systems

MDPI

Article

The Smart Factory and Its Risks

Frank Herrmann

OTH Regensburg, Innovation and Competence Centre for Production Logistics and Factory Planning, P.O. Box 120327, 93025 Regensburg, Germany; Frank.Herrmann@OTH-Regensburg.de; Tel.: +49-941-943-7185; Fax: +49-941-943-1426

Received: 10 October 2018; Accepted: 24 October 2018; Published: 26 October 2018

Abstract: In this paper, the risks of a Smart Factory are to be examined and structured in order to be able to evaluate the status of the Smart Factory. This thesis thus serves as an overview of the technical components of a Smart Factory and the associated risks. The study takes a holistic view of the smart factory. The results show that the greatest need for action lies in the technological field. Thus, the topics of standardization, information security, availability of IT infrastructure, availability of fast internet and complex systems were prioritized. The organizational and financial risks, which also play an important role in a Smart Factory transformation, are addressed.

Keywords: industry 4.0; smart factory; risks

1. Introduction

To meet customer expectations in these days, there is a need for a more flexible production, even with lot size of 1. To achieve these objectives, a new level of automation should be achieved, by the introduction of methods of self-optimization, self-configuration, self-diagnosis, cognition and intelligent support of workers in their increasingly complex work. This is summarized by "smart factory", and especially in Germany by Industry 4.0. In a typical traditional factory, providing high-end quality service or product with the least cost is the key to success and industrial factories are trying to achieve as much performance as possible to increase their profit as well as their reputation. In contrast, in an Industry 4.0 factory, in addition to condition monitoring and fault diagnosis, components and systems are able to gain self-awareness and self-predictiveness, which will provide management with more insight on the status of the factory. Furthermore, peer-to-peer comparison and fusion of health information from various components provides a precise health prediction in component and system levels and force factory management to trigger required maintenance at the best possible time to reach just-in-time maintenance and gain near-zero downtime. There are many papers about smart factory available: overview papers as well as scientific papers. This one extends the overview papers by summarizing and evaluating the risks of a smart factory reported in various papers. It might raise the awareness of this manufacturing trend, mainly for practitioners.

The remainder of this paper is structured as follows. First, smart factory and Industry 4.0, respectively, are introduced. Next, the technologies within a Smart Factory are explained. In Section 4, the risks to these technologies are listed and analysed, based on a literature review. Finally, some conclusions are given.

2. Smart Factory—Industry 4.0

In the past, the steam engine, the assembly line and the computer brought profound economic changes, see Figure 1. Now we are facing the next major industrial transformation, the so-called 4th Industrial Revolution or, in short, Industry 4.0.

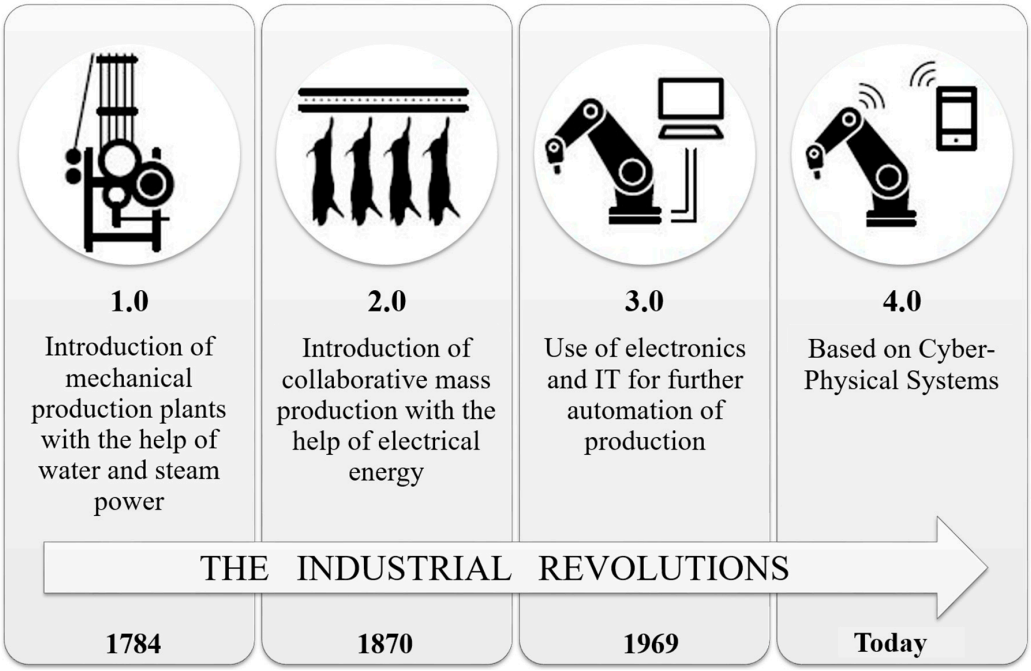

Figure 1. Industrial revolutions as an overview; own illustration.

The idea of the fourth industrial revolution is to integrate production with the latest information and communication technologies. This makes it possible to manufacture products according to individual customer requirements and to produce them in a batch size of one at the price of mass-produced goods. The technical basis is formed by intelligent, digitally networked systems and production processes. Furthermore, Industry 4.0 determines the entire life phase of a product. It deals with the idea, the development, the production, the use and the maintenance up to the recycling of the product [1].

All four levels of revolution have one thing in common. They all have an impact on economic and social life and also increase productivity and create changes in work processes and working conditions. For industrial employees, this means a higher qualification requirement. These changes must also be expected in the forthcoming fourth revolution [2–4].

German companies have to face the challenges of Industry 4.0 and the transition of production to a networked operation. If this does not succeed, there is a risk that German companies will lose their economic ties [5].

If, however, current figures from Industry 4.0 for Germany are considered, a positive development towards Industry 4.0 can be seen. According to [1], annual investments of 40 billion euros in Industry 4.0 applications are planned up to 2020. Additional economic growth of over 153 billion euros is also expected by 2020. Also by 2020, 83% of German companies see a high degree of digitalization in their value chain. Currently, 20% of German companies already use autonomous systems [1].

A completely new type of economic production is created by the stronger, internal as well as external networking. This poses major challenges for German and global companies, as Industry 4.0 affects all dimensions, such as technology, organization, people and business models [5].

