation of the industrial manufacturing sector born out of Industry 4.0 presents innovative and exciting new prospects in terms of manufacturing and technological advancement in general. Industry 4.0 opens the door to new, hyper-efficient manufacturing options that can be utilized by nearly any industry involved in some form of product design from anywhere in the world. Cloud-based design platforms present businesses with the opportunity for outsourcing product design work to external entities, enabling such businesses to concentrate their resources on more important tasks. Collaboration on a global scale via cloud-based services also stimulates innovative design practices and approaches that will present design institutions with a leading edge in their product offerings. Furthermore, the introduction of offsite manufacturing equipment that can be utilized only when needed eliminates the need to acquire expensive manufacturing equipment and high expenditure to develop the required infrastructure.

However, recently occurring cases have warned industries of the possible dangers and threats that they might face if proper security is not viewed in equal measure along with production efficiency and productivity. The development of innovative and next generation industrial manufacturing equipment and technologies that lack proper security measures as integral parts of the design presents an ever-increasing danger to industries aiming at adopting such technologies. Consequently, the evolution of a broad spectrum of unique cyber-physical attacks aimed at disrupting and possibly sabotaging industrial manufacturing entities is becoming the key interest and priority of prospective cyber-physical attackers. Therefore, a significant responsibility lies with research communities and security industries to join forces in order to develop solutions to fill the security gaps in this new and exciting emerging industry.

Despite the apparent dangers that ever-emerging and improving cyber-physical attacks hold for these industries, significant work has already been done to develop new technologies that are aimed, not only at keeping up with the demands of the various industries, but at addressing the apparent gaps in the associated security measures as well. Industries can then utilize a combination of the proposed solutions to ensure maximum effort being invested in securing their industrial manufacturing networks.

This article explored past cases of cyber-physical attacks to highlight the reality of cyber-attacks in the Industry 4.0 environment. These cases present a baseline that serves to create awareness to researchers and developers to take the security aspects of cyber-physical systems seriously. Aspects applicable to Industry 4.0, such as the manufacturing information network architecture, human-machine integration and global collaboration, are viewed in order to identify how these security risks (and future vulnerabilities) could manifest within industries embracing Industry 4.0. By identifying these risks as such, proactive steps can be taken to develop countermeasures against these and future possible forms of attacks. A number of proposed solutions to these forms of attacks are presented to serve as a guide and reference to complement extant literature on the topic, upon which future research and development can be performed to formulate solutions to the unique security problems faced in the Industry 4.0 environment.

Author Contributions: J.P. is the lead author and played a significant research role. S.S. leads the fourth industrial revolution research strategy for the University of Johannesburg and therefore identified the research problem, i.e., the mapping of the successes and “failures” of the internet to cyber-physical environments. B.v.S., a member of the World Economic Forum (WEF) Global Future Council on Cybersecurity, provided oversight to the work and in relation to an international approach.

Funding: This article was partially supported through the National Research Foundation grant, UID 118969. This is a rated-researcher grant to Prof. Saurabh Sinha and was used for direct human-resource related support.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhang, Z.; Demir, K.G.; Gu, G.X. Developments in 4D-printing: A Review on Current Smart Materials, Technologies, and Applications. *Int. J. Smart Nano Mater.* **2019**, *10*, 205–224. [CrossRef]
2. Sayfayn, N.; Madnick, S. *Cybersafety Analysis of the Maroochy Shire Sewage Spill*; MIT Management Sloan School: Cambridge, UK, 2017.
3. Tuptuk, N.; Hailes, S. Security of Smart Manufacturing Systems. *J. Manuf. Syst.* **2018**, *47*, 93–106. [CrossRef]
4. SHODAN Website. Available online: https://www.shodan.io/ (accessed on 25 May 2019).
5. Van der Meulen, R. Gartner Says 8.4 Billion Connected ”Things” Will Be in Use in 2017, Up 31 Percent From 2016. Available online: https://www.gartner.com/newsroom/id/3598917 (accessed on 26 September 2019).
6. Jacob, E.; Astorga, J.; Galan, J.J.U.; Huarte, M.; Conejo, D.G.; De Marcaide, L.N.L. *Towards a 5G Compliant and Flexible Connected Manufacturing Facility*; DYNA: Federación Asociaciones Ingenieros Industriales: Bilbao, Spain, 2018.
7. Chang, J.; He, J.; Mao, M.; Zhou, W.; Lei, Q.; Li, X.; Li, D.; Chua, C.K.; Zhao, X. Advanced Material Strategies for Next-Generation Additive Manufacturing. *Materials* **2018**, *11*, 166. [CrossRef] [PubMed]
8. Thames, L.; Schaefer, D. *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing*; Springer: Cham, Switzerland, 2017.
9. Gilchrist, A. *Industry 4.0: The Industrial Internet of Things*; Apress Media: Berkeley, CA, USA, 2016.
10. NASA Office of Inspector General. *Industrial Control System Security within NASA’s Critical and Supporting Infrastructure*; NASA: Washington, DC, USA, 2017.
11. Zeltmann, S.E.; Gupta, N.; Tsoutsos, N.G.; Maniatakos, M.; Rajendran, J.; Karri, R. Manufacturing and Security Challenges in 3D Printing. *JOM J. Miner. Met. Mater. Soc.* **2016**, *68*, 1872–1881. [CrossRef]

