WHITEPAPER

How the Industrial Internet of Things is changing the Automation landscape

How the Industrial Internet of Things is changing the Automation landscape

***Vasileios Boutlas**, Industrial IoT specialist,*
FORCE Technology Digital (vasb@forcetechnology.com)

Contents

Table of Figures

Executive Summary

"Industrie 4.0" or the fourth industrial revolution can be better described as a political vision than a new technical paradigm and it is basically the movement towards achieving a complete overview and control over the entire production process (Schütze, Helwig, & Schneider, 2018). The Industry 4.0 (I4.0) agenda includes many technologies, such as AR/VR, digital twins, cloud computing, big data analytics, but their functionality principles and the nature of their business potential rely heavily on the availability of data. Internet of the Things (IoT) can offer the infrastructure that satisfies the generation and collection of data paving the way for the transition towards a digital supply chain. The role of IoT as the transparency enabling technology makes it the technology backbone of the industrial digital transformation towards I4.0 (Colli, 2020).

The global market size for the Industrial Internet of Things (IIoT), i.e. the application of IoT in industrial settings was 263.52 billion USD in 2021 and is estimated to reach a compound annual growth rate (CAGR) of 23.1% in the year range 2022-2030 (Grand View Research, 2021). This shows that the benefits of IIoT are clear for the companies, as the interest in adopting such technologies is going to rise exponentially.

The application of IIoT enables transparency across factories and the entire supply chain, paving the way for better decision-making and for entirely new business models. IIoT is also a key factor in improving the sustainability of industries through monitoring important environmental indicators such as energy consumption and CO_2 emissions to achieve the UN sustainable development goals (Kamalakkannan & Kulatunga, 2021).

This white paper is aimed at production and engineering managers, or specialists in production companies, who are interested in getting a general understanding of the application of IoT in the industrial environment from a technical and infrastructural standpoint. Specifically, it is shown how IIoT is changing the information structure of organizations, the challenges that arise through this process and potential ways to meet these challenges.

A genuine approach is to think of all the various levels that the IIoT integration can occur, whether in siloed projects, or as part of a holistic strategy for maximizing the benefit of I4.0 adoption.

- **Field Level**: Use of smart sensors for complete supply chain overview
- **Control Level**: IIoT- enabled controllers for adapting to I4.0 standards
- **Supervisory Level**: Supervisory Control and Data Acquisition (SCADA) systems combined with IIoT platforms for full-scale interoperability
- **Operations and Business Level**: Connection with shop floor to deliver real-time analytical insights

There are many challenges that organizations will face on the way to become a full I4.0 enterprise. To assist the industry in overcoming the existing issues huge efforts are made from many companies, which offer valuable products and services by utilizing state-of-the-art technologies. Production companies should have a deep understanding of the problems, but also continuously gain knowledge of the available solutions to remain competitive in the market.

- **Connectivity Reliability**: Time-Sensitive Networking (TSN) in Wired and Wireless communications
- **Lack of Alignment between Operational Technology (OT) and Information Technology (IT):** Convergence of IT and OT departments through collaborative projects
- **OT cybersecurity:** Risk management and compliance to new standards
- **Non-central data architecture:** Concept of the Unified Namespace (UNS)

Abstract

Through the last years, the industrial sector has evolved to a great extent, machines and equipment have become extremely efficient and various processes have been automated and optimized. However, there are technologies where we have only scratched the surface and would lead to even further optimization of monitoring and control of industrial processes. I4.0 describes the current revolution that the industry is undergoing, which involves a variety of technologies that lead to achieving the “smart factory” by enabling changes at all levels of the automation pyramid that current production processes are built on top of to improve productivity and flexibility. Most of these technologies rely heavily on data generation and collection, which makes IIoT the foundation of I4.0. This paper presents an overview of how the IIoT can be integrated in the different layers of the automation pyramid, the challenges that arise during this process as well as how the companies can utilize existing or emerging technologies to face these challenges.

Introduction

Road to Industry 4.0

The industry is currently undergoing its fourth revolution. The third industrial revolution introduced automation, which created data. I4.0 is the movement to translate data into information. This is paving the way for introducing a high level of autonomy by utilizing smart decision-making through advanced physical or statistical modelling to achieve self-adaptation, self-diagnosis, and self-healing. This is truly relevant for the companies, as the conventional systems are unable to adapt to the highly increasing complexity and dynamic of the production environment (Park & Tran, 2014).

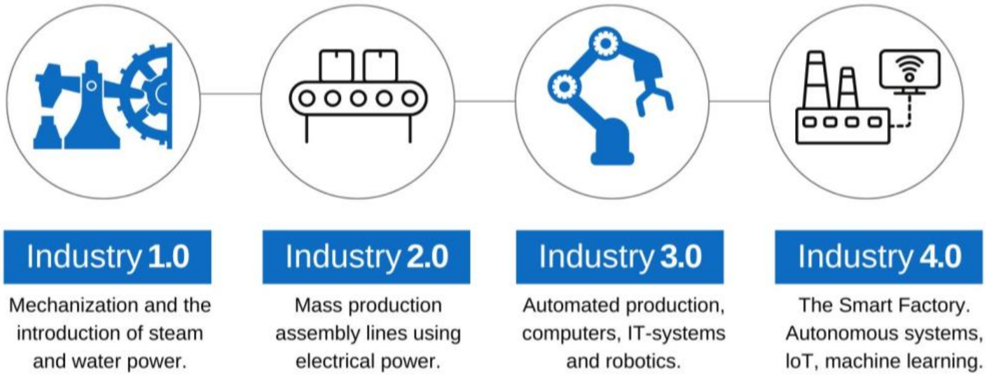

Figure 1: The four Industrial Revolutions

Even though IoT was not originally intended for Industrial applications, its immense potential in accelerating the fourth industrial revolution became clear quickly. IoT and I4.0 have caught the attention of the academia since 2005, with a rise in publications since then. In the later years there has been a hike in both domains showing the increasing interest in analyzing them.

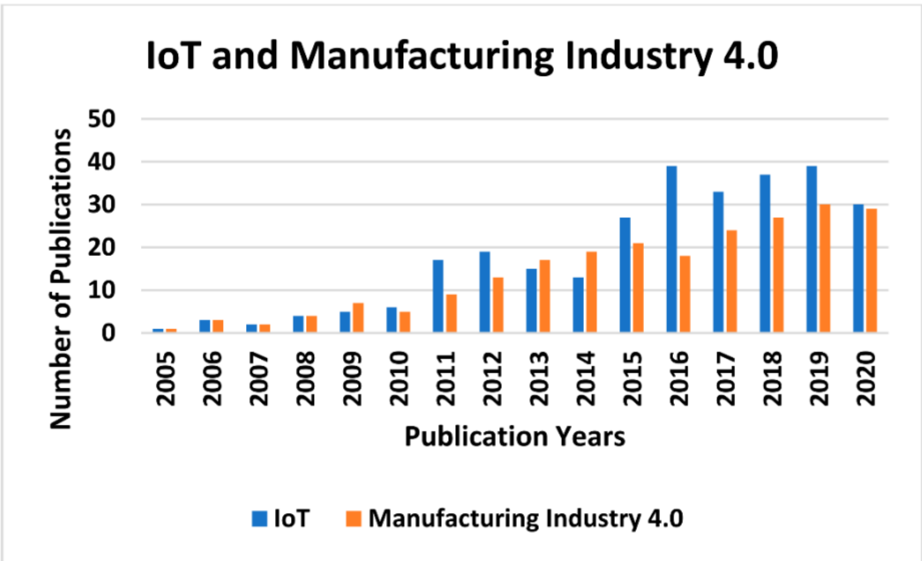

Figure 2: Yearly number of published papers on IoT and I4.0.
Reproduced from (Kalsoom, et al., 2021) without modifications, licensed under [CC BY 4.0]