In order to be able to examine the risks and challenges for companies in Industry 4.0 more closely, the modern production environment must first be described with the current state of the art.

3. Technologies within a Smart Factory

The Smart Factory is at the heart of Industry 4.0 [6]. Basically, the Smart Factory is about networking machines and systems by means of software, so that intelligent communication with each other is made possible and the work steps can be automatically coordinated with each other. In

order to achieve this, basic technologies must be used. The technological requirements are explained in this section [7].

To demonstrate the technical requirements of a Smart Factory [6], the Cyber-Physical Systems (CPS), which form the basis of a Smart Factory, must first be described [8]. The key term CPS first appeared in the USA in 2006. Systems are given the suffix "cyber" if they are used for the discrete processing of information and for communication. In addition, the real systems are referred to as "physical". This means that the CPS are autonomous and can configure and extend themselves independently [9,10]. Another key feature of the CPS is that they can connect via open and global information networks such as the Internet. This allows systems to connect arbitrarily, change, terminate and rebuild their connections during operation. It is possible to provide and use available data, information, and services anywhere in the CPS [11,12]. CPS can be objects, products, devices, buildings, production facilities or logistics components that contain embedded systems [8].

Embedded systems are microprocessors or small computers. They are a central topic in the realization of CPS. By combining hardware and software components, the corresponding system is controlled, regulated or monitored. With the help of this technology, the flexible and intelligent systems described above are created [9,10,13].

The embedded systems are equipped with sensors and actuators. The production data are recorded via sensors. The collected data is evaluated and stored with available data and services. Through the use of actuators, a CPS has the possibility of physically influencing its environment [8]. The CPS communicates via the internet or intranet. You can use internet services and/or offer them yourself.

The term Internet of Things (IoT) was first used in 1999. The classic internet has been extensively expanded. As a result, the virtual and real world are melting more and more together through the networking of and with everyday objects. Physical objects (things) become uniquely identifiable, receive a virtual representation and can communicate via the internet [9,10,13]. Communication takes place via open and global information platforms. Services and data are used and made available via these networks. Such services are referred to in the literature as the Internet of Things and Services (IoTS). The vision of adaptive and flexible production systems that configure themselves and partly organize themselves arises [11,12].

Cyber-Physical Production Systems (CPPS) are required within a production environment to control intelligent production plants. The task of the CPPS is to coordinate the individual CPS and to control the changes in production [5]. With the help of this platform, the three different types of the internet can be linked together. On the human internet, people stay in contact through social networks. Furthermore, there is the Internet of Things (IoT) and the Internet of Things and Services (IoTS) described above [8].

Even if the goal of the Smart Factory [6] is a networked, self-organized production environment, the human being must not be missing in this scenario. People must continue to be at the center of attention, although their field of activity will change significantly. People mainly have to carry out controlling activities, while the operational tasks take a back seat. To carry out these activities, the human being must be connected to the CPS via a multimodal interface, also known as a human-machine interface (HMI) [5]. For example, a CPS can be controlled via voice or touch displays. In the future, people will be able to act accordingly by means of gestures [8]. Mobile devices integrate people directly into the communication network of the Smart Factory [7]. Suitable mobile devices are tablets or smartphones, making the intuitive use of these devices result in an ease of use for employees. The keyword Augmented Reality (AR) serves as an aid for the production employee. Augmented Reality represents the real world with additional information from the virtual world. The displayed information is displayed in the correct size and position. This new technology is used in Smart Glasses or in data gloves that are connected to the backend system [5].

In the context of CPS, machine-to-machine communication (M2M communication) must also be mentioned. Here not only the human being can communicate with the machine, but the machine

can independently come into contact with other machines or tools. With this solution, machine and production data can be recorded and forwarded in real time [7].

The real-time processing of information is also called Real Time Enterprise (RTE) and is a central element within a Smart Factory. The information should always be available to the user immediately. The keyword Big Data plays an important role in the processing of large amounts of data [5].

Big data is often referred to as the "raw material of the 21st century". The basic prerequisite here is the collection, storage, filtering, analysis, compression and visualization of large amounts of data. Both structured and unstructured data can be used. The main task is to identify patterns and causalities. With the correct use of Big Data, it becomes clear that the more data there is, the more meaningful it becomes.

Technically, Big Data systems can be based on Not Only SQL (NoSQL) databases or on a Hadoop framework. Hadoop is an open source framework for storing large amounts of data on distributed systems. Another big data system is the in-memory database. This is used for rapid evaluations. Here, the RAM of a computer serves as data memory. SAP SE is one of the best-known in-memory database providers [5].

Accepted standards and interfaces must be used to enable common networking and communication between different environments and object types. To this end, the internet protocol IPv6 was introduced in 2012. Using the IPv6 protocol, a sufficient number of addresses are available for resources, information, objects and people in a Smart Factory. This results in an area-wide networking [2–4].

Cloud computing solutions are an important component of a Smart Factory. Here a needs-oriented and flexible use of different IT benefits is offered via the Internet in the form of services. In a cloud approach, data or services are generally outsourced to an internal or external service provider [5]. The billing of such services is always usage-dependent. Three service elements can be differentiated. Infrastructure-as-a-Service (IaaS) is the supply of computing, storage and network capacity through a cloud provider. The Platform-as-a-Service (PaaS) service element provides the user with a development environment in the form of a technical framework via an internet provider. These are standardized environments. They simplify and accelerate software development by eliminating the need to implement the offered environment. Software-as-a-Service (SaaS) provides standardized application services via a cloud and can be used by end users [14].

The above definitions make it clear that production in the sense of a Smart Factory cannot take place without automation. Automation accelerates and optimizes production processes. This is done by transferring the production process functions to artificial systems. An automatic machine is a machine that executes certain previously defined processes either autonomously or automatically. Depending on the degree of automation, it is referred to as partial or full automation. In the area of the Smart Factory, full automation is required. This means that rigid and recurring production processes are not completely passed on to machines. In a Smart Factory, processes with different tasks are executed by flexible manufacturing systems [9,10,13].

The sensitive robots are regarded as the epitome of automation and are closely linked to the topics of CPS and M2M communication. A sensitive robot is equipped with sensitive joint sensors to perform activities in conjunction with human colleagues. Within a Smart Factory, the robots move freely and are not separated from humans by grid fences. The close cooperation relieves the human being of physically heavy work or supports him in ergonomically unfavorable activities [5].