12. 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).
13. 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.
14. WinRAR 4.20 ZIP File Name Spoofing Vulnerability. Available online: https://www.rarlab.com/vuln_zip_spoofing_4.20.html (accessed on 29 May 2019).
15. Birkel, H.S.; Veile, J.W.; Müller, J.M.; Hartmann, E.; Voigt, K.-I. Development of a Risk Framework for Industry 4.0 in the Context of Sustainability for Established Manufacturers. *Sustainability* **2019**, *11*, 384. [CrossRef]
16. 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.
17. Kiel, D.; Arnold, C.; Müller, J.M.; Voigt, K.-I. Sustainable Industrial Value Creation: Benefits and Challenges of Industry 4.0. *Int. J. Innov. Manag.* **2017**, *21*, 1740015. [CrossRef]
18. Müller, J.M.; Kiel, D.; Voigt, K.I. What Drivers the Implementation of Industry 4.0? The Role of Opportunities and Challenges in the Context of Sustainability. *Sustainability* **2018**, *10*, 247. [CrossRef]
19. Yan, J.; Meng, Y.; Lu, L.; Li, L. Industrial Big Data in an Industry 4.0 Environment: Challenges, Schemes and Applications for Predictive Maintenance. *IEEE Access* **2017**, *5*. [CrossRef]
20. 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.
21. Liao, Y.; Deschamps, F.; De Freitas Rocha Loures, F.; Pierin Ramos, L.F. Past, Present and Future of Industry 4.0—A Systematic Literature Review and Research Agenda Proposal. *Int. J. Prod. Res.* **2017**, *55*, 3609–3629. [CrossRef]
22. Elkington, J. Partnerships from cannibals with forks: The triple bottom line of 21st-century business. *Environ. Qual. Manag.* **1998**, *8*. [CrossRef]
23. Norman, W.; MacDonald, C.; Arnold, D.G. Getting to the Bottom of "Triple Bottom Line". *Bus. Ethics Q.* **2004**, *14*, 243–262. [CrossRef]
24. Roberts, P.F. Zotob, PnP Worms Slam 13 DaimlerChrysler Plants. Available online: https://www.eweek.com/security/zotob-pnp-worms-slam-13-daimlerchrysler-plants (accessed on 29 May 2019).
25. W32.Zotob.E. Available online: https://www.symantec.com/security-center/writeup/2005-081615-4443-99 (accessed on 29 May 2019).
26. Microsoft Security Bulletin MS05-039—Critical. Available online: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2005/ms05-039 (accessed on 29 May 2019).
27. Falliere, N.; Murchu, L.O.; Chien, E. *W32.Stuxnet Dossier*; Symantec Security Response: Cupertino, CA, USA, 2011.
28. Microsoft Security Bulletin MS10-046—Critical. Available online: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-046 (accessed on 16 October 2019).
29. Symantec. *W32.Duqu: The Precursor to the Next Stuxnet*; Symantec Security Response: Mountain View, CA, USA, 2011.
30. Nahorney, B. *Symantec Intelligence Report: May 2012*; Symantec Intelligence: Mountain View, CA, USA, 2012.
31. Miková, T. Cyber Attack on Ukrainian Power Grid. Bachelor's Thesis, Masaryk University, Brno, Czech Republic, 2018.
32. Bilge, L.; Dumitras, T. *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World*; Symantec Research Laboraties: Raleigh, CA, USA, 2012.
33. Symantec. *An ISTR Special Report: Ransomware and Businesses 2016*; Symantec: Mountain View, CA, USA, 2016.
34. Song, C.; Lin, F.; Ba, Z.J.; Ren, K.; Zhou, C.; Xu, W.Y. My Smartphone Knows What You Print: Exploring Smartphone-based Side-channel Attacks against 3D Printers. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016.