Benefits of IoT

The answer to why IoT is so important when it comes to supply chain and production can be given by its very definition and characteristics. The IoT refers to the network or networks encompassing the use of standard Internet Protocol (IP) and other networking technologies to connect people, processes, and things to enable new cyber-physical systems. IIoT should be understood as a subset of the broader IoT, where these connections exist mainly to facilitate the production of physical goods for the marketplace as well as to maintain the physical assets of production. The Concept of IoT can be seen in Figure 3.

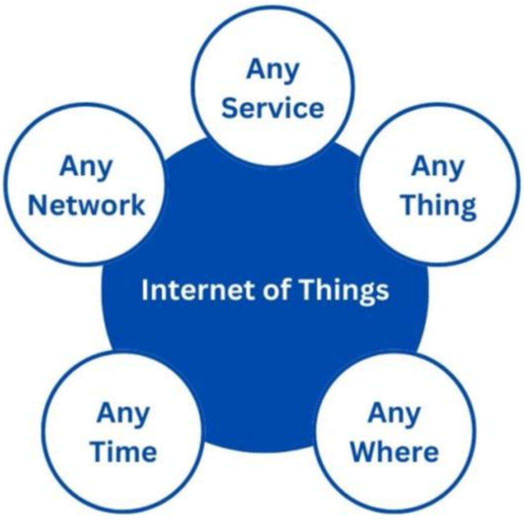

Figure 3: IoT concept

This means that IoT enables data collection from any place at any time on any device using any network path and can be applied to any business. These characteristics can help with the realization of the "smart factory" by providing:

- **Connectivity**: The interconnected property of the "smart factory" is its most significant advantage leading to minimized manual intervention and increased reliability (Garrido-Hidalgo, Olivares, Ramirez, & Roda-Sanchez, 2019).
- **Operations Optimization:** The comprehensive view of the supply chain processes in combination with automated workflows is the key to efficiency, improved traceability, enhanced quality, uptime, and waste reduction (Frank, Dalenogare, & Ayala, 2019).
- **Self-configurability:** An optimized "smart factory" can reach a level of self-awareness that enables the automatic adjustment of equipment and workflows and identify their outcome in real-time (Ulieru & Cobzaru, 2005).
- **Agility and Proactivity:** The "smart factory" allows flexible modifications of production with minimum downtime (Birkel & Hartmann, 2019). A proactive system can monitor the processes and equipment and predict problems, as well as react before they occur (Newbert, 2007).

A more detailed view of how the aforementioned benefits can be gained is discussed in the next chapter.

IoT Integration in the industrial environment

Automation Layers

ISA-95 model is the international standard for the integration of enterprise and control systems. It includes the terminology and the models that determine information exchange between all the systems used in the automation pyramid, even though the model itself does not impose this pyramidal structure. The automation pyramid as it is conventionally used in the industry can be seen in Figure 4. As intelligent manufacturing gains momentum, the existing frameworks are challenged and ISA-95 is also evolving to support the modern technologies, such as IIoT. This help companies implementing these technologies by defining new ways of data exchange along with new information object models e.g. Operations Event Model.

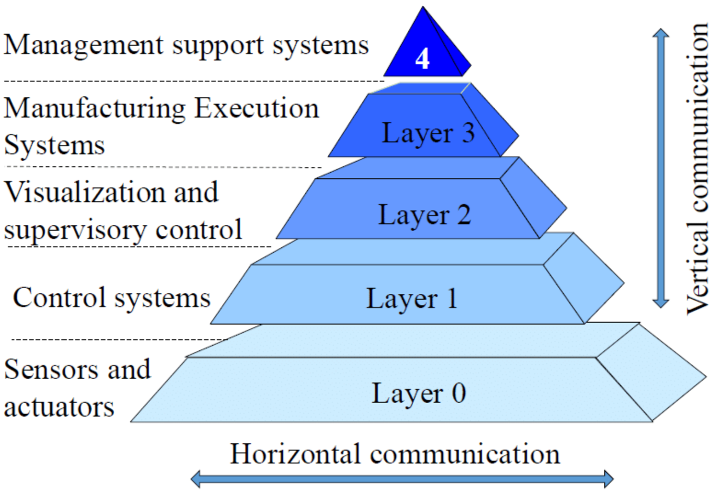

Figure 4: Automation Pyramid.
Reproduced from (Cupek, Drewniak, Ziebinski, & Fojcik, 2019) without modifications, licensed under CC BY 4.0

All the levels of the pyramid connect with various communication systems that are used to achieve reliable information exchange. However, these industrial communication solutions are highly incompatible with each other. If all the data exchange between all these levels, along with the information processing is easily done without manual intervention then the optimal goal would be achieved. IIoT can solve many of these problems and can help reinventing the automation pyramid for satisfying the needs of the “smart factory”.

As mentioned in the previous section, the fourth industrial revolution’s main goal is to convert data into information that can be used to improve production processes. It is equally important though, to be able to make this information available for every stakeholder at real-time, which is what IIoT technology can offer.

Levels of Integration

In general, IIoT provides the necessary data from physical objects such as machines and products, as well as production lines and logistics operations through wired or wireless communication. The data is then combined along with all the customer and supplier information in a cloud-based system to effectively improve the manufacturing processes. Figure 5 shows the smart manufacturing components that lead to a digital supply chain ecosystem.