Digital product memory is a product to be manufactured with an automatically readable data carrier that helps to achieve a fully decentralized production environment. Thus, the products themselves become information carriers. The relevant data is passed on to the processing machines independently of the server systems. Digital product memory is a decisive step for autonomous, decentralized production and for individualized products. It enables continuous product documentation throughout the entire product life cycle. The product data can be read out at any time

and faulty components can be identified immediately in case of problems. Digital product memory enables optimal resource optimization [2–4].

In the context of flexible and efficient production, the new technology of the 3D printer must be mentioned. This technology enables additive manufacturing processes. Additive in this environment means the creation of a component by adding a material layer by layer. The desired object is created layer by layer on the basis of a 3D model from the desired materials. The advantages over conventional production are enormous. Small series can be produced economically and profitably and the production of difficult components is facilitated. Another positive aspect is the minimization of material usage and the elimination of production steps. The production environment of the Smart Factory can be implemented and designed more simply and flexibly with the help of this new technology [5].

Robust networks are significant in a Smart Factory. High availability of cable and radio networks is essential for the CPS to be able to communicate with each other. The challenge of the abundance of data and the associated high data transfer rate must not be underestimated. To overcome this problem, broadband networks are used. Wireless LANs (Local Area Network) play a special role so that the mobility of robots and machines can be guaranteed. There is still a need for development in the area of radio networks [2–4].

This section shows the complex environment of a Smart Factory and draws attention to the high technical requirements. Figure 2 is used to classify terms within a Smart Factory. Some of these technologies already exist and some are still in development. Nevertheless, the technologies and methods mentioned have not yet been used to the desired extent and interplay. IT plays a central role in the implementation of cooperation between the individual technologies. It provides the necessary networking and architectures. Only through the correct use of IT all these components can be controlled. Due to the increasing networking of technologies, many risks arise and require new concepts and mechanisms in companies. The risks that can occur are explained in the section "Risks within a Smart Factory".

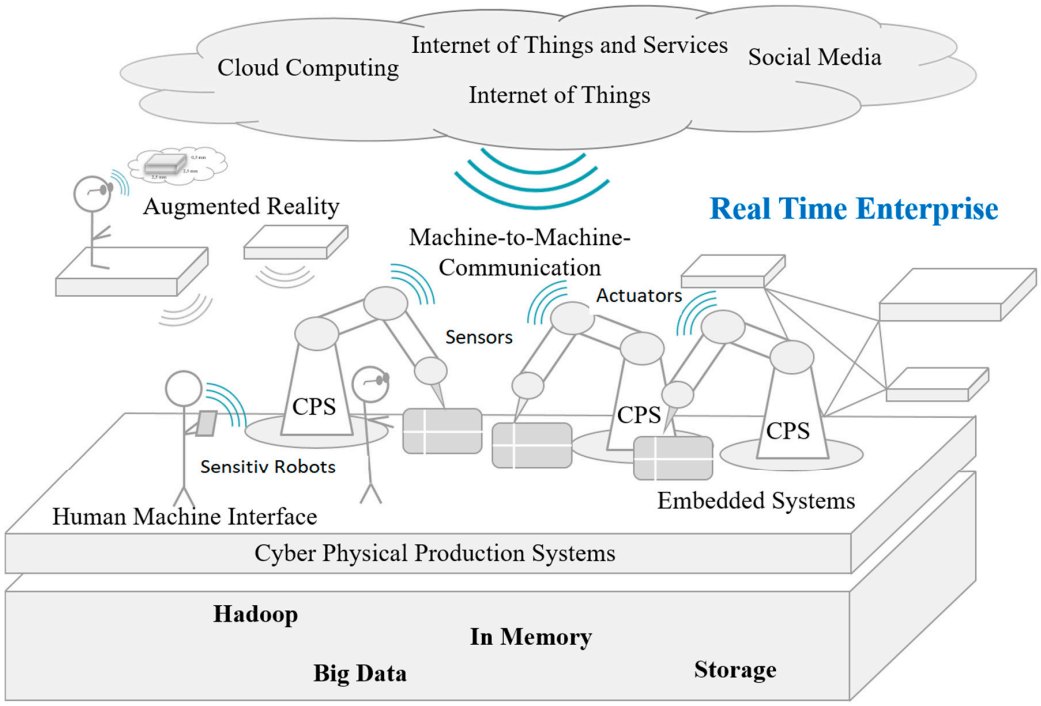

Figure 2. Terminology within a Smart Factory; own illustration.

4. Risks within a Smart Factory

As Industry 4.0 takes shape, more and more risks are emerging in addition to the many advantages. It is essential to examine these more closely in order to subsequently evaluate the status of the Smart

Factory. Due to the fact that Industry 4.0 is a highly technologically driven topic, the technological risks are examined more closely. Since this topic is very extensive, the focus is on the topics of standardization, information security, availability of the IT infrastructure, availability of fast Internet and complex systems. The organizational and economic risks are only briefly discussed for completeness.

4.1. Standardization

The implementation of Industry 4.0 means the use of many IT systems implemented by different companies. These IT systems needs to be connected. This is still a very difficult and time consuming task. Standardisation might substantially simplify this task. This enables a large number of network partners to work together efficiently and thus exploit the full economic potential of Industry 4.0. For the most part, the supplying companies are adapting to the standards of the larger companies, which has the consequence that the possibilities for action of the smaller companies are inhibited. Similarly, too high capital expenditures are incurred when companies rely on technologies that are not future-oriented [15]. A reference architecture model for Industry 4.0 (RAMI 4.0) was developed to realize a Smart Factory and provide a basis for standardization [7]. This was presented for the first time at the Hanover Fair 2015 and defined jointly by the industrial associations Bitkom, VDMA and ZVEI [16]. On the basis of the model a common understanding is to be created, which standards, use cases, and norms are necessary for a Smart Factory. The aim of the reference architecture model is to use as few standards as possible and to create a clear and simple architectural model as a reference [17].