35. Hojjati, A.; Adhikari, A.; Struckmann, K.; Chou, E.; Tho, N.; Thi, N.; Madan, K.; Winslett, M.S.; Gunter, C.A.; King, W.P. Leave Your Phone at the Door: Side Channels that Reveal Factory Floor Secrets. In Proceedings of the 2016 ACM SIGSAC Conference, Vienna, Austria, 24–28 October 2016.
36. Backes, M.; Durmuth, M.; Gerling, S.; Pinkal, M.; Sporleder, C. Acoustic Side-Channel Attacks on Printers. In Proceedings of the 19th USENIX Security Symposium, Washington, DC, USA, 11–13 August 2010.
37. Faruque, M.A.A.; Chhetri, S.R.; Canedo, A.; Wan, J. Acoustic Side-Channel Attacks on Additive Manufacturing Systems. In Proceedings of the 7th International Conference on Cyber-Physical Systems, Vienna, Austria, 11–14 April 2016.
38. Yampolskiy, M.; Andel, T.R.; Mcdonald, J.T.; Glisson, W.; Yasinsac, A. Intellectual Property Protection in Additive Layer Manufacturing: Requirements for Secure Outsourcing. In Proceedings of the 4th Program Protection and Reverse Engineering Workshop, New Orleans, LA, USA, 9 December 2014.
39. Riel, A.; Kreiner, C.; Macher, G.; Messnarz, R. Integrated design for tackling safety and security challenges of smart products and digital manufacturing. *CIRP Ann.* **2017**, *66*, 177–180. [CrossRef]
40. Riel, A.; Kreiner, C.; Messnarz., R.; Alexander, M. An architectural approach to the integration of safety and security requirements in smart products and systems design. *CIRP Ann.* **2018**, *67*, 173–176. [CrossRef]
41. National Defense Industrial Association. *Cybersecurity for Advanced Manufacturing White Paper*; National Defense Industrial Association: Arlington, WV, USA, 2014.
42. Pham, G.N. Two-Dimensional (2D) Slices Encryption-Based Security Solution for Three-Dimensional (3D) Printing Industry. *Safe Secur. Embed. Syst.* **2018**, *7*, 64. [CrossRef]
43. Shamir, A. *How to Share a Secret*; Communications of the ACM: Cambridge, MA, USA, 1979; pp. 612–613.
44. Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A. *Guide to Industrial Control Systems (ICS) Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014.
45. DesRuisseaux, D. *Cybersecurity Assessment—The Most Critical Step to Secure an Industrial Control System*; Schneider Electric: Andover, MA, USA, 2018.
46. Li, S.; Xu, L.D.; Zhao, S. 5G Internet of Things: A Survey. *J. Ind. Inf. Integr.* **2019**, *10*, 1–9. [CrossRef]
47. GSA. *The Road to 5G: Drivers, Applications, Requirements and Technical Development*; Global Mobile Suppliers Association: Farnham, UK, 2015.
48. ONF. *Software-Defined Networking: The New Norm for Networks*; Open Networking Foundation: Palo Alto, CA, USA, 2012.
49. Latif, Z.; Sharif, K.; Li, F.; Karim, M.M.; Wang, Y. A Comprehensive Survey of Interface Protocols for Software Defined Networks. *arXiv* **2019**, arXiv:1902.07913v1.
50. Haleplidis, E.; Salim, J.H.; Halpern, J.M.; Hares, S.; Pentikousis, K.; Ogawa, K.; Wang, W.; Denazis, S.; Koufopavlou, O. Network Programmability with Forces. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1423–1440. [CrossRef]
51. Ben, P.; Bruce, D. The Open Switch Database Management Protocol. Internet Engineering Task Force, RFC 7047. December 2013. Available online: http://www.ietf.org/rfc/rfc7047.txt (accessed on 5 October 2019).
52. Song, H. Protocol-oblivious Forwarding: Unleash the Power of SDN through a Future-proof Forwarding Plane. In Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, Hong Kong, China, 16 August 2013.
53. Éluard, M.; Maetz, Y.; Doërr, G. Geometry-preserving Encryption for 3D Meshes. In Proceedings of the IEEE International Conference on Image Processing, Paris, France, 27–30 October 2014.
54. Pham, G.N.; Kwon, K.-R.; Lee, E.-J.; Lee, S.-H. Selective Encryption Algorithm for 3D Printing Model Based on Clustering and DCT Domain. *J. Comput. Sci. Eng.* **2017**, *11*, 152–159. [CrossRef]
55. Chhetri, S.R.; Canedo, A.; Al Faruque, M.A. KCAD: Kinetic Cyber-Attack Detection Method for Cyber-Physical Additive Manufacturing Systems. In Proceedings of the 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Austin, TX, USA, 7–10 November 2016.
56. Bayens, C.; Le, T.; Garcia, L.; Beyah, R.; Javanmard, M.; Zonouz, S. See No Evil, Hear No Evil, Feel No Evil, Print No Evil? Malicious Fill Pattern Detection in Additive Manufacturing. In Proceedings of the USENIX Security Symposium, Vancouver, BC, Canada, 16–18 August 2017.