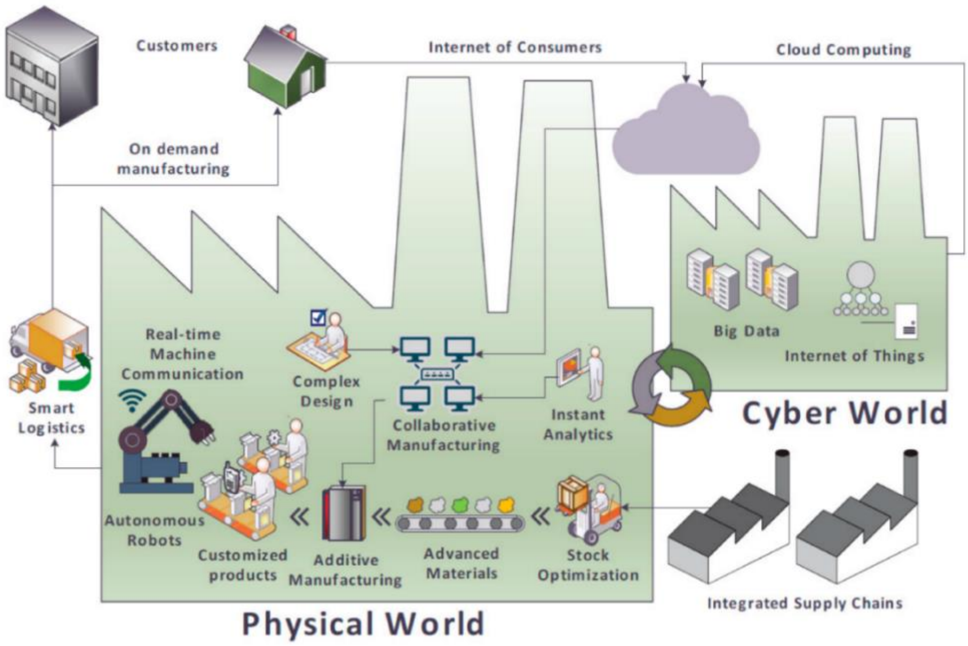

Figure 5: Smart Supply Chain Ecosystem.
Reproduced from (Mehrpouya, et al., 2019) without modifications, licensed under CC BY 4.0

This concept seems unrealistic and overly complicated for many companies and the main reason is that they do not know exactly where to start their digital transformation journey. This paper shows a simple approach breaking down the IIoT integration for each level of the automation pyramid structure that companies are already familiar with, so it is clearer how they can step-by-step adopt the emerging technologies.

Sensor level

In Supervisory Control and Data Acquisition (SCADA) systems, sensors are connected to Programmable Logic Controllers (PLCs) so the data can be stored in a Historian database or displayed to the operators through a Human Machine Interface (HMI). However, sensors with processing capabilities can directly transmit data to a software platform through lightweight IIoT protocols. The advancements in sensor technologies opens a whole new world of possibilities for the companies to utilize a huge amount of collected data and was not feasible in the past mainly because of network bandwidth limitations. The companies also can take advantage of the collection of additional supposedly non-useful data because data patterns not recognized by humans could lead to extremely useful information if processed by a machine learning model.

The vast number of sensors generates the problem of cable management, but it can be overcome by using wireless connectivity. This is still a big challenge for companies and is discussed in the next chapter.

Examples of applications enabled by IIoT sensors are:

- **Asset Tracking and Tracing:** The release of Bluetooth 5.1 in January 2019 enabled cost-effective asset tracking up to a few centimeters of accuracy by utilizing Angle of Arrival (AoA) and Angle of Departure (AoD) based on the use of an antenna array (Pau, Arena, Gebremariam, & You, 2021). RFID technology is also utilized for scanning multiple tags across the warehouse without requiring line of sight.
- **Tracking of Goods:** An outdoor tracking system can be implemented by using a combination of the Sigfox network and GNSS (Gnimpieba, Nait-Sidi-Moh, Durand, & Fortin, 2015) to trace in real-time the product parts between production sites for better planning as well as inventory optimization. Tracking of finished goods across the supply chain can also create a better customer experience by offering full order visibility.
- **Condition-based and Predictive Maintenance:** Additional sensors in critical equipment can be easily installed and produce meaningful data for monitoring key parameters or for advanced analytics to predict machine failure (Cakir, Guvenc, & Mistikoglu, 2021).

- **Digital Twin:** A digital twin based on a physical model can be enhanced by using real-time sensor data by normal operation and failure states of machines to give recommendations for future operation and maintenance (Boschert, Heinrich, & & Rosen, 2018).
- **Proof-of-Concept (PoC) Implementation:** Easy sensor installation with connectivity to a software platform can be beneficial for demonstrating new project ideas, as it is done independently of the process control system, which minimizes risk as well as reduces implementation time and cost. A rapid prototyping approach can provide tangible results and quick calculations of Return on Investment (ROI) for making business cases for scaled implementations. Small and Medium Size Enterprises (SMEs) normally have specific use case tailored solutions that need to be developed and tested. This means developing a prototype that can quickly demonstrate the capabilities and benefits of digitization. This is also in line with the "test before invest" principle that has been touted as a strategic means for driving the digital transformation of European SMEs (Asplund, Macedo, & Sassanelli, 2021) by European Commission Digital Innovation Hubs. Moreover, the culture of digital processes is not sufficiently introduced, and prototyping is the key to raising awareness of the benefits.
- **Retrofitting:** In many companies, especially SMEs, there tends to be a large amount of legacy equipment that is installed without any means of connectivity to collect and analyze the possible data they can provide. There are cases where data is collected by a controller device, e.g., PLC, which is responsible for the operation of the equipment, but the PLC is not designed to expose it to the network. IIoT Gateways, designed to securely connect to the internet using Wi-Fi, LAN or cellular communication, can be used as middleware to enable the connectivity of these devices and retrofit old SCADA equipment. It can also occur that the equipment does not have any digital capabilities and external sensors need to be installed along with a smart data acquisition device to enable network communication (Kolla, Lourenço, Kumar, & Plapper, 2022), (Di Carlo, Mazzuto, Bevilacqua, & Ciarapica, 2021). Zerynth is an example of a company that offers "Ready-to-Use" IoT-enabled hardware for easy installation that can send monitoring data to a cloud portal, which can be exposed by using a webhook. This forms a non-invasive, flexible and easy-to-use system that can be used e.g., for machine condition monitoring. The introduction of IIoT Gateways into industrial and mission critical applications helps to address the issue of interoperability of legacy systems and helps avoiding the incredibly large cost of replacing existing infrastructure with next generation equipment. Ideally, in the future only IoT-enabled industrial products will be manufactured. Still, a business decision must be made to identify the pros and cons of retrofitting instead of buying new equipment (Ilari, Carlo, Ciarapica, & Bevilacqua, 2021).

Sensors are a key component of an IIoT architecture, as the amount and variety of data plays a vital role in the decision-making process, which is based on information. While a small number of measurements provides low quality of information, data fusion from various measurements can lead to valuable results. The importance of sensors, measurement science, and smart evaluation for I4.0 has been recognized and led to the statement "Industry 4.0: nothing goes without sensor systems ("Industrie 4.0: Ohne Sensorsysteme geht nichts") (Arnold, 2014).

Control Level

PLCs are essential elements of Industrial Control Systems (ICS) and will continue to be the technological basis in the age of I4.0. However, the features and characteristics of these controllers must be revisited, so they fulfill the necessary requirements of the "smart factory." These requirements include:

- **Reconfigurability, autonomy and agility (Plug-and-Play):** Activation of new control algorithms and Input/Output (I/O) configuration can be done on the fly.
- **Local and cloud connectivity:** Remote Control and data availability in the cloud without additional effort.
- **Interoperability between heterogeneous systems:** Easy connection with I/O modules and drives from different manufacturers.
- **Introduction of the Service Paradigm:** Integration of service functions in the controllers (Langmann & Stiller, 2019)

Historically, the PLCs have been proprietary systems, operated locally by using proprietary communication protocols built on top of TCP/IP such as Profinet or Modbus TCP. Although PLCs started being more interconnected, the core architecture of IEC 61131 handles PLCs as logically independent blocks with their own configuration. Such an architecture is not flexible enough for the demands of I4.0 for deeper cooperation, as controllers need to communicate and exchange data with systems outside of the factory floor that lie in the cloud for global networking of process data and used in processing customer orders and requests in real time. Recently, manufacturers started integrating modern IT technologies from the web development domain, so they can adapt to the next generation of the production environment and provide IIoT-enabled components to the market. The rising importance of networking requires also more powerful processors, so they can deal with security enhanced protocols such as Transaction-Layer Security (TLS). There are also considerable efforts being made at the introduction of Infrastructure-as-a-Service (IaaS) principles (Colombo, et al., 2014) and the virtualization of PLCs (Schmitt, Goldschmidt, & Vorst, 2014).