RAMI 4.0 [16,17] consists of a three-dimensional coordinate system, which is shown in Figure 3. Basically, its main features are based on the Smart Grid Architecture Model (SGAM), because this enables a good initial approach to presenting the Industry 4.0 situation: It deals with the power grid from generation through transmission and distribution to the consumer. Industry 4.0 focuses on product development and production scenarios. This means that it must be described how development processes, production lines, manufacturing machines, field devices and the products themselves are or function. In order to be able to describe machines as well as components and factories better, the component layer of SGAM has been replaced by an asset layer, inserted into the model as the lower layer and then added to the integration layer. This layer allows the assets to be digitized for virtual representation. The Communication Layer deals with protocols and transmission of data and files, the Information Layer contains the relevant data, the Functional Layer contains all necessary (formally described) functions and the Business Layer contains the relevant business process. This division corresponds to the IT way of thinking when clustering complex projects into manageable subunits.

The third axis of RAMI 4.0 describes the functional classification of a situation within Industry 4.0. This is not about implementation, it is solely about functional classifications. For classification within a factory, the reference architecture model for this axis is based on the IEC 62264 and IEC 61512 standards. The terms “Enterprise“, “Work Unit“, “Station“ und “Control Device“ were used from the options listed there to provide a uniform view across as many industries as possible from process industry to factory automation. The “Field Device“ has also been added. It represents the functional level of an intelligent field device, for example an intelligent sensor. Since the product to be manufactured itself is also important for the considerations, it was also listed as a “Product“. In addition, an addition was made at the top end of the hierarchy levels. The two standards mentioned represent only the levels within a factory. Industry 4.0 also describes the factory network, cooperation with external engineering offices, suppliers and customers, etc. This aspect is taken into account in the “Connected World”.

The approach also allows the meaningful encapsulation of functionalities. Thus the prerequisites are created to describe and realize highly flexible concepts by means of the reference architecture model. The model allows step-by-step migration from the current world to the Industry 4.0 world and the definition of application domains with special specifications and requirements. This reference architecture model RAMI 4.0 has now been standardized as DIN SPEC 91345.

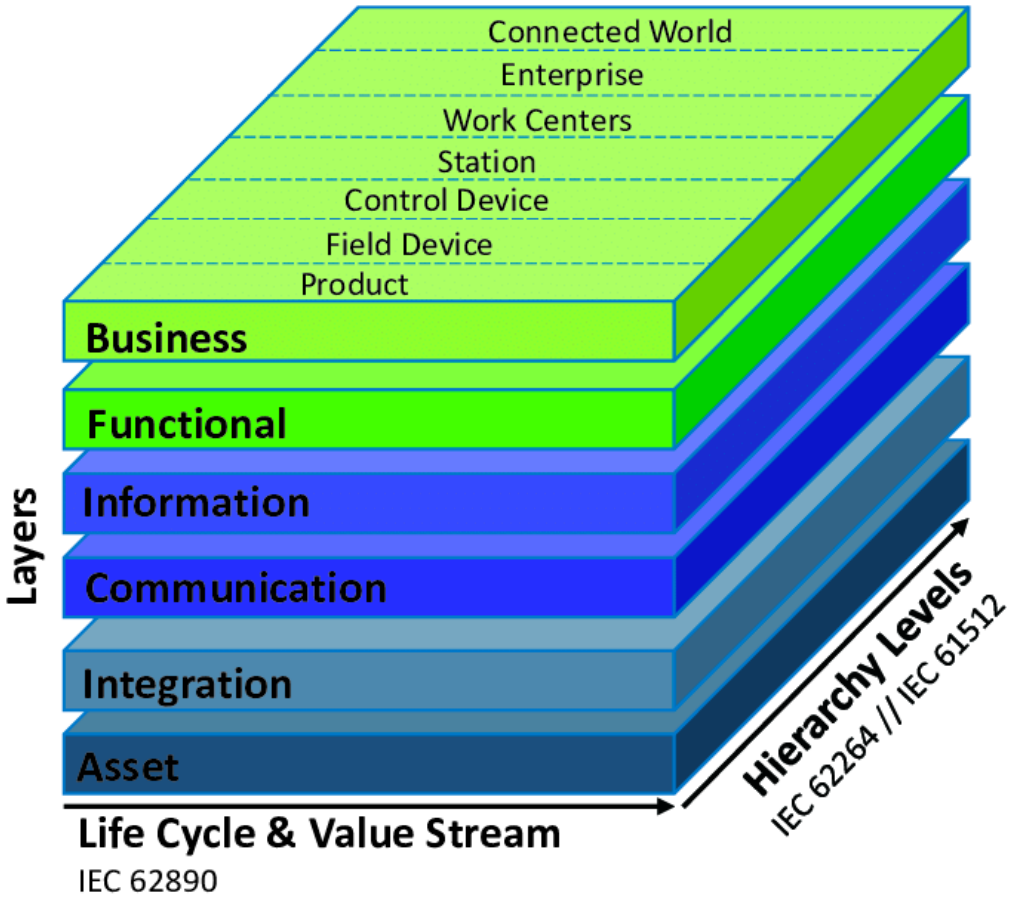

Figure 3. RAMI 4.0; own illustration.

The hardware and software components in production become Industry 4.0-compatible when they implement the communication capability of the asset with the respective information and functions. An important prerequisite for this is that Industry 4.0 components collect and carry data in a secure electronic container throughout their lifecycle. The electronic container can also be described as an administration shell. All relevant data of a hardware or software component is stored in the administration shell and together form a virtual image. This creates new opportunities for networked production and provides added value for all those involved in the value chain process.

Open Platform Communications Unified Architecture, OPC UA for short, is a fundamental prerequisite for communication along the value chain. This communication protocol was developed for M2M and PC-to-machine communication and was introduced in 2006 as the standard protocol in the Industry 4.0. OPC UA can transmit machine data and also semantically describe it in machine-readable form. This distinguishes OPC UA from conventional communication protocols [18].

These examples for a need on the subject of "standardization" give just small insights and can be seen as the beginning of the implementation of a networked Smart Factory. There is an urgent need to develop international standards and norms in the near future, making use of existing technologies and interfaces.

4.2. Information Security

One of the biggest technical risks within a Smart Factory is information security. In recent years, cyber-attacks against companies and private individuals have increased steadily [19–21]. Due to the lack of data protection and data security, cyber attacks cause high financial damages—various very serious damages can occur and their effects should be expressed by a financial loss. The spread of new business models and the use of cloud solutions are also hampered by the emerging threats [2–4].