Supervisory level

SCADA software gathers real-time data from the production line and makes it available to the plant supervisors through a graphical user interface. Modern SCADA software can function as a server exposing information to the internet through IIoT protocols like OPC UA. Until recently, SCADA applications were running only on-premises on some local machine, so equipment data is available, but it is stored mostly locally for each plant, which makes bigger-scale data visibility not possible. SCADA systems can also store only a finite amount of data so historical data is not preserved for deeper analytics. However, SCADA platform providers have started moving towards web-based solutions, which offer greater flexibility and reliability. Particularly, cloud storage offers great benefits as the volume of the data stored will vastly increase over time. The usage of complex statistical models, e.g., machine learning models, would require extremely fast data access, thus a classical relational database is not recommended.

The limitations of SCADA systems can be overcome by introducing an IIoT platform that can work together with SCADA, as additional functions manually coded by users cannot go far enough to allow full interoperability with different machines, applications and the cloud. Customized add-on solutions can help with accomplishing part of the "smart factory" but are also resource intensive and require high expertise that is usually not available in-house. IIoT platforms will not replace SCADA systems and their role to efficient real-time production monitoring but will enable data intelligence for operations improvement by adding analytics at the edge. Manufacturers can continue using their already in place SCADA system and deploy an IIoT platform for unifying, analyzing and easily sharing operational data across enterprise applications.

Modern IIoT platforms are built using lightweight micro-services architecture based on Docker virtualization technology that enables the easy replacement of services with other containerized alternatives, making it a plug-and-play solution. They also consist of edge and cloud components to support both low latency processing and feedback providing, but also high computational resources and big data analytics (Cerquitelli, et al., 2020). An overview of the IIoT platform architecture that includes a data hub and supports communication to all the different systems is shown in Figure 6.

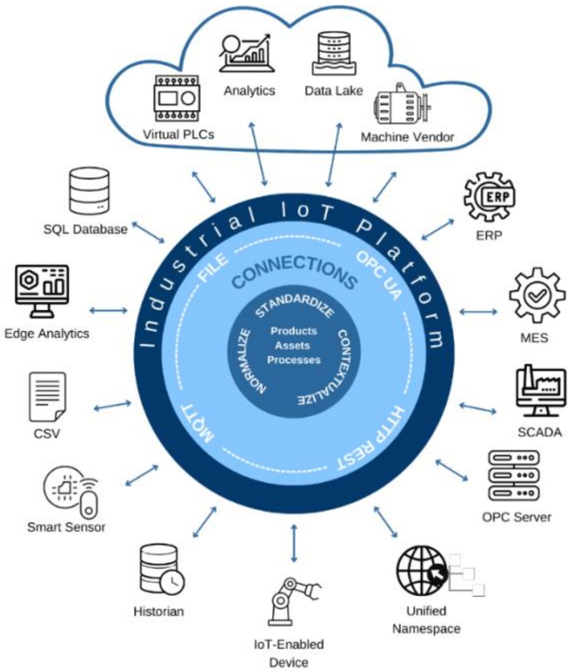

Figure 6: IIoT platform architecture

Companies like Siemens (Mindshpere) and Highbyte (Highbyte Intelligence Hub) offer great IIoT platform solutions that meet all the necessary criteria:

- **Effortless application deployment:** Wide range of off-the-shelf-solutions with codeless configuration possibilities, which significantly reduces integration time and risk.
- **Data integration**: Ability to connect to IoT cloud services that offer pre-built integration with third-party platforms for advanced analytic. A particularly useful feature is the integration of the data coming from Operational Technology edge devices with IT applications laying in the local servers or in the cloud offering bi-directional stream of data.
- **Cybersecurity**: Robust ecosystem that ensures end-to-end data security, and compliance to industry standards.
- **Edge-to-cloud connectivity and Data management**: Smooth connectivity between devices, assets and systems for fast and scalable provisioning of edge devices and secure remote access for updates and configuration changes.

Inductive Automation has developed Ignition, which is an IIoT platform that contains a full-featured SCADA system (Chariot SCADA), which can completely replace an existing SCADA solution and offer the advantages of an IIoT platform as well.

Operations and Business Level

Manufacturing Execution System (MES) and Enterprise Resource Planning (ERP) software are the heart of the decision-making process in industrial environments. This is a complex matter, as people need to analyze a big amount of information from various sources and often this information is not so easily obtained. These systems were originally created as self-contained, monolithic entities, each with their own data repositories and were not designed to support open communication standards for interoperability purposes. Companies are often building custom middleware to connect the ERP and MES with other systems, which are not future proof and are not a good practice.

It also the case that companies have problems with their current ERP software, because their planning module does not fit their purpose, as it does not have a user-friendly graphical user interface or convenient visualization. However, they cannot easily find an external planning module that is easily compatible with their existing systems, because proprietary vendor software does not usually support open communication standards, so the IT integration between these systems is extremely difficult to implement. Therefore, cloud solutions that provide easy integration with third party modules, e.g., planning modules, offer the best solution, because all these applications can be replaced without any problems.

Big companies like Microsoft (Microsoft Cloud for Manufacturing) and Amazon (AWS Manufacturing) offer cloud platform solutions that are easily integrated with applications of several partner companies including web-based ERP, MES. This leads to a Platform-as-a-service (PaaS) implementation offering hardware and software tools to the users and resulting to increased time savings, because companies do not have to maintain their own IT infrastructure saving human and physical (software and hardware) resources costs, as well as maintenance costs. PaaS is future proof, as it provides state-of-the-art data center, hardware and operating systems as well as great security technologies from the providers' expertise (Gd & Bist, 2012). A web-based approach allows also different stakeholders to access the platform from any mobile device offering high flexibility.

Another limitation of traditional ERP and MES is that they were not designed to continuously digest and analyze data from sensors, cameras and other IoT devices which is an issue that has negatively impacted the readiness of I4.0 adoption in enterprise environments. Especially ERP systems do not support real-time decision making that today's market environments demand. IIoT supports all kinds of real-time data availability to these platforms enabling advanced decision making and automating business decisions with rule-based engines. The data pipeline is established by using IIoT platforms as discussed in the previous subsection.

It is important to consider that MES does not refer to a specific software, but it is a collection of different features, whose relevance differs from company to company, because it must be closely tied to the corresponding production activities. Most off-the-self MES software on the market will never fit exactly the purpose of the company and therefore there are a lot of customizations must take place on top of the bought product. Modular cloud integrations assist in meeting these needs by offering open architecture flexible solutions that can be scaled up and down on demand and be adjusted for the specific use.

Setting up an ERP system is a particularly complex, high-cost and risky process, because it is not just a change in the computer systems of an organization but impacts its core operations, so management often discourages such migration, but the flexibility and agility to adapt to market changes, as well as the productivity increase potential by streamlining business operations makes it a valuable investment. (Prakash, Savaglio, Garg, Bawa, & Spezzano, 2022).

Summary

In conclusion, IIoT is changing the way industrial equipment and software were perceived, leading to major evolutions in the currently used frameworks and standards, as the automation pyramid of Industry 3.0 is transforming into the automation network of Industry 4.0.

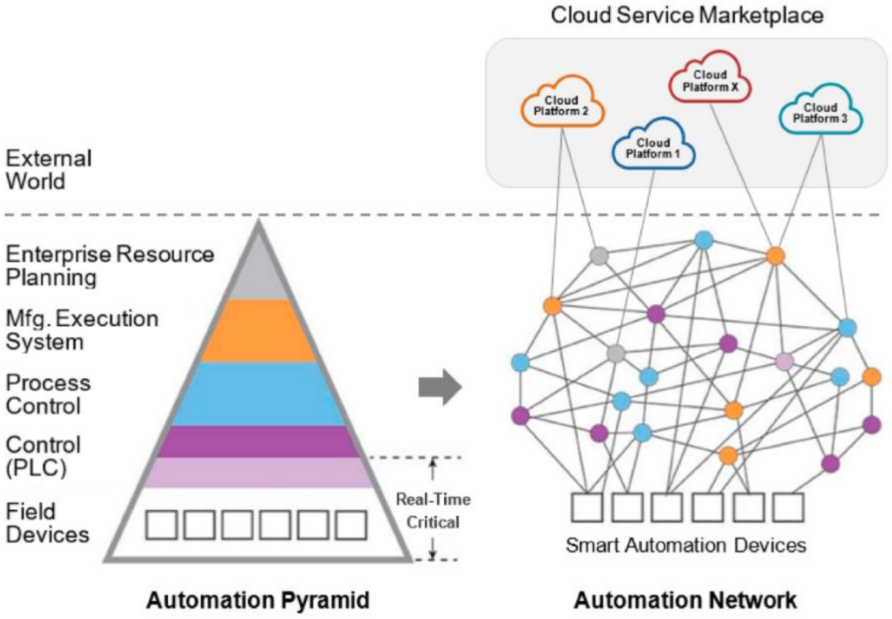

Figure 7: Evolution of the Automation Pyramid.
Reproduced from (Zeid, Sundaram, Moghaddam, Kamarthi, & Marion, 2019) without modifications, licensed under [CC BY 4.0](CC BY 4.0)

IIoT Protocols

Industrial network protocols form the basis for communication between industrial network devices and many industry-specific network protocols have been developed over the past decades, each designed for specific purposes and environments.

A central consideration and challenge in achieving a connected "smart factory" is protocol division. Depending on the specific operation, system integrators may encounter numerous disparate automation protocols that must be connected to achieve the operational or optimization goals. The emergence of IIoT and new possibilities for connectivity with wireless and Ethernet are changing the protocol landscape. Integrating diverse types of devices, public and private enterprise clouds, operational systems and business domains, as well as sharing the vast amount of high-quality data across IT and OT platforms is presenting new opportunities for protocol harmonization in industrial environments. Figure 8 shows the evolution of industrial communication protocols and the beginning of migration to cloud-based solutions.

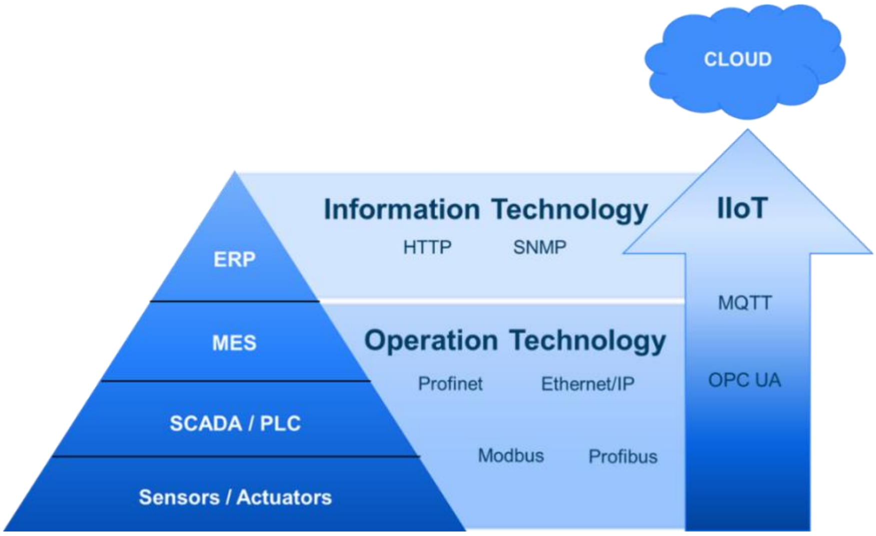

Figure 8: Automation Layers IIoT Protocols Evolution

Previously, IT and OT layers used different protocols making cumbersome the interoperability between them. Platform-independent protocols like OPC UA and MQTT that communicate data across IT and OT are important to enable I4.0 technologies. It should be noted here that the different protocols that exist today will not necessarily be completely replaced, at least for the following years, but they will not lead the way for the new IIoT solutions.

OPC UA is much more than a communication protocol, it is a framework, which is transport-agnostic, so it can be easily adapted to different transport layers. It offers a secure cross-platform protocol, but it is really resource intensive, not easily scalable, and not edge driven, though it is continuously developed, so in the future it might support more use cases.

MQTT on the other hand is a lightweight protocol that uses a publish/subscribe model (OPC UA also includes a Pub/Sub feature). It is bandwidth-efficient and requires minimal effort to be implemented, but it lacks a well-defined data structure for metadata handling, which makes it non-optimal for industrial usage. However, Eclipse foundation designed the Sparkplug B specification using MQTT 3.1.1, that defines how data is sent and received, as well as interprets the MQTT message payload.

Challenges and Recommendations

Connectivity Reliability

Communication plays a key role in digital transformation and the evolution of IoT presents big challenges for networking technologies, as there is a massive increase in the number of connected devices across the supply chain (Da Xu, He, & Li, 2014). The extraction of more data from processes in combination with analysis provides meaningful information for the transparency and deep comprehension of the supply chain operations.

This need to extract data from physical and digital assets and to be able to provide real-time feedback that affects the production processes requires reliable and predictable communication methods, which offer a certain level of deterministic behavior. The technology that is advancing to meet this need is Time-Sensitive Networking (TSN). TSN regulates the data communication layer and provides the basic mechanisms to allow engineers and technicians to precisely understand the delays and variations of network traffic as well as ensure time synchronization. Another important feature of TSN is bandwidth efficiency and the ability to converge multiple communication networks ("islands"), which is usually the case in automation systems. The latter is beneficial when it comes to connecting IT and OT systems.