The CPS-based production systems create new information security requirements because they have a high degree of networking. They are networked with a large number of machines, IT systems, and automation components involved. The technical system components operate partly autonomously with a time-critical data and information exchange, whereby several parties along the value chain are involved at the same time. It can therefore be said that the topic of Industry 4.0 throws up a completely new perspective on the field of information security [18].

Basically, the topic of information security can be divided into two areas. On the one hand, the topic of operational safety and on the other hand, the topic of attack safety must be considered. When it comes to health and safety, machines, production systems, workpieces, and products must at no time be a hazard to people. Functional safety and high reliability are prerequisites for operational safety. Ensuring these conditions proves to be complex, as there are high demands on distributed IT architectures in a production. The plants in production are expected to run for several years without interruption.

The second area is information security. Information security protects data and services in systems against misuse, unauthorized access, modification, and destruction. The goal of information security is to increase confidentiality and integrity, and, most important, the availability of systems and applications [7], therefore, there is an additional section for this.

In order for the concept of Industry 4.0 to be realized and implemented, all relevant safety risk areas must be considered. These include production and manufacturing with its embedded systems, big data, cloud computing and mobile solutions. This shows that new forms of cooperation are emerging and that new, at least adapted information security concepts are required.

Possible dangers in the Industry 4.0 area are the infection by means of malware via the internet or Intranet and external hardware. In addition to targeted attacks, companies must also arm themselves against unintentional problems, such as human error, sabotage and espionage. Furthermore, remote maintenance accesses, the use of mobile devices and Distributed Fenial of Service (DDoS) represent further risks within a modern production environment [5]. DDoS attacks are a threat difficult to protect for any externally accessible interface. Many requests are made to a recipient, so that the servers and networks are overloaded and legitimate requests can no longer be processed [22].

Another threat scenario goes hand in hand with the targeted standardization of plants and machinery. Information about systems and their specifications will be available on the Internet worldwide and will, therefore, be easily manipulable [5].

The protection of personal data is another important aspect. Due to the strong networking of processes and digitalization, great attention must be paid to this topic [5].

The BYOD (Bring your own Device) approach also involves many threats. In 2013, approximately 23% of employees in German companies used their own mobile devices for corporate purposes. This trend results in cost savings for the companies, as the acquisition costs for mobile devices are eliminated. Employees are already familiar with their mobile device, which can increase employee satisfaction. Last but not least, the location-independent work brings more flexibility and productivity into the daily work routine of the employees. In addition to the advantages, many dangers can also be pointed out. A comprehensive control cannot take place and is only based on the trust shown in the employees, who must adhere to the agreed guidelines. Furthermore, personal and company data is stored on each mobile device [23]. With the help of the central management platform MDM (Mobile Device Management) and EMM (Enterprise Mobile Management), mobile devices with additional tracking and reporting can be integrated into the company infrastructure. The MDM system must perform data encryption of data carriers as standard in order to guarantee the information security of end devices [5]. Company related software and applications for mobile devices are already being developed to support companies [23].

To ensure production stability within a Smart Factory, the automation networks must be segmented. The automation networks are divided into small cells between which firewalls take control [5]. It makes sense to use firewalls with Deep Packet Inspection (DPI) capability for

business-critical devices. DPI checks special commands or requests to determine whether they may or may not pass through the firewall. This prevents unauthorized access to production objects [24]. In principle, however, the well-known measures should not be forgotten, such as cameras, card readers, organizational measures and password control. Positive lists are also a simple protection against uncontrolled access. Here you determine on which computer which processes, programs or operations may run. Another approach to increasing information security is the so-called Security by Design, i.e., software has been designed from the foundation to be secure, and the so-called Security by Default which means that the default configuration settings are the most secure settings possible, which are not necessarily the most user friendly settings. It is beneficial to take certain safety aspects into account during product development. It is often not sufficient to add security functions to CPS-based production systems at a later date [5].

Using the Security by Design approach, the platform-independent and globally recognized OPC UA (Unified Architecture) communication protocol was developed (see section "Standardization"). This results in a secure networking of the production processes and represents a central module on the way to Industry 4.0 [22].

Many approaches to introducing suitable information security measures come from the Federal Office for Information Security (BSI). The BSI deals with many information security topics, most of which, however, are still in the development phase. Basic IT protection, the ICS Security Compendium (Industrial Control Systems) and LARIS ICS can be named as main topics for the BSI. Basic information security is the most widely used standard for information security in Germany and is currently undergoing a modernization process. The ICS Security Compendium contains the basics of information security and the relevant norms and standards. It also includes best practices and recommendations on cyber security for plant operators. The LARIS ICS software, on the other hand, is structured as a tool that includes a questionnaire and recommendations for further measures. The tool contributes to the development of comprehensive information security management in companies.

The information security experience in industrial companies can currently be assessed as rather low. For this reason, the BSI must go through further development and optimization phases in order to make the entry into industrial information security as easy as possible for companies [25]. Nevertheless, information security remains an individual task for each individual company. These must set themselves the goal of designing a system with inherent information security. However, it should be noted that there are still many open construction sites in the field of information security and that many approaches are not yet ready for productive use [5].

4.3. Availability of the IT Infrastructure

Another challenge in the Industry 4.0 environment is the availability of the IT infrastructure. The increased use of software and networked machines and systems increases companies' dependence on a powerful, scalable and available IT infrastructure [19–21]. For this reason, IT must create a modern and virtualized IT landscape. This can be made possible with the help of standardization and consolidation of IT systems. Furthermore, all components and systems in the company must be networked and the availability of consistent data must be guaranteed. In order to meet these requirements, the classical automation pyramid must be broken down [7].

Communication in companies is currently reflected in the hierarchical system of the automation pyramid. The goal of the automation pyramid is to minimize the complexity of industrial production. This is achieved by classifying the company processes into the individual levels. The different levels are each supported by different systems [26,27]. Support is provided at the company management Zurawski level by means of the Enterprise Resource Planning (ERP) software and is used as an information system in all areas of a company for business activities. Furthermore, the Manufacturing Execution System (MES) software is used at the operational management level and is familiar with the tasks of production control, steering, and monitoring. This includes the production control level at which short-term production planning takes place. This is done with the help of systems such as the

Supervisory Control and Data Acquisition (SCADA) system. Meanwhile, the control and regulation systems, such as the so-called Programmable Logic Controller (PLC), are located at the control level. In this level, the signals are evaluated by the shop level and further processed and returned to the shop level. The shop level is equipped with sensors and actuators and supplies production-relevant data to the higher levels [27]. The described situation is shown in Figure 4.