Initially, Fieldbus protocols dominated the automation market because of the unique deterministic features, but the significant efforts in improving Industrial Ethernet made it a viable alternative. Additionally, due to the rise of IIoT, Ethernet became the area of focus because of its greater bandwidth and easier scalability compared to Fieldbus. TSN and OPC-UA can be combined to allow different industrial Ethernet protocols to share the same network while allowing different systems to communicate using a common language. To achieve this goal, many open industrial Ethernet associations along with the OPC foundation are adopting TSN compatibility to their portfolios. Network convergence offered by TSN is a key element of I4.0, enabling transparency by offering streamlined highly efficient operations.

Wireless solutions have only been used for a limited number of applications in industry, because of the strict production environment requirements (Frotzscher, et al., 2014). The current state-of-the-art technologies cannot fulfil these requirements, so industrial networks are constrained in wired communication. The wide connectivity of devices and the flexibility needed for implementing IIoT applications renders wireless communication especially important for achieving the "smart factory", by transforming today's infrastructure that is connected through wires in a real-time reconfigurable and flexible wireless system.

Despite recent advances in 5G and Wi-Fi technologies, low-latency wire-equivalent reliable communication still poses a great challenge. The Wi-Fi alliance is currently designing the successor of Wi-Fi 6 in the wireless local area network (WLAN) ecosystem, Wi-Fi 7, which aims to include TSN features for enabling IIoT scenarios (Adame, Carrascosa-Zamacois, & Bellalta, 2021). 5th Generation (5G) technology is considered one of the best options for supporting I4.0 bringing Ultra-Reliable Low Latency Communications (URLLC). The 3rd Generation Partnership Project for the mobile standard (3GPP) issued the Release 16, which defines the basic functionalities and architecture to support and integrate TSN and 5G with fully centralized management. Private 5G networks can be also used for even further reduction of delay, as well as data protection, which might be interesting for critical infrastructure that do not want their data going through the telecommunication providers (Larrañaga, Lucas-Estañ, Martinez, Val, & Gozalvez, 2020).

Mobile robots and Autonomous Guided Vehicles (AGVs) will be greatly benefited by the adoption of 5G in the industrial environment. The sophisticated algorithms for obstacle detection and control require extensive computational resources that cannot be easily embedded into the robots, e.g., because of high energy consumption. To enable complex collaborative tasks between robots, or between robots and other systems low-latency, high-reliability communication must be established to provide sufficient bandwidth for transferring the computationally intensive tasks in a local cloud infrastructure, as seen in Figure 9 (Kehl, et al., 2022). The adoption of a high-bandwidth high-speed connection is also enabling "Internet of Skills" technologies to build more agile factories. For example, Microsoft has developed the HoloLens 2, which utilizes mixed reality to provide remote support to operators from trained technicians or engineers.

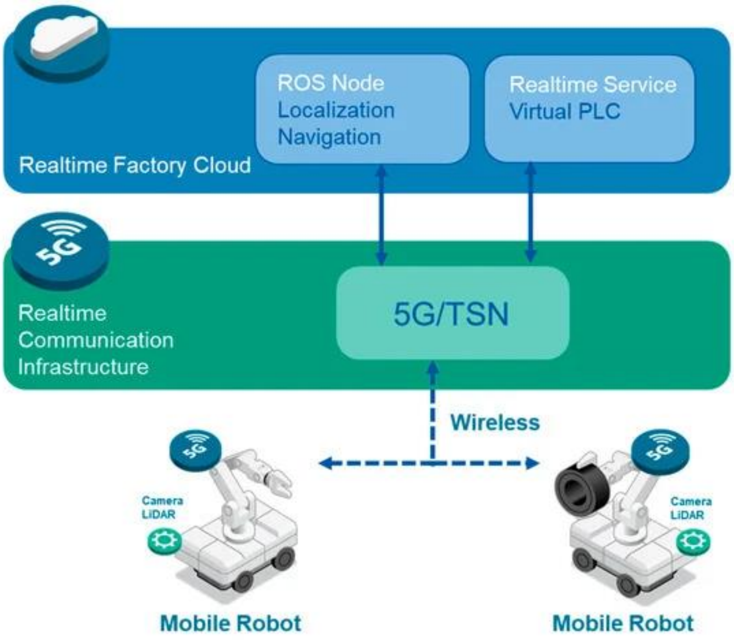

Figure 9: Cloud-controlled Robotics Application with TSN.
Reproduced from (Kehl, et al., 2022) without modifications, licensed under [CC BY 4.0]

Lack of Alignment between OT and IT

Operational Technology includes the processes and equipment that exist on the shop floor. On the contrary, Information Technology in this context consists of all the technologies that facilitate the communication of information for the business to operate.

In the past, manufacturing companies relied solely to the OT to manage their production. The evolution of I4.0 had made it necessary to merge the worlds of IT and OT and this has presented new challenges for the companies. However, IT people usually have no OT experience and vice versa OT people have not any knowledge of modern IT concepts and technologies. Big cultural differences between these two groups mostly because of work focus, priorities and background also generate obstacles that prevent their collaboration.

Additionally, OT focuses mostly on real-time response with no loss of data, operational and maintenance simplicity as well as long operational time, while IT networking is more standards-based, scalable with ease of patching, while it enables remote monitoring of systems and virtualization of processes. To achieve a smooth data flow between IT and OT systems companies should promote mutual participation and close cooperation of these departments for working on digitalization projects.

OT Cybersecurity

In the past, ICS were completely isolated from conventional digital networks such as enterprise (Information and Communication Technology) ICT environments. As such, they were not exposed to outside threats. If connectivity was required, a zoned architecture was adopted using firewalls and demilitarized zones used to protect the core control system components. As digital innovation initiatives expand and IoT technologies are utilized, architectural changes occur to IACS, including greater connectivity to industrial systems, which introduces major vulnerabilities. (Boyes, Hallaq, Cunningham, & Watson, 2018). There have been some major cyberattacks in ICS in the last 20 years and some of them resulted in major economic loss, inflicted serious equipment damage, which could lead to life threatening situations. Most of the security breaches happened by injecting some kind of malware or ransomware into the control systems, which possible because of via phishing emails, insecure connections to the Internet, untrusted and unsanitized USB drives or lack of firewall between OT/IT networks (Alladi, Chamola, & Zeadally, 2020).

Organizations need to find ways to ensure the security of their critical infrastructure. The ISA99 standards development committee develops standards on industrial automation and control systems security, which must be followed when building and operating SCADA systems. Most companies, especially the ones with critical infrastructure are reluctant to adopt extensive systems interoperability, because of the fear of cyberattacks. Apart from network security, there could be additional layers of security based on algorithms that detect faulty behavior of physical systems, so considerable damage to OT infrastructure and big catastrophes are avoided.

It is quite common in industrial applications to connect remote equipment through Virtual Private Networks (VPNs). This demands a powerful router that has the capability to handle the VPN functionality, open a firewall port and connect to a Domain Name System (DNS). In the IIoT approach devices can publish data in a cloud broker using TLS, which eliminates all the issues related to setting up VPNs, DNS and firewalls. The only information that must be managed in the IIoT equipment that transmits data are the security credentials (username and password) linked to the Cloud account.

The variety of products inside an industrial environment makes it a serious challenge for the companies to keep track of all the components and meet all the security requirements. It is a matter of culture to ensure that a number of specific practices is followed to ensure cybersecurity. Frequent software updates, always newest patches, education of the users in the OT environment along with the IT to be aware of the potential dangers and perform risk analysis to be sure. It is also important to know that the products bought from OEMs comply with the cybersecurity standards, as well as the integrators that make the installations should follow specific standards for the system design and meet the specific security level requirements for the specific installations (Bjerre, J. P., 2020).

The truth is that no one can guarantee 100% cybersecurity. In fact, you are as secure as the smartest person that wants to gain access to your systems. However, fear should not be the obstacle to digital innovation. On the other hand, the companies should be aware of the risks related to the criticality of their operations and move forward in their digital transformation journey by adopting the proper cybersecurity strategy.

Non-central data architecture

Until recently, the context of the data and the various “environmental” considerations (metadata) were not captured in SCADA systems, which made it really complex to use them in a different context e.g., in a third-party application, especially when multiple SCADA facilities were involved. The existing data infrastructure is not developed for supporting scale and broad adoption. The main reason is the difficulty in utilizing industrial data in the IT systems, where a lot of custom scripts are deployed, which slow down integration time and create technical debt. This results in the data science team spending a high percentage of their time to find and prepare the data for analytics rather than processing it. Therefore, companies end up with their IT department paying for high, variable cloud storage and processing modules for unusable data, while OT department is backlogged with requests to grant access to and explain machine data.

As discussed previously there are multiple IIoT platforms in the market that can used to ingest and analyze data, but without a centralized data repository, it could take months to deploy a new analytics application across the entire enterprise. This can be solved by introducing a UNS that represents the single source of truth for the data from various systems. Hence, instead of having multiple point-to-point connections, all the data is published to a data hub and other applications can pull the information that is relevant for them without being coupled to the other systems. Essentially, UNS is a middleware solution that enables the collection of data from different industrial systems, contextualize it and produce a readable format for other systems to be able to understand offering data reusability.

The UNS architecture can utilize the Sparkplug specification for implementing ISA-95 specified data objects to exchange information between all kinds of systems. It can get data from a device, convert it to ISA-95 format, push it to the UNS MQTT broker, so the other systems can pull it out. If multiple production sites exist in different geographical locations, then multiple edge UNS brokers can be deployed at each site that are connected to a central cloud based UNS MQTT broker. This ensures low latency when exchanging data between time critical applications. The MQTT broker structure can be seen in Figure 10.

The company HiveMQ offers a Sparkplug compliant broker that can be used as a UNS for ISA-95 based data objects that can be published by industrial hardware or software systems and consumed when needed for a specific action. It can be concluded that the combination of the UNS architectural approach, the ISA-95 Standard and the Sparkplug Specification provide an interesting concept that could be used as a basis for building smart manufacturing systems.

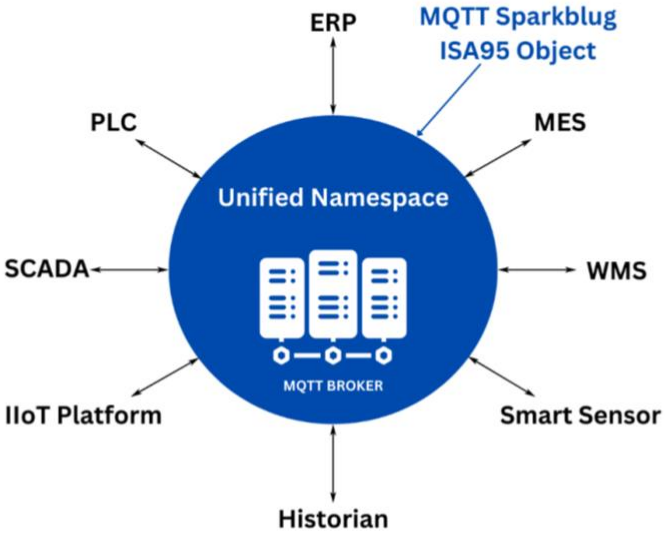

Figure 10: UNS data hub

The concept of a UNS provides a solution for one of the big problems that exist in production plants, which is to be able to map huge amount of data to which equipment in which line, in which plant they came from without human manual intervention. This would be solved by having the different software (MES, SCADA etc.) publishing to the UNS broker so that every stakeholder is aware of the latest information and to avoid having multiplicated data in separate platforms with different tags and IDs.

Conclusion

The adoption of I4.0 technologies and specifically IIoT should start from the management of the organizations, so it is especially important that concrete business cases are built around the new projects. The priority of these companies is to fulfill their customers' needs by producing high quality products in the best way possible. However, to stay in front of market trends and be successful in a highly competitive market requires constant technological advancements.

Companies should start by inheriting a consistent holistic strategy considering all the different possibilities where IIoT can be valuable. A lack of a long-term strategy can be a major obstacle when implementing such technologies and the truth is that a lot of companies suffer because they adopt short-term solutions. However, IoT has a great advantage, because it allows small ad-hoc solutions to be easily scalable without a lot of effort and additional costs. Still, it is important that all these siloed initiatives are part of a strategic journey to achieve optimal business results. IIoT is changing the current automation pyramid and transforming it from a strict structure with clear borders to an interconnected graph of devices and applications that operate seamlessly together.

An important benefit of IIoT infrastructure is that it can offer a high level of visibility across the whole supply chain. This is extremely valuable both from a technology perspective for efficiency and process optimization but also from a business perspective because many companies lack the data to support business cases for potential improvement projects. IIoT will also play a leading role in helping companies reach their sustainable development goals especially related to the environmental dimension and many companies expect that IIoT-enabled digitization could lead to better environmental management (Beier, Niehoff, & Xue, 2018).

There are several challenges for the companies to overcome when adopting IIoT technologies, but the interest towards solving such problems is rising and the market size of IIoT is rapidly expanding. The production companies should carefully consider the existing challenges, however these challenges should not in any case become the obstacle to innovation.

References

Adame, T., Carrascosa-Zamacois, M., & Bellalta, B. (2021). Time-sensitive networking in IEEE 802.11 be: On the way to low-latency WiFi 7. *Sensors, 21*(15), 4954.

Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications, 155*, 1-8. doi:https://doi.org/10.1016/j.comcom.2020.03.007

Arnold, H. (2014). *Industrie 4.0: Ohne Sensorsysteme geht nichts, [Markt & Technik].* Retrieved 10 19, 2022, from http://www.elektroniknet.de/messen-testen/sonstiges/artikel/110776/.

Asplund, F., Macedo, H. D., & Sassanelli, C. (2021). Problematizing the service portfolio of digital innovation hubs. In *Working Conference on Virtual Enterprises* (pp. 433-440). Springer.

Beier, G., Niehoff, S., & Xue, B. (2018). More sustainability in industry through industrial internet of things? *Applied sciences, 8(2)*, 219. doi:https://doi.org/10.3390/app8020219

Birkel, H. S., & Hartmann, E. (2019). Impact of IoT challenges and risks for SCM. *Supply Chain Management: An International Journal*.