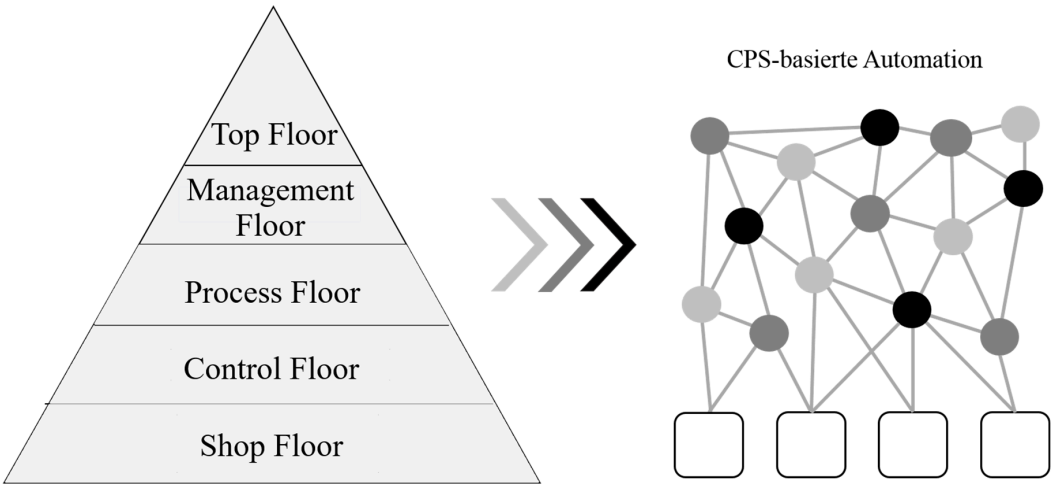

Figure 4. Traditional automation pyramid and CPS-based automation; own illustration.

Nowadays, communication still takes place hierarchically via a few interfaces between the individual levels. For this reason, the view and control of the levels are usually still isolated [8]. The step towards comprehensive networking is currently hardly completed in the field of automation technology. Very large amounts of information about production resources, products and processes are already available in companies' IT systems. Likewise, companies usually have a large number of IT systems and machines next to each other, which have only limited networking or which do not permit data migration due to different semantics [8]. The isolation of information sources causes media disruptions. It can be stated that the benefit of information interpretation in a concrete application can only be achieved when different subsystems are integrated [8]. In addition, there is the problem that the systems, machines, and plants are usually purchased from different manufacturers and have a different age. For these reasons, retooling the automation software is very time-consuming in order to achieve the required compatibility. Another challenge is to establish the data flow to adjacent internal and external areas [15]. An ideal result is only achieved when the rigid hierarchical automation pyramid is resolved. However, this does not imply the complete disappearance of systems at different levels. The focus here is rather on a seamless connection between the levels to a network structure. In order to achieve this goal, time and financial integration efforts must be made [26,27]. In the area of integration, the flexible connectivity and disconnectivity of the individual components, the technical programming effort and the information security of the distributed information are considered. So-called middleware systems are used for the application-specific distribution of information and bring together information from various source systems. These are made available via uniform interfaces in technology-independent form for interpretation systems. If the initial structure of such a communication architecture is considered from the point of view of the investments to be made, this represents the greatest effort. Once the basic architecture has been implemented, additional data sources or interpretation systems can be connected to the existing infrastructure with manageable effort. On the other hand, the identification of the data to be exchanged, the implementation of the connection to data sources and the interpretation systems currently represent the greatest effort in the technical implementation of applications. Current projects, such as the research project Cy-ProS (Cyber-Physical Production Systems), are researching components that decisively accelerate the feasibility of such architectures [8].

In principle, national and international coordination is required with regard to standards for communication between the individual hardware and software applications. Therefore, companies must be advised against in-house developments, as international standards are required for an available and secure IT structure [26,27]. It will take some time before the automation pyramid can be resolved and an available IT infrastructure can be set up.

4.4. Availability of Fast Internet

An equally important issue is the availability of fast internet. With regard to the expansion and availability of broadband networks, Germany is at the bottom of the international rankings. But especially in the age of Industry 4.0 and digitalization, the "Always on" state is an absolute must [19–21]. A comprehensive use of CPS requires an infrastructure that enables a better and higher quality data exchange. In order to implement low latency, high reliability, high quality and a comprehensive broadband network, existing communication networks must be expanded [18]. The International Telecommunication Unit (ITU) defines a transmission rate of two megabits per second as a broadband connection. This specified transmission speed is not sufficient to organize production across companies and on the internet or to define downstream services. For this reason, stable high-performance transmission paths via fiber optic cables are necessary. Another argument in favor of pushing ahead with the fiber optic expansion is that, given the current state of the art, there is no alternative. A Smart Factory cannot be implemented without fiber optic cables, making the expansion of the broadband connection indispensable [15].

The Federal German Government [28], recognizes the urgent need for a fast internet and reacts with support programs, laws and strategies. The federal government's goal is for all households to have access to fast internet with a transmission rate of at least 50 megabits per second by 2018. The government is also committed to establishing a nationwide broadband network by 2025 to connect commercial and industrial areas and harbors to the fiber optic network. The publicly accessible areas of the commercial and industrial areas will also be equipped with free WLAN (Wireless Local Area Network). The law "Gesetz zur Erleichterung des Ausbau digitaler Hochgeschwindigkeitsnetze" (DigiNetwork Act) was passed by the German government in 2016 and promotes broadband expansion in areas not yet developed. By means of the DigiNetwork Act, fiber optic cables will always be laid in the future when new residential and commercial areas are developed.

There are also some new developments in mobile communications technology. By 2015, Germany had already made 700 MHz frequencies available for mobile communications, establishing itself as a European pioneer. However, a new generation of mobile radio, called the 5G network standard, is currently being developed. With this new technology, data volumes can be reliably transmitted at up to 20 GB/s. For these reasons, the Federal Government developed the "5G Strategy Germany". The 5th generation of mobile radio will thus become a key digital technology in the age of networking and enable a multitude of new business models, such as autonomous and networked driving and Industry 4.0. 5G technology will be ready for the market by 2020, according to the German Government [28].