Bjerre, J. P. (2020). Sådan sikrer man cybersikkerheden af industrielle IoT-produkter med standarder. *Aktuel Elektronik*. Retrieved from https://forcetechnology.com/da/artikler/cybersikkerhed-industrielle-iot-produkter

Boschert, S., Heinrich, C., & & Rosen, R. (2018). Next generation digital twin. *Proc. tmce*, *2018*, pp. 7-11. Las Palmas de Gran Canaria, Spain.

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in industry, 101*, 1-12.

Cakir, M., Guvenc, M. A., & Mistikoglu, S. (2021). The experimental application of popular machine learning algorithms on predictive maintenance and the design of IIoT based condition monitoring system. *Computers & Industrial Engineering, 151*, 106948. doi:https://doi.org/10.1016/j.cie.2020.106948

Cerquitelli, T., Nikolakis, N., Bethaz, P., Panicucci, S., Ventura, F., Macii, E., . . . M.Ippolito. (2020). Enabling predictive analytics for smart manufacturing through an IIoT platform. *IFAC-PapersOnLine, 53*(3), 179-184.

Colli, M. (2020). *Designing the transformation towards a digital supply chain: How to match the Industry 4.0 agenda to contextual needs and translate it into value.*

Colombo, A. W., Bangemann, T., Karnouskos, S., Delsing, J., Stluka, P., Harrison, R., . . . Lastra, J. L. (2014). Industrial cloud-based cyber-physical systems. *The Imc-aesop Approach, 22*, 4-5.

Cupek, R., Drewniak, M., Ziebinski, A., & Fojcik, M. (2019). “Digital Twins” for highly customized electronic devices–Case study on a rework operation. *IEEE Access, 7*, 164127-164143. doi:10.1109/ACCESS.2019.2950955

Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on industrial informatics, 10*(4), 2233-2243.

Di Carlo, F., Mazzuto, G., Bevilacqua, M., & Ciarapica, F. E. (2021). Retrofitting a process plant in an industry 4.0 perspective for improving safety and maintenance performance. *Sustainability, 13*(2), 646.

Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. *International Journal of Production Economics, 210*, 15-26.

Frotzscher, A., Wetzker, U., Bauer, M., Rentschler, M., Beyer, M., Elspass, S., & Klessig, H. (2014). *2014 IEEE international conference on communications workshops (ICC)*, 67-72.

Garrido-Hidalgo, C., Olivares, T., Ramirez, F. J., & Roda-Sanchez, L. (2019). An end-to-end internet of things solution for reverse supply chain management in industry 4.0. *Computers in Industry, 112*, 103127.

Gd, M. A., & Bist, M. (2012). EaaS-ERP as a Service. *Journal of Information Operations Management, 3*(1), 141-145.

Gnimpieba, Z. D., Nait-Sidi-Moh, A., Durand, D., & Fortin, J. (2015). Using Internet of Things technologies for a collaborative supply chain: Application to tracking of pallets and containers. *Procedia Computer Science, 56*, 550-557.

Grand View Research. (2021). *Industrial Internet Of Things Market Size, Share & Trends Analysis Report By Component (Solution, Services, Platform), By End Use (Manufacturing, Logistics & Transport), By Region, And Segment Forecasts, 2022 - 2030.* Retrieved from www.grandviewresearch.com/industry-analysis/industrial-internet-of-things-iiot-market

Ilari, S., Carlo, F. D., Ciarapica, F. E., & Bevilacqua, M. (2021). Machine Tool Transition from Industry 3.0 to 4.0: A Comparison between Old Machine Retrofitting and the Purchase of New Machines from a Triple Bottom Line Perspective. *Sustainability, 13*(18), 10441.

Kalsoom, T., Ahmed, S., Rafi-ul-Shan, P. M., Azmat, M., Akhtar, P., Pervez, Z., . . . Ur-Rehman, M. (2021). Impact of IoT on Manufacturing Industry 4.0: A new triangular systematic review. *Sustainability, 13*(22), 12506.

Kamalakkannan, S., & Kulatunga, A. K. (2021). IIOT Applications for Sustainable Manufacturing. In *Handbook of Smart Materials, Technologies, and Devices: Applications of Industry 4.0* (pp. 1-22). Springer.

Kehl, P., Ansari, J., Jafari, M. H., Becker, P., Sachs, J., König, N., . . . Schmitt, R. H. (2022). Prototype of 5G Integrated with TSN for Edge-Controlled Mobile Robotics. *Electronics, 11*(11), 1666.

Kolla, S. S., Lourenço, D. M., Kumar, A. A., & Plapper, P. (2022). Retrofitting of legacy machines in the context of Industrial Internet of Things (IIoT). *Procedia Computer Science*, 200, 62-70.

Langmann, R., & Stiller, M. (2019). The PLC as a smart service in industry 4.0 production systems. *Applied Sciences, 9*(18), 3815.

Larrañaga, A., Lucas-Estañ, M. C., Martinez, I., Val, I., & Gozalvez, J. (2020). Analysis of 5G-TSN integration to support industry 4.0. *2020 25th IEEE International conference on emerging technologies and factory automation (ETFA)* (pp. 1111-1114). IEEE.

Mehrpouya, M., Dehghanghadikolaei, A., Fotovvati, B., Vosooghnia, A., Emamian, S. S., & Gisario, A. (2019). The potential of additive manufacturing in the smart factory industrial 4.0: A review. *Applied Sciences, 9*(18), 3865.

Newbert, S. L. (2007). Empirical research on the resource-based view of the firm: an assessment and suggestions for future research. *Strategic management journal, 28*(2), 121-146.

Park, H. S., & Tran, N. H. (2014). Autonomy for smart manufacturing. *Journal of the Korean Society for Precision Engineering, 31*(4), 287-295.

Pau, G., Arena, F., Gebremariam, Y. E., & You, I. (2021). Bluetooth 5.1: An analysis of direction finding capability for high-precision location services. *Sensors, 21*(11), 3589.

Prakash, V., Savaglio, C., Garg, L., Bawa, S., & Spezzano, G. (2022). Cloud-and Edge-based ERP systems for Industrial Internet of Things and Smart Factory. *Procedia Computer Science, 200*, 537-545.

Schmitt, J., Goldschmidt, T., & Vorst, P. (2014). Cloud-enabled Automation Systems using OPC UA. *atp magazin, 56*(07-08), 34-40.

Schütze, A., Helwig, N., & Schneider, T. (2018). Sensors 4.0 – smart sensors and measurement technology enable Industry 4.0. *J. Sens. Sens. Syst., 7*, 359–371. doi:https://doi.org/10.5194/jsss-7-359-2018

Ulieru, M., & Cobzaru, M. (2005). Building holonic supply chain management systems: An e-logistics application for the telephone manufacturing industry. *IEEE Transactions on Industrial Informatics, 1*(1), 18-30.

Zeid, A., Sundaram, S., Moghaddam, M., Kamarthi, S., & Marion, T. (2019). Interoperability in smart manufacturing: Research challenges. *Machines, 7*(2), 21.