4.5. Complex Systems

The next problem associated with Industry 4.0 is the increasing complexity within a Smart Factory. Due to the technological developments in recent decades, the complexity of products and systems has already grown very strongly. As a result, the complexity of industrial development and manufacturing processes is also increasing considerably. The development and production of the products, therefore, seem less and less manageable [29].

It has already become clear in the past that too high levels of IT and automation are not a panacea. The newly introduced technologies can no longer be adequately controlled and companies are becoming increasingly inflexible [19–21]. This is referred to the Computer Integrated Manufacturing (CIM) approach, which was adopted in the 1980s. Starting with the planning up to the production a full automation should take place. The approach failed because the necessary technologies were

not available or were unaffordable at that time. An overbred and overpriced production was created, which was difficult to control. Due to the complex problems and lack of economic viability, the approach was not continued at this time [8].

Over time, the performance of the technologies improved, as did the skills of the developers. At the present time, engineers in the middle of Europe are in a good position because they are very good at combining embedded software with a wide variety of industrial products. Some companies combine software and electronics with mechanics better than others and thus secure a place at the top of the world market. This advantage is based on the experience accumulated in the industry over the past decades. But it becomes clear that the lead is not secured in the long term. However, the conditions are very good for maintaining or even expanding this. Industry must adapt skills, methods, processes and business models to the challenges of networked and software-controlled systems. If this process of change is successful, a global competitive advantage can arise. In addition to high quality, durability and environmental compatibility, European products and systems would also score points for safety, as future cooperation between many specialist disciplines in the development and construction of the systems will take place. This cooperation enables complex systems to run smoothly and processes to be designed as simply as possible. In addition, the engineers learn to control the complexity of a Smart Factory. Understanding the interplay of the various disciplines within a modern production environment is fundamental to this. The engineers must succeed in transferring the simple operation of today's mobile devices to the processes and products of industrial development and production. This process is often referred to as simplicity [29].

4.6. Organizational Risks

In general, the topic of the Smart Factory is almost exclusively about the introduction of new technologies. However, organizational risks must also be considered. If the organizational changes caused by Industry 4.0 are not taken into account, this leads to considerable problems, reduced potentials, and delays in the implementation of Industry 4.0 [19–21].

The company organization plays an important role especially at the highest hierarchy level [30,31]. Management must define a clear strategy and plan for digitalization and demonstrate an understanding of IT and processes. Furthermore, organizational models must be found that enable cooperation without hierarchical boundaries and ensure a communication between all participants. In order for employees to be prepared for the new tasks in a Smart Factory, management must carry out active change management [7]. But often this is not used. As a result, the acceptance of new technologies among the workforce and employee satisfaction is decreasing [7]. Therefore, change management must be used for the development of competencies and the qualification of employees in companies [30,31].

The new Industry 4.0 technologies are changing the work processes and requirements for apprenticeships and job profiles in production. Due to digitalization, more and more skilled workers are needed in production, whereby the demand for unskilled or even trained employees is decreasing. Currently, many employees are not able to use the new technologies and understand the new processes. Lifelong learning, changes in work organization, team composition, and knowledge management will therefore still play a major role in the future [7].

4.7. Financial Risks

In addition to technical and organizational risks, economic risks must also be considered. Several challenges have to be taken into account. The first obstacle is a lack of willingness to invest. Investments in the Industry 4.0 environment are currently still rather low. The biggest problem is the lack of transparency of economic added value. Already today, the mechanical and plant engineering industries have to consider what requirements the products will have to meet in the future. Basically, it can be seen that companies have long recognized and perceived the relevance of Industry 4.0 investments across all sectors [2–4]. Companies must provide the necessary funds for investments and resources so

that a Smart Factory can be implemented. Studies show an annual investment of 40 billion euros in Industry 4.0 applications in Germany [7].

Another risk is the loss of jobs within a Smart Factory. Simple production work is replaced by digitalization. However, the goal of introducing a Smart Factory should be to increase automation and reduce costs and not to reduce the number of jobs [19–21]. The introduction of a Smart Factory requires the flexible deployment of personnel. There are already strong fluctuations in personnel demand. In the future, these fluctuations will be even greater. The demands on the production employee with regard to qualification also change [2–4]. The academic professions, such as mathematics, computer science, natural sciences, and technology, must be further promoted in order to meet the high demand in the economy as well as the non-academic professions of mechatronics and automation technology. Trainers must increase the skills of trainees in the areas of Industry 4.0 technologies. Internal training and further education ensure that the production employees are at the cutting edge of technology [15]. The introduction of the Smart Factory encourages employees to organize themselves and thus assume more personal responsibility [2–4].

Subsequently, the loss of some business areas can be identified as an economic risk. The new market players are throwing out established manufacturers, such as bookstores and publishing houses. So-called start-ups open up new paths for manufacturers. Furthermore, the lack of support for research is a major obstacle. Germany is making a good investment in research and funding. Nevertheless, countries such as China and Japan invest more in research and development than Germany [19–21].

The economic risks identified indicate that without consideration of the issues, no competitive and networked production environment can emerge.

5. Conclusions and Outlook

This paper gives the reader a structured overview of the risks that can occur in a Smart Factory. Different risks are considered in the areas of technology, organization, and economy. A closer examination of the various risk areas makes it clear that there is still a need for action in many areas. Particularly in the technical areas, companies are dependent on federal aid, for example, to drive forward the digitalization of the economy.

The Industry 4.0 implementation is not only successful with the help of the German government but also requires the support of companies. It is necessary that the companies and their management are sensitized to the topic of Smart Factory and digitalization and perceive the urgency for a change in the production. If this is not taken into account by German companies, Germany's competitiveness will decline in the coming years. An adjustment of the production employees within the Smart Factory is also required.

Since the 4th Industrial Revolution is only just beginning and there is still the possibility of clearly identifying the emerging risks, appropriate countermeasures can thus be taken. In this way, Industry 4.0 topics can be successfully implemented and the emerging potentials exploited.

Not all risks of a networked production environment could be addressed. Likewise, not all risks were presented in detail and in full. This paper describes certain risks that have been classified as relevant. Since this topic is very topical and is still in the development phase, the investigations must be pushed parallel to the development progress. For this reason, further research in this area is necessary and recommended to provide a complete overview of the Smart Factory and its status.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. *Industrie 4.0*; Federal Ministry of Economy and Energy: Berlin, Germany, 2018; Available online: https://www.bmwi.de/Redaktion/EN/Dossier/industrie-40.html (accessed on 3 September 2018).
2. Oliver, K.; Roland, H.; Dao, D.-K. Studie Industrie 4.0—Eine Standortbestimmung der Automobil-und Fertigungsindustrie. Hg. v. Mieschke Hofmann und Partner (MHP). 2014. Available online: https://www.mhp.com/fileadmin/mhp.de/assets/studien/MHP-Studie_Industrie4.0_V1.0.pdf (accessed on 3 September 2018).
3. Alp, U.; Emre, C. *Industry 4.0: Managing the Digital Transformation*; Springer Series in Advanced Manufacturing; Springer: New York, NY, USA, 2017.
4. Wessel, S.J.; Erlend, A.; Jan Ola, S.; Reed, V.L. *The Fit of Industry 4.0 Applications in Manufacturing Logistics—A Multiple Case Study*; Norwegian University: Trondheim, Norway, 2017.
5. Alur, R. *Principles of Cyber-Physical Systems*; The MIT Press: Philadelphia, PA, USA, 2015.
6. Möller, D.P.F. *Guide to Computing Fundamentals in Cyber-Physical Systems: Concepts, Design Methods, and Applications (Computer Communications and Networks)*; Springer: Bagalore, India, 2016.
7. Holtkamp, B.; Iyer, A. *Industry 4.0—The Future of Indo-German Industrial Collaboration*; Bertelsmann Stiftung: Gütersloh, Germany, 2017.
8. Mabkhot, M.M.; Al-Ahmari, A.M.; Salah, B.; Alkhalefah, H. Requirements of the Smart Factory System: A Survey and Perspective. *Machines* **2018**, *6*, 23. [CrossRef]
9. Herbert, L. *Digital Transformation: Build Your Organization's Future for the Innovation Age*, 1st ed.; Bloomsbury Business: London, UK, 2017.
10. Bauernhansl, T.; Hompel, M.T.; Vogel-Heuser, B. *Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien, Migration*; Springer Vieweg: Wiesbaden, Germany, 2014.
11. Lee, J.; Lapira, E.; Bagheri, B.; Kao, H.-A. Recent advances and trends in predictive manufacturing systems in big data environment. *Manuf. Lett.* **2013**, *1*, 38–41. [CrossRef]
12. Lee, J.; Lapira, E.; Bagheri, B.; Kao, H.-A. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 8–23. [CrossRef]
13. Mauerer, J. Was ist was bei Industrie 4.0? 2016. Available online: http://www.computerwoche.de/a/was-ist-was-bei-industrie-4-0,3313199 (accessed on 3 October 2018).
14. Buyya, R.; Broberg, J.; Goscinski, A.M. *Cloud Computing. Principles and Paradigms*; John Wiley & Sons: Hoboken, NJ, USA, 2010.
15. Schröder, C. The Challenges of Industry 4.0 for Small and Medium-Sized Enterprises. Available online: http://library.fes.de/pdf-files/wiso/12683.pdf (accessed on 21 September 2018).
16. Hankel, M.; Rexroth, B. The Reference Architectural Model Industrie 4.0 (RAMI 4.0). Available online: https://www.zvei.org/fileadmin/user_upload/Themen/Industrie_4.0/Das_Referenzarchitekturmodell_RAMI_4.0_und_die_Industrie_4.0-Komponente/pdf/ZVEI-Industrie-40-RAMI-40-English.pdf (accessed on 21 September 2018).
17. Zehl, S. Implementation Strategy Industrie 4.0—Report on the results of the Industrie 4.0 Platform. Available online: https://www.bitkom.org/NP-Themen/Branchen/Industrie-40/20160107-implementation-strategy-industrie40-en.pdf (accessed on 3 September 2018).
18. Kagermann, H.; Wahlster, W.; Helbig, J. *Recommendations for Implementing the Strategic Initiative Industrie 4.0: Final Report of the Industrie 4.0 Working Group*; ACATECH: Munich, Germany, 2013.
19. Huber, W. Industrie 4.0 und die Risiken. Available online: https://www.computerwoche.de/a/industrie-4-0-und-die-risiken,3324008 (accessed on 12 September 2018).
20. Tupa, J.; Simota, J.; Steiner, F. Aspects of risk management implementation for Industry 4.0. In Proceedings to the 27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, Modena, Italy, 27–30 June 2017; Volume 11, pp. 1223–1230.
21. Schwab, K. *The Fourth Industrial Revolution*; World Economic Forum: Cologny, Switzerland, 2017.
22. Federal Office for Security in Information Technology. Report on the State of IT Security 2017. Available online: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2017.pdf?__blob=publicationFile&v=3 (accessed on 3 September 2018).
23. Morrow, B. BYOD security challenges: Control and protect your most sensitive data. *Netw. Secur.* **2012**, 5–8. [CrossRef]

24. Parvata, T.J.; Chandra, P. A Novel Approach to Deep Packet Inspection for Intrusion Detection. *Procedia Comput. Sci.* **2015**, *45*, 506–513. [CrossRef]
25. Wittkop, J. *Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices*, 1st ed.; Apress: Boulder, CO, USA, 2016.
26. Zurawski, R. *Integration Technologies for Industrial Automated Systems*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2016.
27. Manesis, S.; Nikolakopoulos, G. *Introduction to Industrial Automation*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2018.
28. Federal Government. From the Digital towards the Gigabit Society. Available online: https://www.bmvi.de/SharedDocs/EN/Dossier/broadband/broadband.html (accessed on 3 September 2018).
29. Dori, D. *Model-Based Systems Engineering with OPM and SysML*; Springer: Cambridge, MA, USA, 2016.
30. Gronau, N.; Ullrich, A.; Teichmann, M. Development of the Industrial IoT Competences in the Areas of Organization, Process, and Interaction based on the Learning Factory Concept. In Proceedings of the 7th Conference on Learning Factories, CLF, Darmstadt, Germany, 4–5 April 2017.
31. Zezulka, F.; Marcon, P.; Vesely, I.; Sajdl, O. Industry 4.0—An Introduction in the phenomenon. *IFAC PapersOnLine* **2016**, *49*, 8–12. [CrossRef]

© 2018 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).